

A complex network diagram with numerous nodes (small blue dots) connected by thin, light blue lines, forming a web-like structure across the center of the page.

UserGate NGFW 7.x
Руководство администратора

Оглавление

- Введение
 - Безопасность сети и защита от сетевых угроз
 - Межсетевое экранирование
 - Обнаружение и предотвращение вторжений
 - Защита от DOS-атак и сетевого флуда
 - Антивирусная проверка трафика
 - Проверка почтового трафика
 - Управление трафиком АСУ ТП
 - Работа с внешними системами безопасности
 - Настройка политик безопасности при помощи сценариев
 - Улучшение производительности и надежности интернета
 - Поддержка кластеризации и отказоустойчивости
 - FTP поверх HTTP
 - Поддержка нескольких провайдеров
 - Управление пропускной способностью
 - Поддержка WCCP
 - Управление трафиком и контроль доступа в интернет
 - Маршрутизация трафика и публикация ресурсов
 - Аутентификация и авторизация пользователей
 - Поддержка гостевого портала
 - Проксирование приложений
 - Перенаправление трафика на вышестоящий прокси-сервер
 - Журналы и отчеты
 - Журналы и отчеты(описание)
 - Контент-фильтрация и контроль приложений
 - Интернет-фильтрация
 - Выборочная блокировка рекламы
 - Активация безопасного поиска
 - Блокировка приложений социальных сетей
 - Инжектирование кода на веб-страницы
 - Инспектирование SSL-трафика
 - VPN и веб-портал
 - Другие функции
 - Функция балансировщика нагрузки
 - DNS-фильтрация
 - Использование оповещений
 - Ролевой доступ администраторов к элементам управления UserGate NGFW
 - Типы интерфейсов

- [Алгоритм обработки трафика](#)
 - [UserGate NGFW 7 Packet Flow](#)
- [Первоначальная настройка](#)
 - [Общие сведения](#)
 - [Развертывание виртуального образа](#)
 - [Автоматизация развертывания UserGate NGFW с помощью Cloud-init](#)
 - [Требования к сетевому окружению](#)
 - [Подключение к UserGate NGFW](#)
- [Лицензирование](#)
 - [Лицензирование UserGate NGFW](#)
- [Интерфейс](#)
 - [Интерфейс UserGate NGFW](#)
- [Настройка устройства](#)
 - [Настройка общих параметров](#)
 - [Управление устройством](#)
 - [Управление доступом к интерфейсам администрирования](#)
 - [Управление сертификатами](#)
 - [Профили клиентских сертификатов](#)
 - [Системные утилиты](#)
 - [Расширение системного раздела](#)
 - [Работа с вышестоящими прокси-серверами](#)
 - [Кластеризация и отказоустойчивость](#)
 - [Кластеризация и отказоустойчивость \(версия 7.5.0 и выше\)](#)
- [Настройка сети](#)
 - [Настройка зон](#)
 - [Настройка интерфейсов](#)
 - [Настройка шлюзов](#)
 - [Настройка DHCP](#)
 - [Настройка DNS](#)
 - [Виртуальные маршрутизаторы](#)
 - [WCCP](#)
- [Пользователи и устройства](#)
 - [Пользователи и группы](#)
 - [Серверы аутентификации](#)
 - [Профили аутентификации](#)
 - [Настройка Captive-портала](#)
 - [Пользователи терминальных серверов](#)
 - [Профили MFA \(многофакторной аутентификации\)](#)
 - [UserID-агент](#)
 - [Radius accounting](#)
 - [Агент аутентификации для Windows](#)
 - [Прокси-агент для Windows](#)
 - [Управление гостевыми пользователями](#)
 - [Конечные устройства UserGate Client](#)
 - [UserID-агент для серверов AD, WEC](#)

- [Политики сети](#)
 - [Общие сведения](#)
 - [Межсетевой экран](#)
 - [NAT и маршрутизация](#)
 - [Балансировка нагрузки](#)
 - [Пропускная способность](#)
- [Политики безопасности](#)
 - [Общие сведения](#)
 - [Фильтрация контента](#)
 - [Веб-безопасность](#)
 - [Инспектирование туннелей](#)
 - [Инспектирование SSL](#)
 - [Инспектирование SSH](#)
 - [Защита почтового трафика](#)
 - [Работа с внешними ICAP-серверами](#)
 - [Защита от DoS атак](#)
 - [Система обнаружения и предотвращения вторжений](#)
 - [Защита АСУ ТП](#)
- [Глобальный портал](#)
 - [Общие сведения](#)
 - [Веб-портал \(SSL VPN\)](#)
 - [Публикация ресурсов с помощью reverse-прокси](#)
- [Настройка VPN](#)
 - [Общие сведения](#)
 - [VPN для защищенного соединения офисов \(Site-to-Site VPN\)](#)
 - [VPN для удаленного доступа клиентов \(Remote access VPN\)](#)
 - [Настройка раздельного туннелирования для UserGate Client](#)
 - [Примеры настройки VPN](#)
 - [Пример настройки Site-to-Site VPN с L2TP/IPSec\(IKEv1\)](#)
 - [Пример настройки Site-to-Site VPN с L2TP/IPSec\(IKEv1\) с помощью интерфейса CLI](#)
 - [Пример настройки Site-to-Site VPN с IPSec\(IKEv2\)](#)
 - [Пример настройки Remote access VPN с L2TP/IPSec\(IKEv1\)](#)
 - [Пример настройки Remote access VPN с IPsec\(IKEv2\)](#)
 - [Пример настройки Remote access VPN с IPsec\(IKEv2\) с аутентификацией через EAP для OS Linux](#)
 - [Пример настройки Remote access VPN с IPsec\(IKEv2\) с аутентификацией через EAP, PEAP для OS Windows](#)
 - [Настройка VPN \(версия 7.5.0 и выше\)](#)
 - [Общие принципы](#)
 - [Настройка VPN для защищенного соединения офисов](#)
 - [Настройка VPN для удаленного доступа в сеть](#)
 - [Журналирование событий VPN-сервера](#)
 - [VPN в режиме полного туннелирования](#)

- [Раздельное туннелирование для UserGate Client](#)
- [Примеры настройки](#)
 - [Пример настройки site-to-site VPN с L2TP/IPSec \(IKEv1\)](#)
 - [Пример настройки site-to-site VPN с L2TP/IPSec \(IKEv1\) с помощью интерфейса CLI](#)
 - [Пример настройки site-to-site VPN с IPSec \(IKEv2\) и аутентификацией посредством сертификатов](#)
 - [Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux](#)
- [Библиотеки элементов](#)
 - [Общие сведения](#)
 - [Морфология](#)
 - [Сервисы](#)
 - [Группы сервисов](#)
 - [IP-адреса](#)
 - [Useragent браузеров](#)
 - [Типы контента](#)
 - [Списки URL](#)
 - [Календари](#)
 - [Полосы пропускания](#)
 - [Шаблоны страниц](#)
 - [Категории URL](#)
 - [Измененные категории URL](#)
 - [Приложения](#)
 - [Профили приложений](#)
 - [Группы приложений](#)
 - [Почтовые адреса](#)
 - [Номера телефонов](#)
 - [Сигнатуры COB](#)
 - [Профили COB](#)
 - [Профили оповещений](#)
 - [Профили Netflow](#)
 - [Профили LLDP](#)
 - [Профили SSL](#)
 - [Профили пересылки SSL](#)
 - [NIP объекты](#)
 - [NIP-профили](#)
 - [Профили BFD](#)
 - [Syslog-фильтры UserID агента](#)
 - [Сценарии](#)
 - [Теги](#)
- [Диагностика и мониторинг](#)
 - [Мониторинг трафика](#)
 - [Маршруты](#)
 - [OSPF](#)

- [VPN](#)
- [Веб-портал](#)
- [Заблокированные COB/L7 IP-адреса](#)
- [Захват пакетов](#)
- [Запросы в белый список](#)
- [Трассировка правил](#)
- [Ping](#)
- [Traceroute](#)
- [Запрос DNS](#)
- [LLDP-соседи](#)
- [Статистика LLDP](#)
- [Оповещения](#)
 - [Правила оповещений](#)
 - [SNMP](#)
 - [Параметры SNMP](#)
 - [Профили безопасности SNMP](#)
- [Журналы и отчеты](#)
 - [Журналы](#)
 - [Общие сведения](#)
 - [Журнал событий](#)
 - [Журнал веб-доступа](#)
 - [Журнал DNS](#)
 - [Журнал трафика](#)
 - [Журнал COB](#)
 - [Журнал инспектирования SSH](#)
 - [История поиска](#)
 - [Журнал защиты почтового трафика](#)
 - [UserID-агент](#)
 - [Экспорт журналов](#)
 - [Поиск и фильтрация данных](#)
 - [Описание форматов журналов](#)
 - [Отчеты](#)
 - [Описание](#)
 - [Шаблоны отчетов](#)
 - [Правила отчетов](#)
 - [Созданные отчеты](#)
- [Гостевой портал](#)
 - [Управление гостевыми пользователями](#)
- [Интерфейс командной строки](#)
 - [Общие положения](#)
 - [Общие положения \(Описание\)](#)
 - [Команды, доступные до первоначальной инициализации узла](#)
 - [Команды, доступные до первичной инициализации узла \(Описание\)](#)

- [Первоначальная инициализация](#)
 - [Первоначальная инициализация NGFW](#)
 - [Мастер первоначальной настройки узла](#)
- [Команды диагностики и мониторинга](#)
 - [Команды диагностики и мониторинга \(Описание\)](#)
- [Режим конфигурации](#)
 - [Режим конфигурации \(описание\)](#)
- [Настройка устройства](#)
 - [Настройка устройства \(Описание\)](#)
 - [Настройка кластеров](#)
 - [Настройка кластеров \(версия 7.5.0 и выше\)](#)
 - [Настройка управления доступом к консоли UserGate NGFW](#)
 - [Настройка сертификатов](#)
 - [Настройка параметров устройства](#)
 - [Настройка прокси-сервера](#)
 - [Настройка работы с вышестоящими прокси-серверами](#)
 - [Настройка параметров мониторинга устройства](#)
 - [Настройка профилей клиентских сертификатов](#)
 - [Настройка параметров управления телеметрией](#)
 - [Функция экспорта и импорта конфигурации](#)
- [Настройки сети](#)
 - [Зоны](#)
 - [Интерфейсы](#)
 - [Шлюзы](#)
 - [DHCP](#)
 - [DNS-настройки](#)
 - [Настройка виртуальных маршрутизаторов](#)
 - [Настройка WCCP](#)
- [Настройка раздела Пользователи и устройства](#)
 - [Настройка групп пользователей](#)
 - [Настройки пользователей](#)
 - [Настройка серверов аутентификации](#)
 - [Настройка профилей аутентификации](#)
 - [Настройка Captive-профилей](#)
 - [Captive-портал](#)
 - [Настройка терминальных серверов](#)
 - [Настройка профилей MFA \(мультифакторной аутентификации\)](#)
 - [Просмотр информации об авторизованных пользователях](#)
 - [Настройка применения политик к пользователям](#)
 - [Настройка UserID-агента](#)
- [Настройка раздела Политики сети](#)
 - [Настройка правил межсетевого экрана](#)
 - [Настройка правил NAT и маршрутизации](#)
 - [Настройка балансировки нагрузки](#)
 - [Настройка правил управления пропускной способностью](#)

- [Настройка раздела Политики безопасности](#)
 - [Настройка фильтрации контента](#)
 - [Настройка веб-безопасности](#)
 - [Настройка правил инспектирования туннелей](#)
 - [Настройка инспектирования SSL](#)
 - [Настройка инспектирования SSH](#)
 - [Настройка COB](#)
 - [Настройка защиты почтового трафика](#)
 - [Настройка правил ICAP](#)
 - [Настройка ICAP-серверов](#)
 - [Настройка профилей DoS](#)
 - [Настройка правил защиты DoS](#)
- [Настройка глобального портала](#)
 - [Настройка веб-портала](#)
 - [Настройка правил reverse-прокси](#)
 - [Настройка серверов reverse-прокси](#)
- [Настройка VPN в CLI](#)
 - [Настройка серверных правил](#)
 - [Настройка клиентских правил](#)
 - [Настройка сетей VPN](#)
 - [Настройка профилей безопасности VPN](#)
 - [Настройка VPN в CLI \(в версии 7.5.0 и выше\)](#)
 - [Настройка серверных правил VPN](#)
 - [Настройка клиентских правил VPN](#)
- [Настройка библиотек](#)
 - [Настройка библиотек \(Описание\)](#)
- [Настройка раздела журналы и отчеты](#)
 - [Настройка экспорта журналов](#)
 - [Настройка отчетов](#)
- [Интерфейс командной строки PMC](#)
 - [Общие сведения](#)
- [UserGate Application and Security Language \(UASL\)](#)
 - [UserGate Application and Security Language \(UASL\)](#)
 - [Метаинформация](#)
 - [Идентификатор](#)
 - [Фильтрация по IP-адресам](#)
 - [Фильтрация по портам](#)
 - [Сканирование пакетов без полезной нагрузки](#)
 - [Поиск шаблонов](#)
 - [Модификаторы области поиска](#)
 - [Частота срабатывания](#)
 - [Направление анализа](#)
 - [Поиск бинарных данных](#)
 - [Работа с метками](#)
 - [Протокольные анализаторы](#)

- [Примеры](#)
- [UserGate Policy Language \(UPL\)](#)
 - [UserGate Policy Language \(Описание\)](#)
 - [Общие положения](#)
 - [Условия](#)
 - [Встроенные библиотеки](#)
 - [Определения](#)
 - [Свойства](#)
 - [Действия](#)
 - [Типы правил](#)
 - [Список поддерживаемых HTTP-заголовков](#)
- [Дашборд](#)
 - [Работа с дашбордами и виджетами](#)
- [Техническая поддержка](#)
 - [Раздел технической поддержки](#)
 - [Аварийные ситуации](#)
- [Приложения](#)
 - [Установка сертификата локального удостоверяющего центра](#)
 - [Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0](#)
 - [Требования к сетевому окружению](#)
 - [Опции DHCP](#)
 - [Примеры генерации сертификатов для IKEv2 VPN](#)

ВВЕДЕНИЕ

БЕЗОПАСНОСТЬ СЕТИ И ЗАЩИТА ОТ СЕТЕВЫХ УГРОЗ

Межсетевое экранирование

Межсетевой экран нового поколения UserGate NGFW фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

Обнаружение и предотвращение вторжений

Система обнаружения и предотвращения вторжений (COB) позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление отчетов.

Администратор может создавать собственные сигнатуры COB для защиты определенных сервисов и включать их в профили COB наряду с сигнатурами, поставляемыми UserGate. Профили COB интегрируются в правила меж сетевого экрана. При срабатывании сигнатур такого профиля будет произведено действие, настроенное в сигнатурах и произведена соответствующая запись в [Журнале COB](#).

Защита от DOS-атак и сетевого флуда

NGFW позволяет задать параметры защиты каждой зоны сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP), указав порог уведомления - количество запросов с одного IP-адреса, после которого происходит запись в

журнал - и порог отбрасывания пакетов - количество запросов, после которого пакеты отбрасываются с соответствующей записью в журнале.

Возможно настроить исключения, например, для зон, использующих IP-телефонию и поэтому отправляющих большое количество UDP-пакетов.

Антивирусная проверка трафика

Потоковый антивирус UserGate позволяет обеспечить антивирусную проверку трафика без ущерба для производительности и быстродействия сети. Модуль использует обширную базу сигнатур.

Проверка почтового трафика

NGFW способен обрабатывать транзитный почтовый трафик (SMTP(S), POP3(S)), анализируя его источник, а также содержание письма и вложений, что гарантирует надежную защиту от спама, pharming- и phishing- атак. NGFW также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

Управление трафиком АСУ ТП

В новой версии платформы администратор может контролировать прохождение трафика автоматизированных систем управления технологическими процессами (АСУ ТП) через NGFW с помощью профилей COB и приложений. В библиотеке сигнатур, поставляемых компанией UserGate, имеется набор сигнатур, которые идентифицируют известные уязвимости протоколов АСУ ТП по CVE/BDU.

Работа с внешними системами безопасности

Имеется возможность передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами.

Администратор может указать, какой трафик требуется передавать на ICAP, а также настроить работу с фермами серверов.

Настройка политик безопасности при помощи сценариев

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря автоматизации безопасности при помощи механизма сценариев (SOAR — Security Orchestration, Automation and Response).

Эта концепция находится на пике популярности и позволяет администратору создавать сценарии (запускаемые по плану или при обнаружении атаки), где прописываются автоматические действия в ответ на те или иные события. Такой подход обеспечивает гибкую настройку политик безопасности, сокращает участие человека благодаря автоматизации повторяющихся задач, а также дает возможность приоритизировать сценарии для скорейшей реакции на критичные угрозы.

УЛУЧШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ И НАДЕЖНОСТИ ИНТЕРНЕТА

Поддержка кластеризации и отказоустойчивости

UserGate NGFW поддерживает 2 типа кластеров: кластер конфигурации, позволяющий задать единые настройки узлам в рамках кластера, и кластер отказоустойчивости, призванный обеспечить бесперебойную работу сети. Кластер отказоустойчивости может работать в двух режимах: Актив-Актив и Актив-Пассив. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

FTP поверх HTTP

Модуль FTP поверх HTTP позволяет обращаться к содержимому FTP-сервера из браузера пользователя.

Поддержка нескольких провайдеров

При подключении системы к нескольким провайдерам UserGate NGFW позволяет настроить для каждого из них свой шлюз для обеспечения доступа к интернету. Администратор также может настроить балансировку трафика между провайдерами, указав вес каждого шлюза, или указать один из шлюзов как основной с переключением на других провайдеров в случае недоступности основного шлюза.

Управление пропускной способностью

Правила управления пропускной способностью служат для ограничения канала для определенных пользователей, хостов, сервисов или приложений.

Поддержка WCCP

Поддержка протокола WCCP позволяет использовать NGFW в инфраструктуре с WCCP-серверами, например, маршрутизаторами Cisco.

УПРАВЛЕНИЕ ТРАФИКОМ И КОНТРОЛЬ ДОСТУПА В ИНТЕРНЕТ

Маршрутизация трафика и публикация ресурсов

NGFW позволяет использовать как статическую, так и динамическую маршрутизацию. Динамическая маршрутизация осуществляется по протоколам

OSPF и BGP, что позволяет использовать NGFW в сложной маршрутизируемой сети предприятия.

Администратор может создавать в системе правила NAT (для предоставления пользователям доступа в интернет), а также правила безопасной публикации внутренних ресурсов в интернет с использованием reverse-прокси для HTTP/HTTPS и DNAT для других протоколов.

Аутентификация и авторизация пользователей

Платформа поддерживает различные механизмы аутентификации пользователей: Captive-портал, Kerberos, NTLM, при этом учетные записи могут поступать из различных источников — LDAP, Active directory, FreeIPA, TACACS+, RADIUS, SAML IDP. Аутентификация SAML IDP, Kerberos или NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory на устройстве UserGate. В Captive-портале также возможна аутентификация пользователей посредством сертификатов, использующих инфраструктуру открытых ключей (PKI).

Благодаря функциональности UserID возможна прозрачная аутентификация пользователей на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Active Directory, syslog и сообщения RADIUS accounting. Для этого агент UserID осуществляет запросы посредством протокола WMI на серверы AD, в сценарии с syslog осуществляет прослушивание порта syslog и сбор информации, которую присылают серверы syslog, а в сценарии с RADIUS-серверами принимает сообщения RADIUS accounting от серверов NAS. Далее информация фильтруется по событиям входа/выхода пользователей. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя отправляются на все устройства UserGate, указанные в Профиле редистрибуции источника и производится вход пользователя на NGFW.

Администратор может настроить правила безопасности, ширину канала, правила межсетевого экранирования, контентной фильтрации и контроля приложений для отдельных пользователей, групп пользователей, а также всех известных или неизвестных пользователей. Дополнительно к этому продукт поддерживает применение правил безопасности к пользователям терминальных служб с помощью специальных агентов (Terminal Services Agents), а также использование агента авторизации для Windows-платформ.

Для обеспечения большей безопасности учетных записей рекомендуется использовать мультифакторную аутентификацию с помощью токенов TOTP (Time-based One Time Password Algorithm), SMS или электронной почты.

Поддержка гостевого портала

NGFW позволяет предоставлять пользователям временный доступ к сети, что актуально, например, для публичных Wi-Fi сетей. Профили могут быть как созданы администратором, так и зарегистрированы самими пользователями с подтверждением через email или SMS. Платформа позволяет указывать отдельные настройки безопасности для временных пользователей.

Проксирование приложений

Для пользователей, работающих с ОС Windows, можно настроить прокси-агент, позволяющий использовать возможности прокси приложениям, не умеющим работать с прокси-серверами. Прокси-агент также может быть использован для предоставления таким приложениям доступа в интернет в случаях, когда NGFW не является шлюзом по умолчанию.

Перенаправление трафика на вышестоящий прокси-сервер

С помощью функциональности Upstream proxy UserGate NGFW позволяет перенаправлять пользовательский трафик на вышестоящий прокси-сервер, благодаря чему возможно создание каскадной иерархии, когда трафик с одного прокси-сервера передается на следующий в цепочке прокси-серверов. Подобное каскадирование обычно используется для обеспечения конфиденциальности коммуникаций или для организации доступа к контенту с региональными ограничениями. Также благодаря технологии каскадирования упрощается встраивание новых региональных офисов в существующую иерархию глобальной сети компании.

ЖУРНАЛЫ И ОТЧЕТЫ

Журналы и отчеты(описание)

Платформа позволяет осуществлять мониторинг работы системы в режиме реального времени при помощи журналов событий, веб-доступа, COB и трафика. Для удобства анализа администратор может настроить автоматический экспорт журналов на сервера SSH, FTP и Syslog. С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

КОНТЕНТ-ФИЛЬТРАЦИЯ И КОНТРОЛЬ ПРИЛОЖЕНИЙ

Интернет-фильтрация

Использование модуля интернет-фильтрации обеспечивает административный контроль за использованием интернета, загружаемыми данными. Модуль обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

Для анализа безопасности сайтов, запрашиваемых пользователями, используются репутационные сервисы, типы контента (фото, видео, тексты и др.), специальные морфологические словари, предоставляемые UserGate, а также черные и белые списки URL и Useragent, с помощью которых администратор может запретить или разрешить работу с определенным типом браузеров. NGFW предоставляет возможность создавать собственные черные и белые списки, словари, типы контента, морфологические словари и Useragent, применяя их как правила к пользователям и группам пользователей.

Выборочная блокировка рекламы

Даже безопасные сайты могут содержать нежелательные изображения на баннерах, содержимое которых не зависит от владельца ресурса. UserGate NGFW решает эту проблему, блокируя баннеры и защищая пользователей от негативного контента.

Активация безопасного поиска

NGFW позволяет принудительно активировать функцию безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. Такая защита позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту. Также можно заблокировать поисковые системы, в которых не реализована функция безопасного поиска.

Блокировка приложений социальных сетей

NGFW дает возможность блокировки игр и других приложений для наиболее популярных социальных сетей, таких, как Facebook, VK, Одноклассники. Администраторы могут разрешать использование социальных сетей в целом, при этом контролируя и ограничивая непродуктивные действия.

Инжектирование кода на веб-страницы

Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователями. Эта возможность может быть использована для получения различных метрик, сокрытия некоторых элементов веб-страниц, а также показа рекламы или другой информации.

Инспектирование SSL-трафика

UserGate NGFW позволяет фильтровать не только обычный, но и зашифрованный трафик (протоколы HTTPS, SMTPS, POP3S), дешифруя их при

помощи технологии MITM (Man In The Middle) и подписывая доверенным корневым сертификатом с последующим шифрованием после анализа. Система позволяет настроить выборочную проверку трафика, например, не расшифровывать ресурсы категории «Финансы».

VPN и веб-портал

VPN (Virtual Private Network) служит для того, чтобы настраивать виртуальные логические сети поверх других сетей, например, интернет. UserGate NGFW поддерживает два типа VPN-сетей: Remote Access VPN (модель клиент-сервер) и Site-to-Site VPN (модель сервер-сервер).

Для создания защищенных туннелей используются протоколы L2TP/IPsec или IKEv2/IPsec. UserGate имеет собственный VPN клиент UserGate Client, также поддерживается работа со стандартными клиентами большинства популярных операционных систем: Windows, Linux, Mac OS X, iOS, Android и других.

Веб-портал (SSL VPN) позволяет предоставить безопасный доступ сотрудникам компании к внутренним веб-ресурсам, серверам SSH и серверам терминальных служб без необходимости установки специального клиента VPN, используя только протокол HTTPS.

ДРУГИЕ ФУНКЦИИ

Функция балансировщика нагрузки

NGFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена для внутренних серверов, публикуемых в интернет (DNAT или reverse-прокси), внутренних серверов без публикации.

DNS-фильтрация

NGFW позволяет осуществлять настройку работы с DNS-серверами, а также настраивать сервис DNS-прокси, позволяющий перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Платформа также позволяет подключить фильтрацию DNS-запросов пользователей.

Использование оповещений

UserGate NGFW поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается как управление с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps).

Помимо этого, система позволяет создавать профили оповещений, уведомляющие пользователей об определенных событиях по протоколам SMTP (email) и SMPP (SMS).

Ролевой доступ администраторов к элементам управления UserGate NGFW

По умолчанию в системе существует один суперадминистратор, который может создавать учетные записи других администраторов и выдавать им права на просмотр и изменение различных разделов.

Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Типы интерфейсов

UserGate NGFW позволяет добавлять и настраивать тегированные VLAN-интерфейсы, а также объединять ряд физических интерфейсов в один логический агрегированный интерфейс (бонд) с использованием протокола LACP (link aggregation control protocol) для повышения пропускной способности или для отказоустойчивости канала.

Существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании. Если мост создается в ПАК NGFW, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить два интерфейса в байпас-мост. Подробнее читайте в разделе [Настройка интерфейсов](#).

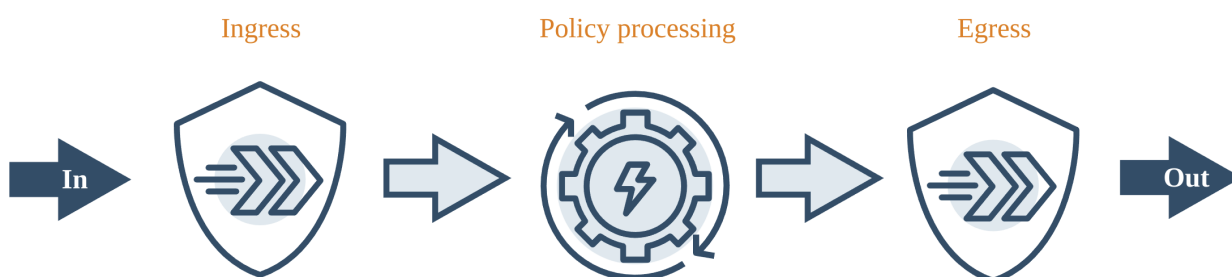
АЛГОРИТМ ОБРАБОТКИ ТРАФИКА

UserGate NGFW 7 Packet Flow

В данной статье представлен обобщённый высокоуровневый алгоритм обработки трафика (packet flow), реализованный в UserGate NGFW версии 7.1.x.

Пакеты трафика проходят три основные стадии обработки:

1. Стадия предварительной обработки входящего трафика (Ingress).
2. Стадия обработки политиками сети и политиками безопасности (Policy processing).
3. Стадия завершающей обработки исходящего трафика (Egress).



На стадии предварительной обработки трафик подвергается базовым проверкам от DoS-атак и IP-спуфинга, маркируется для дальнейшей обработки, при необходимости происходит распаковка и дешифрация пакетов IPsec VPN, подмена адресов и портов назначения.

На стадии обработки политиками в зависимости от сценариев обработки трафика и наличия соответствующих правил происходит инспектирование трафика, фильтрация контента, проверка потоковым антивирусом, обработка правилами межсетевого экрана, COV и фильтрации приложений (L7).

На стадии завершающей обработки исходящий трафик обрабатывается правилами управления пропускной способности, подмены исходящих адресов (SNAT), при необходимости происходит инкапсуляция и шифрование IPsec VPN и передача пакетов в выходной интерфейс.

В общем случае путь прохождения пакетов через UserGate NGFW можно представить с помощью следующей функциональной диаграммы:

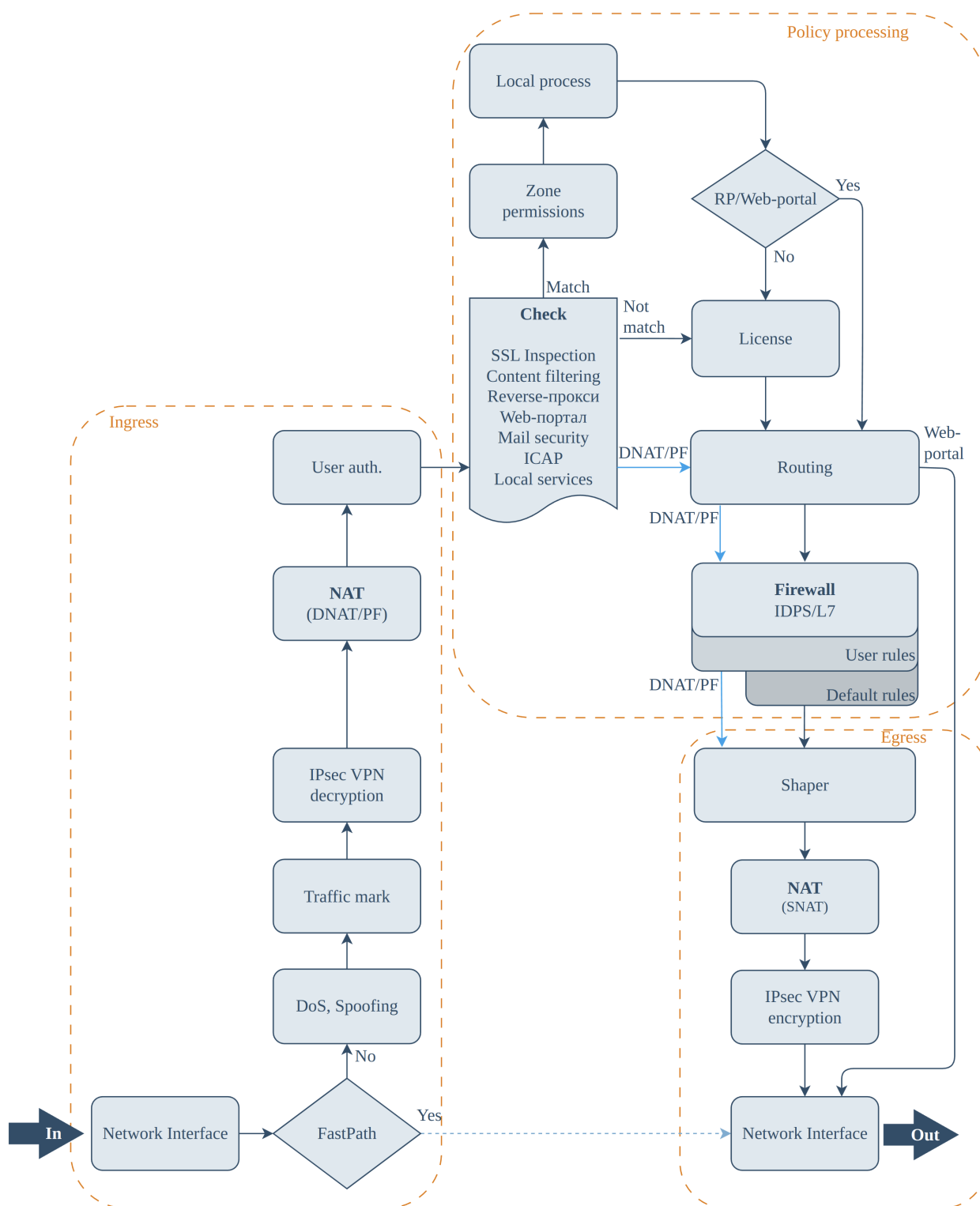


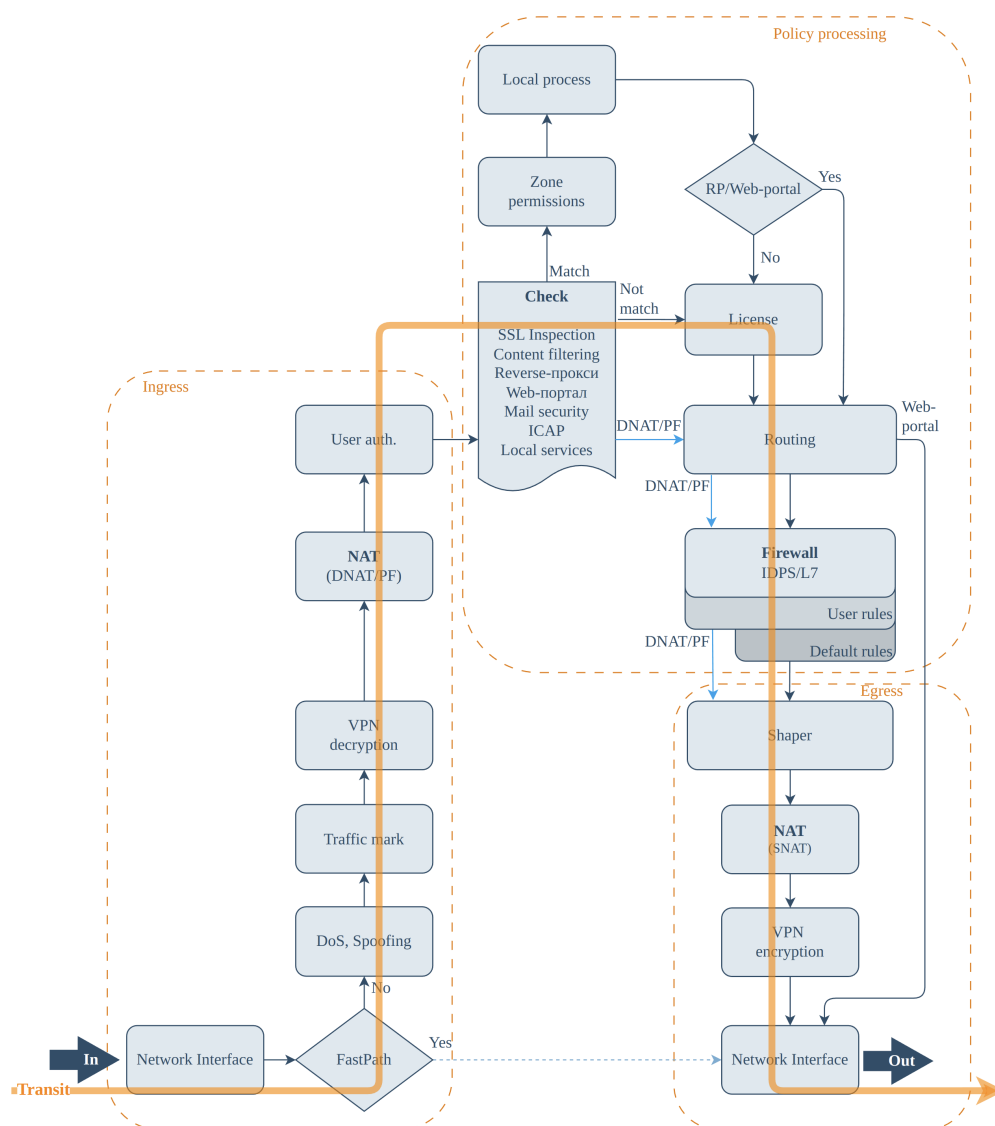
Диаграмма описывает обобщённый путь прохождения пакетов через NGFW. При этом пакеты могут не подвергаться обработке или изменениям во всех функциональных блоках, представленных на диаграмме. Это зависит от типа пакета, настроек функциональности NGFW и сценариев прохождения трафика.

Далее будут рассмотрены следующие сценарии обработки трафика в UserGate NGFW:

- Транзит трафика без фильтрации контента.
- Прозрачный прокси с фильтрацией контента.
- Явный прокси.
- Трафик DNAT/порт-форвардинг.
- Трафик через reverse-прокси.
- Публикация ресурсов через веб-портал.

Транзит трафика без фильтрации контента

Путь прохождения пакетов транзитного трафика без фильтрации контента на функциональной диаграмме обозначен с помощью цветовой маркировки:



Стадия предварительной обработки входящего трафика (Ingress)

Пакеты, пришедшие на входной интерфейс NGFW, попадают под действие правил зоны — в блок **DoS, Spoofing**. Если в настройках зоны включены соответствующие параметры, на этом этапе производится базовая проверка трафика на наличие DoS-атак или выявление аномалий трафика по выставленным порогам уведомлений/отбрасывания пакетов и правилам агрегирования, также в этом блоке проверяются условия защиты от IP-спуфинга. Уже на этом этапе может произойти отбрасывание пакета при срабатывании условий защиты.

Примечание

Настройка защиты от DoS-атак в свойствах зоны является грубой. Более гибкая настройка с указанием сервисов и адресов производится с помощью правил защиты DoS.

Прошедшие далее пакеты помечаются (маркируются) для последующей обработки правилами политик сети и политик безопасности.

Если входящие пакеты определяются как пакеты, относящиеся к VPN туннелю, совпадающему с настройками на NGFW, производится их распаковка и расшифровка в условном блоке **IPsec VPN decryption**. В случае возникновения ошибок при расшифровке пакеты отбрасываются.

В блоке **NAT** происходит проверка наличия правил подмены IP-адресов и портов. При отсутствии правил с совпавшими условиями пакеты проходят блок без изменений.

В условном блоке **User auth** производится аутентификация пользователей со статусом Unknown.

Стадия обработки политиками сети и политиками безопасности (Policy processing)

В блоке с условным названием **Check** происходит проверка трафика на предмет соответствия условиям политик безопасности. Если трафик не попадает под условия правил инспектирования, контентной фильтрации, принадлежности сервисам ICAP и защиты почтового трафика, созданных на NGFW, то пакеты проходят дальше в блок лицензирования, откуда попадают в блок **Routing**, где происходит проверка всех записей подключённых сетей, проверка доступности шлюзов, проверка записей (статических и динамических) виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка транзитного трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, данные начинают анализироваться сигнатурами профилей безопасности COV и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COV не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Стадия завершающей обработки исходящего трафика (Egress)

В блоке **Shaper** происходит настройка пропускной способности исходящего трафика при наличии соответствующих правил.

В блоке **NAT** при наличии соответствующего совпавшего правила происходит обработка пакета и подмена адреса источника в исходящем пакете (SNAT).

При наличии соответствующих правил исходящие пакеты инкапсулируются и шифруются в условном блоке **IPsec VPN encryption**.

Далее пакеты передаются на выходной интерфейс.

Функция быстрой обработки сетевых пакетов

В UserGate NGFW реализована функция быстрой обработки сетевых пакетов (**FastPath**). Принцип такой обработки прост: если сессия уже установлена и остальные пакеты сессии по какой-то причине не требуют проверки и специальной обработки, то их можно сразу перенаправлять со входного интерфейса в выходной, выполнив необходимые соответствующие преобразования (DNAT, Port forwarding итд.).

Функция FastPath активирована по умолчанию. Сброс правил модуля осуществляется одновременно со сбросом сессий в межсетевом экране. Для этого на странице **Политики сети → Межсетевой экран** доступна кнопка **Принудительно применить**.

Функция FastPath выключается автоматически при записи трафика. Под обработку модуля не попадают фрагментированные пакеты и пакеты, предназначенные для COB/L7 инспектирования.

Статус функции можно проверить с помощью команды CLI:

```
Admin@nodename# show settings fastpath

enabled      : on
```

Отключить функцию можно командой:

```
Admin@nodename# set settings fastpath enabled
+ on      Enable
+ off     Disable
```

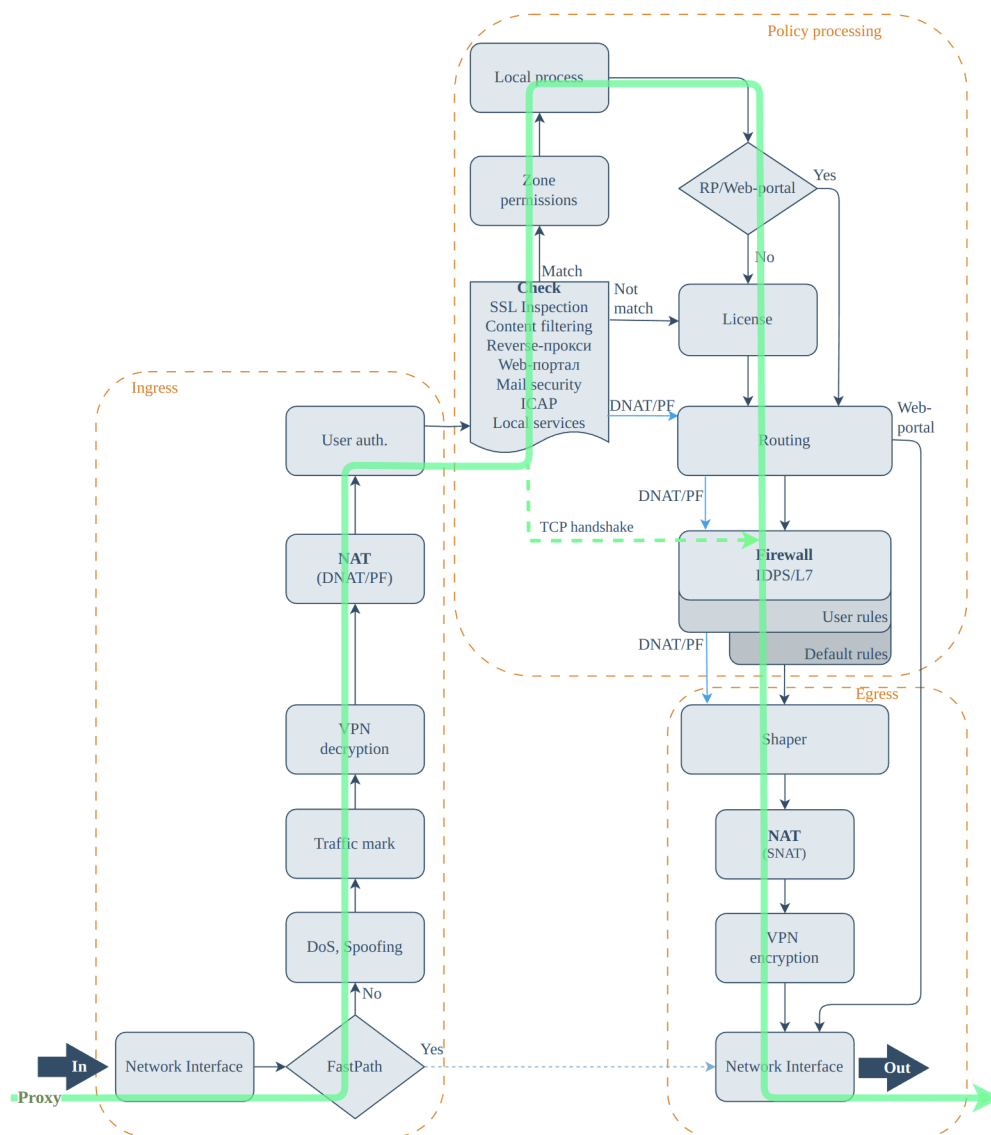
Прозрачный прокси с фильтрацией контента

Режим прозрачного прокси применяется к транзитному трафику, проходящему через NGFW. В режиме прозрачного прокси NGFW является посредником между клиентом и конечным сервером, выполняющим обработку и перехват трафика в соответствии с настроенными политиками безопасности.

В случае использования режима прозрачного прокси NGFW по умолчанию будет анализировать TCP-пакеты, отправляемые по портам 80 (HTTP) и 443 (HTTPS).

При наличии правил защиты почтового трафика NGFW также будет анализировать TCP-пакеты по портам, указанным в правилах защиты почтового трафика. Это могут быть как стандартные порты 110 (POP3) / 995 (POP3S) / 25 (SMTP) / 465 (SMTPS), так и выбранные администратором порты, добавленные в настройках используемых в правилах сервисов.

Путь прохождения пакетов в режиме прозрачного прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:



Стадия предварительной обработки входящего трафика (Ingress)

Путь прохождения пакетов в стадии предварительной обработки в целом аналогичен пути, описанному [ранее](#).

Стадия обработки политиками сети и политиками безопасности (Policy processing)

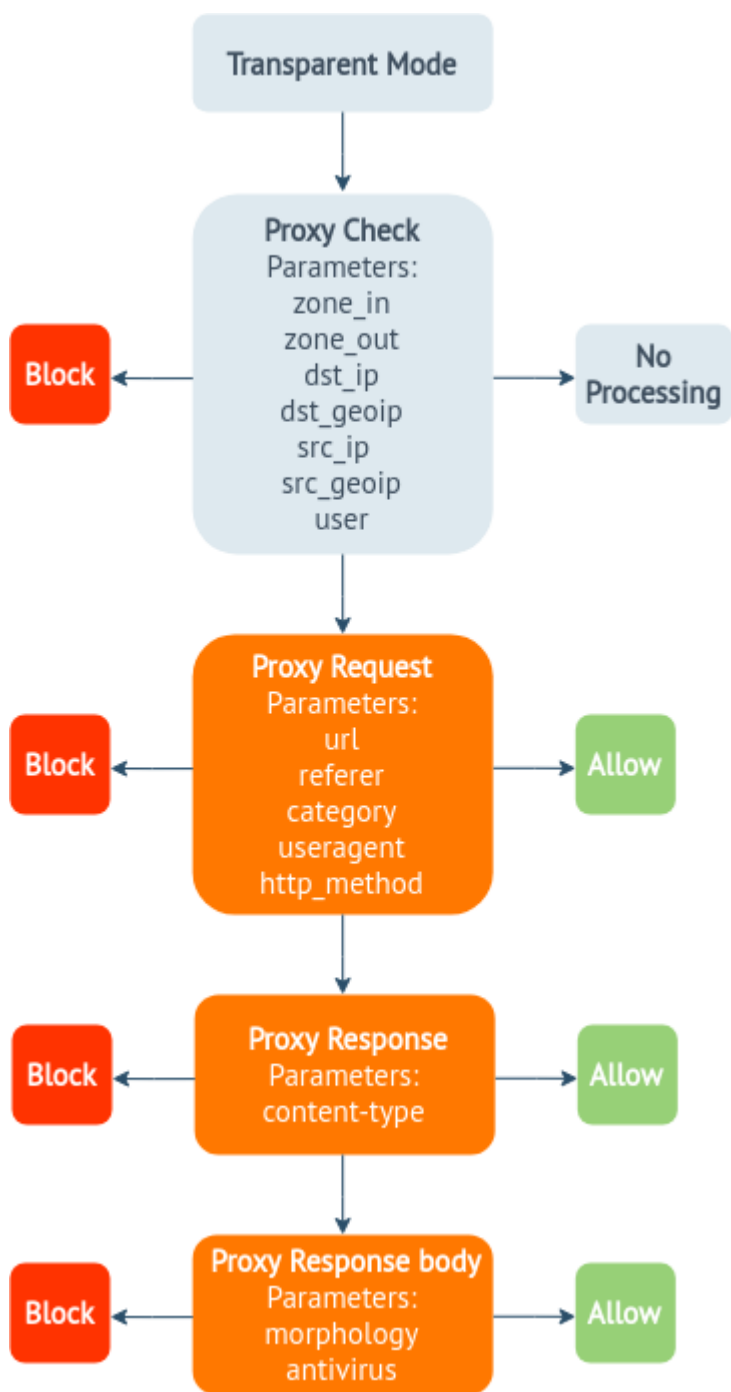
В режиме прозрачного прокси из всего потока в обработку модулем **Local Process** попадает только трафик, удовлетворяющий условиям политик, настроенных на NGFW.

Перехват трафика модулем Local Process осуществляется на финальной стадии установления TCP-соединения, т.е. на последнем этапе «трёхстороннего рукопожатия» (three-way handshake).

Изначально, на этапе установления TCP-соединения, пакеты доходят до межсетевого экрана и проверяются правилами политик сети. При наличии блокирующего пользовательского правила, под которое попадают эти пакеты, они будут отброшены и TCP-соединение не будет установлено. В случае отсутствия разрешающих пользовательских правил все пакеты будут отброшены правилом межсетевого экрана Default Block, созданным по умолчанию.

Если трафик не был заблокирован правилами межсетевого экрана на этапе установления TCP-соединения, то происходит проверка соответствия условиям правил контентной фильтрации.

Проверка соответствия условиям правил инспектирования, контентной фильтрации осуществляется путём поэтапного анализа трафика в соответствии с параметрами алгоритма блока **CHECK**:



Transparent Proxy Mode	
HTTPS	Rule Condition
TCP • IP; • Zone; • User.	• Zone; • IP; • User.
Client Hello • SNI.	• Domain; • Category.
SSL Decrypt • Fetch Certificate.	• Zone; • IP; • User; • Domain; • Category.
HTTP (Method) req • Method; • User-Agent; • Referer; • URL.	• Method; • User-Agent; • Referer; • URL.
HTTP (Method) res • Type; • HTTP Body.	• Content Type; • Morphology; • Antivirus

- Если трафик попадает под какое-либо правило контентной фильтрации, то происходит проверка соответствия условиям правила, запрещающим трафик по зонам, адресам источников/назначений и/или пользователям. В случае соответствия NGFW заблокирует данное соединение и отобразит страницу блокировки.
- В случае отсутствия блокирующих правил контентной фильтрации по зонам, адресам источников/назначений или пользователям NGFW проверяет наличие правил фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.). Если таких правил нет, то блок Proxy Check пропускает трафик дальше без обработки. Если такие правила есть,

блок Proxy Check пропускает трафик без обработки, но продолжает его отслеживать до установления TLS-сессии.

- После получения сообщения **Client Hello**, содержащего SNI, доступна фильтрация по доменам и категориям сайтов.
- Если настроено инспектирование SSL, то на этом же этапе происходит проверка сертификата (корректность сертификата, срок действия и т.д.). Настройка правил инспектирования доступна по зонам, адресам, пользователям, категориям URL, доменам.
- Если на данном этапе блокировка не произошла, то далее NGFW получает от пользователя **HTTP Request** (GET, PUT и т.д.), из которого можно получить информацию о реферере, URL, Useragent браузера, методе HTTP. Соответственно, эти же параметры могут быть использованы в качестве параметров фильтрации при настройке политик. На этом этапе доступна работа с URL. Поэтому, если трафик не расшифровывается, то доступна только фильтрация по доменным именам.
- При получении ответа от сервера (**HTTP Response**) доступна информация о типе контента (содержится в заголовке **HTTP Response**) и тело сообщения. Соответственно, на данном этапе доступна фильтрация по типу контента, проверка морфологии, а также работает потоковый антивирус UserGate.

Если после проверки соответствия политикам NGFW трафик не был заблокирован, то он будет передан в блоки **License** (лицензирование трафика), **Routing** (проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов).

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COB и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COB не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7)

определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

i Примечание

Т.к. в режиме прозрачного прокси из всего потока в обработку попадает только трафик, удовлетворяющий условиям политик, настроенных на NGFW, то этот режим является более производительным при большом потоке веб-трафика по отношению к режиму явного прокси.

Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Явный прокси

В режиме явного прокси весь трафик направлен на NGFW. На стороне клиента в веб-браузере или в других приложениях в явном виде указывается адрес и порт прокси-сервера NGFW (порт 8090 по умолчанию).

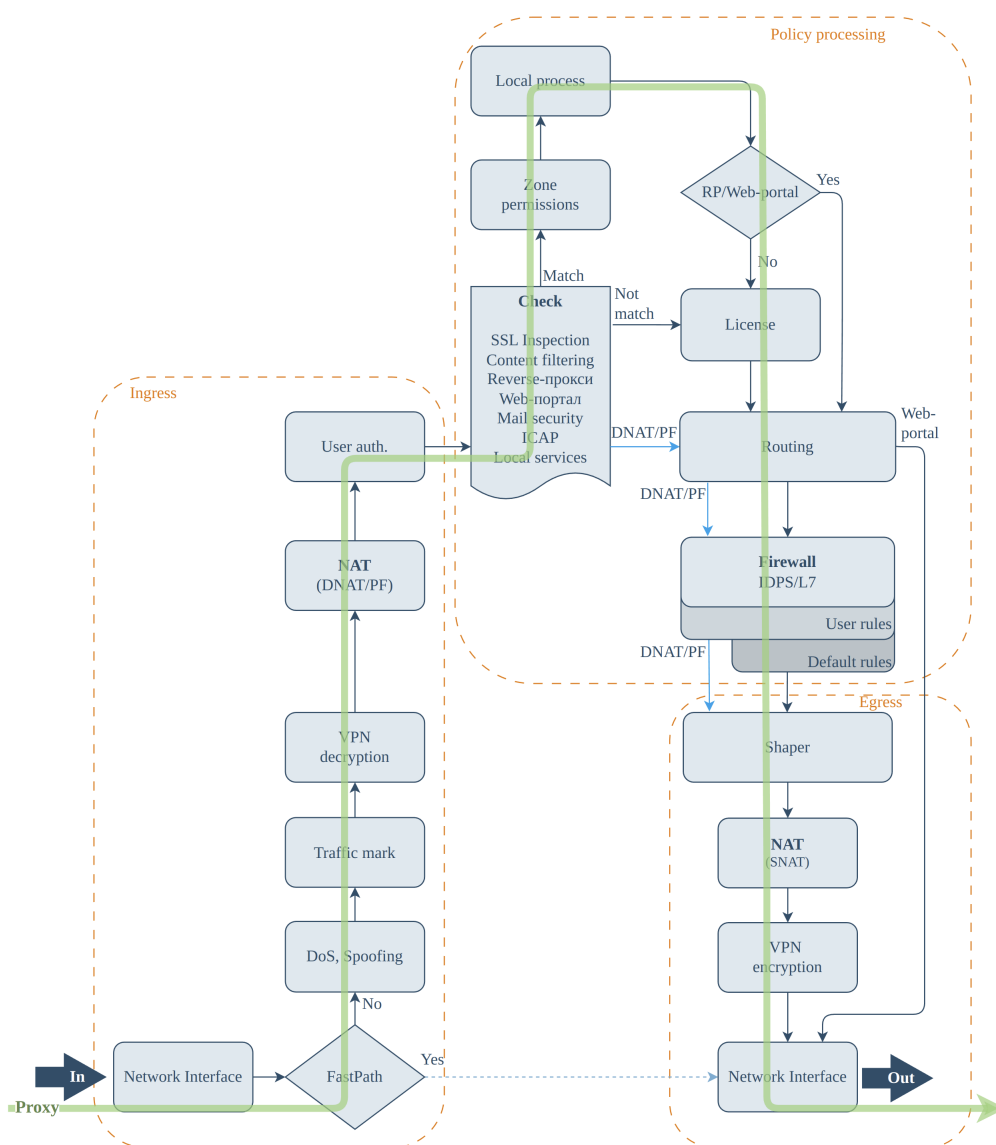
В момент запроса клиентом внешнего ресурса формируется две TCP-сессии:

- Первая сессия: КЛИЕНТ — NGFW. Обращение от клиента происходит непосредственно к NGFW и начинается с HTTP Connect.
- Вторая сессия: NGFW — КОНЕЧНЫЙ СЕРВЕР. При этом трафик от NGFW до сервера является транзитным для блока **Firewall** (если настроено запрещающее правило по IP-адресу назначения, т.е. указан адрес конечного сервера, то трафик будет заблокирован).

i Примечание

Для использования NGFW в режиме явного прокси необходимо в настройках доступа зоны разрешить сервис HTTP(s)-прокси, иначе пакет будет отброшен.

Путь прохождения пакетов в режиме явного прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:

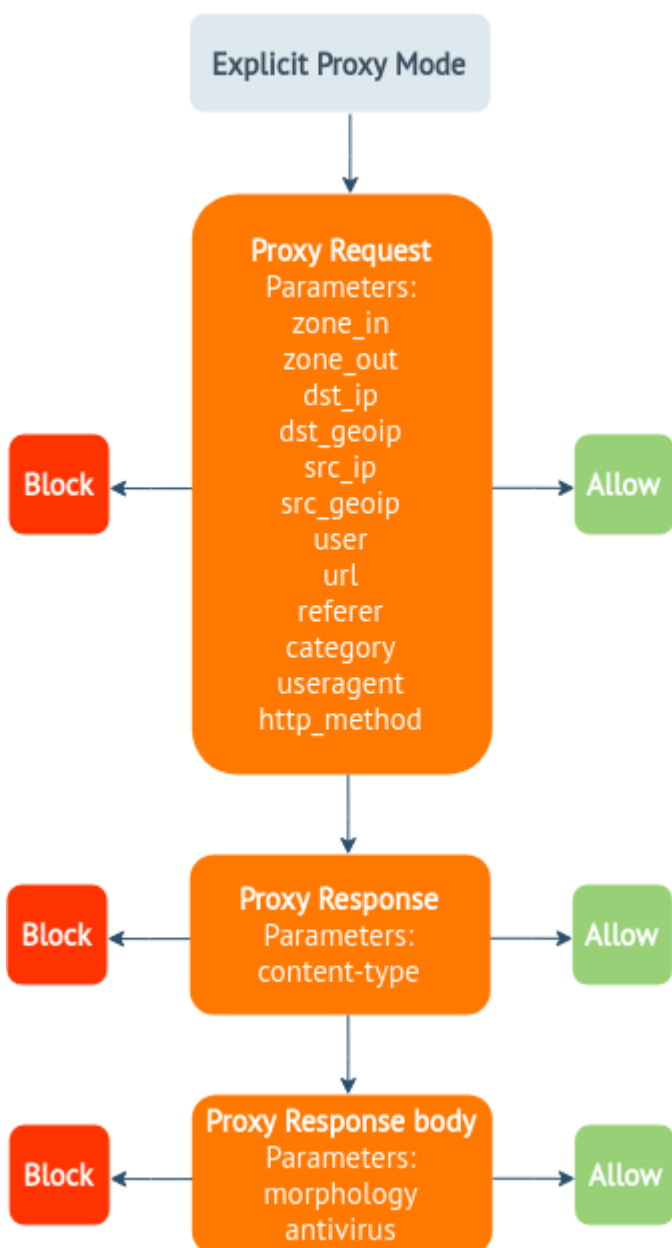


Стадия предварительной обработки входящего трафика (Ingress)

Путь прохождения пакетов в стадии предварительной обработки в целом аналогичен пути, описанному [ранее](#).

Стадия обработки политиками сети и политиками безопасности (Policy processing)

В блоке **CHECK** весь трафик будет проходить проверку соответствия условиям правил инспектирования, контентной фильтрации, а также принадлежности сервисам ICAP, reverse-прокси, веб-портала, АСУ ТП и защиты почтового трафика. Проверка осуществляется путём поэтапного анализа трафика в соответствие с параметрами алгоритма блока **CHECK**:



Explicit Proxy Mode	
HTTPS	Rule Condition
HTTP Connect • IP; • Zone; • User.	• Zone; • IP; • User; • Method.
Client Hello • SNI.	• Domain; • Category.
SSL Decrypt • Fetch Certificate.	• Zone; • IP; • User; • Domain; • Category.
HTTP (Method) req • Method; • User-Agent; • Referer; • URL.	• Method; • User-Agent; • Referer; • URL.
HTTP (Method) res • Type; • HTTP Body.	• Content Type; • Morphology; • Antivirus

- В режиме явного прокси первое сообщение, которое NGFW получает от клиента — **HTTP Connect**, из которого можно извлечь информацию о зонах, адресах источника/назначения, пользователя.
- Если по таким параметрам, блокировка не происходит, то следующий пакет, который ожидает NGFW — это пакет **Client Hello**, с которым становится доступна идентификация по имени сервера (SNI). На основании SNI доступна фильтрация по доменам и категориям сайтов.
- Если настроено инспектирование SSL, то на этом же этапе происходит проверка сертификата (корректность сертификата, срок действия и т.д.).

Настройка правил инспектирования доступна по зонам, адресам, пользователям, категориям URL, доменам.

- Если на данном этапе блокировка не произошла, то далее NGFW получает от пользователя **HTTP Request** (GET, PUT и т.д.), из которого можно получить информацию о реферере, URL, Useragent браузера, методе HTTP. Соответственно, эти же параметры могут быть использованы в качестве параметров фильтрации при настройке политик. На этом этапе доступна работа с URL. Поэтому, если трафик не расшифровывается, то доступна только фильтрация по доменным именам.
- При получении ответа от сервера (**HTTP Response**) доступна информация о типе контента (содержится в заголовке **HTTP Response**) и тело сообщения. Соответственно, на данном этапе доступна фильтрация по типу контента, проверка морфологии, а также работает потоковый антивирус UserGate.

После обработки в блоке **CHECK** трафик будет направлен в блок лицензирования трафика (**License**). В блоке **Routing** происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COB и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COB не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

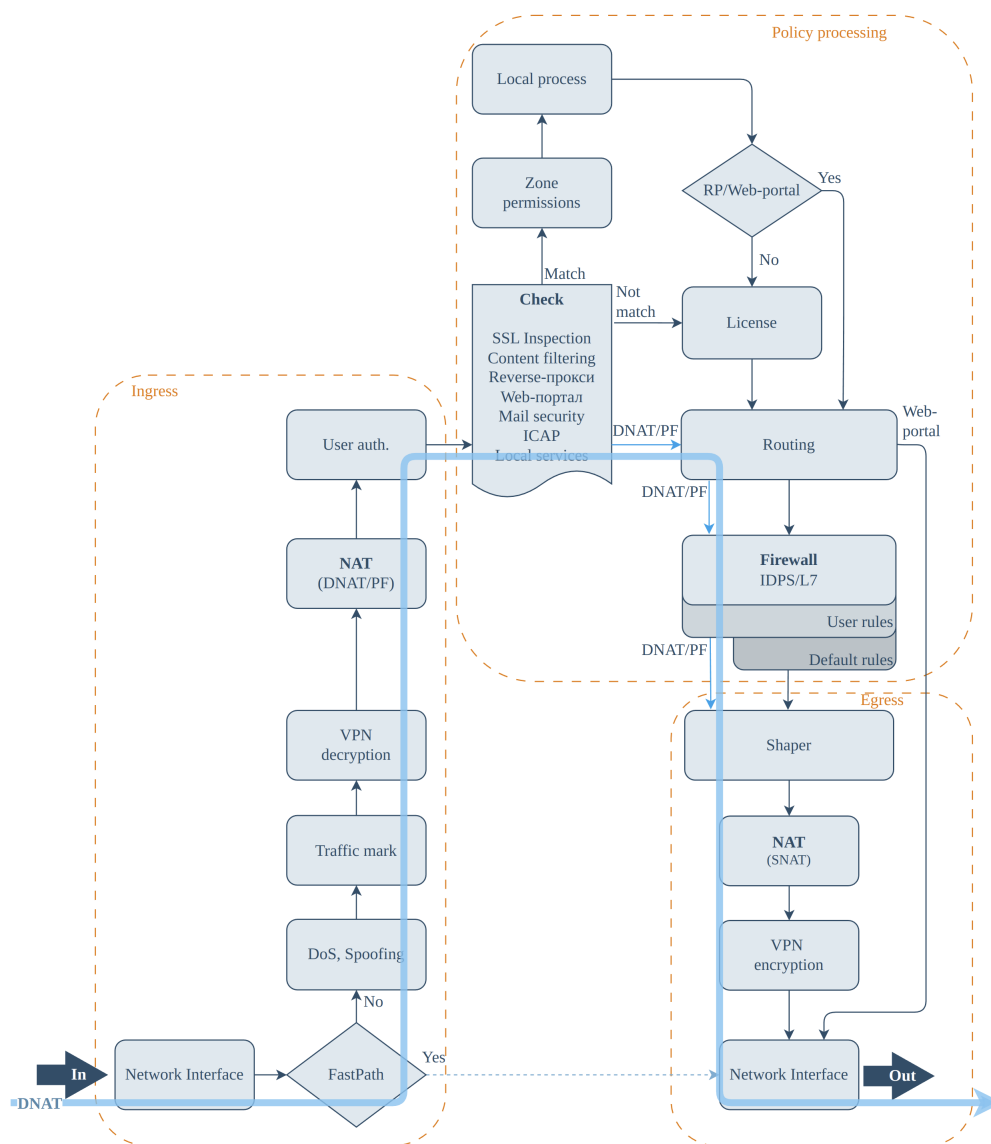
Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Трафик DNAT/порт-форвардинг

Трафик DNAT/порт-форвардинг является транзитным и подчиняется созданным правилам фильтрации межсетевого экрана, к нему могут применяться правила инспектирования и, соответственно, фильтрации контента при определённых условиях.

Путь прохождения пакетов трафика DNAT на функциональной диаграмме обозначен с помощью цветовой маркировки:



Стадия предварительной обработки входящего трафика (Ingress)

Пакеты, пришедшие на входной интерфейс NGFW, попадают под действие правил зоны — в блок **DoS, Spoofing**. Если в настройках зоны включены соответствующие параметры, на этом этапе производится базовая проверка трафика на наличие DoS-атак или выявление аномалий трафика по

выставленным порогами уведомлений/отбрасывания пакетов и правилам агрегирования, также в этом блоке проверяются условия защиты от IP-спуфинга. Уже на этом этапе может произойти отбрасывание пакета при срабатывании условий защиты.

Прошедшие далее пакеты помечаются (маркируются) для последующей обработки правилами политик сети и политик безопасности.

Если входящие пакеты определяются как пакеты, относящиеся к VPN туннелю, совпадающему с настройками на NGFW, производится их распаковка и расшифровка в условном блоке **IPsec VPN decryption**. В случае возникновения ошибок при расшифровке пакеты отбрасываются.

В блоке **NAT** при совпадении условий соответствующего правила происходит подмена адреса назначения (порта — в случае порт-форвардинга).

В условном блоке **User auth** производится аутентификация пользователей со статусом Unknown.

Стадия обработки политиками сети и политиками безопасности (Policy processing)

Анализ трафика начинается на этапе установления TCP-соединения с портами назначения 80 и 443. NGFW анализирует весь TCP-трафик, но его перехват осуществляет на финальной стадии установления надёжного TCP-соединения, т.е. на последнем этапе «трёхстороннего рукопожатия» (three-way handshake). Таким образом, первые пакеты пройдут путь до блока **Firewall** и будут отброшены в случае наличия запрещающего правила, под условия которого подходят эти пакеты. Правила межсетевого экрана, созданные по умолчанию (Default block), не применяются к трафику DNAT и порт-форвардинг.

Обработка трафика DNAT и порт-форвардинг проходит следующим образом:

- Проверяется соответствия трафика условиям правил фильтрации контента по зонам, адресам источника/назначения и/или пользователям.
- Если есть правила контентной фильтрации по другим параметрам (URL, категория сайта, тип контента и т.д.) и настроено SSL инспектирование, то NGFW ожидает установки TLS-сессии, после чего производит проверку соответствия.

В случае соответствия условиям блокирующего правила контентной фильтрации трафик будет заблокирован, а пользователю вернётся страница блокировки. Блокирующие правила межсетевого экрана не возвращают страницу блокировки.

В случае, если нет соответствия условиям блокирующих правил, трафик будет перенаправлен в блок **Routing**. В блоке **Routing** происходит проверка всех записей подключённых сетей, проверка доступности шлюзов, проверка записей (статических и динамических) виртуальных маршрутизаторов.

В блоке **Firewall** пакеты обрабатываются только в случае наличия правил, созданных администратором. Правилами по умолчанию (Default block) DNAT-трафик не обрабатывается.

После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COV и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COV не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

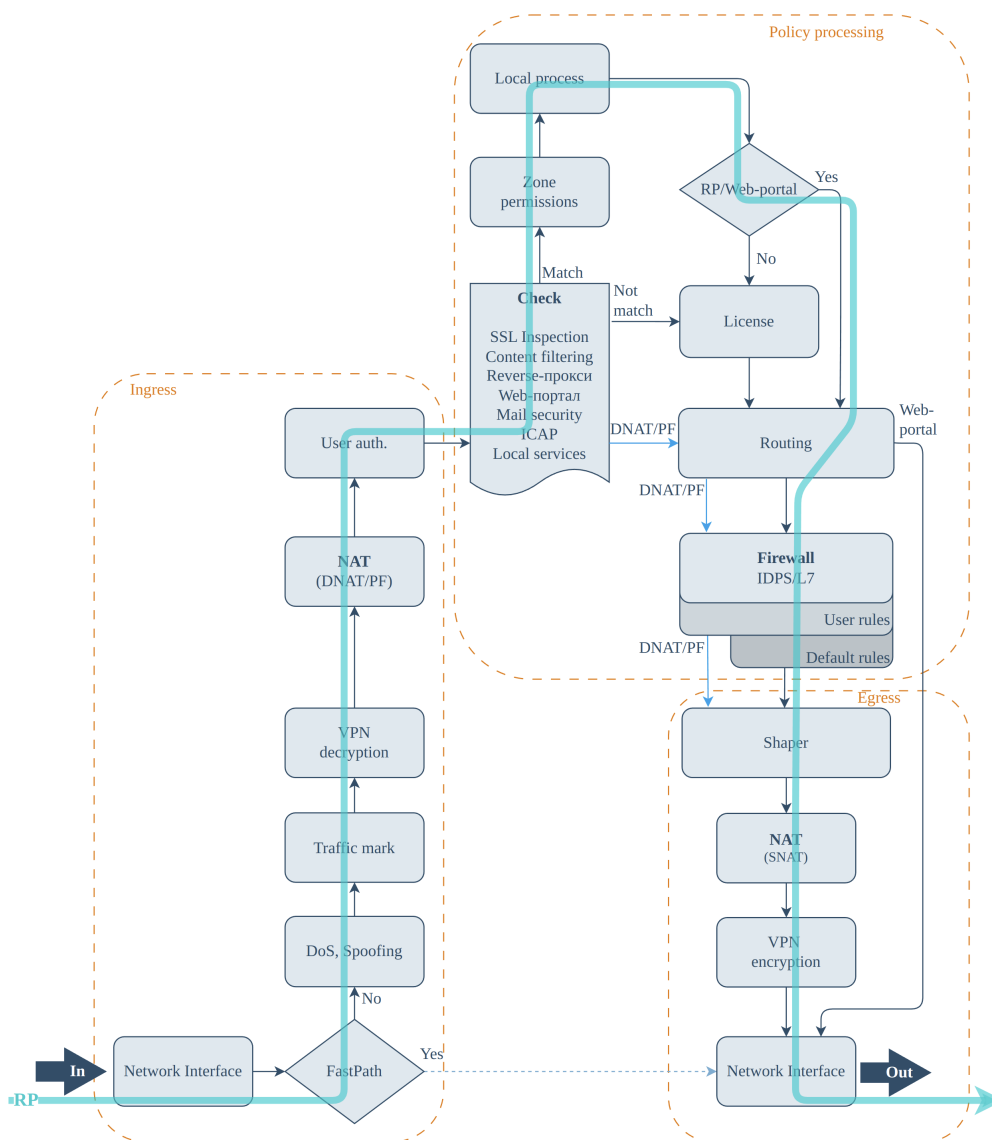
Стадия завершающей обработки исходящего трафика (Egress)

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Публикация ресурсов через reverse-прокси

С помощью правил reverse-прокси производится публикация серверов по протоколам HTTP/HTTPS.

Путь прохождения пакетов в режиме reverse-прокси на функциональной диаграмме обозначен с помощью цветовой маркировки:



Обработка пакетов в целом аналогична режиму прозрачного прокси, но перехват включается сразу же при обращении к публикуемому серверу (без дополнительного анализа tcp-трафика для перехвата).

После сопоставления трафика политикам NGFW в блоке **CHECK** пакеты перенаправляются для обработки в блок **Local process** через блок **Zone Permission**. Для работы сервиса reverse-прокси в настройках доступа зоны необходимо разрешить сервис **Reverse-прокси**, иначе пакеты будут отброшены.

Трафик сервиса reverse-прокси не анализируется в блоке **License**, а сразу переходят в блок **Routing**, где происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов.

В блоке **Firewall** происходит проверка трафика на соответствие политикам сети. В качестве условий правил межсетевого экрана могут выступать зоны и IP-адреса источника/назначения, пользователи, сервисы. Правила межсетевого экрана применяются поочерёдно сверху вниз в том порядке, в котором они

указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещён.

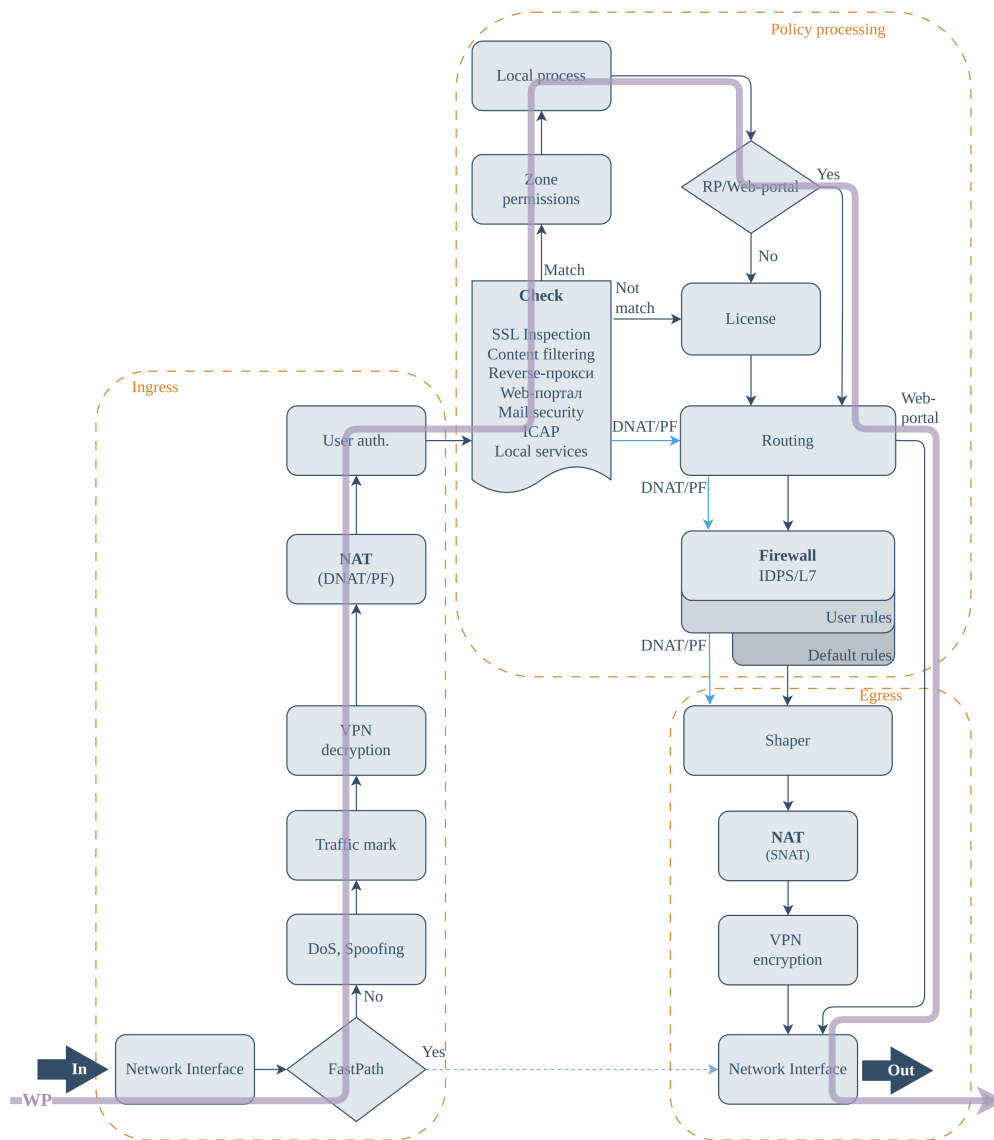
После того, как определено первое совпавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей безопасности COV и/или L7 (если профили безопасности добавлены в это правило). При срабатывании сигнатур к трафику применяется действие, настроенное в профиле. Если в профиле COV не совпало ни одной сигнатуры, трафик передаётся дальше без изменений. В профиле приложений (L7) определяются действия в том числе и для трафика, который не удалось идентифицировать сигнатурами профиля.

Путь прохождения пакетов в стадии завершающей обработки в целом аналогичен пути, описанному [ранее](#).

Публикация ресурсов через веб-портал

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удалённых или мобильных пользователей, используя при этом только протокол HTTPS.

Путь прохождения пакетов в режиме веб-портала на функциональной диаграмме обозначен с помощью цветовой маркировки:



Обработка пакетов аналогична режиму прозрачного прокси, но перехват включается сразу же при обращении к веб-порталу (без дополнительного анализа tcp-трафика для перехвата).

После сопоставления трафика политикам NGFW в блоке **CHECK** пакеты перенаправляются для обработки в блок **Local process** через блок **Zone Permission**. Для работы сервиса веб-портала в настройках доступа зоны необходимо разрешить сервис **Веб-портал**, иначе пакеты будут отброшены.

Трафик сервиса веб-портала не анализируется в блоке **License**, а сразу переходит в блок **Routing**, где происходит проверка записей подключённых сетей, доступности шлюзов, записей виртуальных маршрутизаторов. Далее трафик передаётся на выходной интерфейс.

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Общие сведения

Межсетевой экран UserGate поставляется в виде программно-аппаратного комплекса (ПАК) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины межсетевой экран UserGate поставляется с десятью Ethernet-интерфейсами. В случае поставки в виде ПАК — может содержать от 2 до 64 Ethernet-портов.

Развертывание виртуального образа

UserGate NGFW Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают системы виртуализации VMware, Oracle VirtualBox, и в формате Qcow2 для систем виртуализации QEMU-KVM. Для Microsoft Hyper-V поставляется образ диска виртуальной машины.

Примечание

Для корректной работы виртуальной машины рекомендуется использовать минимум 12 ГБ оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Примечание

Для корректной работы внутренней базы данных требуется поддержка набора микрокоманд SSE4.2 архитектуры x86 процессорами виртуальной среды. Любой процессор на базе архитектуры x86, выпущенный после 2008 года, должен поддерживать SSE4.2.

Работа с виртуальным образом

Для начала работы с виртуальным образом выполните следующие шаги:

1. Скачайте последнюю версию виртуального образа [с официального сайта UserGate](#).
2. Импортируйте образ в свою систему виртуализации. Инструкцию по импорту образа вы можете найти на сайтах систем виртуализации, например VirtualBox или VMware. Для Microsoft Hyper-V необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.
3. До включения виртуальной машины настройте её параметры в своей системе виртуализации:
 - Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8 ГБ и добавьте по 1 ГБ на каждые 100 пользователей.
 - Добавьте дополнительный диск нужного размера. Размер диска по умолчанию составляет 100 ГБ, чего обычно недостаточно для хранения всех журналов и параметров. Используя свойства виртуальной машины, установите размер диска не меньше 200 ГБ. Рекомендованный размер — 300 ГБ или больше.
4. Для систем виртуализации QEMU-KVM размер системной области по умолчанию составляет 8 ГБ. При первом запуске система сама определит наличие дополнительного диска и расширит свои системные разделы. Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:

```
qemu-img create -f qcow2 -o  
preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_  
size=4K <имя-вашего-диска>.qcow2 100G
```

5. Запустите виртуальную машину UserGate. Во время загрузки выполняется процедура **Factory reset**. Система UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного ранее.

UserGate NGFW поставляется с четырьмя интерфейсами, назначенными в зоны:

- **Management** — первый интерфейс виртуальной машины;
- **Trusted** — второй интерфейс виртуальной машины;
- **Untrusted** — третий интерфейс виртуальной машины;
- **DMZ** — четвертый интерфейс виртуальной машины.

Порядок нумерации интерфейсов в виртуальной среде

В веб-консоли администратора сетевые интерфейсы отображаются по своим названиям. Сопоставление названия интерфейса и его адреса (H/W path или MAC) называется маппингом. Данные о маппинге интерфейсов хранятся в специальном системном файле. Посмотреть содержимое файла маппинга интерфейсов можно с помощью CLI-команды:

```
Admin@nodename> show network interface-mapping
```

После сброса до первоначального состояния (factory reset) при изменении количества сетевых адаптеров в системе (при добавлении или удалении адаптеров средствами гипервизора) происходит сортировка интерфейсов и их маппинг.

Выбор метода сортировки (по H/W path или по MAC-адресам) зависит от типа гипервизора и используемого эмулятора аппаратного обеспечения. В некоторых случаях (VirtualBox, QEMU, Bochs) сортировка интерфейсов производится по параметру H/W path, в остальных — по MAC-адресам интерфейсов.

При сортировке интерфейсов по параметру H/W path:

- Все имеющиеся на устройстве интерфейсы при любом изменении их количества (удаление, добавление) будут пересортированы в порядке возрастания аппаратных адресов (H/W path); системный файл с данными маппинга будет полностью перезаписан.

```
Admin@canntoralcti> show network interface-mapping
```

Interface	Info
port0	(H/W_Path) /0/100/3
port1	(H/W_Path) /0/100/8
port2	(H/W_Path) /0/100/9
port3	(H/W_Path) /0/100/10

- Удаленные интерфейсы отображаются как неиспользуемые, помечаются соответствующим значком и помещаются в конец списка интерфейсов в веб-консоли.

Сетевой адаптер	port0	DHCP	192.168.56.142/255.255.255.0	08:00:27:9e:14:7f	Management	1500	—	—	100 Mb/s
Сетевой адаптер	port1	Статический	10.10.0.2/255.255.255.0	08:00:27:c7:47:87	Trusted	1500	—	—	100 Mb/s
Сетевой адаптер	port2	Статический	172.16.1.3/255.255.255.0	08:00:27:68:77:9d	Untrusted	1500	—	—	100 Mb/s
Сетевой адаптер	port3	Статический	192.168.1.4/255.255.255.0	08:00:27:e9:c9:58	DMZ	1500	—	—	100 Mb/s
Удалённый интерфейс	port4	Без адреса		08:00:27:e9:c9:58	DMZ2	1500	—	—	0 Mb/s
VPN	tunnel1	Статический	172.30.250.1/255.255.255.0		VPN for remote access	1420			0 Mb/s
VPN	tunnel2	Статический	172.30.255.1/255.255.255.0		VPN for Site-to-Site	1420			0 Mb/s
VPN	tunnel3	Динамический			VPN for Site-to-Site	1420			0 Mb/s

При сортировке интерфейсов по MAC-адресам:

- Интерфейсы, уже добавленные в систему, остаются на своих местах.
- Удаляемые интерфейсы отмечаются в веб-консоли как неиспользуемые и помечаются специальными значками.
- Новые добавленные интерфейсы добавляются в конец списка в порядке возрастания MAC-адресов.

Сетево...	port0	Статичес...	146.185.211.135/255.255.252.0	fa:16:3e:20:91:f7	Manage...	1500	—	—	100 Mb/s
Сетево...	port1	DHCP	10.0.0.14/255.255.255.0	fa:16:3e:02:4e:2d	Trusted	1500	—	—	100 Mb/s
Удалённые интерфейсы	port2	Без адре...		fa:16:3e:0b:76:09	Trusted	1500	—	—	0 Mb/s
Сетево...	port3	DHCP	192.168.0.16/255.255.255.0	fa:16:3e:40:5a:fd	DMZ	1500	—	—	100 Mb/s
Сетево...	port4	Без адре...		fa:16:3e:8c:ef:ad	DMZ	1500	—	—	0 Mb/s
Добавленные интерфейсы	port5	DHCP	10.10.10.104/255.255.255.0	fa:16:3e:15:09:c1	Зона не уста...	1500	—	—	100 Mb/s
	port6	DHCP		fa:16:3e:39:a0:c0	Зона не уста...	1500	—	—	100 Mb/s
	port7	DHCP	10.10.20.111/255.255.255.0	fa:16:3e:52:93:bd	Зона не уста...	1500	—	—	100 Mb/s
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s
VPN	tunnel3	Динамич...			VPN for S...	1420			0 Mb/s

```
Admin@hinstathible> show network interface-mapping
```

Interface	Info
port0	(MAC) fa:16:3e:20:91:f7
port1	(MAC) fa:16:3e:02:4e:2d
port2	(MAC) fa:16:3e:0b:76:09
port3	(MAC) fa:16:3e:40:5a:fd
port4	(MAC) fa:16:3e:8c:ef:ad
port5	(MAC) fa:16:3e:15:09:c1
port6	(MAC) fa:16:3e:39:a0:c0
port7	(MAC) fa:16:3e:52:93:bd

Если использовать консольную команду `clear network interface-mapping`, файл существующего маппинга интерфейсов будет удален и все имеющиеся интерфейсы после перезапуска машины будут пересортированы заново по принципу возрастания адресов.

Важно!

Виртуальный образ устройства UserGate, доступный для скачивания в личном кабинете, не имеет файла маппинга интерфейсов. Сортировка интерфейсов и их маппинг осуществляются при первом запуске в виртуальной среде пользователя. При подготовке собственного виртуального образа устройства UserGate для его разворачивания впоследствии на облачной платформе необходимо также удалить данные маппинга сетевых адаптеров перед сохранением образа. Файл маппинга можно удалить консольной командой: `clear network interface-mapping`.

Примечание

Если виртуальная машина UserGate клонируется через vSphere, то в VMX-файле параметров скопированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие виртуальной машине источника.

Оптимизация производительности сетевых интерфейсов на основе virtio

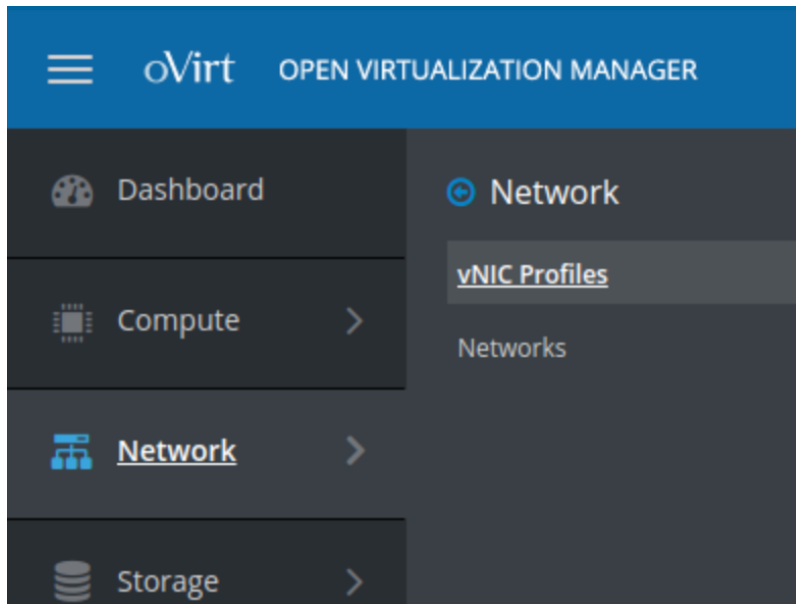
Для оптимизации производительности сетевых интерфейсов на основе virtio в средах виртуализации KVM, oVirt, zVirt рекомендуется включить на гипервизоре режим Multi Queues и устанавливать 8 очередей на сетевой интерфейс. Например, в случае платформы OVirt (см. [документацию oVirt](#)), для того чтобы выставить 8 очередей для vNIC, необходимо подключиться к CLI гипервизора и ввести команду:

```
engine-config -s "CustomDeviceProperties={type=interface;prop={other-nic-properties;queues=[1-9][0-9]*}}"
```

Вместо параметра `other-nic-properties` нужно вставить список существующих кастомизированных правил (если такие правила есть). Посмотреть, существуют ли кастомизированные правила, можно с помощью команды:


```
engine-config -g "CustomDeviceProperties"
```

После ввода команды необходимо на портале администратора зайти в профили vNIC.



Далее необходимо выбрать редактирование профиля сетевых карт, назначенного для NGFW, в выпадающем списке **Custom Properties** выбрать **queues**, после чего указать нужное количество очередей.

VM Interface Profile

Data Center

Test

Network

IN

Name

IN

Description

QoS

[Unlimited]

Network Filter

vdsm-no-mac-spoofing

☐ Passthrough

☒ Migratable

☐ Port Mirroring

Custom Properties

queues

queues

8

+

-

OK

Cancel

Автоматизация развертывания UserGate NGFW с помощью Cloud-init

Cloud-init — индустриальный стандарт для кросс-платформенной инициализации виртуальных машин (инстансов) в облачных сервисах провайдеров. Межсетевой экран UserGate поддерживает возможность первоначальной настройки с помощью механизма Cloud-init. Настройка межсетевого экрана осуществляется с помощью двух модулей:

- С помощью команд CLI (файл с заголовком `#utm-config`). Возможно использовать все CLI-команды для полной настройки виртуальной машины.
- Посредством активации лицензии (файл с заголовком `#utm-license`).

Другие модули Cloud-init не поддерживаются.

Пример файла конфигурации с CLI командами (user-data):

```
#utm-config
#set password for initial Administrator (Admin). Obligatory comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
#Create network gateway to Internet:
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
#Create firewall rule to allow traffic from Trusted to untrusted
security zones:
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
```

— обозначает начало комментария, обратный слеш — переход на следующую строку.

В данный файл можно добавлять все доступные для администратора команды CLI. Подробнее о CLI-командах — в разделе «[Интерфейс командной строки \(CLI\)](#)».

Активировать создаваемую виртуальную машину можно через указание параметров для лицензирования в отдельном файле. Следует учитывать, что активация возможна только при наличии у виртуальной машины доступа в сеть интернет. Пример содержимого файла для активации лицензии (vendor-data):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email: email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
country: Russia
region: Novosibirsk
```

Оба файла можно объединить в один файл, используя формат multipart:

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0
--//
Content-Type: text/utm-config; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config.txt"
#utm-config
password 123
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
```

```

ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
--//
Content-Type: text/utm-license; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license.txt"
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email: email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
country: Russia
region: Novosibirsk
--//

```

Настройки могут быть переданы в NGFW:

- Через облачный провайдер. Например, в провайдере Digital Ocean при создании виртуальной машины (droplet) настройки необходимо вставить в опциональное поле **User data (Select additional options → User data)**. Аналогичным образом настройки можно передать и через другие поставщики облачных услуг.

- Через подключаемый ISO-диск. На диске должны быть файлы `meta-data`,
- `user-data`, `vendor-data` со следующим содержимым:

- `meta-data: instance-id: vm1`
- `user-data` — с CLI-командами настройки инстанса:

```
#utm-config
#set password for initial Administrator (Admin). Obligatory
comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
...
```

- `vendor-data` — с информацией о лицензировании (опционально):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email: email@company.com
...
```

Для создания ISO-диска на Linux можно использовать следующую утилиту:

```
mkisofs -joliet -rock -volid "cidata" -output nocloud.iso meta-data
user-data vendor-data
```

Полученный ISO-диск необходимо подключить к виртуальной машине UserGate. После успешной первой загрузки виртуальная машина получит все настройки, указанные для нее в созданных файлах.

Требования к сетевому окружению

Для корректной работы межсетевой экран UserGate должен иметь доступ к следующим серверам в интернете:

- сервер регистрации — reg2.usergate.com, порты TCP 80, 443;
- сервер обновления ПО UserGate — updates.usergate.com, порты TCP 80, 443.

При создании кластера конфигурации необходимо обеспечить прохождение следующих протоколов между узлами:

- репликация настроек — порты TCP 4369, TCP 9000-9100;
- сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности — в приложении «[Требования к сетевому окружению](#)».

Подключение к UserGate NGFW

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, его можно явно задать, используя CLI (Command Line Interface). Подробнее об использовании CLI — в разделе «[Интерфейс командной строки](#)».

Примечание

Если устройство не прошло первоначальную инициализацию, для доступа к CLI необходимо использовать в качестве имени пользователя **Admin**, в качестве пароля — **usergate**.

Остальные интерфейсы отключены и требуют последующей настройки.

Для первоначальной настройки выполните следующие шаги:

Шаг	Описание
1. Подключитесь к интерфейсу управления	Подключитесь к интерфейсу устройства: • При наличии DHCP-сервера. Подключите интерфейс port0 к сети предприятия с работающим DHCP-сервером. Включите NGFW. После загрузки в консоли NGFW будет указан полученный интерфейсом IP-адрес. Подключитесь к веб-консоли устройства по адресу: <code>https://<NGFW_IP_address>:8001</code> для дальнейшей активации продукта. • Статический IP-адрес. Включите UserGate NGFW. Используя CLI, назначьте необходимый IP-адрес на интерфейс port0. Произведите первоначальную инициализацию в интерфейсе командной строки или подключитесь к веб-консоли UserGate NGFW по указанному адресу (он должен иметь вид: <code>https://<NGFW_IP_address>:8001</code>). Подробнее об использовании CLI — в разделе «Интерфейс командной строки»
2. Выберите язык	
3. Задайте пароль	
4. Настройте зоны, IP-адреса интерфейсов, подключите UserGate NGFW в сеть предприятия	В разделе Настройки → Сеть → Интерфейсы включите необходимые интерфейсы, установите корректные IP-адреса, соответствующие вашим сетям, и назначьте интерфейсы соответствующим зонам. Подробнее об управлении интерфейсами — в разделе «Настройка интерфейсов». Система поставляется с предопределенными зонами: • Management (сеть управления), интерфейс port0; • Trusted (LAN); • Untrusted (Internet); • DMZ; • Cluster; • VPN for remote access; • VPN for Site-to-Site; • Tunnel inspection zone

Шаг	Описание
5. Настройте шлюз в интернет	В разделе Настройки → Сеть → Шлюзы укажите IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет (зона Untrusted). Подробнее о настройке шлюзов — в разделе « Настройка шлюзов »
6. Укажите системные DNS-серверы	В разделе Настройки → Сеть → DNS укажите IP-адреса серверов DNS вашего провайдера или серверов, используемых в вашей организации. Подробнее об управлении DNS — в разделе « Настройка DNS »
7. Настройте время сервера	В разделе Настройки → UserGate → Настройки → Настройка времени сервера настройте синхронизацию времени с серверами NTP.
8. Зарегистрируйте NGFW	В разделе Дашборды в виджете Лицензия нажмите Нет лицензии и введите ПИН-код для регистрации продукта. Для активации системы необходим доступ в интернет. Подробнее о лицензировании продукта — в разделе « Лицензирование »
9. Создайте правила NAT	В разделе Настройки → Политики сети → NAT и Маршрутизация создайте необходимые правила NAT. Для доступа в интернет пользователей сети Trusted правило NAT уже создано: NAT from Trusted to Untrusted . Подробнее о правилах NAT — в разделе « NAT и маршрутизация »
10. Создайте правила межсетевого экрана	В разделе Настройки → Политики сети → Межсетевой экран создайте необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети Trusted уже создано правило Allow trusted to untrusted , необходимо только включить его. Подробнее о правилах межсетевого экрана — в разделе « Межсетевой экран »

После выполнения этих шагов UserGate NGFW готов к работе. Вы также можете дополнительно настроить другие параметры.

Шаг	Описание
Создать дополнительных администраторов	В разделе Настройки → UserGate → Администраторы UserGate создайте дополнительных администраторов системы, наделите их необходимыми полномочиями (ролями)

Шаг	Описание
Настроить авторизацию пользователей	В разделе Настройки → Пользователи и устройства создайте необходимые методы авторизации пользователей. Самый простой вариант — создать локальных пользователей NGFW в разделе Настройки → Пользователи и устройства → Пользователи с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя Any во всех правилах). О других вариантах авторизации пользователей — в разделе «Пользователи и устройства»
Создать правила контентной фильтрации	В разделе Настройки → Политики безопасности → Фильтрация контента создайте правила фильтрации HTTP(S). Подробнее о фильтрации контента — в разделе «Фильтрация контента»
Создать правила веб-безопасности	В разделе Настройки → Политики безопасности → Веб-безопасность создайте дополнительные правила веб-защиты. Подробнее о правилах веб-безопасности — в разделе «Веб-безопасность»
Создать правила инспектирования SSL	В разделе Настройки → Политики безопасности → Инспектирование SSL создайте правила для перехвата и расшифровывания HTTPS-трафика. Подробнее о дешифровании HTTPS — в разделе «Инспектирование SSL»

ЛИЦЕНЗИРОВАНИЕ

Лицензирование UserGate NGFW

Для использования UserGate NGFW необходима [базовая лицензия](#), в рамках которой предоставляется бессрочный доступ к основным функциям продукта. Чтобы получать обновления UserGate NGFW и использовать его расширенные функции, вам необходимо приобрести [дополнительные лицензии](#).

В веб-интерфейсе продукта администраторы могут активировать и обновить лицензию, а также проверить срок ее действия [в онлайн-режиме](#). Для этого

необходим доступ к серверу лицензирования reg2.usergate.com. Если доступ к серверу отсутствует, вы можете [активировать лицензию офлайн](#).

Базовая лицензия

Этот тип лицензии определяется параметрами производительности UserGate NGFW. В процессе активации базовой лицензии проверяется следующее:

- **Тип аппаратной платформы.** Для продукта, поставляемого в виде программно-аппаратного комплекса, тип аппаратной платформы должен совпадать с тем, который указан в лицензии.
- **Количество ядер виртуальной машины.** Для продукта, поставляемого в виде виртуального образа, количество поддерживаемых ядер процессора должно совпадать с количеством ядер, разрешенных лицензией.

В случае несоответствия параметров продукта, указанным в лицензии, процесс активации будет завершен с ошибкой. Кроме того, если после активации лицензии в виртуальную машину будет добавлено больше ядер, чем предусмотрено базовой лицензией, продукт будет использовать только разрешенное количество ядер.

Дополнительные лицензии

Дополнительно лицензируются следующие модули UserGate NGFW.

Модуль	Предоставляемые функции	По истечении лицензии
Security Updates (SU)	Обновление ПО UserGate, а также сигнатур системы обнаружения вторжений и приложений L7. Срок действия лицензии на модуль — 1 год	Прекращается обновление ПО и сигнатур. Продолжает действовать последняя установленная версия продукта
Advanced Threat Protection (ATP)	Годовая подписка: • на базу категорий сайтов для URL-фильтрации; • обновляемые URL-списки, например такие, как список фишинговых сайтов, белый и черный список UserGate, а также списки запрещенных сайтов Роскомнадзора; • морфологические словари;	Отключается сервис веб-безопасности. Прекращается фильтрация по категориям и морфологии. Остаются загруженные URL-списки

Модуль	Предоставляемые функции	По истечении лицензии
	сервис веб-безопасности, используемый для блокировки рекламы и приложений социальных сетей, а также для безопасного поиска	
Mail security	Годовая подписка на антиспам-модуль UserGate для проверки почтового трафика	Прекращается фильтрация почты
Потоковый антивирус UserGate	Годовая подписка на потоковый антивирус UserGate	Отключается антивирус
Cluster	Поддержка кластеризации. Срок действия лицензии на модуль не ограничен	—
UserGate Client	Взаимодействие с конечными устройствами, на которых установлен UserGate Client (компонент экосистемы UserGate SUMMA), только по каналу VPN. Контроль доступа к сети конечных устройств с помощью правил межсетевого экрана, использующих HIP-профили. Отправка данных о событиях конечных устройств в SIEM-системы. Лицензия на модуль (сроком от 1 года до 5 лет) выписывается по количеству лицензируемых конечных управляемых устройств наборами по 10, 100 и 1000 шт.	Перестают срабатывать правила межсетевого экрана, использующие HIP-профили в качестве условий фильтрации

Онлайн-лицензирование

При активации, проверке и обновлении лицензии UserGate NGFW подключается к серверу лицензирования и передает номер версии ПО UserGate, лицензионный ключ, название продукта и модель устройства. В ответ продукт получает данные о сроке действия лицензии и поддерживаемых модулях.

Активация лицензии

Чтобы активировать лицензию:

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии**.
2. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.

Если UserGate NGFW установлен в изолированной сети (без доступа в интернет), вы можете активировать лицензию с использованием прокси-сервера. Для этого выберите **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.

3. Следуйте указаниям мастера активации продукта.

Проверка срока действия лицензии

Автоматическая проверка срока действия лицензии выполняется раз в сутки, ее результаты отображаются в журнале событий UserGate NGFW. По окончании проверки отключаются те модули, срок поддержки которых истек, и подключаются вновь доступные.

Если в ходе проверки не удастся получить доступ к серверу лицензирования, выполняется 14 попыток подключения к серверу с интервалом в 2 минуты. При неуспешных попытках проверка приостанавливается на сутки, после чего попытки повторяются. Если за это время истечет срок действия лицензии на один из модулей, модуль будет отключен.

Вы также можете запускать проверку срока действия лицензии вручную. Действие доступно в разделе **Дашборды** в виджете **Лицензия** по ссылке **Проверить лицензию**.

Обновление лицензии

Важно!

Лицензионные ключи версий продукта 6 и 7 несовместимы. При переходе с более низких версий на версию 7 необходимо запросить новый ключ у вашего менеджера UserGate и обновить лицензию.

Важно!

При обновлении лицензии в UserGate NGFW будут принудительно сброшены все установленные сессии, а также будут перезапущены правила межсетевого экрана.

Чтобы обновить лицензию:

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Зарегистрированная версия**.
2. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.

Если UserGate NGFW установлен в изолированной сети (без доступа в интернет), вы можете обновить лицензию с использованием прокси-сервера. Для этого выберите **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.

3. Следуйте указаниям мастера активации продукта.

Офлайн-активация лицензии

Вы можете активировать лицензию продукта в офлайн-режиме. Это нужно в том случае, если UserGate NGFW установлен в изолированной сети (без доступа в интернет) и нет возможности использовать прокси-сервер для активации.

Чтобы выполнить офлайн-активацию лицензии:

1. Войдите в веб-интерфейс UserGate NGFW по ссылке <https://<IP-адрес веб-интерфейса>:8001?features=offline-reg>.
2. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии**.
3. Нажмите **Начать активацию в автономном режиме**.
4. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.

Будет сгенерирован файл с запросом на активацию лицензии (далее также — файл запроса).

5. Сохраните файл запроса на съемный носитель.
6. Закройте окно по кнопке **Отмена**.
7. Получите файл активации через сервис офлайн-активации лицензий poa.usergate.com, выполнив указанные ниже действия.

Примечание

Для выполнения действий требуется подключение к интернету и учетная запись для авторизации в сервисе офлайн-активации. Получить учетную запись можно зарегистрировавшись в Едином центре авторизации id.usergate.com.

- Загрузите файл запроса по кнопке **Выбрать**.

Требования к загружаемым файлам

- Закачиваемые файлы должны иметь расширение - ".dat"
- Максимальный размер закачиваемых файлов - 20 Kb
- Максимальное кол-во обрабатываемых файлов - 10

[Документация](#) | [Тех.поддержка](#)

Обратите внимание

- Для продуктов версии 6 активировать можно только первоначальные пин-коды, начинающиеся с префикса **UGN** (не пин-коды продления)

Файлы для обработки

Выбрать файлы ...

Выбрать ...

Версия по-умолчанию ☐ v6

☐ v7

#	Файл	Размер	Версия	Статус	Действия
---	------	--------	--------	--------	----------

- Выберите версию ПО UserGate NGFW и нажмите **Обработать**.

Требования к загружаемым файлам

- Закачиваемые файлы должны иметь расширение - ".dat"
- Максимальный размер закачиваемых файлов - 20 Kb
- Максимальное кол-во обрабатываемых файлов - 10

[Документация](#) | [Тех.поддержка](#)

Обратите внимание

- Для продуктов версии 6 активировать можно только первоначальные пин-коды, начинающиеся с префикса **UGN** (не пин-коды продления)

Файлы для обработки

Выбрать файлы ...

Выбрать ...

Версия по-умолчанию ☐ v6

☐ v7

#	Файл	Размер	Версия	Статус	Действия
1	activation-request.dat	1.1 Kb	☐ v6 ☒ v7	ожидание обработки	

Очистить список

Обработать

- Скачайте активированный файл запроса (далее также — файл активации).

Требования к загружаемым файлам

- Закачиваемые файлы должны иметь расширение - ".dat"
- Максимальный размер закачиваемых файлов - 20 Kb
- Максимальное кол-во обрабатываемых файлов - 10

[Документация](#) | [Тех.поддержка](#)

Обратите внимание

- Для продуктов версии 6 активировать можно только первоначальные пин-коды, начинающиеся с префикса **UGN** (не пин-коды продления)

Файлы для обработки

Выбрать файлы ...

Выбрать ...

Версия по-умолчанию ☐ v6

☐ v7

#	Файл	Размер	Версия	Статус	Действия
1	activation-request.dat	1.1 Kb	☐ v6 ☒ v7	успешно активирован	

Очистить список

Обработать

8. Повторите шаг 2 инструкции.

9. Нажмите **Завершить активацию в автономном режиме**.

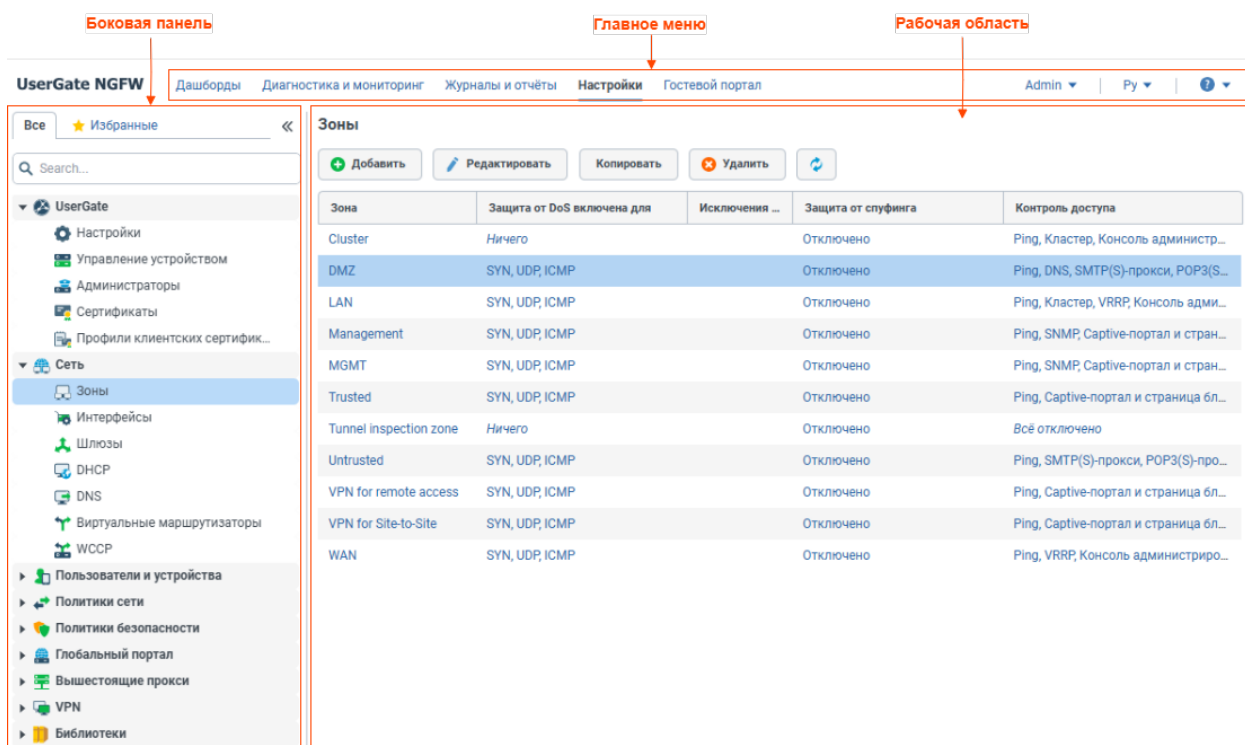
10. Загрузите файл активации и нажмите **Далее**.

11. Следуйте указаниям мастера активации продукта.

ИНТЕРФЕЙС

Интерфейс UserGate NGFW

Все действия вы можете выполнять в веб-интерфейсе, доступном после входа в UserGate NGFW.



Главное меню

В верхней части любой страницы расположено главное меню, которое содержит разделы для перехода к страницам веб-интерфейса:

- **Дашборды** — страница со статистическими данными о состоянии устройства и результатах его работы, представленными в виде таблиц, списков и графиков. При входе в UserGate NGFW эта страница открывается по умолчанию. Подробнее о дашбордах — в разделе [«Работа с дашбордами и виджетами»](#).
- **Диагностика и мониторинг** — страница для отслеживания сетевого трафика, просмотра сетевой конфигурации, выполнения захвата пакетов, запуска базовых сетевых утилит, а также для управления оповещениями.
- **Журналы и отчеты** — страница для просмотра журналов и настройки генерации отчетов.
- **Настройки** — страница для настройки устройства и политик безопасности.
- **Гостевой портал** — страница для создания списков гостевых пользователей. Эта возможность полезна, когда необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время, например когда пользователи запрашивают доступ используя публичные сети Wi-Fi.

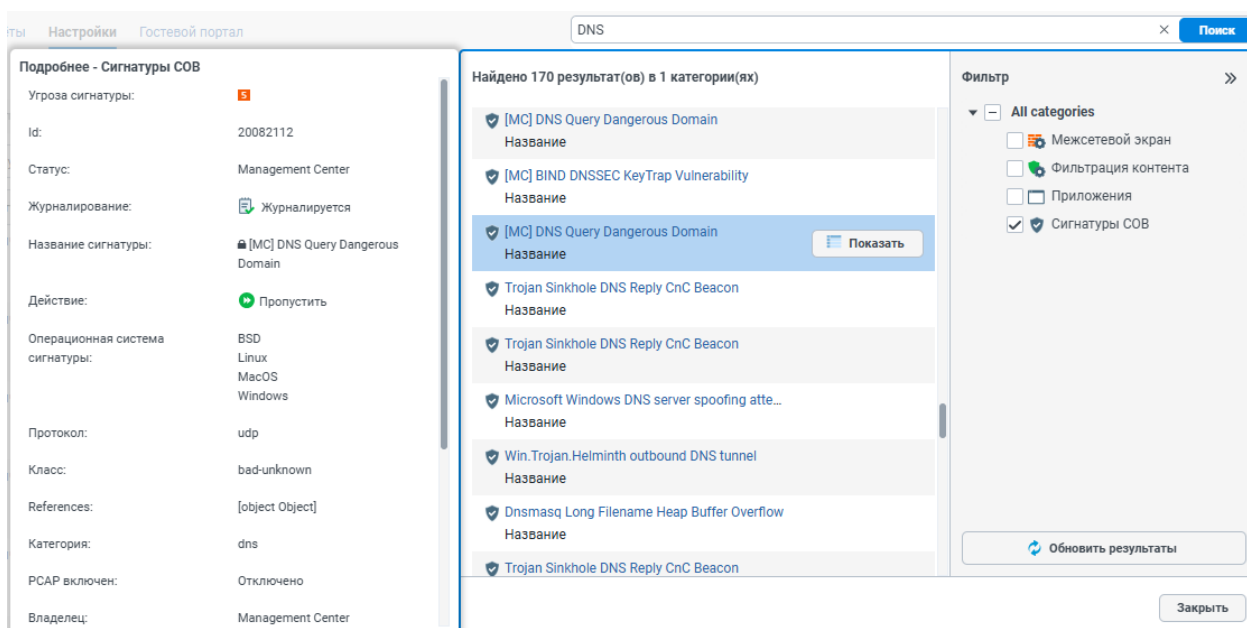
Поиск

В верхней панели любой страницы справа от главного меню расположено поле поиска (начиная с версии 7.5.0 и выше). Поиск выполняется в разделах **Приложения**, **Сигнатуры COB**, **Фильтрация контента** и **Межсетевой экран**.

Вы можете искать:

- Приложения по их названию и описанию.
- Сигнатуры COB по их названию и описанию.
- Правила межсетевого экрана по их названию, описанию, профилю приложения или сигнатуры COB, сценарию, а также по зоне, имени, адресу источника или назначения. При поиске по адресу источника или назначения также доступен поиск по IP-адресу в подсетях. Например, если в правиле в качестве адреса назначения указана подсеть 192.168.1.0/24, правило будет найдено по IP-адресу 192.168.1.5.

Результаты поиска отображаются под полем в раскрывающемся окне.



В окне найденных элементов вы можете:

- Фильтровать результаты, выбирая нужные разделы на панели **Фильтр**. При изменении фильтра нужно обновить результаты поиска, нажав на соответствующую кнопку.
- Просматривать подробную информацию по найденному элементу, наведя на него курсор.

- Перейти на страницу раздела с найденным элементом, нажав **Показать в** строке выбранного элемента.
- Изменить параметры найденного элемента. Если изменение параметров доступно, по нажатию на название элемента откроется окно с его параметрами.

Прочие элементы управления

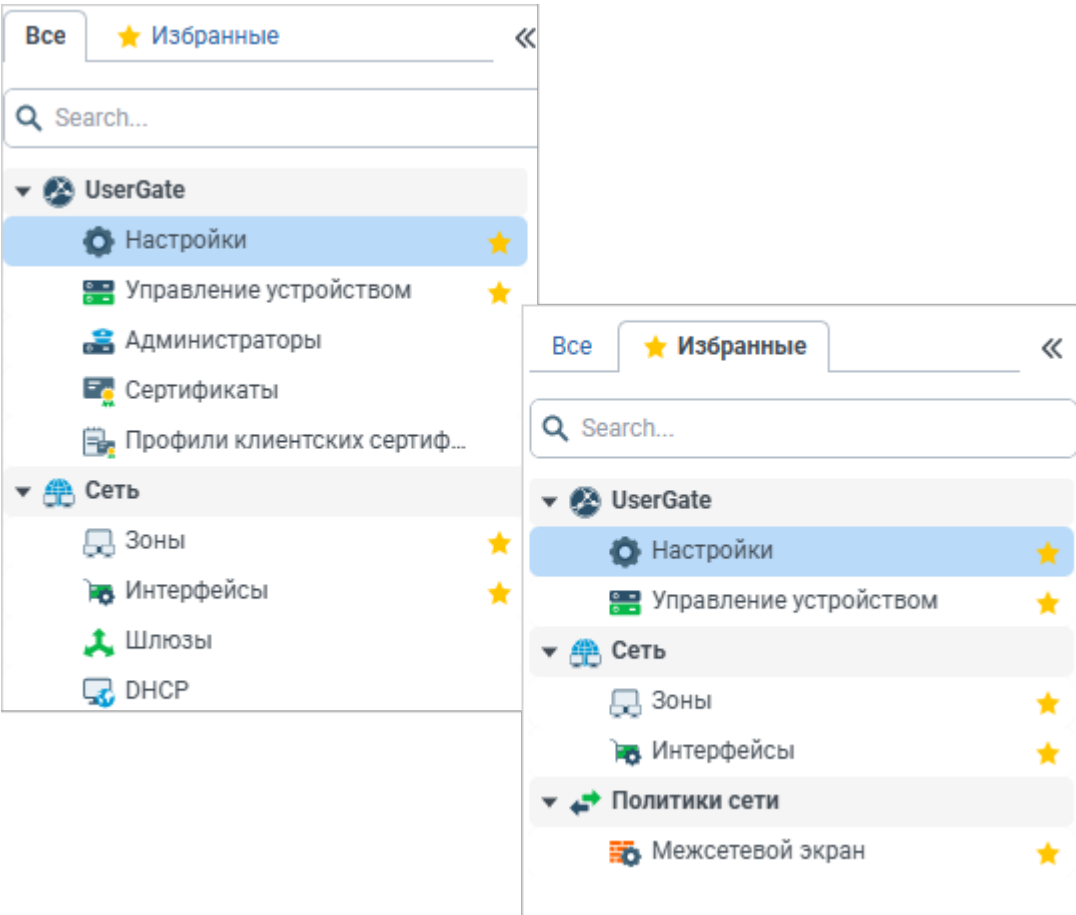
Также в верхней панели находятся следующие элементы управления:

- Логин вашей учетной записи — раскрывает меню для смены пароля учетной записи, выбора темы оформления интерфейса, настройки числа отображаемых записей на страницах с табличными данными, изменения пользовательских фильтров журналов. Также вы можете завершить работу с текущей учетной записью, нажав в этом меню **Выход**.
- Язык — выбор языка интерфейса.
- Значок вопроса — раскрывает меню, в котором можно выбрать просмотр документации или обучающего видео, а также перейти на портал технической поддержки <https://www.usergate.com/ru/support>, где вы можете получить дополнительную информацию по настройке UserGate или оставить заявку на решение возникшей проблемы.

Страницы интерфейса

Все страницы, кроме страницы **Дашборды**, состоят из рабочей области и боковой панели. Содержимое и вид рабочей области зависят от выбранной страницы, информация может отображаться в виде таблицы, виджетов или блоков параметров. Боковая панель содержит список разделов, предоставляющих доступ к различным возможностям UserGate NGFW, например к настройке конфигурации, созданию политики безопасности, просмотру журналов и диагностической информации.

Вкладка **Избранные** на боковой панели предназначена для формирования списка разделов, с которыми вы работаете чаще всего. Чтобы раздел отобразился в избранном, на вкладке **Все** его нужно отметить звездочкой.



НАСТРОЙКА УСТРОЙСТВА

Настройка общих параметров

В этом разделе описаны общие параметры UserGate NGFW, которые отображаются на странице веб-консоли **Настройки** в разделе **Консоль администратора → Настройки**, а также приведены рекомендации по настройке этих параметров.

Блок параметров	Параметр	Описание
Настройки интерфейса	Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения

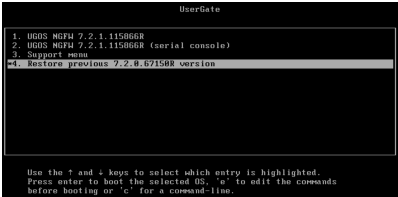
Блок параметров	Параметр	Описание
		времени и даты, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-консоли устройства по умолчанию
	Режим аутентификации веб-консоли	Доступны следующие режимы аутентификации: • По имени и паролю. Вход администратора в веб-консоль по логину и паролю учетной записи. • По X.509-сертификату. Вход администратора в веб-консоль по цифровому сертификату. Этот сертификат должен быть подписан сертификатом удостоверяющего центра, обеспечивающим доступ к веб-консоли, и установлен в браузере. При включении режима отключается аутентификация по логину и паролю, к ней можно вернуться с помощью команд CLI. • Профиль клиентского сертификата. Вход администратора в веб-консоль по сертификату инфраструктуры открытых ключей (PKI). Проверка подлинности этого сертификата выполняется с помощью профиля клиентского сертификата, обеспечивая тем

Блок параметров	Параметр	Описание
		самым безопасностью сетевого соединения
	Профиль SSL для веб-консоли	Профиль SSL , с использованием которого создается защищенный канал для доступа к веб-консоли
	Профиль SSL для страниц блокировки/аутентификации	Профиль SSL , с использованием которого создается защищенный канал для отображения страниц авторизации captive-портала, а также страниц блокировки доступа к веб-ресурсам
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-консоль должна завершаться его сессия. Также необходимо включить параметр Автоматическое закрытие сессии по таймеру
	Автоматическое закрытие сессии по таймеру	При включенном параметре сессия администратора будет завершаться по истечении таймера автоматического закрытия сессии. По умолчанию параметр отключен
	Профиль SSL конечного устройства	Профиль SSL , с использованием которого создается защищенный канал взаимодействия UserGate NGFW и конечных устройств UserGate Client
	Сертификат конечного устройства	Сертификат, с использованием которого создается защищенный канал взаимодействия UserGate

Блок параметров	Параметр	Описание
		NGFW и конечных устройств UserGate Client. i Важно! При изменении сертификата требуется установить корневой сертификат удостоверяющего центра (Root CA) на подключенных конечных устройствах. В качестве хранилища на локальном компьютере необходимо выбрать «Доверенные корневые центры сертификации»
Настройка времени сервера	Использовать NTP	При включенном параметре для синхронизации времени на устройстве будут использоваться серверы NTP из указанного списка
	Основной NTP-сервер	Адрес основного сервера точного времени. Значение по умолчанию — <code>pool.ntp.org</code>
	Запасной NTP-сервер	Адрес запасного сервера точного времени
	Время на сервере (UTC)	Время на сервере UserGate NGFW в часовом поясе UTC
Настройка кэширования HTTP	Режим кэширования	Включение или отключение кэширования

Блок параметров	Параметр	Описание
	Исключения кэширования	Список URL, которые не будут кэшироваться
	Максимальный размер объекта (МБ)	Объекты с размером, превышающим указанный в этом параметре, не будут кэшироваться. Рекомендуется оставить значение по умолчанию — 1 МБ
	Размер RAM-кэша (МБ)	Размер оперативной памяти, отведенный под кэширование. Не рекомендуется использовать значение, превышающее 20% от объема оперативной памяти системы
Настройка PCAP	Захват пакетов	Настройка записи трафика при срабатывании сигнатур системы обнаружения вторжений. Для выбора доступны следующие режимы захвата пакетов: • Без захвата; • Один пакет; • Предшествующие пакеты (от 4 до 30 пакетов); • Предшествующие и последующие пакеты (предшествующие — от 4 до 30 пакетов, последующие — от 2 до 15 пакетов).

Блок параметров	Параметр	Описание
		 Важно! Запись PCAP-файлов большого размера может привести к значительному замедлению обработки данных
Учет изменений	Настройка учета изменений	Для настройки учета изменений в веб-консоли устройства необходимо включить параметр и добавить типы изменений (например, распоряжение, приказ или регламентные работы). Учет изменений предполагает, что при внесении какого-либо изменения через веб-консоль администратору необходимо указать тип и причину этого изменения
Обновления ПО (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Канал обновлений	Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate. Вы можете выбрать Стабильные (стабильные версии ПО) или Бета (версии ПО для бета-тестирования). Если настроена интеграция с UserGate Management Center, параметр примет значение Management Center и будет недоступен для изменения
	Обновления	

Блок параметров	Параметр	Описание
		Проверка наличия обновлений UGOS в репозитории UserGate. После проверки вы можете вручную загрузить и установить доступные обновления. В процессе установки обновления UGOS вы можете создать точку восстановления. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню после установки обновления UGOS 
	Офлайн-обновление	Загрузка файла обновления UGOS офлайн
Обновления библиотек (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Обновления	Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate. После проверки вы можете вручную обновить необходимые библиотеки
	Расписание автоматических обновлений	Настройка расписания автоматического обновления библиотек. При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–

Блок параметров	Параметр	Описание
		31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Для ручного ввода вы можете использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями. При установке флажка Един ое расписание для всех обновлений расписание выбранной библиотеки будет применено ко всем библиотекам в списке. Начиная с версии 7.1.2 после активации лицензии следующие библиотеки будут обновляться автоматически: • «Сигнатуры приложений L7»; • «UserGate-антивирус»; • «IP-список бот-сетей»; • «Сигнатуры COB»; • «URL-список фишинговых сайтов»; • «UserGate URL filtering (URLF)» — компактная и полная библиотеки;

Блок параметров	Параметр	Описание
		• «Блокировка рекламы»; • «Доверенные УЦ». Вы можете изменить список автоматически обновляемых библиотек при настройке расписания.  Примечание В целях уменьшения нагрузки на систему рекомендует ся настраивать расписание автоматического обно вления только для используемых библио тек
Модули	HTTP(S)-прокси-порт	Дополнительный порт для подключения к встроенному прокси-серверу. По умолчанию используется порт TCP 8090 (после настройки параметра этот порт продолжит функционировать). Для выбора недоступны порты 2200, 8001, 4369, 9000–9100, которые используются внутренними сервисами UserGate NGFW
	Домен Auth captive-портала	Служебный домен, который используется UserGate NGFW для авторизации пользователей через captive-портал. Необходимо, чтобы пользователи могли преобразовывать этот

Блок параметров	Параметр	Описание
		домен в IP-адрес интерфейса UserGate NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера устройства, преобразование адресов настроено автоматически. По умолчанию используется домен auth.captive, вы можете изменить его на доменное имя, принятое в вашей организации
	Домен Logout captive-портала	Служебный домен, который используется UserGate NGFW для окончания сессии пользователей, авторизованных через captive-портал. Необходимо, чтобы пользователи могли преобразовывать этот домен в IP-адрес интерфейса UserGate NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера устройства, преобразование адресов настроено автоматически. По умолчанию используется домен logout.captive, вы можете изменить его на доменное имя, принятое в вашей организации
	Домен Cert captive-портала	Служебный домен, который используется UserGate NGFW для авторизации пользователей через captive-портал с помощью сертификатов. Необходимо, чтобы пользователи могли преобразовывать этот домен в IP-адрес

Блок параметров	Параметр	Описание
		интерфейса UserGate NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера устройства, преобразование адресов настроено автоматически. По умолчанию используется домен cert.captive, вы можете изменить его на доменное имя, принятое в вашей организации
	Домен страницы блокировки	Служебный домен, который используется для отображения страницы блокировки. Необходимо, чтобы пользователи могли преобразовывать этот домен в IP-адрес интерфейса UserGate NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера устройства, преобразование адресов настроено автоматически. По умолчанию используется домен block.captive, вы можете изменить его на доменное имя, принятое в вашей организации
	FTP поверх HTTP	Включение или отключение модуля, который позволяет получить доступ к содержимому FTP-серверов из браузера пользователя. Для использования FTP-протокола в браузере пользователя должен быть явно указан прокси-сервер. Вы можете ограничивать доступ к FTP-ресурсам с помощью правил фильтрации

Блок параметров	Параметр	Описание
		контента (по условиям срабатывания Пользователи и URL)
	FTP поверх HTTP домен	Служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. Необходимо, чтобы пользователи могли преобразовывать этот домен в IP-адрес интерфейса UserGate NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера устройства, преобразование адресов настроено автоматически. По умолчанию используется домен <code>ftpclient.captive</code>, вы можете изменить его на доменное имя, принятое в вашей организации
	Зона для инспектируемых туннелей	Включение или отключение модуля инспектирования туннелей, а также выбор зоны инспектирования
	Пароль агентов терминального сервиса	Настройка пароля для подключения агентов авторизации терминальных серверов
	Настройка LLDP	Настройка использования LLDP-протокола канального уровня, с помощью которого UserGate NGFW обменивается данными с соседними устройствами в локальной сети. Для настройки

Блок параметров	Параметр	Описание
		доступны следующие параметры: • Transmit delay — интервал отправки LLDP-пакетов (от 1 до 3600 секунд). Изменяя этот параметр, вы можете управлять частотой, с которой UserGate NGFW будет отправлять данные соседним устройствам. • Transmit hold — множитель для вычисления времени жизни LLDP-пакетов (параметр TTL). Укажите значение (от 1 до 100), на которое следует умножить значение Transmit delay, чтобы определить время хранения данных, полученных от соседних устройств. По истечении этого времени данные удаляются из кэша UserGate NGFW. Для использования LLDP-протокола необходимо предварительно создать LLDP-профиль и назначить его сетевому интерфейсу устройства. Список соседних LLDP-устройств отображается в разделе веб-консоли Диагностика и мониторинг → Сеть → LLDP-соседи (см. раздел «LLDP-соседи»)
Log Analyzer (начиная с версии 7.3.0 — Состояние базы данных журналов)	Сервер	Сервер базы данных журналов (локальный сервер или внешний сервер UserGate Log Analyzer).

Блок параметров	Параметр	Описание
		 Примечание При интеграции с внешним сервером UserGate Log Analyzer обработка и экспорт журналов, а также создание отчетов и обработка других статистических данных выполняются этим сервером
	Версия сервера	Версия ПО сервера базы данных журналов
	Версия устройства	Версия ПО UserGate NGFW
	Код устройства	Уникальный код UserGate NGFW для интеграции с внешним сервером UserGate Log Analyzer
Веб-портал	Адрес веб-портала	Для доступа удаленных пользователей к внутренним ресурсам компании через веб-портал (SSL VPN) необходимо включить параметр и настроить его свойства
Агент UserGate Management Center	Настройка агента	Настройка интеграции с UserGate Management Center (UGMC). Для настройки доступны следующие параметры: • Включено — управление состоянием подключения UserGate NGFW к UGMC;

Блок параметров	Параметр	Описание
		• Адрес UserGate Management Center — адрес сервера UGMC в формате IPv4-адреса или FQDN (возможно использование IDN-адреса); • Код устройства — идентификатор UserGate NGFW для подключения к UGMC.  Примечание Для подключения UserGate NGFW к UGMC необходимо, чтобы порт межсетевого экрана находился в виртуальном маршрутизаторе по умолчанию. В качестве портов подключения к серверу UGMC используются порты TCP 2022 и TCP 9712

Блок параметров	Параметр	Описание
Вышестоящий прокси (блок параметров доступен в версиях 7.1.x, 7.2.x, 7.3.x)	Настройки вышестоящего прокси (параметр доступен в версиях 7.1.x, 7.2.x, 7.3.x)	Для перенаправления пользовательского трафика на вышестоящий прокси-сервер необходимо включить параметр и настроить его свойства: тип (HTTP, HTTPS или SOCKS5), IP-адрес и порт, а также логин и пароль, если на вышестоящем прокси-сервере необходима аутентификация

Управление устройством

В разделе **Настройки → UserGate → Управление устройством** вы можете настраивать следующие параметры устройства:

- кластеры отказоустойчивости;
- кластер конфигурации;
- диагностика;
- операции с сервером;
- резервное копирование;
- экспорт и импорт настроек.

Информация о настройке кластеров приведена в разделе «[Кластеризация и отказоустойчивость](#)».

Диагностика

Этот блок предназначен для настройки параметров диагностики и предоставления удаленного доступа службе технической поддержки UserGate с целью анализа и устранения неисправностей.

Параметры диагностики

С помощью параметра **Детализация диагностики** вы можете установить уровень журналирования устройства. Доступны следующие уровни:

- **Off** — ведение журналов диагностики отключено.
- **Error** — журналировать только ошибки в работе устройства.
- **Warning** — журналировать только ошибки и предупреждения.
- **Info** — журналировать только ошибки, предупреждения и дополнительную информацию.
- **Debug** — журналировать все возможные события.

При журналировании с уровнями **Warning**, **Info** и **Debug** может снижаться производительность устройства, поэтому рекомендуется устанавливать уровни **Error** или **Off**, если технической поддержкой UserGate не было предложено иное.

Управление журналами

Вы можете скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно после их архивирования командой **Начать архивирование журналов**.

Чтобы удалить архивные (не активные в настоящий момент) журналы, нажмите **Очистить файлы логов**.

Удаленный помощник

Чтобы предоставить доступ к устройству для службы технической поддержки UserGate с целью диагностирования и устранения неисправностей, необходимо активировать функцию удаленного помощника и получить параметры сеансового доступа.

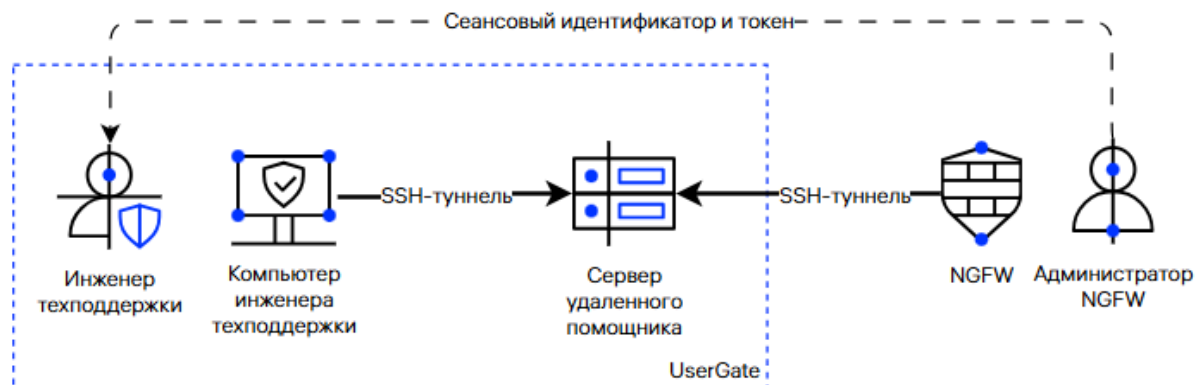
Процесс подключения к устройству происходит следующим образом:

1. Администратор устройства UserGate активирует функцию удаленного помощника.
2. Устройство устанавливает защищенное соединение с сервером удаленного помощника UserGate по протоколу SSH. При успешном подключении в

интерфейсе устройства UserGate отобразятся параметры сеансового доступа: идентификатор и токен.

3. Администратор устройства UserGate передает параметры сеансового доступа специалисту технической поддержки UserGate.

4. Специалист технической поддержки устанавливает защищенное соединение по протоколу SSH с сервером удаленного помощника UserGate и с помощью параметров сеансового доступа подключается к устройству UserGate.



Операции с сервером

В этом блоке вы можете перезагрузить или выключить сервер UserGate NGFW, а также настроить вышестоящий прокси-сервер для проверки лицензий и обновлений продукта.

UserGate предоставляет обновления в рамках лицензии на модуль Security Update (см. раздел «[Лицензирование](#)»). При наличии обновлений в блоке **Операции с сервером** отобразится соответствующее оповещение. Установка обновлений может занять длительное время, поэтому рекомендуется планировать этот процесс с учетом возможного времени простоя UserGate NGFW.

Перед установкой обновлений рекомендуется создать резервную копию UserGate NGFW. Это позволит восстановить предыдущее состояние продукта, если возникнут проблемы, связанные с применением обновлений.

Управление резервным копированием

В этом блоке вы можете:

- [создавать резервные копии](#);
- [восстанавливать продукт из резервной копии](#);

- [настраивать расписание экспорта резервных копий на удаленный сервер;](#)
- [настраивать SSH-ключи.](#)

Чтобы создать резервную копию продукта:

В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Еще → Создание резервной копии**.

Начнется создание резервной копии. Вы можете прервать процесс по кнопке **Остановить**.

По окончании процесса резервная копия UserGate NGFW будет сохранена в файле `backup_PRODUCT_NODENAME_DATE.gpg`, где:

- **PRODUCT** — тип продукта: NGFW, LogAn, MC;
- **NODENAME** — имя узла продукта;
- **DATE** — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM (в часовом поясе UTC+0).

Запись о создании резервной копии отобразится в журнале событий продукта.

Чтобы восстановить продукт из резервной копии:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Еще → Восстановление резервной копии** и подтвердите восстановление.

2. Укажите путь к файлу с резервной копией UserGate NGFW.

Восстановление будет предложено в консоли TTY при перезагрузке сервера UserGate NGFW.

Администраторы могут создавать правила экспорта, по которым резервные копии будут выгружаться на удаленные серверы по расписанию.

Чтобы создать правило экспорта резервной копии продукта:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Добавить**.

2. На вкладке **Общие** укажите имя правила.

3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:

- тип — FTP или SSH;
- адрес;
- порт для подключения;
- учетные данные для авторизации — логин и пароль (при выборе FTP-сервера) или логин (при выборе SSH-сервера);
- путь к существующей папке для сохранения файлов экспорта.



Внимание!

Если вы создаете правило для SSH-сервера, необходимо [предварительно настроить SSH-ключи](#). Кроме того, необходимо проверить соединение с SSH-сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта резервной копии.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Перед подключением к удаленному SSH-серверу, необходимо настроить SSH-ключи, используемые для авторизации на этом сервере.

Чтобы настроить SSH-ключи:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Еще → Настроить SSH-ключ**.

2. Нажмите **Сгенерировать новый ключ**.

Будет сгенерирована пара SSH-ключей (закрытый и открытый). Открытый ключ отобразится в окне настройки, закрытый ключ будет автоматически сохранен на сервере UserGate NGFW.

Примечание

Если у вас уже есть пара SSH-ключей, вы можете добавить закрытый ключ на сервер UserGate NGFW вручную по кнопке «Загрузить ключ».

3. Добавьте открытый SSH-ключ на удаленный сервер.

По умолчанию SSH-ключи хранятся в папке `/home/user/.ssh/` в файле `authorized_keys`.

Экспорт и импорт настроек

В этом блоке вы можете экспортировать текущие параметры UserGate NGFW в виде файлов экспорта в формате BIN. Впоследствии такие файлы могут понадобиться [для восстановления параметров продукта](#), а также для импорта в другие NGFW.

Экспорт может выполняться вручную или [по расписанию](#). Вы можете экспортировать [все текущие параметры](#) (за исключением данных о кластерах и лицензии) или [только сетевые](#). К сетевым относятся параметры зон, интерфейсов, шлюзов, виртуальных маршрутизаторов, а также параметры сервисов DNS, DHCP и WCCP. Сетевые параметры настраиваются в разделе **Настройки → Сеть** (см. раздел «[Настройка сети](#)»).

Чтобы экспортировать все параметры продукта:

В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Экспорт → Экспортировать все настройки**.

Параметры будут сохранены в файле `utm-utmcore@NODENAME_VERSION_DATE.bin`, где:

- NODENAME — имя узла продукта;

- **VERSION** — версия UGOS;
- **DATE** — дата и время выгрузки параметров в формате — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Чтобы экспортировать только сетевые параметры продукта:

В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Экспорт → Экспортировать сетевые настройки**.

Параметры будут сохранены в файле `utm-net-utmcore@NODENAME_VERSION_DATE.bin`, где:

- **NODENAME** — имя узла продукта;
- **VERSION** — версия UGOS;
- **DATE** — дата и время выгрузки параметров в формате — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Администраторы могут создавать правила экспорта, по которым параметры продукта будут выгружаться на удаленные серверы по расписанию. Если узлы продукта объединены в кластер, то при создании правила экспорта на одном из узлов это правило будет распространяться на все узлы кластера. Параметры каждого узла при экспорте будут сохраняться в отдельном файле.

Чтобы создать правило экспорта параметров продукта:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Добавить**.
2. На вкладке **Общие** укажите имя правила.
3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:
 - тип — FTP или SSH;
 - адрес;
 - порт для подключения;
 - учетные данные для авторизации;
 - путь к существующей папке для сохранения файлов экспорта.

i Примечание

Для авторизации на удаленном SSH-сервере вы можете использовать SSH-ключи. Для этого их нужно [предварительно настроить](#).

i Внимание!

Если вы создаете правило для SSH-сервера с авторизацией по SSH-ключам, необходимо проверить соединение с SSH-сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта параметров.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Вы можете восстанавливать параметры продукта из файлов экспорта. Эти файлы не содержат данные о кластерах и лицензии, поэтому после восстановления параметров вам потребуется повторно активировать лицензию и настроить кластеры. Кроме того, если для входа в UserGate NGFW вы используете многофакторную аутентификацию через TOTP, после восстановления необходимо повторно добавить ключи инициализации.

i Примечание

Для импорта правил фильтрации, в которых указаны пользователи или группы пользователей, необходим доступ к LDAP-серверу. В противном случае эти правила будут восстановлены без данных о пользователях. Для корректного восстановления правил, использующих обновляемые списки, необходима лицензия на модули Security Update и Advanced Threat Protection.

i Внимание!

При восстановлении параметров UserGate NGFW из файла экспорта, созданного в более поздней версии продукта, работоспособность сервера UserGate NGFW не гарантируется.

Чтобы восстановить параметры продукта из файла экспорта:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Импорт**.
2. Выберите файл экспорта.
3. В окне **Импортировать настройки** выберите тип импорта (все параметры или только сетевые).
4. Нажмите **Старт**.

Начнется восстановление параметров. По окончании процесса сервер UserGate NGFW будет перезагружен.

После перезагрузки сервера вам необходимо обновить библиотеки сигнатур в разделе **Настройки → UserGate → Настройки → Обновление библиотек**. Если доступ к ресурсу с библиотеками отсутствует, вы можете загрузить файл обновления вручную в разделе **Настройки → UserGate → Обновление ПО**.

i Примечание

При выполнении операции импорта всех настроек происходит сброс конфигурации устройства к первоначальному состоянию (factory reset) с удалением всех журналов.

Управление доступом к интерфейсам администрирования

При первоначальной настройке UserGate NGFW по умолчанию создается локальная учетная запись суперадминистратора (Admin). Используя эту учетную запись, вы можете управлять доступом других администраторов к интерфейсам устройства: веб-интерфейсу, интерфейсу командной строки, а также программному интерфейсу API.

Суперадминистратор может [создавать учетные записи дополнительных администраторов](#) и назначать им [профили доступа](#). Каждому профилю доступа соответствует набор разрешений на использование тех или иных функций продукта. Например, с помощью профиля доступа можно разрешить или запретить администратору подключаться к UserGate NGFW через интерфейс командной строки.

Вы также можете управлять доступом [с помощью настройки зон](#). Для этого в разделе **Настройки → Сеть → Зоны** в свойствах зоны на вкладке **Контроль доступа** вы можете разрешить или запретить необходимое подключение.

В разделе **Настройки → UserGate → Администраторы** вы можете создавать учетные записи:

- **Локальных администраторов.** Учетные данные для аутентификации хранятся на сервере UserGate NGFW.
- **Пользователей или групп пользователей LDAP.** Аутентификация выполняется с помощью доменных учетных записей пользователей или групп пользователей. Предварительно в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** необходимо настроить LDAP-коннектор. Логин учетной записи при аутентификации указывается в формате <логин администратора>@domain.
- **Администраторов с профилем аутентификации.** Для аутентификации используются профили аутентификации, настроенные в разделе **Настройки → Пользователи и устройства → Профили аутентификации**.

Инструкции по настройке серверов аутентификации приведены в разделе «[Серверы аутентификации](#)», по настройке профилей аутентификации — в разделе «[Профили аутентификации](#)».

Вы можете удалять созданные учетные записи и изменять их параметры, а также управлять состоянием учетных записей (включать и отключать их). Кроме того,

вы можете разблокировать локальную учетную запись, которая была заблокирована (например в случае, если было превышено количество неудачных попыток аутентификации).

Для дополнительной защиты локальных учетных записей можно [настроить парольную политику](#). Для доменных учетных записей, а также для учетных записей с профилями аутентификации параметры защиты определяются внешним источником учетных записей.

По умолчанию аутентификация администраторов выполняется по логину и паролю, вы можете изменить способ аутентификации в разделе **Настройки → UserGate → Настройки → Настройки интерфейса → Режим аутентификации веб-консоли**. Например, для более безопасного подключения можно выбрать аутентификацию по сертификатам и [настроить цифровые сертификаты](#).

Создание профиля доступа

Для создания учетной записи должен быть создан хотя бы один профиль доступа с набором разрешений, которые предоставляются администратору.

Чтобы создать профиль доступа:

1. В разделе **Настройки → UserGate → Администраторы → Профили администраторов** нажмите **Добавить**.
2. На вкладке **Общие** укажите название профиля.
3. На вкладке **Разрешение доступа** выберите действия, которые может выполнять администратор в веб-интерфейсе.
4. На вкладке **Разрешение для API** выберите действия, которые может выполнять администратор при подключении через REST API.
5. На вкладке **Разрешение для CLI** разрешите или запретите администратору доступ к интерфейсу командной строки.
6. Нажмите **Сохранить**.

Теперь вы можете перейти к созданию учетной записи администратора.

Создание учетной записи администратора

Чтобы создать учетную запись администратора:

1. В разделе **Настройки → UserGate → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите тип учетной записи.
2. Выберите профиль доступа и укажите параметры, необходимые для выбранного типа учетной записи.
3. Нажмите **Сохранить**.

Все администраторы, подключившиеся к UserGate NGFW одним из способов, отображаются в разделе **Настройки → UserGate → Администраторы → Сессии администраторов**. Вы можете закрывать сессии администраторов по кнопке **Заккрыть сессию**.

Настройка парольной политики

Для локальных учетных записей можно настроить парольную политику, а именно указать:

- параметры сложности пароля;
- максимальное количество неудачных попыток аутентификации;
- время блокировки учетной записи при превышении количества неудачных попыток аутентификации.

Чтобы настроить парольную политику:

1. В разделе **Настройки → UserGate → Администраторы** в блоке **Администраторы** нажмите **Еще → Настроить**.
2. Укажите параметры, которым должен соответствовать пароль локальной учетной записи администратора.
3. Нажмите **Сохранить**.

Настройка цифровых сертификатов

Вы можете использовать аутентификацию администраторов по сертификатам, это обеспечит дополнительную защиту при подключении к UserGate NGFW. Для этого цифровые сертификаты должны быть настроены.

i Примечание

Ниже приводится инструкция по настройке сертификатов в OpenSSL. Вы можете выполнять инструкцию в этой же утилите или в ее аналогах.

Чтобы настроить цифровые сертификаты:

1. Создайте сертификат удостоверяющего центра для доступа к веб-интерфейсу, последовательно выполнив команды:

```
openssl req -x509 -subj '/C=RU/ST=Moscow/O= MyCompany /
CN=ca.mycompany.com' -newkey rsa:2048 -keyout ca-key.pem -out
ca.pem -nodes

openssl rsa -in ca-key.pem -out ca-key.pem
```

Будут созданы файл закрытого ключа `ca-key.pem` и файл открытого ключа `ca.pem`. [Импортируйте открытый ключ](#) на сервер UserGate NGFW.

2. Создайте сертификат администратора для каждой учетной записи, выполнив команду:

```
openssl req -subj '/C=RU/ST=Moscow/O= MyCompany /CN=<логин
администратора>' -out admin.csr -newkey rsa:2048 -keyout admin-
key.pem -nodes
```

3. Подпишите сертификат администратора каждой учетной записи сертификатом удостоверяющего центра, последовательно выполнив команды:

```
openssl x509 -req -days 9999 -CA ca.pem -CAkey ca-key.pem -
set_serial 1 -in admin.csr -out admin.pem
```

```
openssl pkcs12 -export -in admin.pem -inkey admin-key.pem -out
admin.p12 -name '<логин администратора> client certificate'
```

Подписанные сертификаты администраторов будут сохранены в файл `admin.p12`. Вам необходимо добавить этот файл в операционную систему и в браузер, которые будут использовать администраторы для подключения к устройству.

Управление сертификатами

UserGate NGFW использует защищенный протокол HTTPS для управления устройством, может перехватывать и расшифровать транзитный трафик пользователей, передаваемый по протоколу SSL (HTTPS, SMTPS, POP3S), а также производить авторизацию администраторов в веб-консоли на основе их сертификатов.

Для выполнения этих функций NGFW использует различные типы сертификатов.

Сертификат	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW
SSL captive-портала	Используется для создания безопасного HTTPS-подключения пользователей к странице авторизации captive-портала, отображения страницы блокировки и страницы Logout captive-портала, для работы прокси-сервера FTP. Этот сертификат должен быть выпущен со следующими параметрами: • Subject name — значение, установленное для домена Домен Auth captive-портала в разделе Настройки → UserGate → Настройки → Модули. • Subject Alternative names — необходимо указать все домены, для которых используется данный сертификат и которые заданы на странице Настройки → UserGate → Настройки: ◦ Домен Auth captive-портала; ◦ Домен Logout captive-портала; ◦ Домен страницы блокировки; ◦ FTP поверх HTTP; ◦ Адрес веб-портала. По умолчанию используется сертификат, подписанный с помощью сертификата SSL-инспектирования и выпущенный для домена <code>auth.captive</code>, со следующими параметрами: • Subject name = <code>auth.captive</code>

Сертификат	Описание
	• Subject alternative names = auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive Если администратор не загрузил собственный сертификат для обслуживания этой роли, UserGate NGFW в автоматическом режиме перевыпускает такой сертификат при изменении администратором одного из доменов на странице Настройки (домены для auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive).  Внимание! Если администратор использует отдельный сертификат для домена captive-портала, необходимо в сертификате в расширении Subject Alternative name добавить не только свой домен Auth captive-портала, но также и фиксированный домен cert.captive. Если cert.captive не добавить, при аутентификации через сертификат в браузере будет выдаваться ошибка безопасности
SSL-инспектирование	Сертификат класса удостоверяющего центра. Используется для генерации SSL-сертификатов для интернет-узлов, для которых производится перехват трафика HTTPS, SMTPS, POP3S. Например, рассмотрим перехват HTTPS-трафика сайта yahoo.com. Оригинальный сертификат выглядит следующим образом: Subject name = yahoo.com Issuer name = VeriSign Class 3 Secure Server CA – G3, Сертификат подменяется на: Subject name = yahoo.com Issuer name = <компания, указанная в сертификате удостоверяющего центра, заведенного в UserGate NGFW>. Этот сертификат также используется для создания сертификата по умолчанию для роли SSL captive-портала
SSL-инспектирование (промежуточный)	Промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата SSL-инспектирования. Для корректной работы необходим только открытый ключ сертификата

Сертификат	Описание
SSL-инспектирование (корневой)	Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата SSL-инспектирования. Для корректной работы необходим только открытый ключ сертификата
Пользовательский сертификат	Сертификат, который назначается пользователю UserGate NGFW. Пользователь может быть как локальным, так и использующим LDAP-аутентификацию. Сертификат может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси
УЦ для авторизации в веб-консоли	Сертификат удостоверяющего центра для доступа к веб-консоли. Для успешной авторизации сертификат администратора должен быть подписан сертификатом этого типа
SAML server	Используется для работы UserGate NGFW с сервером SSO SAML IDP. Подробнее о настройке работы UserGate NGFW с сервером авторизации SAML IDP — в соответствующем разделе руководства
Веб-портал	Сертификат, используемый для веб-портала. Если сертификат не указан явно, UserGate NGFW использует сертификат SSL captive-портала, выпущенный сертификатом SSL-инспектирования. Подробнее о настройке веб-портала — в соответствующем разделе руководства

Сертификатов для SSL веб-консоли, SSL captive-портала и SSL-инспектирования может быть несколько, но только один сертификат каждого типа может быть активным и использоваться для выполнения задач. Сертификатов типа **УЦ для авторизации в веб-консоли** может быть несколько, и каждый из них может быть использован для проверки подлинности сертификатов администраторов.

Создание сертификата

Чтобы создать новый сертификат:

1. В разделе **Настройки → UserGate → Сертификаты** нажмите **Создать** и укажите информацию о сертификате.

i Примечание

В поле Common name указывается имя сертификата. Рекомендуется использовать только символы латинского алфавита для обеспечения совместимости с большинством браузеров.

1. Укажите роль сертификата в UserGate NGFW: выделите необходимый сертификат в списке сертификатов, нажмите **Редактировать** и в поле **Используется** выберите тип сертификата. В случае если вы выбрали тип **SSL веб-консоли**, UserGate NGFW перезагрузит сервис веб-консоли и предложит подключиться уже с использованием нового сертификата. Сертификат SSL-инспектирования начинает работать сразу после того, как его выбрали. Подробнее об инспектировании HTTPS — в разделе «[Инспектирование SSL](#)».

Экспорт и импорт сертификатов

UserGate NGFW позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например сертификаты, выписанные доверенным удостоверяющим центром вашей организации.

Чтобы экспортировать сертификат:

1. В разделе **Настройки → UserGate → Сертификаты** выделите нужный сертификат в списке и нажмите **Экспорт**.
2. Выберите тип сертификата для экспорта:
 - **Экспорт сертификата** — экспортируются данные сертификата в DER-формате без экспортирования закрытого ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для SSL-инспектирования, для его установки в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом — в приложении «[Установка сертификата локального удостоверяющего центра](#)».
 - **Экспорт CSR** — экспортируется CSR сертификата, например для его подписи удостоверяющим центром.

i Примечание

Рекомендуется сохранять сертификат, чтобы впоследствии иметь возможность его восстановить.

i Примечание

В целях безопасности UserGate не разрешает экспорт закрытых ключей сертификатов.

i Примечание

Вы можете скачать для установки сертификат SSL-инспектирования по ссылке http://usergate_ip:8002/cps/ca, где usergate_ip — IP-адрес вашего UserGate NGFW.

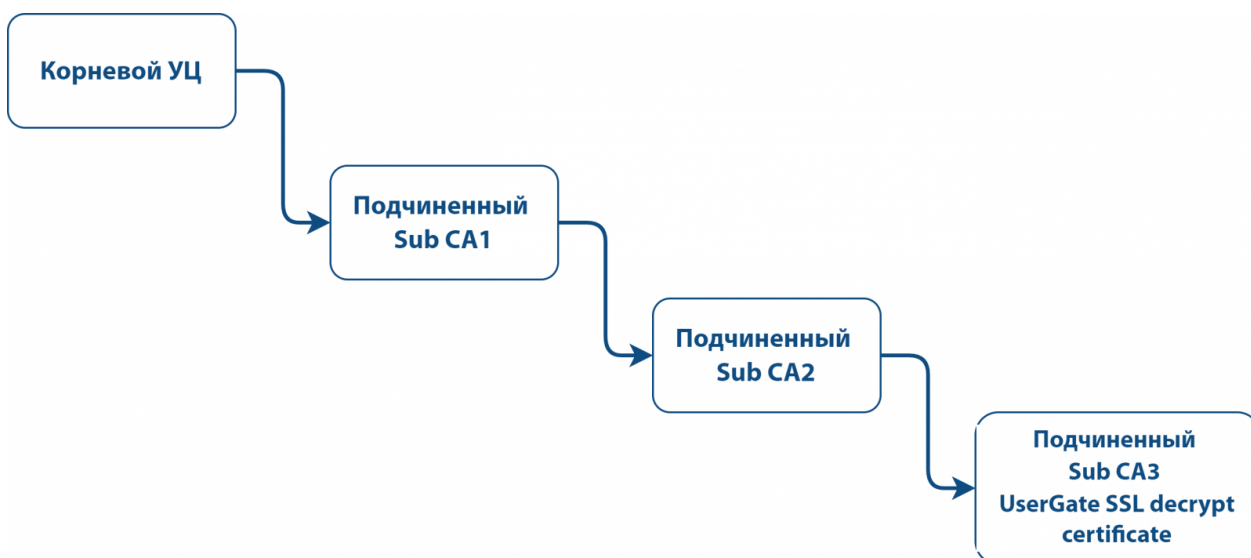
Чтобы импортировать сертификат:

1. В разделе **Настройки → UserGate → Сертификаты** нажмите **Импорт**.
2. Заполните поля, указав необходимую информацию о сертификате.

Использование корпоративного УЦ для создания сертификата SSL-инспектирования

Если в компании уже существует внутренний УЦ или цепочка удостоверяющих центров, в качестве сертификата для SSL-инспектирования можно указать сертификат, созданный внутренним УЦ. В случае если внутренний УЦ является доверенным для всех пользователей компании, перехват SSL будет происходить незаметно, пользователи не будут получать предупреждения о подмене сертификата.

Рассмотрим более подробно процедуру настройки UserGate NGFW. Допустим, что в организации используется внутренний УЦ на базе Microsoft Enterprise CA, интегрированный в Active Directory. Структура УЦ следующая.



Необходимо выпустить с помощью Sub CA2 сертификат для UserGate NGFW и настроить его в качестве сертификата для SSL-инспектирования. Также необходимо выпустить сертификат UserGate SSL decrypt в качестве удостоверяющего центра.

В качестве сертификата для SSL-инспектирования могут быть использованы только те импортированные сертификаты, которые соответствуют требованиям ниже:

- Сертификат относится к классу удостоверяющего центра (CA). В расширении X509v3 Basic Constraints ([RFC 5280](#)) сертификата должен быть атрибут **CA:TRUE**. В разделе **Настройки → UserGate → Сертификаты** консоли администратора такие сертификаты помечаются значком **Файл сертификата УЦ** слева от названия сертификата.
- Ограничение использования сертификата не установлено или в его назначении в явном виде указаны атрибуты **Digital signature** и **Certificate signing**.
- В сертификате не использованы никакие атрибуты расширения X509v3 Key Usage ([RFC 5280](#)). В столбце **Назначение сертификата** консоли администратора для такого сертификата будет указано **Отсутствует**.
- Если в сертификате используется расширение X509v3 Key Usage, для SSL-инспектирования должны присутствовать атрибуты **digitalSignature** и **keyCertSign**. В столбце **Назначение сертификата** консоли администратора для такого сертификата будет указано **Digital signature** и **Certificate signing**.

i Внимание!

UserGate не поддерживает алгоритм подписи rsassaPss. Необходимо, чтобы в цепочке сертификатов, используемой для выписывания сертификата для SSL-инспектирования, не содержался этот алгоритм подписи.

Для выполнения этой задачи:

1. В разделе **Настройки → UserGate → Сертификаты** нажмите **Новый CSR**, заполните необходимые поля и создайте CSR.
Будут созданы закрытый ключ и файл запроса.
2. В списке сертификатов выделите CSR и с помощью кнопки **Экспорт** скачайте файл запроса.
3. В Microsoft CA создайте сертификат на основе полученного CSR-файла с помощью утилиты certreq (certreq.exe -submit -attrib "CertificateTemplate:SubCA" HTTPS_csr.pem) или с помощью веб-консоли Microsoft CA, указав в качестве шаблона «Подчиненный центр сертификации». Вы получите сертификат (открытый ключ), подписанный УЦ Sub CA2.
4. Скачайте созданный сертификат из веб-консоли Microsoft CA.
5. В UserGate NGFW на вкладке **Сертификаты** выберите созданный ранее CSR-файл и нажмите **Редактировать**. Загрузите файл сертификата и нажмите **Сохранить**.
6. На вкладке **Сертификаты** повторно выберите созданный ранее CSR-файл и нажмите **Редактировать**. В поле **Используется** укажите **SSL-инспектирование** и нажмите **Сохранить**.
7. В веб-консоли Microsoft CA выберите и скачайте сертификаты для УЦ Sub CA1 и Sub CA2.
8. На вкладке **Сертификаты** с помощью кнопки **Импорт** загрузите скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2.
9. На вкладке **Сертификаты** для каждого из этих сертификатов нажмите **Редактировать**, в поле **Используется** укажите **SSL-инспектирование (промежуточный)** и нажмите **Сохранить**.

Дополнительно вы также можете с помощью кнопки **Импорт** загрузить корневой сертификат организации в UserGate NGFW. После загрузки выберите

сертификат, нажмите **Редактировать**, в поле **Используется** укажите **SSL-инспектирование (корневой)**

Профили клиентских сертификатов

Профиль клиентского сертификата предназначен для проверки сертификатов, которые предоставляет клиент для аутентификации и получения доступа к приложению, сегменту сети или ресурсу. Проверка состоит из трех действий: получения имени пользователя из соответствующего атрибута в сертификате клиента, проверки иерархии доверия и подлинности сертификата.

В профиле указываются сертификаты УЦ, методы проверки актуальности пользовательских сертификатов, методы выбора имени пользователя для аутентификации.

При выборе режима аутентификации по сертификатам (PKI) указывается сконфигурированный ранее профиль клиентского сертификата, который в дальнейшем можно будет использовать в различных подсистемах UserGate NGFW, например на captive-портале, веб-портале, в VPN, reverse proxy.

Чтобы создать профиль клиентского сертификата:

В разделе **Настройки → UserGate → Профили клиентских сертификатов** нажмите **Добавить** и укажите значения следующих параметров.

Наименование	Описание
Название	Название профиля клиентских сертификатов
Описание	Описание профиля (необязательное для заполнения поле)
Получать имя пользователя из	Выбор атрибута сертификата, из которого межсетевой экран будет извлекать имя пользователя, используемое при аутентификации: • Common-name — доменное имя или имя узла в поле Subject, для которого предназначен сертификат. • Principal name — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. • Subject altname email — для определения имени пользователя используется адрес электронной почты пользователя, указанный в параметре c

Наименование	Описание
	префиксом email в расширении SAN (Subject Alternative Name). • Subject altname IPv4 — для идентификации источника VPN-соединения используется значение IP-адреса, содержащееся в поле iPAddress в расширении SAN (доступно в версии 7.5.0 и выше). Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, используется первое значение, указанное в сертификате
Сертификаты УЦ	Сертификаты корневых и промежуточных удостоверяющих центров, которые участвовали в выдаче сертификатов клиентов. Используются для проверки иерархии доверия к сертификату клиента. Сертификат клиента проверяется на подлинность для каждого сертификата УЦ из списка. Перебор списка идет сверху вниз
Проверка отозванных сертификатов	В списках отозванных сертификатов (CRL) содержатся сертификаты, которые были скомпрометированы либо срок действия которых истек. Такие сертификаты больше не могут использоваться для аутентификации. Возможно установить следующие значения параметра: • Не проверять — доступ будет предоставляться вне зависимости от того, является ли сертификат отозванным. • Вся цепочка — проверять все сертификаты в иерархии и требовать, чтобы они все были действительными. В профиль в разделе Сертификаты УЦ должны быть добавлены сертификаты корневого и всех промежуточных удостоверяющих центров, которые участвовали в выдаче сертификатов клиентов. • Сертификат пользователя — проверять только сертификат клиента. В профиль в разделе Сертификаты УЦ должен быть добавлен сертификат удостоверяющего центра, которым подписан сертификат клиента. • Считать валидным, если статус неизвестен — проверять сертификат и, если его статус не удалось определить по каким-то причинам (например, UG NGFW не смог получить CRL), считать сертификат действительным. При этом сертификат в результате проверки может получить статус invalid, если он найден в списке отозванных

Наименование	Описание
Тайм-аут проверки	Дополнительный связанный параметр определяет интервал времени, по истечении которого UserGate NGFW перестает ожидать ответа о статусе сертификата от службы списков отозванных сертификатов. В этом случае сертификат считается подлинным, и при соблюдении прочих условий аутентификация по нему может быть выполнена

Системные утилиты

Системные утилиты доступны администратору во время загрузки UserGate NGFW через меню загрузки (boot menu). Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру — к разъему USB (при наличии соответствующих разъемов на устройстве). Вы также можете подключить свой компьютер к NGFW, используя специальный кабель для последовательного порта или переходник USB-Serial. Далее необходимо запустить терминал, позволяющий подключиться через последовательный порт (например, через PuTTY для Windows) и установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

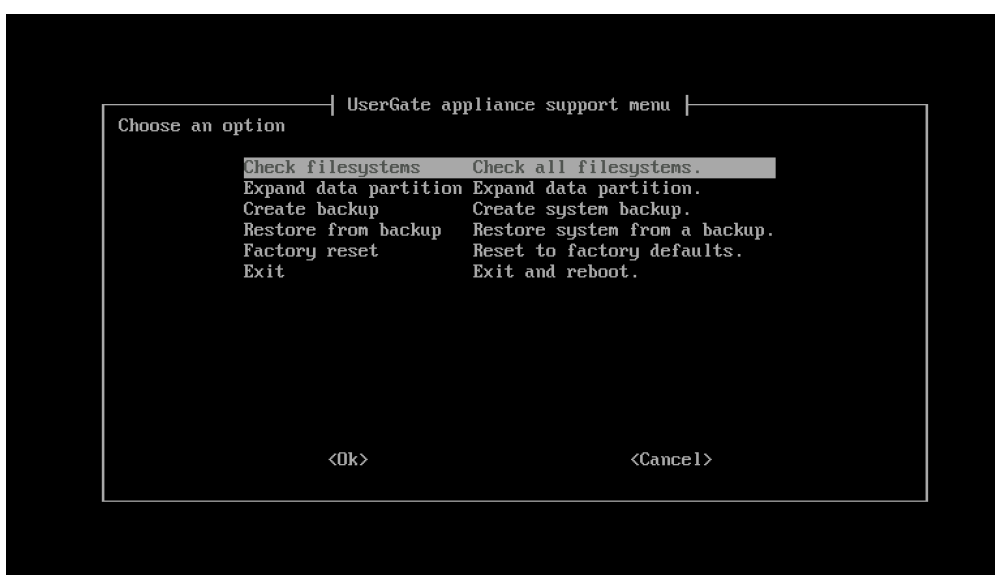
Администратор может выбрать один из нескольких способов загрузки в boot-меню.



Способ загрузки	Описание
UGOS NGFW	Загрузка UserGate NGFW с выводом диагностической информации о загрузке в последовательный порт

Способ загрузки	Описание
UGOS NGFW (serial console)	Загрузка UserGate NGFW в упрощенном видеорежиме консоли
Support menu	Вход в раздел системных утилит с выводом информации в консоль tty1 (монитор)
Restore previous version	Раздел доступен после обновления или создания резервной копии

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:



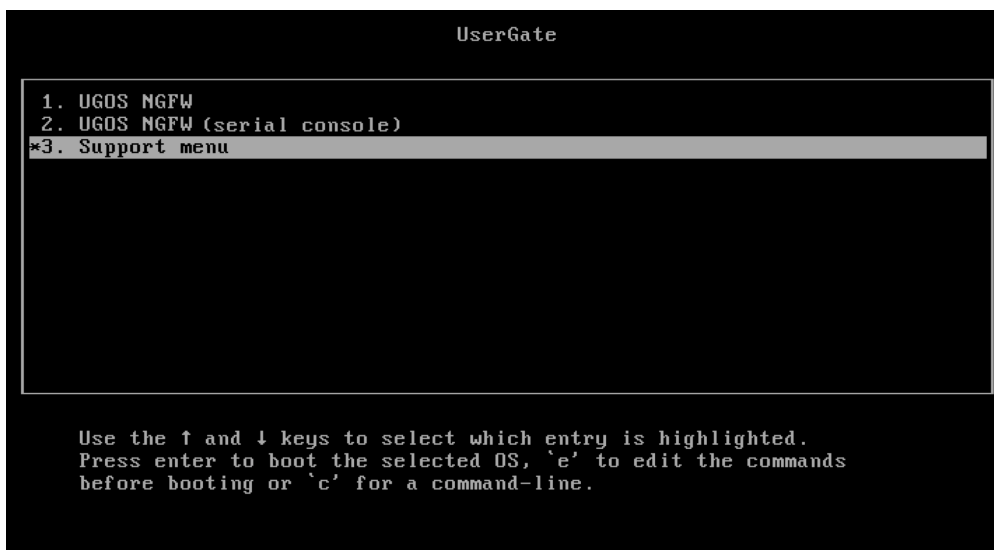
Действие	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление
Expand data partition	Увеличение раздела для хранения данных. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate NGFW. Внимание! Для расширения системного раздела с сохранением данных и параметров UserGate NGFW необходимо с помощью средств гипервизора добавить новый диск и затем выполнить операцию Expand data partition, как указано в разделе «Расширение системного раздела»
Create backup	Создание полной копии диска UserGate NGFW на внешнем USB-носителе.

Действие	Описание
	Внимание! Перед созданием резервной копии USB-носитель будет отформатирован
Restore from backup	Восстановление UserGate NGFW с внешнего USB-носителя
Factory reset	Сброс состояния UserGate NGFW. Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
Exit	Выход и перезагрузка устройства

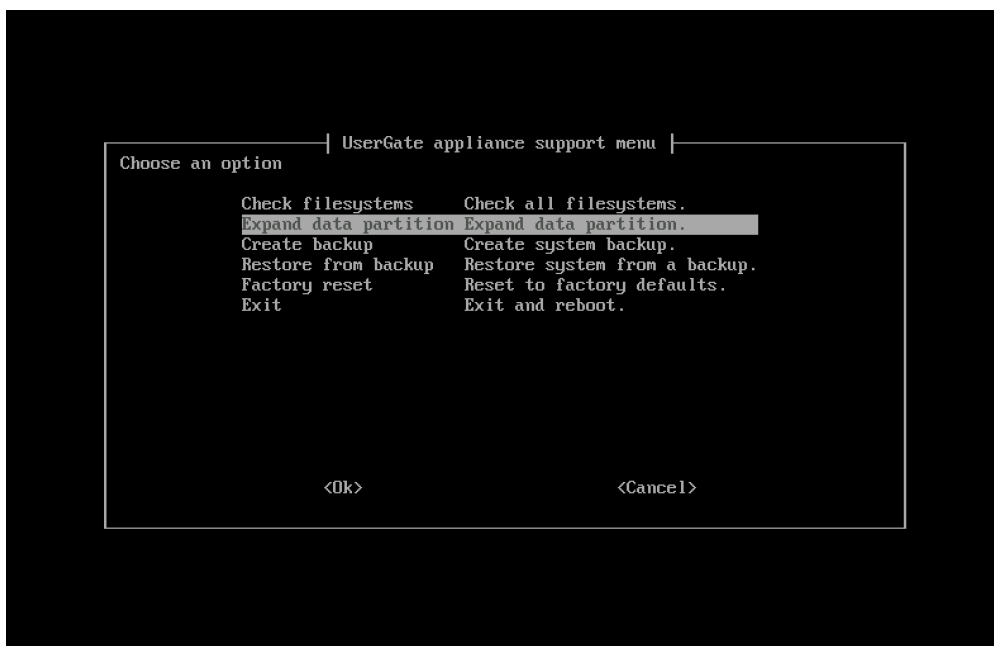
Расширение системного раздела

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate:

1. С помощью гипервизора добавьте новый диск необходимого размера в свойствах виртуальной машины UserGate.
2. В меню загрузки узла UserGate войдите в раздел **Support menu**.



3. В открывшемся разделе выберите **Expand data partition** и запустите процесс расширения системного раздела.



4. После завершения процесса расширения загрузите узел и в разделе **Дашборды** в виджете **Диски** проверьте размер системного раздела.

i Примечание

Расширение системного раздела путем увеличения размера имеющегося диска виртуальной машины возможно только при сбросе узла до заводских параметров, то есть при выполнении операции **factory reset**.

Работа с вышестоящими прокси-серверами

UserGate NGFW позволяет создавать каскадную иерархию прокси-серверов. В этой иерархии межсетевой экран выступает в роли явного прокси-сервера и [перенаправляет входящий веб-трафик](#) на другой (вышестоящий) прокси-сервер, создавая тем самым цепочку прокси-серверов.

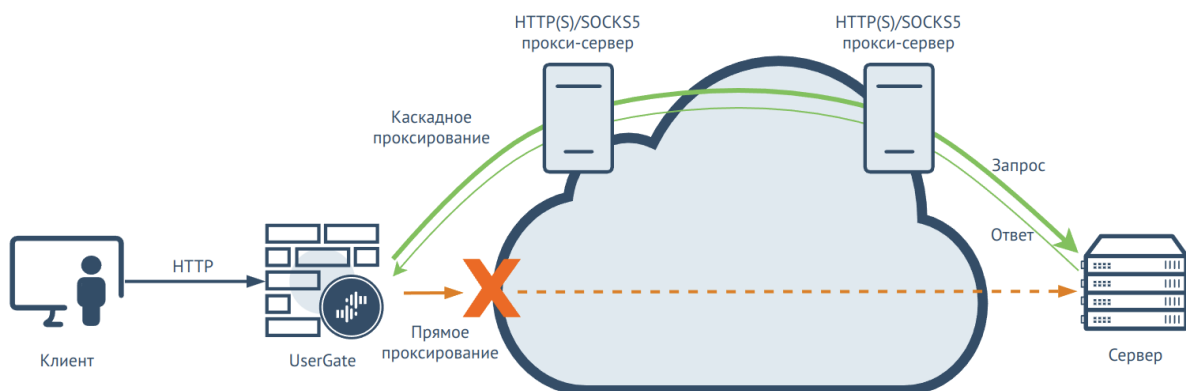
С помощью каскадной иерархии вы можете управлять доступом пользователей к веб-ресурсам. Например, используя вышестоящий прокси-сервер, можно обойти региональные ограничения или получить доступ к веб-ресурсам, обращение к которым возможно только через определенные сети.

Также вы можете использовать вышестоящий прокси-сервер [для получения лицензий и обновлений продукта](#). Это может понадобиться, например, если UserGate NGFW установлен в изолированной сети (без доступа в интернет).

Опционально на вышестоящем прокси-сервере вы можете настроить аутентификацию по логину и паролю. Кроме того, начиная с версии 7.4.0 и выше вы можете управлять доступом к отдельным веб-ресурсам с помощью правил вышестоящих прокси-серверов.

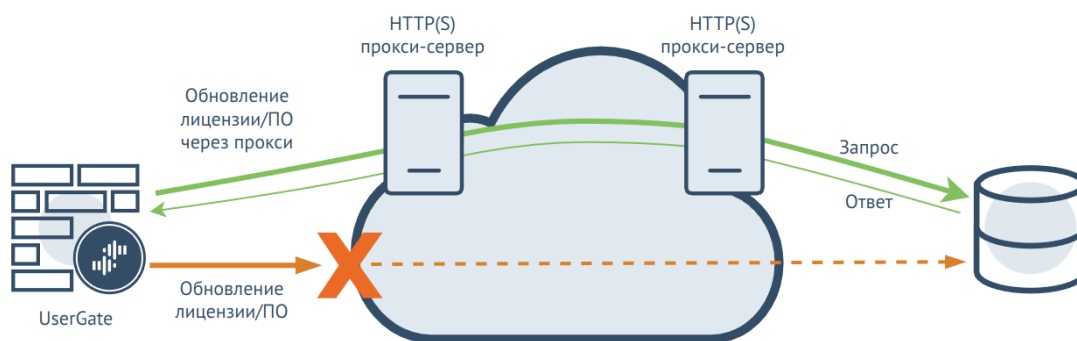
Использование вышестоящего прокси-сервера

Для перенаправления трафика. Входящий веб-трафик, отфильтрованный правилами UserGate NGFW, перенаправляется на вышестоящий прокси-сервер. В этом случае вышестоящим может быть прокси-сервер HTTP, HTTPS или SOCKS5. Процесс перенаправления трафика представлен на рисунке ниже.



При запросе клиентом внешнего ресурса устанавливаются две TCP-сессии: первая — между клиентом и UserGate NGFW, вторая — между UserGate NGFW и вышестоящим прокси-сервером. Адрес назначения трафика — это IP-адрес вышестоящего прокси-сервера, для межсетевого экрана трафик является транзитным. Если ранее на UserGate NGFW было настроено запрещающее правило по IP-адресам назначения, то оно не будет срабатывать.

Для получения лицензий и обновлений продукта. Вы можете [настроить получение лицензий и обновлений продукта](#) через вышестоящий прокси-сервер. В этом случае вышестоящим может быть прокси-сервер HTTP или HTTPS. Процесс получения лицензий и обновлений представлен на рисунке ниже.



При активации лицензии или установке обновлений UserGate NGFW обращается к серверу лицензирования или серверу обновления UserGate не напрямую, а через вышестоящий прокси-сервер. Для каждого обращения в журнале событий межсетевого экрана отображается IP-адрес и порт вышестоящего прокси-сервера, например proxy: `https://192.0.2.1:1080`.

Настройка прокси-сервера для перенаправления трафика

Примечание

Вы можете настраивать вышестоящий прокси-сервер для перенаправления трафика как в веб-интерфейсе, так и [в интерфейсе командной строки UserGate NGFW](#). Ниже приведены инструкции для веб-интерфейса продукта.

Чтобы настроить вышестоящий прокси-сервер для перенаправления трафика, необходимо:

- [Подключить прокси-сервер к UserGate NGFW](#).
- [Создать профиль вышестоящего прокси-сервера](#). С помощью профилей вы можете выбирать прокси-серверы, которые будут использоваться в качестве вышестоящего прокси-сервера, а также изменять параметры проверки их состояния. Это обеспечивает отказоустойчивое подключение вышестоящего прокси-сервера к UserGate NGFW.
- [Создать правило вышестоящего прокси-сервера](#). С помощью правил вы можете управлять доступом к выбранным веб-ресурсам. В качестве условий срабатывания правила можно выбрать зоны и адреса источника, пользователей и их группы, URL-категории и URL-списки.

Примечание

Если в UserGate NGFW версий 7.1–7.3.2 был настроен вышестоящий прокси-сервер, то при обновлении продукта до версии 7.4.0 и выше автоматически будут добавлены один прокси-сервер, один профиль, одно правило.

Чтобы подключить прокси-сервер к UserGate NGFW:

1. В разделе **Настройки** → **Вышестоящие прокси** → **Серверы** нажмите **Добавить**.

2. Укажите параметры подключения прокси-сервера.

i Примечание

Если в качестве прокси-сервера вы подключаете UserGate NGFW, то вы можете выбрать только режим HTTP(S).

3. Нажмите **Сохранить**.

Подключенный прокси-сервер отобразится в списке серверов раздела. Напротив прокси-сервера отображается статус его подключения к UserGate NGFW. Доступные серверы помечаются значком зеленого цвета. Проверка подключения прокси-сервера выполняется автоматически каждые 30 секунд.

Чтобы создать профиль вышестоящего прокси-сервера:

1. В разделе **Настройки → Вышестоящие прокси → Профили Профили** нажмите **Добавить**.
2. На вкладке **Общие** укажите название и описание профиля.
3. На вкладке **Серверы вышестоящего прокси** выберите прокси-серверы.

i Примечание

Если выбрано несколько прокси-серверов, то в качестве вышестоящего прокси-сервера будет использоваться первый доступный сервер из списка.

4. На вкладке **Проверка состояния** укажите параметры проверки состояния вышестоящего прокси-сервера:

- адрес веб-ресурса, к которому будет подключаться вышестоящий прокси-сервер;
- метод HTTP-запроса, посредством которого выполняется подключение к веб-ресурсу;
- интервал проверки;
- время ожидания ответа.

5. Нажмите **Сохранить**.

Созданный профиль отобразится в списке профилей раздела.

Чтобы создать правило вышестоящего прокси-сервера:

1. В разделе **Настройки → Вышестоящие прокси → Правила** нажмите **Добавить**.

2. На вкладке **Общие** укажите параметры правила:

- состояние;
- название и описание;
- действие при срабатывании правила: **Напрямую** — трафик будет направлен через шлюз по умолчанию, **Через прокси** — трафик будет направлен через вышестоящий прокси-сервер;
- журналирование срабатываний правила;
- местоположение в списке правил.

При выборе действия **Через прокси** укажите дополнительные параметры правила:

- профиль вышестоящего прокси-сервера;
- действие в случае, если недоступны прокси-серверы, указанные в профиле.

3. На вкладках **Источник**, **Пользователи**, **Категории URL** и **URL** укажите объекты, для которых будет срабатывать правило.

Вы можете выбирать объекты из списков или создавать новые по кнопке **Создать и добавить новый объект**. При установке флажка **Инвертировать** (соответствует логическому отрицанию) указанные объекты будут исключены из условий срабатывания правила.

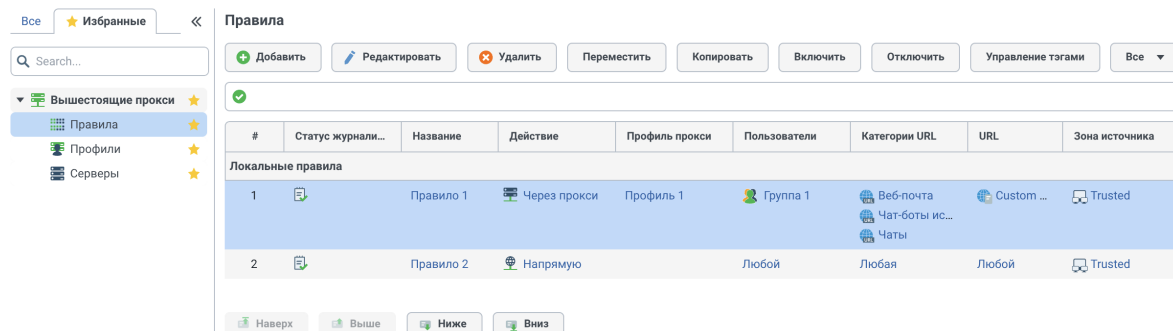
4. На вкладке **Время** укажите расписание работы правила.

Вы можете выбирать [календари](#) из списка или создавать новые по кнопке **Создать и добавить новый объект**.

5. Нажмите **Сохранить**.

Созданное правило отобразится в списке правил раздела. Правила применяются поочередно в том порядке, в котором они указаны в списке.

Срабатывает первое правило среди тех, в которых совпали все указанные условия. Для изменения порядка применения правил используйте кнопки **Выше**, **Ниже**, **Наверх**, **Вниз** или перетащите правила курсором.



Настройка прокси-сервера для получения лицензий и обновлений

Чтобы настроить получение лицензий и обновлений продукта через вышестоящий прокси-сервер:

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии** (при активации лицензии) или **Зарегистрированная версия** (при обновлении лицензии).
2. В окне активации продукта установите флажок **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.
3. Выполните [активацию или обновление лицензии](#).

Кластеризация и отказоустойчивость

UserGate NGFW поддерживает следующие типы кластеров:

- **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые параметры фильтрации и обработки трафика в рамках кластера.
- **Кластер отказоустойчивости.** До четырех узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме «активный — активный» или «активный — пассивный». Возможно собрать несколько кластеров отказоустойчивости.

Кластер конфигурации

Ряд параметров уникален для каждого из узлов кластера. К уникальным относятся параметры:

- Log Analyzer,
- диагностики,
- интерфейсов,
- шлюзов,
- DHCP,
- маршрутов,
- OSPF,
- BGP.

Чтобы создать кластер конфигурации:

1. Выполните [первоначальную настройку](#) на первом узле кластера.
2. Настройте на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера: в разделе **Настройки → Сеть → Зоны** создайте выделенную зону для репликации кластера или используйте существующую (**Cluster**). В параметрах зоны в блоке **Контроль доступа** разрешите сервисы **Консоль администрирования** и **Кластер**.



Внимание!

Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например к интернету.

3. Укажите IP-адрес, который будет использоваться для связи с другими узлами кластера: в разделе **Настройки → UserGate → Управление устройством → Кластер конфигурации** выберите текущий узел кластера, нажмите **Редактировать** и укажите IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
4. В блоке **Кластер конфигурации** нажмите **Еще → Сгенерировать секретный код** и скопируйте полученный код в буфер обмена. Код

необходим для одноразовой авторизации второго узла при его добавлении в кластер.

5. Подключитесь к веб-консоли второго узла кластера, выберите язык установки. Укажите интерфейс, который будет использован для подключения к первому узлу кластера, и назначьте ему IP-адрес. Оба узла кластера должны находиться в одной подсети. Например, интерфейсам eth2 обоих узлов могут быть назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера.

Укажите IP-адрес первого узла, настроенный на шаге 3, вставьте секретный код и нажмите **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и все параметры первого кластера реплицируются на второй.

Состояние узлов кластера конфигурации можно определить по цветовой индикации напротив названия узла UserGate в разделе **Настройки → UserGate → Управление устройством → Кластер конфигурации**:

- Зеленый: узел доступен.
- Желтый: происходит синхронизация между узлами кластера конфигурации.
- Красный: связь с узлом потеряна, узел недоступен.

6. В веб-консоли второго узла кластера в разделе **Настройки → Сеть → Интерфейсы** назначьте каждому интерфейсу корректную зону. Зоны и их параметры получены в результате репликации данных с первого узла кластера.

7. Настройте шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

Примечание

При вводе дополнительного узла в кластер конфигурации в явном виде указываются параметры интерфейса и шлюза для подключения к первому узлу. Тип присвоения IP-адреса этого интерфейса будет статическим.

Кластер отказоустойчивости «активный — пассивный»

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько, например в кластер конфигурации могут быть добавлены узлы A, B, C и D, на основе которых будет создано два кластера отказоустойчивости — A-B и C-D.

Поддерживаются два режима кластера отказоустойчивости — «активный — активный» или «активный — пассивный». Состояние узлов кластера можно определить по цвету индикатора около названия узла NGFW в разделе

Настройки → UserGate → Управление устройством → Кластеры отказоустойчивости:

- Нет цветового индикатора: узел кластера доступен
- Желтый: кластер отказоустойчивости не запущен на узле.
- Красный: нет связи с соседними узлами конфигурации.

Отсутствие индикатора напротив названия узла говорит о доступности узла кластера.

В режиме «активный — пассивный» один из межсетевых экранов выступает в роли мастер-узла, обрабатывающего транзитный трафик пользователей, а остальные — в качестве резервных, которые находятся в состоянии готовности начать обработку трафика. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

Примечание

Режим «активный — пассивный» поддерживает синхронизацию пользовательских сессий — это обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси-сервер, например трафик HTTP(S).

При переходе главной роли на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Резервный узел не получает подтверждения о том, что мастер-узел находится в сети (таймеры: Adver — 1 сек., MasterDown — 3 сек.), например если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (см. раздел «[Настройка шлюзов](#)») и ни через один из шлюзов нет доступа в интернет.
- Если узел, указанный в свойствах проверки сети, недоступен на всех узлах кластера, то кластер отказоустойчивости будет отключен.
- Сбой в работе ПО UserGate NGFW.

Отключение одного или нескольких сетевых интерфейсов, на которые назначены виртуальные IP-адреса, понижает приоритет узла, но не обязательно приводит к изменению его роли. Переход на резервный узел произойдет, если приоритет резервного узла окажется выше, чем приоритет мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла — 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, который физически не подключен к сети.

Соответственно, если на кластере отказоустойчивости, состоящем из двух узлов, один из интерфейсов на мастер-узле будет физически отключен от сети, резервный узел станет мастером (при условии, что на резервном узле все кластерные интерфейсы подключены к сети). В таком случае приоритет мастер-узла будет равен 248, приоритет резервного — 249). При восстановлении физического подключения на первоначальном мастер-узле этот узел снова станет мастером, поскольку его приоритет вернется в значение 250 (справедливо для случая, когда виртуальные адреса сконфигурированы на двух и более интерфейсах; если на одном, то роль мастер-узла не возвращается).

Отключение одного или нескольких кластерных сетевых интерфейсов на резервном узле понижает приоритет узла, тем не менее этот резервный узел может стать мастером при безусловном переходе роли или в случае, когда приоритет мастер-узла станет меньше, чем приоритет резервного узла.

Примечание

Если кластерные IP-адреса назначены VLAN-интерфейсам, отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на этом физическом интерфейсе.

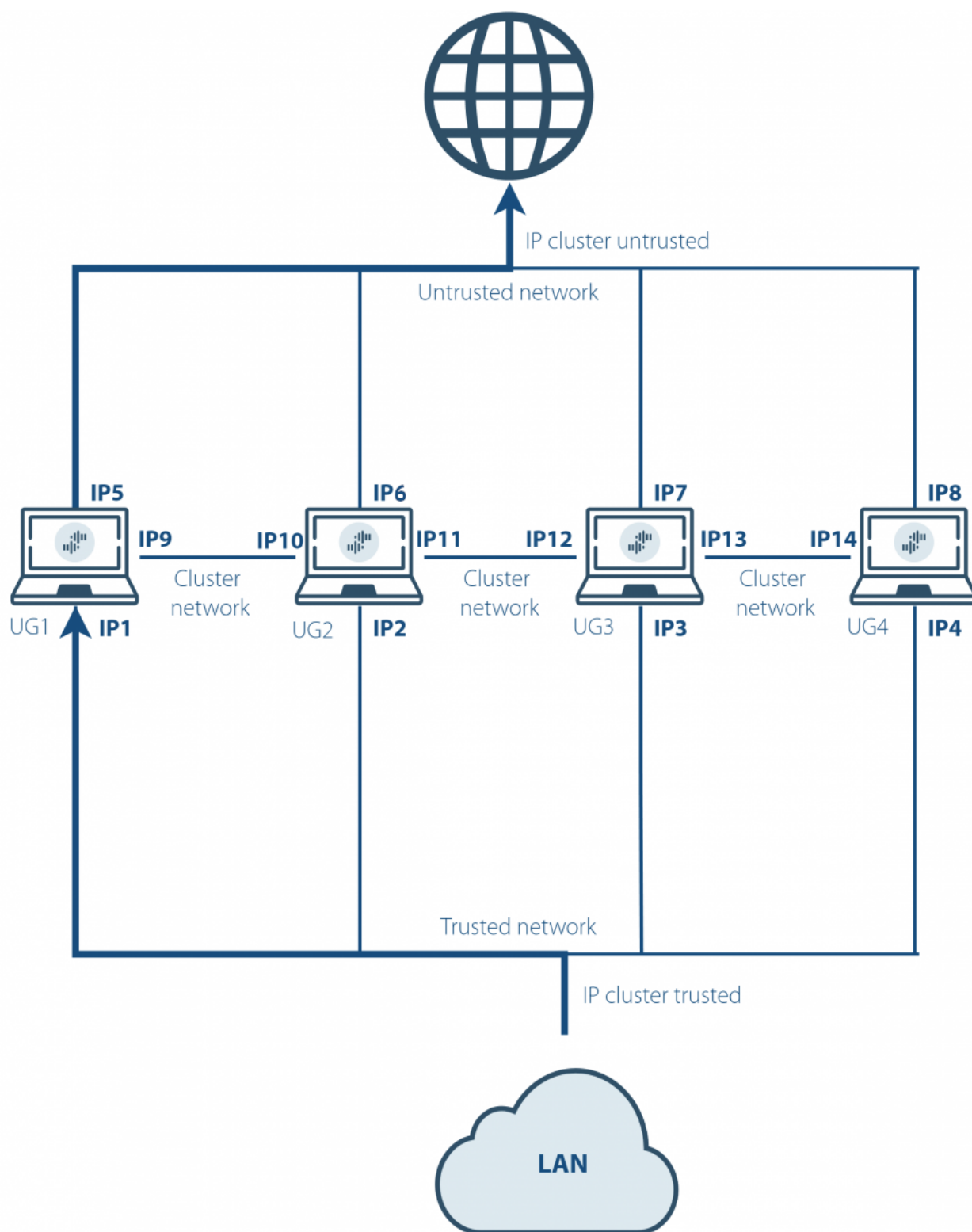
i Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на резервный узел при переключении, UserGate NGFW посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается UserGate NGFW каждую минуту и при переходе роли мастера на резервный узел.

Ниже представлена пример сетевой диаграммы отказоустойчивого кластера в режиме «активный — пассивный». Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- Зона **Untrusted**: IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- Зона **Cluster**: IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации параметров.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий узел, который станет мастером, например на UG2.



Кластер отказоустойчивости в режиме «активный — пассивный»

Кластер отказоустойчивости «активный — активный»

В режиме «активный — активный» один из межсетевых экранов выступает в роли мастер-узла, распределяющего трафик на все остальные узлы кластера.

На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

Виртуальные IP-адреса всегда находятся на интерфейсах мастер-узла, поэтому мастер-узел получает ARP-запросы клиентов и отвечает на них, последовательно отдавая MAC-адреса всех узлов отказоустойчивого кластера, обеспечивая равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий.

Примечание

Балансировка трафика будет работать только в одном широковещательном домене. Например, если для клиентов VIP-адрес будет шлюзом по умолчанию, балансировка трафика будет работать, так как разным клиентам будут поочередно отдаваться разные MAC-адреса узлов. Но в случае если между UserGate NGFW и клиентами находится маршрутизатор, балансировка работать не будет, так как ARP-запрос на VIP-адрес отправит только сам маршрутизатор и ему вернется MAC-адрес только одного из узлов, через который он и отправит весь трафик.

Примечание

Режим «активный — активный» поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси-сервер, например трафик HTTP(S).

При переходе мастер-роли на резервный узел на него переносятся все виртуальные IP-адреса всех кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Резервный сервер не получает подтверждения о том, что мастер-узел находится в сети (таймеры: Adver — 1 сек., MasterDown — 3 сек.), например если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (см. раздел «[Настройка шлюзов](#)») и ни через один из шлюзов нет доступа в интернет.
- Сбой в работе ПО UserGate NGFW.

Отключение одного или нескольких сетевых интерфейсов, на которые назначены виртуальные IP-адреса, понижает приоритет узла, но не обязательно приводит к изменению его роли. Переход на резервный узел произойдет, если приоритет резервного узла окажется выше, чем приоритет мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла — 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, который физически не подключен к сети.

Соответственно, если на кластере отказоустойчивости, состоящем из двух узлов, один из интерфейсов на мастер-узле будет физически отключен от сети, резервный узел станет мастером (при условии, что на резервном узле все кластерные интерфейсы подключены к сети). В таком случае приоритет мастер-узла будет равен 248, приоритет резервного — 249). При восстановлении физического подключения на первоначальном мастер-узле этот узел снова станет мастером, поскольку его приоритет вернется в значение 250 (справедливо для случая, когда виртуальные адреса сконфигурированы на двух и более интерфейсах; если на одном, то роль мастер-узла не возвращается).

Отключение одного или нескольких кластерных сетевых интерфейсов на резервном узле, понижает приоритет узла, а также исключает этот узел из балансировки трафика. Тем не менее этот резервный узел может стать мастером при безусловном переходе роли или в случае, когда приоритет мастер-узла станет меньше, чем приоритет резервного узла.

Примечание

Если кластерные IP-адреса назначены VLAN-интерфейсам, отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на данном физическом интерфейсе.

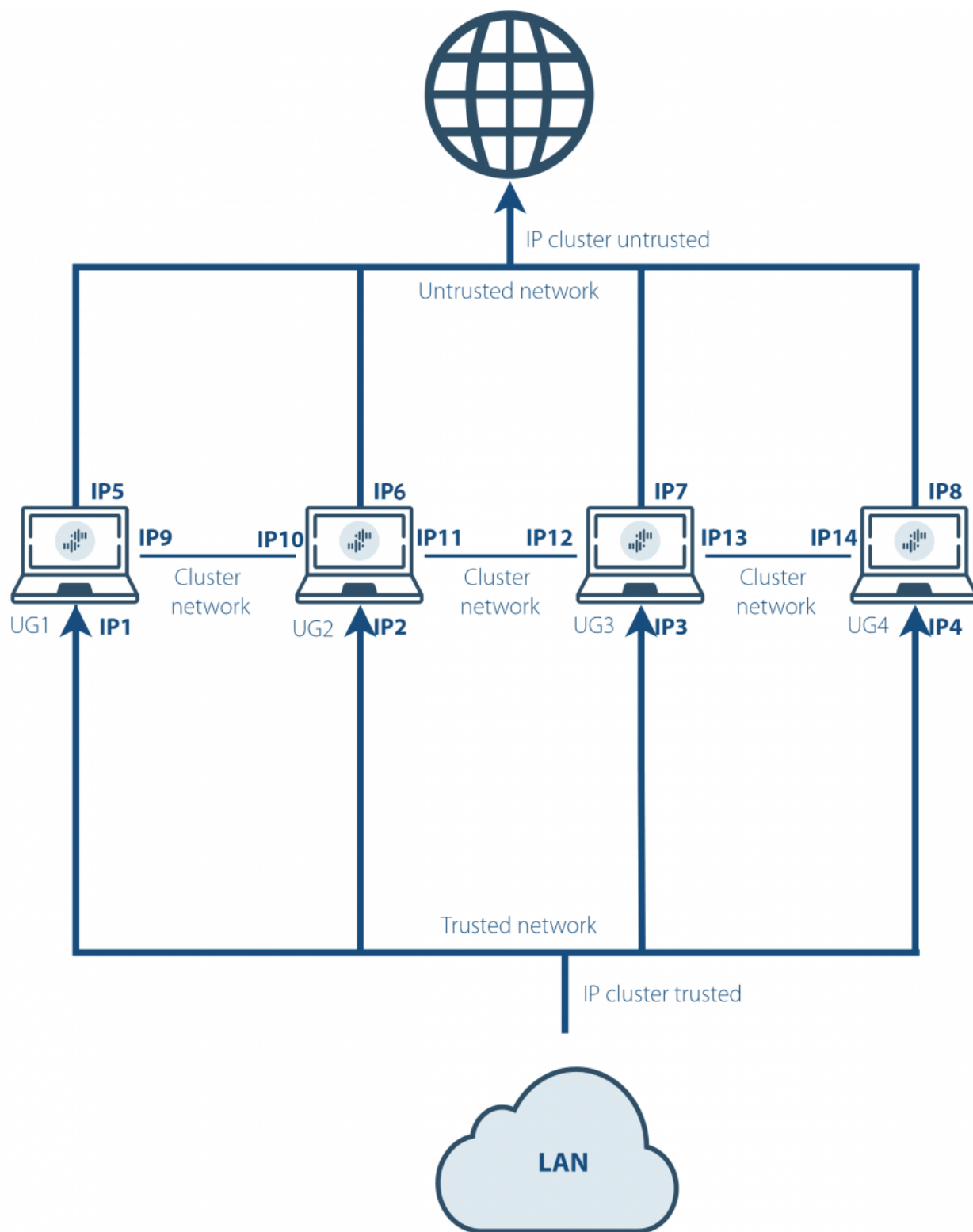
Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на резервный узел при переключении, UserGate NGFW посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме «активный — активный» пакет GARP отсылается UserGate NGFW только при переходе роли мастер-узла на резервный узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме «активный — активный». Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- Зона **Untrusted**: IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- Зона **Cluster**: IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации параметров.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий узел, который станет мастером, например на узел UG2.



Кластер отказоустойчивости в режиме «активный — активный»

i Примечание

Для корректной обработки трафика необходимо, чтобы обратный трафик от сервера к клиенту вернулся через тот же узел UserGate NGFW, через который он был инициирован от клиента, то есть чтобы сессия пользователя всегда проходила через один и тот же узел кластера. Самое простое решение этой задачи – использование NAT, ведущего из сети клиента в сеть сервера (NAT из зоны Trusted в зону Untrusted).

Чтобы создать кластер отказоустойчивости:

1. Создайте кластер конфигурации (см. инструкцию выше).
2. В разделе **Настройки → Сеть → Зоны** разрешите сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зоны **Trusted** и **Untrusted** на диаграммах выше).
3. Создайте кластер отказоустойчивости: в разделе **Настройки → UserGate → Управление устройством → Кластер отказоустойчивости** нажмите **Добавить** и укажите параметры кластера отказоустойчивости.
4. Укажите виртуальный IP-адрес для узлов auth.captive, logout.captive, block.captive, ftpclient.captive. Если вы хотите использовать авторизацию с помощью captive-портала, необходимо, чтобы системные имена узлов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, преобразовывались (resolve) в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более детально эти параметры описаны в разделе «[Общие настройки](#)».

Ниже описаны параметры отказоустойчивого кластера:

Параметр	Описание
Включено	Включение и отключение кластера отказоустойчивости.
Название	Название кластера отказоустойчивости.
Описание	Описание кластера отказоустойчивости.

Параметр	Описание
Режим кластера	Режим кластера отказоустойчивости: • Актив-Актив — нагрузка распределяется на все узлы кластера. • Актив-Пассив — нагрузка идет на мастер-узел и переключается на резервный узел в случае, если мастер-узел недоступен.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий на всех узлах, входящих в кластер отказоустойчивости. Делает переключение с одного устройства на другое удобным для пользователей, но добавляет существенную нагрузку на платформу UserGate NGFW. Синхронизация сессий актуальна только для режима кластера активный — пассивный.
Мультикаст идентификатор	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального маршрутизатора (VRID)	Идентификатор виртуального маршрутизатора должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети нет сторонних кластеров VRRP, рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для их объединения в кластер отказоустойчивости. Здесь же можно назначить роль мастера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и задается их соответствие интерфейсам узлов кластера.
Синхронизация UDP/ICMP	Управление режимом синхронизации пользовательских сессий: • Синхронизировать все сессии — включение и отключение режима синхронизации всех пользовательских сессий, в том числе сессий UDP/ICMP. В случае если этот параметр не активирован, а параметр Синхронизировать сессии на вкладке Общие активирован, синхронизироваться будут только TCP-сессии.

Параметр	Описание
	Важно! Когда режим включен, синхронизация пользовательских сессий по умолчанию происходит через случайно выбранный сетевой интерфейс узла кластера. Чтобы настроить синхронизацию сессий только через интерфейс, принадлежащий зоне кластера, в параметрах кластера отказоустойчивости на вкладке «Виртуальные IP» необходимо создать виртуальный IP-адрес для кластерных интерфейсов. • Исключенные из синхронизации IP — IP-адреса, с которыми не будут синхронизироваться пользовательские сессии.

Кластеризация и отказоустойчивость (версия 7.5.0 и выше)

Вы можете объединить несколько межсетевых экранов в кластер и управлять им как единым логическим устройством. Кластеры позволяют повысить производительность, управлять сетевой нагрузкой и обеспечивать бесперебойную работу сетевых устройств.

UserGate NGFW поддерживает два типа кластеров:

- **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые параметры фильтрации и обработки трафика в рамках кластера. Такая синхронизация гарантирует, что набор политик будет одинаковым на всех узлах кластера и все изменения конфигурации будут выполняться с минимальными задержками. В кластер конфигурации можно объединить до 12 узлов.
- **Кластер отказоустойчивости.** Если в сети настроен кластер конфигурации, то до четырех узлов, входящих в него, можно объединить в кластер отказоустойчивости, который обеспечит непрерывную фильтрацию и обработку трафика. В дополнение к возможностям кластера конфигурации

кластер отказоустойчивости поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла кластера на другой, — за исключением сессий, использующих прокси-сервер, например трафик HTTP(S). Поддерживаются два режима работы кластера отказоустойчивости: «активный — активный» и «активный — пассивный». Вы можете собрать несколько кластеров отказоустойчивости. Например, если в кластер конфигурации добавлены узлы A, B, C и D, на их основе можно создать два кластера отказоустойчивости — A-B и C-D.

Важно!

Работа устройств UserGate в режимах кластера конфигурации и кластера отказоустойчивости доступна, если в используемую лицензию включен модуль Cluster.

Настройка кластера конфигурации

Настройка кластера конфигурации состоит из двух этапов: настройки первого узла и добавления дополнительных узлов. Каждый дополнительный узел добавляется в кластер на этапе первоначальной настройки этого узла. Если в вашей сети уже есть устройства UserGate NGFW, работающие как независимые, их можно добавить в кластер только выполнив сброс к фабричным параметрам.

Чтобы настроить кластер конфигурации:

1. Выполните [первоначальную настройку](#) первого узла кластера. Убедитесь, что активированная лицензия на первом узле (раздел **Дашборды → Лицензия**) включает в себя модуль Cluster.
2. В веб-консоли первого узла в разделе **Настройки → Сеть → Зоны** добавьте зону, в которой будет выполняться репликация кластера, или выберите существующую зону **Cluster**. Убедитесь, что для выбранной зоны в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешены сервисы **Консоль администрирования** и **Кластер**.

Важно!

Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например к интернету.

3. В разделе **Настройки → Сеть → Интерфейсы** выберите интерфейс, через который будет выполняться репликация кластера, и нажмите **Редактировать**.

4. В окне **Свойства интерфейса**:

- на вкладке **Общие** назначьте интерфейсу зону кластера и установите флажок **Включено**;
- на вкладке **Сеть** выберите режим **Статический**, с помощью кнопки **Добавить** укажите IP-адрес;
- нажмите **Сохранить**.

5. В разделе **Настройки → Консоль администратора → Управление устройством → Кластер конфигурации** выберите текущий узел кластера, нажмите **Редактировать**, укажите IP-адрес, назначенный интерфейсу на предыдущем шаге и нажмите **Сохранить**. Начнется перезагрузка устройства.

6. После завершения перезагрузки в блоке **Кластер конфигурации** выберите текущий узел, нажмите **Сгенерировать секретный код** и скопируйте код для авторизации дополнительного узла кластера.

7. Подключитесь к веб-консоли дополнительного узла. В мастере первоначальной настройки выберите язык интерфейса, примите лицензионное соглашение, выберите часовой пояс и затем в окне **Установка** нажмите **Установка дополнительного узла кластера**.

8. В блоке **Шаг 1** укажите параметры дополнительного узла: кластерный интерфейс, его IP-адрес, маску подсети и IP-адрес шлюза (в случае, если первый и дополнительный узлы кластера находятся в разных подсетях). Например, если оба узла находятся в одной подсети, кластерному интерфейсу **eth2** первого узла может быть назначен IP-адрес **192.168.100.5/24**, а интерфейсу **eth2** дополнительного узла в этом случае можно назначить IP-адрес **192.168.100.6/24**.

Примечание

Так как IP-адрес интерфейса дополнительного узла и шлюз по умолчанию на этом шаге указываются в явном виде, режим присвоения этих параметров будет статическим.

9. В блоке **Шаг 2** укажите IP-адрес кластерного интерфейса первого узла, вставьте созданный на нем секретный код и нажмите **Подключить**. Начнется настройка дополнительного узла, после чего он будет добавлен в кластер и все параметры первого узла реплицируются на дополнительный.

10. В веб-консоли дополнительного узла кластера конфигурации в разделе **Настройки → Сеть → Интерфейсы** назначьте каждому интерфейсу корректную зону, так как текущие параметры были получены в результате репликации данных с первого узла кластера.

11. В веб-консоли дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**, чтобы активировать лицензию на дополнительном узле.

Примечание

Если на первом узле кластера лицензия была активирована онлайн, дополнительному узлу для активации лицензии также потребуется доступ в интернет. При офлайн-активации лицензии на первом узле подключение дополнительного узла к интернету не требуется.

12. Настройте шлюзы, маршруты, параметры OSPF, BGP, уникальные для каждого из узлов.

Примечание

К уникальным относятся параметры диагностики, интерфейсов, шлюзов, DHCP, маршрутов, OSPF, BGP и Log Analyzer.

13. Если первый и дополнительный узлы кластера находятся в разных подсетях, для первого узла в разделе **Сеть → Виртуальные маршрутизаторы** настройте статический маршрут через кластерные интерфейсы до подсети, расположенной за дополнительным узлом кластера.

Вы можете отслеживать состояние узлов кластера конфигурации по статусу узла UserGate в любой из веб-консолей в блоке **Настройки → Консоль администратора → Управление устройством → Кластер конфигурации**:

- Зеленый: узел доступен.
- Оранжевый: узел недоступен, идет перезагрузка узла.

- Красный: узел недоступен, связь с узлом потеряна.
- Черный: идет запуск узла.

Кластер отказоустойчивости «активный — пассивный»

В режиме работы кластера «активный — пассивный» один из межсетевых экранов выступает в роли мастер-узла (в веб-консоли статус этого узла — **master**), а остальные — в качестве резервных (в веб-консоли статус этих узлов — **backup**). Узел, выбранный в качестве мастер-узла, обладает наивысшим приоритетом в кластере, он отвечает на ARP-запросы клиентов и выполняет обработку и инспектирование пользовательского трафика. Резервные узлы не обрабатывают трафик, поступающий на виртуальные IP-адреса кластера, и находятся в режиме ожидания. При этом узлы, выступающие в кластере в роли резервных, могут обрабатывать трафик, который передается на их интерфейсы, не являющиеся кластерными.

На каждом из узлов кластера по умолчанию выбраны сетевые интерфейсы в зоне **Cluster**, которым назначены кластерные IP-адреса. Между кластерными интерфейсами передаются VRRP-объявления — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии. На основании VRRP-объявлений оценивается связность кластера, и уточняются приоритеты всех узлов кластера. Также кластерные интерфейсы участвуют в синхронизации сессий между узлами кластера.

На другие сетевые интерфейсы узлов кластера назначаются виртуальные IP-адреса, на которые направляется трафик. В случае если мастер-узел стал недоступен, роль мастер-узла и все виртуальные IP-адреса переносятся на резервный узел с наибольшим IP-адресом либо — если настроены необходимые параметры — с наибольшим приоритетом. Этот узел продолжит обработку трафика.

Безусловный перенос роли мастер-узла на резервный узел происходит при следующих событиях:

- Резервный узел не получает подтверждения того, что мастер-узел находится в сети, например если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (см. раздел «[Настройка шлюзов](#)»), и ни через один из шлюзов нет доступа в интернет.

i Примечание

Если проверка доступа в интернет настроена на каждом узле кластера и на всех узлах доступ в интернет отсутствует, перенос роли мастер-узла не выполняется, происходит прекращение обмена VRRP-сообщениями, и кластер отказоустойчивости приостанавливает работу.

- Сбой в работе ПО UserGate NGFW.

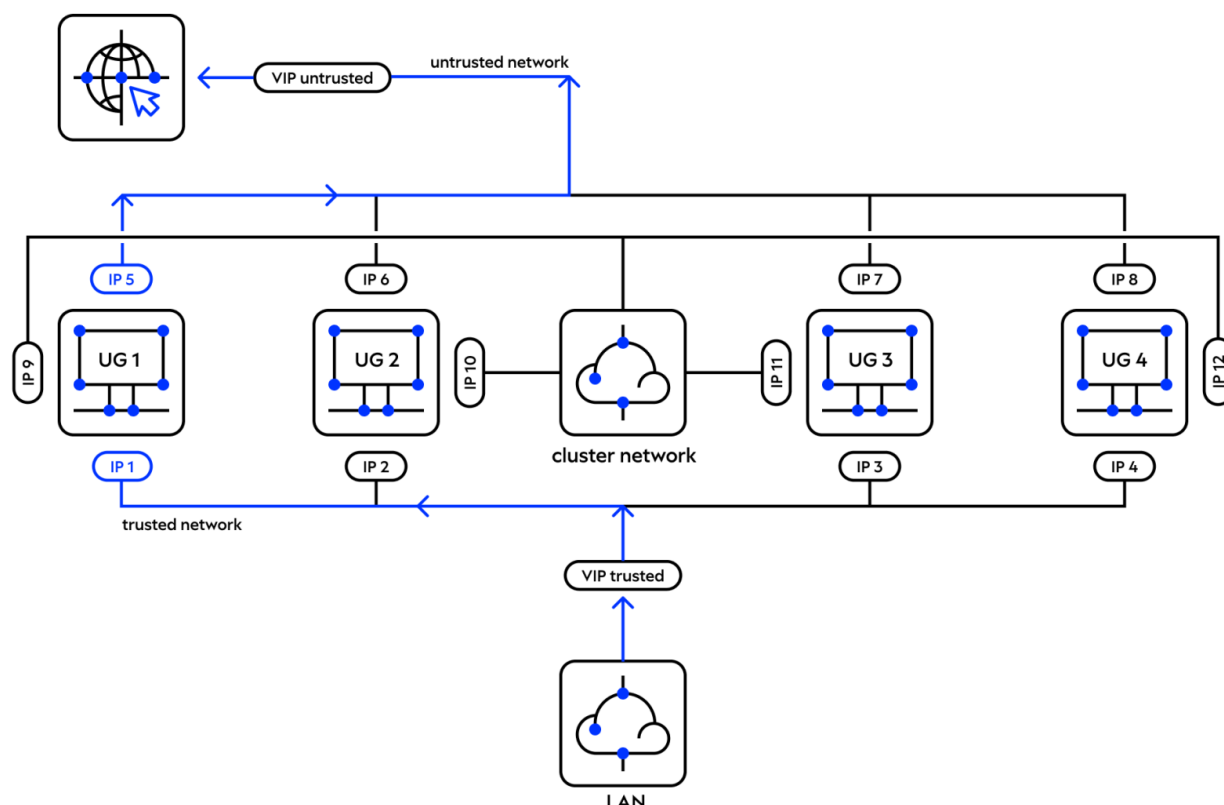
i Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на резервный узел при переключении, устройству UserGate NGFW посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается UserGate NGFW каждую минуту, в том числе при переключении роли мастер-узла на резервный узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме «активный — пассивный». Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и виртуальный cluster IP (VIP trusted).
- Зона **Untrusted**: IP5, IP6, IP7, IP8 и виртуальный cluster IP (VIP untrusted).
- Зона **Cluster**: IP9, IP10, IP11, IP12. Интерфейсы в зоне **Cluster** являются кластерными и используются для передачи VRRP-объявлений.

Оба виртуальных IP-адреса находятся на узле **UG1**. Если узел **UG1** становится недоступным, то оба кластерных IP-адреса перейдут на следующий узел, который станет мастер-узлом, например на **UG2**.



Кластер отказоустойчивости «активный — активный»

В режиме работы кластера «активный — активный» один из межсетевых экранов выступает в роли мастер-узла, распределяющего трафик на все остальные узлы кластера. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает кластерные IP-адреса. Между кластерными интерфейсами передаются VRRP-объявления — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии. На основании VRRP-объявлений оценивается связность кластера, а также уточняются приоритеты всех узлов кластера.

На другие сетевые интерфейсы узлов кластера назначаются виртуальные IP-адреса, на которые направляется трафик. Виртуальные IP-адреса всегда находятся на интерфейсах мастер-узла, поэтому мастер-узел получает ARP-запросы клиентов и отвечает на них, последовательно отдавая MAC-адреса всех узлов отказоустойчивого кластера, обеспечивая равномерное распределение трафика на все узлы кластера и учитывая при этом необходимость неразрывности пользовательских сессий.

i Примечание

Балансировка трафика будет работать только в одном широковещательном домене. Например, если для клиентов виртуальный IP-адрес будет шлюзом по умолчанию, балансировка трафика будет работать, так как разным клиентам будут поочередно отдаваться разные MAC-адреса узлов. Но в случае если между UserGate NGFW и клиентами находится маршрутизатор, балансировка работать не будет, так как ARP-запрос на виртуальный IP-адрес отправит только маршрутизатор и ему вернется MAC-адрес только одного из узлов, через который он и отправит весь трафик.

При переключении мастер-роли на дополнительный узел на него переносятся все виртуальные IP-адреса всех интерфейсов. Безусловное переключение роли происходит при следующих событиях:

- Дополнительный узел не получает подтверждения того, что мастер-узел находится в сети, например если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (см. раздел «[Настройка шлюзов](#)»), и ни через один из шлюзов нет доступа в интернет.
- Сбой в работе ПО UserGate NGFW.

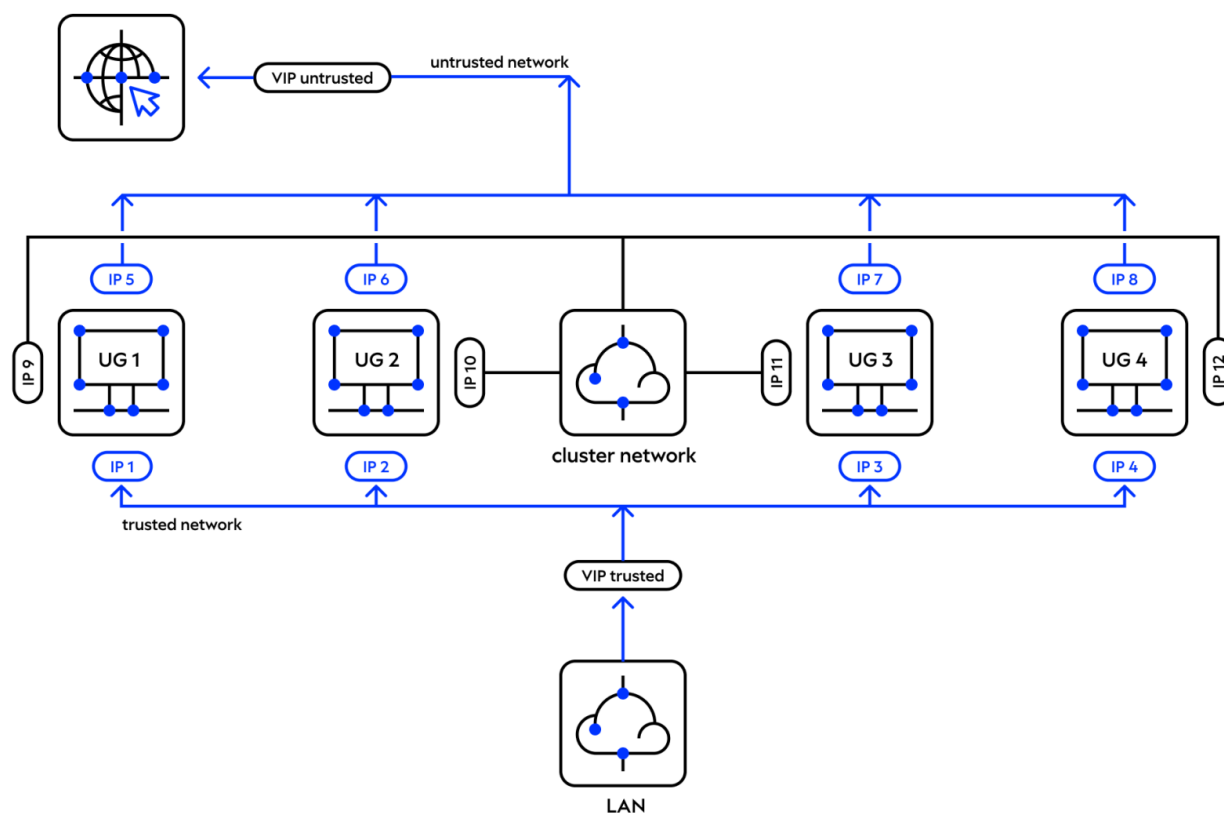
i Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на дополнительный узел при переключении, UserGate NGFW посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме «активный — активный» пакет GARP отсылается UserGate NGFW только при переключении роли мастер-узла на дополнительный узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме «активный — активный». Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и виртуальный cluster IP (VIP trusted).
- Зона **Untrusted**: IP5, IP6, IP7, IP8 и виртуальный cluster IP (VIP untrusted).
- Зона **Cluster**: IP9, IP10, IP11, IP12. Интерфейсы в зоне **Cluster** являются кластерными и используются для передачи VRRP-объявлений.

Оба виртуальных IP-адреса находятся на узле **UG1**. Если узел **UG1** становится недоступным, то оба виртуальных IP-адреса перейдут на следующий узел, который станет мастер-узлом, например на узел **UG2**.



i Примечание

Для корректной обработки трафика необходимо, чтобы обратный трафик от сервера к клиенту возвращался через тот же узел UserGate NGFW, через который он был инициирован от клиента, то есть чтобы сессия пользователя всегда проходила через один и тот же узел кластера. Самое простое решение этой задачи — использование NAT, ведущего из сети клиента в сеть сервера (NAT из зоны Trusted в зону Untrusted).

Настройка кластера отказоустойчивости

Настройка кластера отказоустойчивости доступна только для узлов, входящих в кластер конфигурации.

Чтобы настроить кластер отказоустойчивости:

1. В разделе **Настройки → Сеть → Зоны** выберите зону, в которой планируется добавлять кластерные интерфейсы (зона **Cluster** на рисунках выше), и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешите сервис **VRRP**.
2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между узлами кластера:
 - Выберите сетевой интерфейс, который будет участвовать в организации кластера.
 - В окне **Свойства интерфейса** на вкладке **Общие** установите флажок **Включено** и назначьте интерфейсу кластерную зону.
 - На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.
3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.
4. В окне **Свойства кластера отказоустойчивости** на вкладке **Общие** установите флажок **Включено**, введите название кластера и выберите режим кластера:
 - **Активный — Пассивный** (значение по умолчанию) — трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен.
 - **Активный — Активный** — нагрузка распределяется мастер-узлом на остальные узлы кластера.
5. На вкладке **Узлы** в блоке **Доступные узлы** выберите от двух до четырех узлов, затем в блоке **Настройка кластера** назначьте одному из узлов роль мастер-узла.

i Примечание

Если установлен флажок «Не учитывать приоритет при смене роли мастер-узла», понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя.

6. На вкладке **Виртуальные IP-адреса** нажмите **Добавить** и назначьте интерфейсам узлов кластера, не участвующим в организации кластера и находящимся в одной зоне, общий виртуальный IP-адрес, на который будет

направляться трафик. (На рисунках выше это один виртуальный IP-адрес для интерфейсов в зоне **Trusted** и еще один для интерфейсов в зоне **Untrusted**.)

7. Если необходимо, на вкладке **Общие** в блоке **Режим отправки служебного трафика** выберите режим обмена служебным трафиком между узлами кластера.

i Примечание

Доступность режима «Юникаст» зависит от выбранного режима работы кластера (см. таблицу ниже).

8. Если необходимо, настройте остальные параметры (см. таблицу ниже).

9. Сохраните изменения. В созданном кластере отказоустойчивости одному из узлов будет назначена роль мастер-узла, а на его сетевой интерфейс будет назначен указанный виртуальный IP-адрес.

10. Укажите виртуальный IP-адрес для узлов `auth.captive`, `logout.captive`, `block.captive`, `ftpclient.captive`. Если вы хотите использовать авторизацию с помощью captive-портала, необходимо, чтобы системные имена узлов `auth.captive` и `logout.captive`, которые используются процедурами авторизации в Captive, преобразовывались (`resolve`) в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более детально эти параметры описаны в разделе «[Общие настройки](#)».

В таблице описаны дополнительные параметры кластера отказоустойчивости.

Параметр	Описание
Вкладка Общие	
Описание	Описание кластера отказоустойчивости
Идентификатор виртуального маршрутизатора (VRID)	Идентификатор, уникальный для каждого VRRP-кластера в локальной сети. Если в сети нет сторонних VRRP-кластеров, рекомендуется оставить значение по умолчанию
Режим отправки служебного трафика	Выбор режима обмена служебным трафиком между узлами кластера: • Мультикаст — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. По умолчанию для отправки VRRP-объявлений назначены

Параметр	Описание
	интерфейсы кластера конфигурации. Вы можете выбрать другие интерфейсы. • Юникаст — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера на вкладке Узлы
Интервалы отправки и задержки	Параметры переключения роли мастер-узла на резервный узел: • Периодичность VRRP-объявлений — интервал в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. • Счетчик недоступности — количество интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. • Задержка смены роли по приоритету — время, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Эта задержка предоставляет время для сбора информации (например, о маршрутах) и позволяет избежать сбоев в работе сразу после переключения роли мастер-узла
Использовать виртуальный MAC	Если флажок установлен и на соответствующей вкладке параметров кластера отказоустойчивости назначены виртуальные IP-адреса, узлу с ролью мастер-узла назначается виртуальный MAC-адрес кластера. После этого в разделе Настройки → Сеть → Интерфейсы отобразится интерфейс VMAC. В случае переноса мастер-роли на резервный узел этот MAC-адрес сохраняется, что позволяет избежать задержек в передаче трафика. Доступно только в режиме работы кластера «активный — пассивный»
Разрешить транзит трафика через пассивные узлы	Если флажок установлен, резервный узел будет обрабатывать транзитный трафик, который поступает на его интерфейсы. В целях безопасности вы можете запретить обработку этого трафика, при снятом флажке он будет отбрасываться.

Параметр	Описание
	Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный»
Вкладка Синхронизация сессий	
Синхронизировать сессии TCP, SCTP и DCCP	Включение и отключение синхронизации пользовательских сессий между узлами по протоколам TCP, SCTP, DCCP
Синхронизировать сессии UDP и ICMP	Включение и отключение синхронизации пользовательских сессий между узлами по протоколам UDP и ICMP. Доступно, если установлен флажок Синхронизировать сессии TCP, SCTP и DCCP
Мультикаст-идентификатор	Если в одном кластере конфигурации создано несколько кластеров отказоустойчивости, для синхронизации сессий будет использоваться мультикастовый IP-адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор. Доступно, если установлен флажок Синхронизировать сессии TCP, SCTP и DCCP и на вкладке Общие выбран мультикастовый режим доставки
Интерфейсы синхронизации узла	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме.  Важно! В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий. Доступно, если установлен флажок Синхронизировать сессии TCP, SCTP и DCCP и на вкладке Общие выбран мультикастовый режим доставки
Исключенные из синхронизации IP-адреса	Список IP-адресов, с которыми отключена синхронизация всех пользовательских сессий в мультикастовом режиме. Доступно, если установлен флажок Синхронизировать сессии TCP, SCTP и DCCP и на вкладке Общие выбран мультикастовый режим доставки

Диагностика узлов кластера отказоустойчивости

Доступность узлов кластера определяется в том числе исходя из результатов диагностики состояния узлов. По умолчанию выполняется проверка состояния узлов кластера, локального DNS-сервера, прокси-сервера и кластерных интерфейсов узлов. Дополнительно вы можете например включить диагностику шлюзов или проверку доступа к сервисам, развернутым в ИТ-инфраструктуре, через узлы кластера.

Результаты диагностики влияют на условия переноса роли мастер-узла на резервный узел. По умолчанию перенос роли происходит без учета приоритета узлов. Например, при отключении одного из сетевых интерфейсов мастер-узла весь мастер-узел считается недоступным.

Вы можете настроить параметры таким образом, чтобы перенос роли мастер-узла зависел от понижения его приоритета при отключении одного или нескольких кластерных интерфейсов. Перенос роли мастер-узла на резервный узел произойдет, если приоритет последнего окажется выше приоритета мастер-узла. По умолчанию приоритет, назначенный мастер-узлу, равен 250, приоритет резервного узла — 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, который физически не подключен к сети. Соответственно, если на кластере отказоустойчивости, состоящем из двух узлов, один из интерфейсов на мастер-узле будет физически отключен от сети, резервный узел станет мастер-узлом (при условии, что на резервном узле все кластерные интерфейсы подключены к сети). В таком случае приоритет мастер-узла будет равен 248, приоритет резервного — 249. При восстановлении физического подключения на первоначальном мастер-узле этот узел снова станет мастер-узлом, поскольку его приоритет вернется в значение 250.

Примечание

Отключение одного или нескольких кластерных интерфейсов на резервном узле также будет понижать его приоритет. Тем не менее этот резервный узел может стать мастер-узлом при безусловном переключении роли или в случае, если приоритет мастер-узла станет меньше приоритета резервного узла.

Чтобы настроить диагностику узлов кластера:

1. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** выберите кластер и нажмите **Редактировать**.
2. В окне **Свойства кластера отказоустойчивости** выберите вкладку **Диагностика**.

3. Установите флажок **Проверка шлюзов** и выберите, считать шлюз недоступным или понизить приоритет узла, если результаты проверки будут неудовлетворительными.

i Примечание

Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. Подробнее об этом — в разделе «[Настройка шлюзов](#)».

4. Настройте параметры проверки доступности шлюзов:

- **Периодичность запуска проверки** — регулярная проверка шлюзов через указанный промежуток времени.
- **Счетчик недоступности** — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается.
- **Счетчик доступности** — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет.

5. Установите флажок **Проверка ресурсов** и выберите, считать узел недоступным или понизить приоритет узла, если проверка покажет, что указанные сервисы, развернутые в ИТ-инфраструктуре, недоступны.

6. Нажмите **Проверяемые ресурсы** и укажите IP-адреса или FQDN тех ресурсов, доступ к которым будет проверяться.

7. Настройте параметры проверки доступности ресурсов:

- **Периодичность запуска проверки** — регулярная проверка ресурсов через указанный промежуток времени.
- **Счетчик недоступности** — количество последовательных результатов проверки, после которых узел признается недоступным или его приоритет понижается.
- **Счетчик доступности** — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет.

8. Установите флажок **Проверка интерфейсов**, нажмите **Настройки** и настройте следующие параметры:

- Для каждого из кластерных интерфейсов выберите действие, которое будет применено к узлу в случае недоступности интерфейса.
- Если необходимо отслеживать состояние сетевых интерфейсов, на которые назначены виртуальные IP-адреса, нажмите **Добавить**, выберите соответствующие сетевые интерфейсы и действия для них в случае недоступности.

9. Сохраните изменения.

Настройка кластера отказоустойчивости в облачной среде Yandex Cloud

Вы можете настроить кластер отказоустойчивости UserGate NGFW в сервисе Yandex Cloud. Кластер отказоустойчивости, развернутый в облаке, может включать в себя только два узла, работающих в режиме «активный — пассивный», и поддерживает обмен служебными VRRP-объявлениями в юникаст-режиме.

Работа кластера отказоустойчивости в облачной среде возможна при соблюдении всех следующих условий:

- В кластере только два узла.
- Выбран режим работы кластера «активный — пассивный».
- Обмен служебным трафиком между узлами кластера выполняется в юникаст-режиме.
- Отключено использование виртуального MAC-адреса.
- Интерфейсам узлов кластера не назначены виртуальные IP-адреса.
- Отключена синхронизация пользовательских сессий.
- Маршрутизация входящего трафика выполняется внешним балансировщиком.
- Обеспечен доступ к таблицам маршрутизации Yandex Cloud и к API для работы с виртуальным частным облаком.

Перед тем как настроить параметры работы кластера UserGate NGFW, подготовьте виртуальные машины в облачной среде:

1. Создайте в Yandex Cloud сервисный аккаунт с ролью `vpc.privateAdmin`.
2. Разверните в Yandex Cloud две виртуальные машины UserGate NGFW и объедините их в кластер конфигурации.

i Примечание

Сервис Yandex Cloud поддерживает развертывание виртуальных машин как в одной сетевой зоне, так и в разных. Подробнее об этом — в [справке сервиса](#).

3. В веб-интерфейсе сервиса Yandex Cloud в параметрах каждой виртуальной машины добавьте созданный сервисный аккаунт.
4. Создайте таблицу маршрутизации Yandex Cloud. Когда кластер отказоустойчивости будет настроен, UserGate NGFW передаст в эту таблицу IP-адрес сетевого интерфейса мастер-узла, через который будет направляться трафик. В случае если мастер-узел выйдет из строя, в таблицу статической маршрутизации Yandex Cloud будет передан IP-адрес резервного узла, и трафик перенаправится на этот IP-адрес.

Чтобы настроить кластер отказоустойчивости в облачной среде:

1. В разделе **Настройки → Сеть → Зоны** выберите или создайте зону для кластера и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешите сервис **VRRP**.
2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между узлами кластера:
 - Выберите сетевой интерфейс, который будет участвовать в организации кластера.
 - В окне **Свойства интерфейса** на вкладке **Общие** назначьте интерфейсу кластерную зону.
 - На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.
 - Убедитесь, что на вкладке **Общие** установлен флажок **Включено**.
3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.
4. В окне **Свойства кластера отказоустойчивости** на вкладке **Узлы** в блоке **Доступные узлы** выберите виртуальные машины, развернутые в Yandex

Cloud, затем в блоке **Настройка кластера** назначьте одной из виртуальных машин роль мастер-узла.

5. Убедитесь, что на вкладке **Виртуальные IP-адреса** интерфейсам узлов кластера не назначены виртуальные IP-адреса.

6. На вкладке **Общие** установите флажок **Включено**, введите название кластера и выберите режим кластера **Активный — Пассивный**.

7. В качестве режима отправки служебного трафика выберите **Юникаст** и нажмите **Настройки**.

8. В окне **Настройка интерфейсов для юникаст-трафика** в блоке **Передача VRRP-объявлений** выберите интерфейсы, которые были настроены на шаге 2, укажите их IP-адреса и сохраните изменения.

9. Убедитесь, что на вкладке **Общие** снят флажок **Использовать виртуальный MAC**.

10. Убедитесь, что на вкладке **Синхронизация сессий** сняты флажки сняты флажки **Синхронизировать сессии TCP, SCTP и DCCP** и **Синхронизировать сессии UDP и ICMP**.

11. На вкладке **Настройка облака** выберите в качестве облачного провайдера **Yandex Cloud**.

12. В блоке **Переключение маршрута** нажмите **Добавить** и в окне **Свойства переключения маршрута** настройте параметры, в соответствии с которыми в таблицу статической маршрутизации будет передаваться IP-адрес мастер-узла:

- В поле **Таблица маршрутизации** укажите идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud.
- В поле **Префикс назначения** укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud.
- В поле **<имя_узла_кластера_1>** для первого узла кластера укажите IP-адрес интерфейса, через который доступна внутренняя сеть.
- В поле **<имя_узла_кластера_2>** для второго узла кластера укажите IP-адрес интерфейса, через который доступна внутренняя сеть, и сохраните изменения параметров переключения маршрута.

13. Сохраните изменения.

После сохранения изменений в таблицу статической маршрутизации Yandex Cloud с указанным идентификатором будут переданы префикс назначения и IP-адрес того узла, которому на вкладке **Узлы** назначена роль мастер-узла. Трафик будет направлен на IP-адрес мастер-узла.

Особенности настройки кластера отказоустойчивости с узлами в разных зонах Yandex Cloud

В зависимости от топологии и других особенностей ИТ-инфраструктуры вы можете настроить кластер отказоустойчивости, в котором узлы UserGate NGFW будут располагаться в разных зонах Yandex Cloud. В этом случае, помимо общей настройки кластера, для каждого из узлов необходимо указать статические маршруты до подсети, находящейся за узлом в другой зоне. В противном случае активный узел кластера не сможет передавать ответы на запросы, поступающие из подсети в другой зоне.

Для каждого узла кластера выполните следующие действия:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** нажмите **Добавить**.
2. В раскрывающемся списке выберите **Статические маршруты** и нажмите **Добавить**.
3. В окне **Свойства маршрута** укажите его название, установите флажок **Включено**.
4. Убедитесь, что установлен тип маршрута **Unicast**.
5. В поле **Адрес назначения** укажите подсеть за другим узлом кластера, на которую будет указывать маршрут.
6. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с узла, для которого настраивается маршрут.
7. Выберите сетевой интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate NGFW сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.
8. Сохраните изменения.

Просмотр информации о кластере отказоустойчивости

Вся информация о кластере доступна на странице **Кластеры отказоустойчивости**. Вы можете отслеживать состояние кластера отказоустойчивости и узлов, входящих в него.

Статусы кластера отказоустойчивости:

- Зеленый: кластер доступен.
- Оранжевый: неопределенное состояние кластера, как минимум один узел не участвует в работе кластера.
- Желтый треугольник: нет связи как минимум с одним узлом кластера, узел перезагружается или вышел из строя.

Статусы узлов в кластере отказоустойчивости:

- Зеленый: узел кластера доступен.
- Оранжевый: узел работоспособен, но недоступен в кластере.
- Желтый треугольник: узел перезагружается или вышел из строя.

Также в веб-консоли выбранного узла на странице **Кластеры отказоустойчивости** вы можете временно вывести этот узел из кластера, например для планового обслуживания. Для этого в блоке **Узлы** необходимо включить **Приостановить работу**.

НАСТРОЙКА СЕТИ

Настройка зон

Зона в UserGate NGFW — это логическое объединение сетевых интерфейсов. Политики безопасности UserGate NGFW используют зоны интерфейсов, а не непосредственно интерфейсы. Это дает необходимую гибкость политикам безопасности, а также существенно упрощает управление отказоустойчивым кластером. Зоны одинаковы на всех узлах кластера, то есть данная настройка является глобальной для кластера.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов, подключенных к сети партнера и т. п.

По умолчанию NGFW поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление NGFW.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей.
Untrusted	Зона для интерфейсов, подключенных к недоверенным сетям, например, к интернету.
DMZ	Зона для интерфейсов, подключенных к сети DMZ.
Cluster	Зона для интерфейсов, используемых для работы кластера.
VPN for Site-to-Site	Зона, в которую помещаются все клиенты типа Офис-Офис, подключаемые к NGFW по VPN.
VPN for remote access	Зона, в которую помещаются все мобильные пользователи, подключаемые к NGFW по VPN.
Tunnel inspection zone	Зона для инспектирования туннелей. Зона, которой будут принадлежать все адреса источников и назначения инкапсулированных в туннель пакетов.

Вы можете изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.



Примечание

Можно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону.	В разделе Сеть → Зоны нажать на кнопку Добавить и дать название зоне.

Наименование	Описание
Шаг 2. Настроить параметры защиты зоны от DoS (опционально).	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • Агрегировать — если установлено, то считаются все пакеты, входящие в интерфейсы данной зоны. Если не установлено, то считаются пакеты отдельно для каждого IP-адреса. • Порог уведомления — при превышении количества запросов над указанным значением происходит запись события в системный журнал. • Порог отбрасывания пакетов — при превышении количества запросов над указанным значением NGFW начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 3000 запросов в секунду, для порога отбрасывания пакетов — 6000 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах, за исключением интерфейсов зоны Cluster. Необходимо увеличить пороговое значение отбрасывания пакетов для протокола UDP, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN. Исключения защиты от DoS — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для сервиса IP-телефонии, так как он шлет большое количество UDP-пакетов. Важно! NGFW позволят произвести более гранулированную защиту от DoS атак. Для получения дополнительной информации обратитесь в раздел Защита от DoS атак.
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые NGFW сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • Ping — позволяет пинговать NGFW. • SNMP — доступ к NGFW по протоколу SNMP (UDP 161). • Captive-портал и страница блокировки — необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • XML-RPC для управления — позволяет управлять продуктом по API (TCP 4040).

Наименование	Описание
	• Кластер — сервис, необходимый для объединения нескольких узлов NGFW в кластер (TCP 4369, TCP 9000-9100). • VRRP — сервис, необходимый для объединения нескольких узлов NGFW в отказоустойчивый кластер (IP протокол 112). • Консоль администрирования — доступ к веб-консоли управления (TCP 8001). • DNS — доступ к сервису DNS-прокси (TCP 53, UDP 53). • HTTP(S)-прокси — доступ к сервису HTTP(S)-прокси (TCP 8090). • Агент авторизации — доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • SMTP(S)-прокси — сервис фильтрации SMTP-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • POP3(S)-прокси — сервис фильтрации POP3-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • CLI по SSH — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN — доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • Reverse-прокси — сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Более подробно смотрите раздел Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. • Web-портал — сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Более подробно смотрите раздел Веб-портал. • Log Analyzer/SIEM — сервис для подключения к анализатору журналов Log Analyzer (TCP 2023 и 9713). • OSPF — сервис динамической маршрутизации OSPF. Более подробно смотрите раздел OSPF. • BGP — сервис динамической маршрутизации BGP. Более подробно смотрите раздел BGP. • RIP — сервис динамической маршрутизации RIP. • BFD — сервис быстрого обнаружения сбоев в сетевом соединении. • SNMP-прокси — сервис используется для построения распределённой системы мониторинга (позволяет

Наименование	Описание
	регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • SSH-прокси — сервис, использующийся для инициирования трафика SSH. • Multicast — сервис мультикаста. • NTP сервис — разрешает доступ к сервису точного времени, запущенному на сервере NGFW. • UserID syslog коллектор — сервис для разрешения получения информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт TCP 514). • Подключение конечных устройств — сервис, использующийся для разрешения подключения конечных устройств с установленным ПО UserGate Client (TCP 4045). • API XML RPC поверх HTTPS — разрешает доступ к API поверх HTTPS (TCP 4443). Доступен в версии 7.3.3 и выше. Подробнее о требованиях сетевой доступности читайте в приложении Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально).	Атаки на основе IP-спуфинга позволяют передать пакет из внешней сети, например, из Untrusted, во внутреннюю, например, в Trusted. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес внутренней сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены. С помощью чекбокса Инвертировать администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, для зоны Untrusted можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 и включить опцию Инвертировать.
Шаг 5. Настроить параметры ограничения сессий (опционально).	Ограничение количества одновременных подключений с одного IP-адреса — это мера безопасности, которая ограничивает количество активных соединений сети, исходящих от одного и того же IP-адреса. Это делается по нескольким причинам: • Защита от атак: злоумышленники могут использовать большое количество одновременных подключений с

Наименование	Описание
	одного IP-адреса для проведения DDoS-атак (распределенные атаки, целью которых является отказ системы в обслуживании). Ограничение количества подключений помогает снизить риск таких атак, уменьшая нагрузку на сеть или сервер. • Предотвращение злоупотреблений: некоторые пользователи могут пытаться злоупотреблять ресурсами, путем создания множества одновременных подключений. Ограничение подключений помогает предотвратить избыточное использование ресурсов и поддерживать равномерное распределение нагрузки. • Сохранение доступности: предотвращение ситуаций, когда один пользователь занимает все доступные ресурсы, оставляя мало места для других пользователей. Введение ограничений способствует поддержанию доступности ресурсов для всех пользователей. • Управление ресурсами: более эффективное управление сетевыми и серверными ресурсами, обеспечивая более стабильную и предсказуемую производительность. Для ограничения количества одновременных подключений с одного IP-адреса необходимо: 1. Активировать чекбокс Включить ограничение сессий на IP-адрес. 2. Указать максимально возможное количество сессий с одного адреса. 3. Добавить список IP-адресов, для которых данное ограничение не будет действовать. Подробнее о создании списка смотрите в разделе IP-адреса.

Настройка интерфейсов

В разделе веб-консоли **Настройки → Сеть → Интерфейсы** отображаются все физические и виртуальные интерфейсы, имеющиеся в системе. Если узел является частью кластера, в разделе отображаются также интерфейсы других узлов кластера.

Примечание

Для модели ПАК UserGate FG в разделе веб-консоли «Настройки» → «Сеть» → «Интерфейсы» по умолчанию отображаются только физические сетевые интерфейсы (адаптеры). Для отображения логических интерфейсов нажмите «Типы интерфейса» в меню рабочей области раздела и выберите нужные для отображения типы интерфейсов.

В этом разделе вы можете настраивать параметры имеющихся интерфейсов или добавлять новые логические интерфейсы различных типов.

Для настройки параметров имеющегося в системе интерфейса выберите его в списке и нажмите **Редактировать**. В окне свойств интерфейса вы можете редактировать следующие параметры:

- Состояние интерфейса — включен или отключен.
- Тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
- Зона, к которой относится интерфейс.
- Профиль NetFlow для отправки статистических данных на NetFlow-коллектор.
- Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol. Доступен только для физических сетевых интерфейсов.
- Алиас (псевдоним) — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.
- Физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, получаемый по DHCP.
- Параметры работы DHCP-ретранслятора. Для работы DHCP-ретранслятора его необходимо включить на вкладке **DHCP-релей**, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется

функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Для добавления в систему нового логического интерфейса нажмите **Добавить** и выберите тип логического интерфейса:

- VLAN;
- бонд-интерфейс;
- мост;
- PPPoE;
- VPN;
- туннельный интерфейс;
- loopback.

Создание VLAN-интерфейса

Для создания VLAN-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить VLAN** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение VLAN-интерфейса
Название	Название VLAN-интерфейса. Название присваивается автоматически на основе имени физического порта и тега VLAN
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Описание	Опциональное описание интерфейса
Тип интерфейса	Выбор типа интерфейса — Layer 3 или Mirror . Интерфейсу, работающему в режиме Layer 3 , можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror , может получать трафик со SPAN-порта сетевого оборудования для его анализа

Параметр	Описание
Tag VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов
Имя узла	Имя узла в кластере, на котором создается данный VLAN-интерфейс
Интерфейс	Физический интерфейс, на котором создается VLAN-интерфейс
Зона	Зона, которой принадлежит VLAN-интерфейс
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов Важно! Значение параметра не может содержать символы кириллицы.
Сеть	Способ присвоения IP-адреса (Режим) — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии 7.3.0 и выше)
DHCP-релей	Настройка работы DHCP-ретранслятора на VLAN-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько серверов DHCP, на которые необходимо пересылать DHCP-запросы клиентов

Создание бонд-интерфейса

Вы можете объединить несколько физических интерфейсов в один логический агрегированный бонд-интерфейс с целью повышения пропускной способности или отказоустойчивости канала.

Для создания бонд-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить бонд-интерфейс** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение бонд-интерфейса
Название	Название бонд-интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Имя узла	Имя узла в кластере, на котором создается данный бонд-интерфейс
Зона	Зона, которой принадлежит бонд-интерфейс
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов  Важно! Значение параметра не может содержать символы кириллицы.
Интерфейсы	Интерфейс или интерфейсы, которые будут использованы для построения бонд-интерфейса
Режим	Режим работы бонд-интерфейса должен совпадать с режимом работы интерфейса на соседнем устройстве, к которому он подключается. Доступные режимы работы: • Round robin. Режим применяется с целью балансировки нагрузки и обеспечения отказоустойчивости. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. • Active backup. Режим применяется с целью обеспечения отказоустойчивости. Активен только один сетевой интерфейс из всех объединенных интерфейсов. Переключение на резервный

Параметр	Описание
	интерфейс происходит исключительно при отказе активного. В целях корректной работы с сетевым оборудованием MAC-адрес бонд-интерфейса анонсируется через один физический порт. • XOR. Режим применяется с целью балансировки нагрузки и обеспечения отказоустойчивости. Для распределения трафика между интерфейсами используется функция, которая на основе MAC-адресов источника и назначения определяет, через какой интерфейс отправить пакет. Это гарантирует, что весь трафик между одной парой устройств будет идти через один и тот же физический интерфейс, сохраняя порядок пакетов. Алгоритм распределения передачи пакетов можно уточнить с помощью политики xmit hash. • Broadcast. Режим применяется с целью обеспечения отказоустойчивости. Передача пакетов осуществляется на все сетевые интерфейсы. • IEEE 802.3ad. Режим работы, установленный по умолчанию. Поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых интерфейсов с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать политику <code>xmit_hash</code>. • Adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загруженности каждого сетевого интерфейса (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущий сетевой интерфейс. Если сетевой интерфейс выходит из строя, другой берет себе MAC-адрес вышедшего из строя интерфейса. • Adaptive load balancing. Основываясь на механизме предыдущего режима, дополнительно осуществляя балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых интерфейсов вовне, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевого интерфейса, участвующего в объединении. Таким образом, различные соседние устройства используют различные MAC-адреса сервера.

Параметр	Описание
	Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами
MII monitoring period (мсек)	Периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 (MII-мониторинг отключен)
Down delay (мсек)	Задержка (в миллисекундах) перед отключением интерфейса при обнаружении сбоя. Параметр применяется исключительно при использовании мониторинга MII (miimon). Значение задержки должно быть кратно интервалу опроса miimon, в противном случае оно будет автоматически округлено до ближайшего кратного значения. Значение по умолчанию — 0
Up delay (мсек)	Задержка (в миллисекундах) перед включением интерфейса после восстановления соединения. Параметр действует только при использовании мониторинга MII (miimon). Значение задержки должно быть кратно интервалу опроса miimon, в противном случае оно будет автоматически округлено до ближайшего кратного значения. Значение по умолчанию — 0
LACP rate	Интервал отправки LACPDU-пакетов в режиме 802.3ad. Возможные значения: • Slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • Fast — запрос партнера на передачу LACPDU-пакетов каждую секунду
Failover MAC	Параметр определяет, какой MAC-адрес будет использоваться виртуальным bond-интерфейсом при отказе одного из физических интерфейсов в режиме Active-backup . Возможные значения: • Отключено — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • Active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • Follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем

Параметр	Описание
	интерфейсах этот MAC-адрес не устанавливается, пока они находятся в резервном режиме. MAC-адрес назначается во время обработки отказа: если резервный интерфейс становится активным, он принимает новый MAC-адрес (тот, что принадлежит бонд-интерфейсу), а старому активному интерфейсу прописывается MAC-адрес, который принадлежал текущему активному интерфейсу
Xmit hash policy	Параметр определяет алгоритм распределения трафика между активными интерфейсами в режимах балансировки нагрузки бонд-интерфейса XOR или IEEE 802.3ad. Возможные значения: • Layer 2 — используются только MAC-адреса для распределения трафика. При этом алгоритме трафик для конкретного узла будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • Layer 2+3 — используются как MAC-адреса, так и IP-адреса. Алгоритм совместим с IEEE 802.3ad. • Layer 3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP). Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно с версии ПО 7.3.0 и выше)
DHCP-релей	Настройка работы DHCP-ретранслятора на бонд-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Создание моста (bridge-интерфейс)

Сетевой мост (L2) фильтрует трафик между сегментами сети, пересылая только те кадры, MAC-адрес назначения которых находится за пределами сегмента-отправителя.

Вы можете настроить фильтрацию передаваемого через мост контента на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

При создании моста необходимо указать режим его работы — Layer 2 или Layer 3.

В режиме Layer 2 создаваемому мосту не нужно назначать IP-адрес, прописывать маршруты и шлюзы для его корректной работы. В таком режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом режиме невозможно использовать правила защиты почтового трафика.



Внимание!

Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.

В режиме Layer 3 создаваемому мосту необходимо назначить IP-адрес и указать маршруты в сети, подключенные к интерфейсам моста. В таком режиме могут быть использованы все механизмы фильтрации, доступные в UserGate NGFW.

Если мост создается на ПАК UserGate, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить два интерфейса в байпас-мост. Байпас-мост автоматически переключает два выбранных интерфейса в режим байпас (закорачивает их, пропуская весь трафик мимо NGFW) в случаях, если:

- Электропитание ПАК отключено.
- Система внутренней диагностики обнаружила сбой в работе программного обеспечения. Тайм-аут срабатывания при обнаружении сбоя — 10 секунд.

Управление работой байпас-реле сетевых портов доступно через интерфейс командной строки PMC (подробнее — в разделе [«Команды управления платформой»](#) руководства PMC CLI).

Подробнее о сетевых интерфейсах, поддерживающих режим байпас, смотрите в руководствах по эксплуатации на модели [ПАК UserGate NGFW](#).

Для создания моста:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить мост** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Имя узла	Имя узла в кластере, на котором создается bridge-интерфейс
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, к которой принадлежит интерфейс
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов  Важно! Значение параметра не может содержать символы кириллицы.
Интерфейсы моста	Два интерфейса, которые будут использованы для построения моста
Интерфейсы байпас-моста	Пара интерфейсов, которые можно использовать для построения байпас-моста. Требуется поддержка оборудования ПАК UserGate NGFW
	Использование алгоритма STP для защиты сети от петель

Параметр	Описание
STP (Spanning Tree Protocol)	
Forward delay	Задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP
Maximum age	Время, по истечении которого STP-соединение считается потерянным
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить размер MTU, размер MSS (доступно в версии 7.3.0 и выше)
DHCP-релей	Настройка работы DHCP-ретранслятора на bridge-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Создание PPPoE-интерфейса

PPPoE (Point-to-point protocol over Ethernet) — сетевой протокол канального уровня передачи кадров PPP через Ethernet.

Для создания PPPoE-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить PPPoE** и настройте параметры интерфейса.

Параметры	Описание
Включено	Включение PPPoE-интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается PPPoE-интерфейс

Параметры	Описание
Интерфейс	Интерфейс, на котором будет создаваться PPPoE-интерфейс
Зона	Зона, к которой принадлежит PPPoE-интерфейс
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов  Важно! Значение параметра не может содержать символы кириллицы.
MTU	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet
MSS	Размер MSS. Корректные значения: 0 или число в диапазоне от 4 до значения, полученного по формуле (MTU - 40). Параметр доступен в версии 7.3.0 и выше
Логин	Имя пользователя для соединения PPPoE
Пароль	Пароль пользователя для соединения PPPoE
Переподключаться автоматически	Повторное автоматическое установление соединения при обрыве связи

Параметры	Описание
Тип аутентификации	Протоколы аутентификации, используемые в протоколе PPP: • CHAP (Challenge Handshake Authentication Protocol) — протокол аутентификации с косвенным согласованием. Алгоритм проверки подлинности, предусматривающий передачу не самого пароля пользователя, а косвенных сведений о нем. • PAP (Password Authentication Protocol) — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удаленного доступа открытым текстом (без шифрования)
Интервал между попытками подключения (сек.)	Интервал времени в секундах между разрывом и повторной попыткой установления соединения
Маршрут по умолчанию	Устанавливает PPPoE-интерфейс в качестве маршрута по умолчанию
Интервал проверки соединения (сек.)	Интервал проверки соединения
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которых UserGate NGFW считает, что соединение отсутствует, и разрывает его
Использовать DNS-сервер провайдера	Если опция включена, то UserGate NGFW использует DNS-серверы, выданные провайдером
Количество попыток подключения	Количество последовательных неудачных попыток подключения, по достижении которого автоматическое восстановление соединения прекращается
PPPoE-сервис	Имя сервиса указывается, если его предоставил провайдер. Если имя сервиса не используется, поле необходимо оставить пустым

Создание VPN-интерфейса

Виртуальный сетевой интерфейс используется для подключения VPN-клиентов. Этот тип интерфейса является кластерным — он будет автоматически создаваться на всех узлах UserGate NGFW, входящих в кластер конфигурации. При наличии кластера отказоустойчивости VPN-клиенты будут автоматически

переключаться на запасной узел в случае отказа активного узла без разрыва существующих VPN-соединений.

Для создания VPN-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить VPN** и настройте параметры интерфейса.

Параметр	Описание
Название	Название интерфейса в виде <code>tunnelN</code> , где N — порядковый номер VPN-интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Описание	Описание интерфейса
Зона	Зона, которой принадлежит интерфейс. Все клиенты, подключившиеся по VPN к UserGate NGFW, будут также помещены в эту зону
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов Важно! Значение параметра не может содержать символы кириллицы.
Режим	Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс будет применяться для приема VPN-подключений (site-to-site VPN или remote access VPN), необходимо использовать статический IP-адрес. При использовании интерфейса для инициации VPN-подключения (в сценарии site-to-site VPN), необходимо выбрать динамический режим
MTU	Размер MTU для выбранного интерфейса

Параметр	Описание
MSS	Размер MSS. Корректные значения: 0 или число в диапазоне от 4 до значения, полученного по формуле (MTU - 40). Параметр доступен в версии 7.3.0 и выше

По умолчанию в системе созданы три VPN-интерфейса, которые могут быть использованы для организации VPN-подключений:

- **tunnel1** — предназначен для использования на VPN-сервере в сценарии remote access VPN;
- **tunnel2** — предназначен для использования на стороне VPN-сервера в сценарии site-to-site VPN;
- **tunnel3** — предназначен для использования на стороне VPN-клиента (инициатора соединения) в сценарии site-to-site VPN.

Создание туннельного интерфейса

Туннельный интерфейс — это виртуальный сетевой интерфейс, который может использоваться для создания соединения типа «точка-точка» через IP-сеть.

Поддерживаются следующие типы туннельных интерфейсов:

- GRE — протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер IP-протокола — 47.
- IP/IP — это протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. При инкапсуляции одного IP-пакета в другой добавляется внешний заголовок, в котором в качестве IP-адреса источника используется адрес точки входа в туннель, а в качестве IP-адреса назначения — адрес точки выхода из туннеля.
- VXLAN — это протокол туннелирования Layer 2 Ethernet-кадров в UDP-пакеты, порт 4789.

Для создания туннельного интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить туннель** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение или выключение интерфейса

Параметр	Описание
Название	Название интерфейса в виде greN, где N — порядковый номер туннельного интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Описание	Описание интерфейса
Зона	Зона, которой принадлежит интерфейс
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов  Важно! Значение параметра не может содержать символы кириллицы.
Режим	Режим работы туннельного интерфейса — GRE, IPIP, VXLAN
MTU	Размер MTU для выбранного интерфейса
MSS	Размер MSS. Параметр доступен в версии 7.3.0 и выше. Возможные значения: • 0; • для VXLAN — число в диапазоне от 4 до значения, полученного по формуле (MTU - 40); • для IPIP — число в диапазоне от 4 до значения, полученного по формуле (MTU - 60); • для GRE — число в диапазоне от 4 до значения, полученного по формуле (MTU - 64)
Локальный IP	Локальный адрес интерфейса point-to-point
Удаленный IP	Удаленный адрес интерфейса point-to-point
IP интерфейса	IP-адрес, назначенный туннельному интерфейсу
VXLAN ID	Идентификатор VXLAN. Только для типа туннеля VXLAN

Создание loopback-интерфейса

Для создания loopback-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить loopback-интерфейс** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса в виде <code>loopbackN</code> , где <code>N</code> — целое число
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги ». Параметр доступен в версии 7.3.0 и выше
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается интерфейс
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, которой принадлежит интерфейс.
Профиль NetFlow	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о профилях NetFlow — в разделе « Профили NetFlow »
Профиль LLDP	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе « Профили LLDP »
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов  Важно! Значение параметра не может содержать символы кириллицы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Параметр	Описание
	Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии 7.3.0 и выше)
DHCP-релей	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Настройка шлюзов

Для подключения UserGate NGFW к интернету или к ресурсу в другой подсети компании необходимо указать IP-адрес шлюза. Если для подключения к интернету используется несколько провайдеров, необходимо указать несколько шлюзов. Если несколько узлов объединены в кластер конфигурации, настраивать шлюзы необходимо для каждого из узлов.

Пример настройки сети с двумя провайдерами:

- Интерфейс **eth1** с IP-адресом **192.168.11.2** подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом **192.168.11.1**
- Интерфейс **eth2** с IP-адресом **192.168.12.2** подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом **192.168.12.1**

Добавление шлюза

Чтобы добавить шлюз:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Добавить**.
2. В окне **Свойства шлюза** укажите его параметры: название, имя узла UserGate NGFW, сетевой интерфейс (по умолчанию назначается автоматически), виртуальный маршрутизатор и IP-адрес шлюза.

Примечание

Подробнее о виртуальных маршрутизаторах — в разделе «[Виртуальные маршрутизаторы](#)».

3. Установите флажок **Включено** и сохраните изменения.

Настройка балансировки

Если для UserGate NGFW настроены несколько шлюзов для подключения к интернету, вы можете распределять исходящий трафик между шлюзами и таким образом управлять нагрузкой на них. При балансировке трафик в интернет распределяется с учетом весов шлюзов: чем больше вес, тем большая доля трафика идет через шлюз.

Например, если для балансировки настроены два шлюза, сессии будут распределяться между ними по формуле $n1/w1 = n2/w2$, где:

- **n1, n2** — сессии, проходящие через шлюзы;
- **w1, w2** — веса шлюзов.

Чтобы настроить балансировку трафика между шлюзами:

1. В разделе **Настройки → Сеть → Шлюзы** выберите шлюз, который будут участвовать в балансировке, и нажмите **Редактировать**.
2. В окне **Свойства шлюза** укажите вес шлюза, установите флажок **Балансировка** и сохраните изменения.
3. Выполните настройку других шлюзов, участвующих в балансировке.

Исходящий трафик будет распределяться между шлюзами в соответствии с указанными весами.

Настройка проверки сети

В UserGate NGFW предусмотрена проверка доступности шлюзов. По индикаторам на странице **Шлюзы** можно отслеживать, доступен ли шлюз (зеленый индикатор) или нет (красный индикатор). По умолчанию шлюз считается доступным, если UserGate NGFW может получить его MAC-адрес с помощью ARP-запроса. Но доступность шлюза не означает наличие доступа в интернет. Чтобы проверить подключение шлюза к интернету, вы можете включить дополнительную проверку сети.

Проверка сети может быть полезна в следующих случаях:

- Если доступ к интернету предоставляют несколько провайдеров и добавлено несколько шлюзов, вы можете настроить отказоустойчивое соединение с интернетом. Для этого один из шлюзов назначается шлюзом по умолчанию. Если в результате проверки сети будет обнаружено, что доступ в интернет через шлюз по умолчанию отсутствует, трафик будет переведен на запасные шлюзы в порядке их расположения в веб-консоли (смена порядка сортировки в процессе текущей сессии не влияет на процесс выбора шлюза).
- Если настроен кластер отказоустойчивости, проверку сети можно использовать для диагностики узлов кластера. Подробнее об этом — в разделе [«Диагностика узлов кластера отказоустойчивости»](#).

В процессе проверки сети UserGate NGFW с заданной периодичностью отправляет по пять ICMP-запросов на каждый указанный IP-адрес доступа в интернет. Доступность шлюза в этом случае определяется по порогу неудачных ICMP-запросов. Проверка считается успешной, если общее количество неудачных ICMP-запросов, отправленных на все указанные IP-адреса в рамках заданного интервала, не превышает этот порог.

Чем ниже порог, тем строже критерий доступности. Например:

- При пороге в 10% шлюз недоступен, если не прошел хотя бы один запрос.
- При 100% шлюз недоступен, только если не прошли все запросы.

Чтобы настроить проверку сети:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Проверка сети**.
2. В окне **Свойства проверки сети** установите флажок **Включено**.
3. Нажмите кнопку **Добавить** и укажите IP-адреса для проверки доступа в интернет.



Примечание

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8).

4. В поле **Частота проверки** укажите в секундах, с какой периодичностью UserGate NGFW будет отправлять ICMP-запросы на указанные IP-адреса.

5. В поле **Процент неудачных запросов** задайте порог неудачных ICMP-запросов и сохраните изменения.

Индикаторы доступности шлюзов теперь будут отражать результаты проверки сети.

Настройка DHCP

Служба DHCP (Dynamic Host Configuration Protocol) позволяет автоматизировать процесс выдачи сетевых настроек клиентам в локальной сети. В сети с DHCP-сервером каждому сетевому устройству можно динамически назначать IP-адрес, адрес шлюза, DNS.

UserGate NGFW может также выступать в качестве DHCP-ретранслятора, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный DHCP-сервер. Подробнее о настройке DHCP-ретранслятора — в разделе [«Настройка интерфейсов»](#).

В UserGate NGFW можно создать несколько диапазонов адресов для выдачи по DHCP. DHCP работает на каждом узле отказоустойчивого кластера независимо. Для обеспечения отказоустойчивости сервиса DHCP в кластере необходимо настроить DHCP на обоих узлах, указав непересекающиеся диапазоны IP-адресов.

Для создания диапазона DHCP необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного диапазона DHCP.
Узел	Узел кластера, на котором создается данный диапазон.
Интерфейс	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
Диапазон IP	Диапазон IP-адресов, выдаваемый клиентам DHCP.
Маска	Маска подсети, выдаваемая клиентам DHCP.
Время аренды	Время в секундах, на которое выдаются IP-адреса.
Домен	Название домена, выдаваемое клиентам DHCP.

Наименование	Описание
Шлюз	IP-адрес шлюза, выдаваемый клиентам DHCP.
Серверы имен	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
Зарезервированные адреса	MAC-адреса и сопоставленные с ними IP-адреса.
Игнорируемые MAC	Список MAC-адресов, игнорируемых DHCP-сервером.
DHCP PXE boot	Адрес сервера и имя загрузочного файла, передаваемого на запрос PXE boot.
DHCP опции	Номер опции и ее значение (список опций доступен в разделе «Опции DHCP»).

Выданные IP-адреса отображаются в панели **Арендованные адреса**.
Администратор может освободить любой выданный адрес, выделив адрес и нажав на кнопку **Освободить**.

Примечание

Чтобы выдача адресов по DHCP работала на интерфейсе, который находится в зоне с включенной защитой от IP-спуфинга, необходимо в свойствах зоны во вкладке **Защита от IP-спуфинга** указать диапазоны выдаваемых IP-адресов, а также адрес 0.0.0.0.

Настройка DNS

Для корректной работы устройства необходимо, чтобы UserGate NGFW мог разрешать доменные имена в IP-адреса. Укажите корректные IP-адреса серверов DNS в настройке **Системные DNS-серверы**.

Сервис DNS-прокси позволяет перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Сервис работает как в явном режиме, так и для перехвата транзитных запросов. Для явного режима необходимо разрешить доступ к сервису DNS на соответствующей зоне. Для перехвата транзитных запросов в этой зоне необходимо активировать следующие настройки в разделе DNS-прокси

Настройки DNS-прокси:

Наименование	Описание
Кэширование DNS	Включает или отключает кэширование ответов DNS. Рекомендуется оставить включенным для ускорения обслуживания клиентов.
DNS-фильтрация	Включает или отключает фильтрацию DNS-запросов. При включении DNS-фильтрации NGFW проверяет и перехватывает запросы, отправляя их дальше от своего IP-адреса. Если запрос соответствует запрещающему правилу контентной фильтрации, то он будет заблокирован. Для работы фильтрации необходимо приобрести лицензию на модуль ATP. i Внимание! Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают. i Важно! Правила контентной фильтрации, использующие список IP-адресов во вкладке <u>Назначение → Адрес доставки</u>, не обрабатываются модулем DNS-фильтрации. Обработка таких правил выполняется средствами модуля контентной фильтрации.
Рекурсивные DNS-запросы	Разрешает или запрещает серверу осуществлять рекурсивные DNS-запросы. Рекомендуется оставить эту опцию включенной.
Максимальный TTL для DNS-записей	Устанавливает максимально возможное время жизни для записей DNS.
Лимит количества DNS-запросов в секунду на пользователя	Устанавливает ограничение на количество DNS-запросов в секунду для каждого пользователя. Запросы, превышающие данный параметр, будут отброшены. Значение по умолчанию - 100 запросов в секунду. Не рекомендуется ставить большие значения для данного параметра, поскольку DNS-флуд (DNS DoS attacks) является довольно частой причиной отказа обслуживания DNS-серверов.

Наименование	Описание
Только А и AAAA DNS-записи для не идентифицированных пользователей (защита от VPN поверх DNS)	Если защита включена, то NGFW отвечает только на запросы на записи А и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS.

С помощью правил DNS-прокси можно указать серверы DNS, на которые пересылаются запросы на определенные домены. Данная опция может быть полезна в случае, если внутри компании используется локальный домен, не имеющий связи с интернетом и использующийся для внутренних нужд компании, например, домен Active Directory.

Чтобы создать правило DNS-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить правило.	Нажать на кнопку Добавить , задать Название и Описание (опционально).
Шаг 2. Указать список доменов.	Задать список доменов, которые необходимо перенаправлять, например, localdomain.local. Допускается использование '*' для указания шаблона доменов.
Шаг 3. Указать DNS-серверы.	Задать список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены.

Кроме этого, с помощью DNS-прокси можно задавать статические записи типа host (А-запись). Чтобы создать статическую запись, необходимо выполнить:

Наименование	Описание
Шаг 1. Добавить запись.	Нажать на кнопку Добавить , задать Название и Описание (опционально).
Шаг 2. Указать FQDN.	Задать Fully Qualified Domain Name (FQDN) статической записи, например, www.example.com.
Шаг 3. Указать IP-адреса.	Задать список IP-адресов, которые NGFW будет возвращать при запросе данного FQDN.

Виртуальные маршрутизаторы

Для изоляции трафика между логическими сегментами в крупных сетях с общей инфраструктурой применяется технология виртуальной маршрутизации (Virtual Routing and Forwarding, VRF). С помощью виртуальных маршрутизаторов можно создавать независимые группы интерфейсов, благодаря чему трафик из одной группы не попадет в другую.

Каждый виртуальный маршрутизатор имеет свою собственную таблицу маршрутизации, которая может содержать запись о маршрутах, заданных статически или полученных с помощью протоколов динамической маршрутизации.

В разных виртуальных маршрутизаторах допускается использовать одинаковые IP-сети (IP overlapping).

Интерфейсы, не вошедшие ни в один из виртуальных маршрутизаторов, автоматически назначены на виртуальный маршрутизатор, созданный в системе по умолчанию.

Виртуальные маршрутизаторы имеют следующие ограничения:

- Ряд сервисов может быть использован только в виртуальном маршрутизаторе, созданном по умолчанию:
 - WCCP;
 - ICAP;
 - DNS;
 - авторизация;
 - любой сетевой трафик, генерируемый самим устройством: проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS-сообщений, SNMP-трапов и т. п.;
 - подключение UserGate MC к UserGate NGFW возможно только в случае, если порт UserGate NGFW находится в виртуальном маршрутизаторе, созданном по умолчанию.
- Действие правил NAT, DNAT, Port forwarding распространяется на все виртуальные маршрутизаторы.

- Зоны являются глобальными — параметры зоны и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

Примечание

Виртуальный маршрутизатор, созданный по умолчанию, необходим для корректной работы UserGate NGFW. Он используется для проверки лицензии, получения обновлений, работы DNS-служб.

Создание виртуального маршрутизатора

Чтобы создать новый виртуальный маршрутизатор:

1. В разделе **Настройки** → **Сеть** → **Виртуальные маршрутизаторы** нажмите **Добавить** и задайте имя и описание нового виртуального маршрутизатора. Если настроен кластер, укажите имя узла, на котором создается этот виртуальный маршрутизатор.

Примечание

Имя виртуального маршрутизатора должно содержать минимум три символа. Могут использоваться только строчные буквы латинского алфавита или цифры; в середине и конце имени допускается использование символов «_» и «-». В качестве имени виртуального маршрутизатора нельзя использовать зарезервированные термины (prelocal, local, main, default, unspec) или префиксы (port, gre, egress, ingress, tun, tap, erspan, ppp, bond, bridge, pimreg, mgmt).

2. На вкладке **Интерфейсы** укажите интерфейсы, которые должны принадлежать новому виртуальному маршрутизатору. Интерфейсы, относящиеся к другим виртуальным маршрутизаторам, не могут быть добавлены. Любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. Допускается использовать интерфейсы всех типов — физические, виртуальные (VLAN), bond-интерфейсы, VPN-интерфейсы и другие.

Дополнительно для нового виртуального маршрутизатора вы можете настроить параметры статической и динамической маршрутизации:

1. Статические маршруты (кроме маршрута по умолчанию). Подробнее о статических маршрутах — в разделе [«Статические маршруты»](#). Маршрут

по умолчанию добавляется в разделе **Настройки → Сеть → Шлюзы**.
 Подробнее о настройке шлюзов — в разделе «[Настройка шлюзов](#)».

2. Динамические маршруты, получаемые с помощью протокола маршрутизации OSPF. Подробнее — в разделе «[OSPF](#)».

3. Динамические маршруты, получаемые с помощью протокола маршрутизации BGP. Подробнее — в разделе «[BGP](#)».

4. Динамические маршруты, получаемые с помощью протокола маршрутизации RIP. Подробнее — в разделе «[RIP](#)».

5. Мультикастинг. Подробнее — в разделе «[Мультикастинг](#)».

Статические маршруты

С помощью статических маршрутов вы можете указать путь в сеть, доступную за определенным маршрутизатором. Маршрут применяется локально на том узле кластера и в том виртуальном маршрутизаторе, где он создается.

Для добавления статического маршрута:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **Статические маршруты** и нажмите **Добавить**. Укажите название маршрута. Опционально можно добавить описание маршрута.

3. Выберите тип маршрута:

- **Unicast** — стандартный тип маршрута. Отправляет трафик на адреса назначения через заданный шлюз.
- **Blackhole** — трафик отбрасывается без информирования источника о том, что данные не достигли адресата.
- **Unreachable** — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (тип 3, код 1).
- **Prohibit** — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (тип 3, код 13).

4. Укажите адрес назначения — подсеть, на которую будет указывать маршрут, например 172.16.20.0/24.

5. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с устройства.
6. Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate NGFW сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.
7. Задайте метрику маршрута. Если маршрутов в сеть несколько, то чем меньше значение метрики, тем выше приоритет маршрута.

Протоколы динамической маршрутизации

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. UserGate NGFW обновляет таблицу маршрутизации в соответствии с информацией, которую он получает от соседних маршрутизаторов.

Динамическая маршрутизация не меняет способов, с помощью которых ядро системы осуществляет маршрутизацию на IP-уровне. Ядро так же просматривает свою таблицу маршрутизации, отыскивая маршруты к узлам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: маршруты добавляются и удаляются не вручную, а динамически.

Примечание

Если в системе настроены статические шлюзы, то маршруты по умолчанию, полученные от протоколов динамической маршрутизации, игнорируются.

UserGate NGFW поддерживает работу следующих динамических протоколов маршрутизации: OSPF, BGP, RIP.

OSPF

OSPF (Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы (АС).

i Примечание

Маршруты добавляются только в том виртуальном маршрутизаторе, в котором настроен протокол OSPF.

i Примечание

При работе протокола OSPF в кластере отказоустойчивости в режиме «активный — пассивный» метрики на резервных узлах для всех интерфейсов, списков перераспределения маршрутов и карт маршрутов (route map), применимых к этим спискам перераспределения, увеличиваются вдвое. Таким образом устанавливается приоритет мастер-узла в маршрутизации трафика.

Для настройки параметров OSPF в UserGate NGFW:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.
2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **OSPF**.
3. Для начала настройки параметров OSPF установите флажок **Включено** и укажите идентификатор маршрутизатора. Идентификатор должен быть уникальным и задан в формате IPv4. Для удобства он может совпадать с одним из IP-адресов интерфейсов UserGate NGFW, относящихся к выбранному виртуальному маршрутизатору.
4. Настройте параметры интерфейсов, на которых будет работать OSPF.

Параметр	Описание
Включено	Включение или отключение использования интерфейса
Интерфейс	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в выбранный виртуальный маршрутизатор
Тип сети	Тип сети для оптимизации процесса установления соседства. Доступны следующие параметры: • Не установлен; • Broadcast; • Point-to-point; • Point-to-multipoint

Параметр	Описание
Пассивный режим	Включение или отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается пересылать пакеты обновления протокола маршрутизации
Стоимость	Стоимость (cost) канала интерфейса. Значение передается в объявлениях о состоянии (Link-State Advertisement, LSA) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию — 1
Приоритет	Целое число от 0 до 255. Чем выше значение, тем больше вероятность того, что маршрутизатор станет назначенным (Designated Router, DR) в сети и будет рассылать LSA. Значение 0 исключает маршрутизатор из процедуры выбора DR. Значение по умолчанию — 1
Интервал hello	Интервал в секундах, через который маршрутизатор посылает hello-пакеты. Этот интервал должен быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию — 10 секунд
Интервал dead	Время в секундах, по истечении которого соседний маршрутизатор считается неактивным. Время исчисляется с момента приема последнего hello-пакета от соседнего маршрутизатора. Значение по умолчанию — 40 секунд
Интервал повторения	Устанавливает интервал повторной отправки пакета LSA. Значение по умолчанию — 5 секунд
Задержка передачи	Устанавливает время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию — 1 секунда
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга OSPF. Это позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF. Подробнее — в разделе «Профили BFD»
Аутентификация	Включает требование аутентификации каждого принимаемого маршрутизатором OSPF-сообщения. Аутентификация обычно используется для предотвращения внедрения ложного маршрута от нелегитимных маршрутизаторов
Тип аутентификации	Возможные значения: • Plain — передача ключа в открытом виде для аутентификации маршрутизаторов. Необходимо указать значение поля Ключ.

Параметр	Описание
	• Digest — использование хеш-суммы MD5 для ключа аутентификации OSPF-пакетов. Необходимо указать Ключ и MD5 key ID. Для корректной работы эти параметры должны быть идентичными на всех маршрутизаторах. Значение параметра Ключ может содержать только буквы латинского алфавита, цифры и символ подчеркивания. Максимальное количество символов — 16

5. Настройте параметры областей OSPF.

Параметр	Описание
Включено	Включает или отключает использование области
Имя	Имя области
Стоимость	Стоимость (cost) маршрута по умолчанию, анонсируемая в тупиковую область (stub area). Значение по умолчанию — 1. Если тупиковая область подключена к нескольким пограничным маршрутизаторам области (Area Border Router, ABR), администратор может назначать разные стоимости маршрута по умолчанию для каждого ABR. Это позволяет управлять исходящим из области трафиком, направляя его через предпочтительный шлюз
Идентификатор области	Идентификатор области (area ID) может быть указан в десятичном формате или в формате записи IP-адреса. Для установления соседства OSPF идентификатор области должен совпадать на соседних маршрутизаторах
Тип аутентификации	Возможные значения: • Нет — не требовать аутентификацию OSPF-пакетов. • Plain — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. • Digest — использование MD5 хеш-суммы для ключа аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне области
Тип области	Доступные типы областей: • Нормальная — обычная область, которая создается по умолчанию. Эта область принимает обновления каналов, суммарные маршруты и внешние маршруты.

Параметр	Описание
	• Тупиковая (stub) — тупиковая область не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других областей. Если маршрутизаторам из тупиковой области необходимо передавать информацию за границу автономной системы, они используют маршрут по умолчанию. В тупиковой области не может находиться пограничный маршрутизатор автономной системы (Autonomous System Boundary Router, ASBR). • NSSA — Not-so-stubby area. NSSA-область определяет дополнительный тип LSA — LSA type 7. В NSSA-области может находиться ASBR
Не суммировать	Запрещает добавление суммированных маршрутов в тупиковые типы областей
Интерфейсы	Интерфейсы OSPF, на которых будет доступна эта область
Виртуальные линки	Специальное соединение, которое позволяет соединять части областей или присоединить область через другую магистральную область. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение в случае выхода из строя основных соединений. Укажите идентификаторы маршрутизаторов, которые доступны через такую область

6. Карты маршрутов (route map, доступны в версии 7.3.0 и выше) позволяют фильтровать маршруты при перераспределении и изменять различные атрибуты выбранных маршрутов. На вкладке **Routemaps** указаны глобальные параметры для создания карты маршрутов.

Параметр	Описание
Название	Название карты маршрутов. Не может содержать символы кириллицы
Действие	Устанавливает действие для этой карты маршрутов. Возможные значения: • Разрешить — разрешает прохождение данных, отвечающих условиям карты маршрутов. • Запретить — запрещает прохождение данных, не отвечающих условиям карты маршрутов

Параметр	Описание
Сравнивать по	Условия применения карты маршрутов. Возможные значения: • IP. Если выбрано это условие, на вкладке IP-адреса надо добавить все необходимые IP-адреса для этого условия с возможностью указать le (less or equal) и ge (greater or equal). Например: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0/8::11 — маршруты с первым октетом, равным 10, и префиксом от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты с первым октетом, равным 10, и префиксом от 11 до 13. • AS-путь. Если выбрано это условие, то в закладке AS-путь добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как: ◦ пробел; ◦ запятая; ◦ начало строки; ◦ конец строки; ◦ AS set delimiter { and }; ◦ AS confederation delimiter (and). • Community. Если выбрано это условие, на вкладке Community добавьте все необходимых для него BGP-community
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов
Установить метрику	Установить метрику для отфильтрованных маршрутов
Установить предпочтение	Установить предпочтение для отфильтрованных маршрутов
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута
Установить community	Установить (заменить) значение BGP-community для отфильтрованных маршрутов на указанное
Добавлять community	Установить значение BGP-community для отфильтрованных маршрутов

7. Если необходимо, на вкладке **Route redistribution** настройте перераспределения анонсируемых маршрутов (доступно в версии 7.3.0 и выше) из других протоколов в OSPF. Укажите следующие параметры:

- Выберите протоколы из списка:
 - **Kernel** (статические маршруты, добавленные администратором);
 - **Connected** (маршруты в непосредственно подключенные к NGFW сети);
 - **RIP**;
 - **BGP**.
- Укажите для каждого выбранного протокола OSPF-метрику (0–16777214).
- При необходимости фильтрации анонсируемых маршрутов из других протоколов, укажите для каждого выбранного протокола список route map.
- Параметр **Всегда отправлять маршрут по умолчанию** позволяет анонсировать маршрут 0.0.0.0/0 даже при отсутствии его в таблице маршрутизации.

BGP

BGP (Border Gateway Protocol) — динамический протокол маршрутизации, относящийся к классу протоколов маршрутизации внешнего шлюза (Exterior Gateway Protocol, EGP). На данный момент является основным протоколом динамической маршрутизации в интернете. Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС), то есть группами маршрутизаторов под единым техническим и административным управлением. Маршрутизаторы используют протоколы внутридоменной маршрутизации для определения маршрутов внутри своей АС и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация содержит список АС, к которым есть доступ через собственную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети.

Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол BGP.

Для настройки BGP в UserGate NGFW:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **BGP**.

3. Для начала настройки параметров BGP поставьте флажок **Включено** и укажите в качестве идентификатора маршрутизатора IP-адрес, назначенный одному из сетевых интерфейсов UserGate NGFW, относящихся к выбранному виртуальному маршрутизатору.

4. Укажите номер автономной системы. Автономная система — это группа сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы указывает на принадлежность маршрутизатора к этой системе.

5. Укажите, какие маршруты будут распространяться в другие BGP-маршрутизаторы в порядке перераспределения (redistribution):

- **connected** — маршруты в сети, непосредственно подключенные к этому узлу;
- **kernel** — статические маршруты, добавленные администратором для выбранного виртуального маршрутизатора;
- **ospf** — маршруты, полученные по протоколу OSPF.

6. Если необходимо включить балансировку трафика для маршрутов с одинаковой стоимостью — установите флажок **Multiple path**.

7. На вкладке **Сети** добавьте сети, относящиеся к выбранной автономной системе.

Примечание

Если на вкладке «Сети» добавить сети, которых нет в таблице маршрутизации, они не будут анонсироваться.

8. На вкладке **Routemaps** настройте параметры карты маршрутов (route map) для ограничения количества получаемых маршрутов. Карта маршрутов позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов.

Параметр	Описание
Название	Название карты маршрутов. Не может содержать символы кириллицы
Действие	Устанавливает действие для этого route map: • Разрешить — разрешает прохождение данных, отвечающих условиям карты маршрутов. • Запретить — запрещает прохождение данных, не отвечающих условиям карты маршрутов
Сравнивать по	Условия применения route map: • IP. Если выбрано это условие, на вкладке IP-адреса добавьте все необходимые для него IP-адреса. • AS-путь. Если выбрано это условие, на вкладке AS-путь добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как: ◦ пробел; ◦ запятая; ◦ начало строки; ◦ конец строки; ◦ AS set delimiter { and }; ◦ AS confederation delimiter (and). • Community. Если выбрано это условие, на вкладке Community добавьте строки всех необходимых для него BGP-community
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов
Установить метрику	Установить метрику для отфильтрованных маршрутов
Установить предпочтение	Установить предпочтение для отфильтрованных маршрутов
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута
Community	Установить значение BGP-community для отфильтрованных маршрутов

9. На вкладке **Фильтры** настройте параметры фильтрации при перераспределении маршрутов.

Параметр	Описание
Название	Название фильтра
Действие	Устанавливает действие для фильтра: • Разрешить — разрешает прохождение данных, отвечающих условиям фильтра. • Запретить — запрещает прохождение данных, не отвечающих условиям фильтра
Фильтровать по	Условия применения фильтра: • IP. Если выбрано это условие, на вкладке IP-адреса добавьте IP-адреса для этого условия. Адреса могут быть указаны в следующих форматах: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0/8::11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. • AS-путь. Если выбрано это условие, на вкладке AS-путь добавьте номера автономных систем для этого условия

10. На вкладке **BGP-соседи** нажмите **Добавить** и настройте параметры маршрутизаторов, относящихся к соседней АС.

Параметр	Описание
Включено	Включение или отключение использования BGP-соседа
Host	IP-адрес BGP-соседа
Описание	Произвольное описание BGP-соседа
Удаленная ASN	Номер автономной системы, к которой относится BGP-сосед
Вес	Вес маршрутов, получаемых от этого BGP-соседа
TTL	Максимальное количество переходов (hop), разрешенное до этого BGP-соседа
Профиль BFD	

Параметр	Описание
	Настроить с помощью профиля BFD мониторинг BGP для возможности более быстрого обнаружения неисправностей соединений. Подробнее — в разделе « Профили BFD »
Анонсировать себя в качестве следующего перехода (next-hop-self) для BGP	Заменять значение next-hop-self на собственный IP-адрес, если сосед является BGP-соседом
Multihop для eBGP	Указывает, что путь до этого BGP-соседа имеет больше одного перехода (hop)
Route reflector client	Указывает, является ли этот BGP-сосед клиентом Route reflector
Soft reconfiguration	Использовать функцию soft reconfiguration (без разрыва соединений) для обновления конфигурации
Default originate	Анонсирование BGP-соседу маршрута по умолчанию
Аутентификация	Включение аутентификации для данного BGP-соседа и указание пароля для аутентификации
Фильтры BGP-соседей	Ограничение информации о маршрутах, получаемых от BGP-соседей или маршрутов, анонсируемых для BGP-соседей
Routemaps	Карты маршрутов (route maps) используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами

Важно!

Согласно требованиям RFC-8212 для каждого соседа необходимо указать входящие и исходящие фильтры. Без входящих фильтров маршрутизатор не будет принимать маршруты от BGP-соседа. При отсутствии исходящих фильтров маршрутизатор не будет анонсировать маршруты для BGP-соседа.

Если на интерфейсе UserGate NGFW, с которого устанавливается подключение к BGP-соседу, назначено несколько IP-адресов, то при настройке BGP-соседа, при отсутствии правила NAT, принудительно устанавливающего адрес источника для BGP-сессии с этим соседом, в качестве адреса UserGate NGFW необходимо указать основной (primary) IP-адрес, то есть адрес, который стоит первым в списке параметров интерфейса.

Пример настройки BGP для кластера UserGate NGFW — в статье «[Варианты настройки BGP для кластера Актив-Пассив](#)».

RIP

RIP (Routing Information Protocol) — протокол дистанционно-векторной маршрутизации, который использует параметр hop (переход) в качестве метрики маршрутизации.

Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол RIP.

Для настройки RIP в UserGate NGFW:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.
2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **RIP** и установите флажок **Включено**.
3. Настройте параметры протокола RIP:
 - **Версия RIP** — определяет версию протокола RIP. Как правило используется версия 2.
 - **Метрика по умолчанию** — целочисленное значение в интервале от 1 до 15. Обычно значение метрики по умолчанию равно 1.
 - **Административное расстояние** — стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
 - **Отправлять себя в качестве маршрута по умолчанию** — оповещать другие маршрутизаторы о том, что этот маршрутизатор имеет маршрут по умолчанию.
4. Маршрутизатор RIP будет отправлять обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. На вкладке **Сети RIP** укажите как минимум одну сеть для корректной работы протокола. При настройке сетей RIP администратор может указать сеть в виде CIDR, например 192.168.1.0/24, либо указать сетевой интерфейс, с которого будут отправляться обновления.
5. На вкладке **Интерфейсы** добавьте интерфейсы, на которых будет работать RIP.

Параметр	Описание
Интерфейс	Выберите интерфейс, который будет использоваться для работы протокола RIP. Для выбора доступны только те интерфейсы, которые входят в выбранный виртуальный маршрутизатор
Посылать версию	Версия протокола RIP, с которой будет работать маршрутизатор при отправке сообщений
Принимать версию	Версия протокола RIP, в соответствии с которой маршрутизатор будет принимать сообщения
Пароль	Строка для авторизации, которая будет отправляться и приниматься в пакетах RIP. Все маршрутизаторы, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль
Split horizon	Метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который пришло обновление
Poison reverse	Метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута, равную 16, и отправляет маршрут соседу, от которого его получил
Пассивный режим	Устанавливает режим работы интерфейса, при котором он принимает обновления RIP, но не отправляет их

6. Параметры редистрибуции маршрутов позволяют указать, какие из маршрутов необходимо отправлять соседям. Вы можете задать для редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGP, а также статические маршруты в непосредственно подключенные к UserGate NGFW сети (connected) или маршруты, добавленные администратором в разделе **Маршруты** (kernel).

Мультикастинг

Технология IP-мультикастинга позволяет существенно сократить передаваемый объем трафика, доставляя единый поток информации одновременно множеству потребителей. Применение этой технологии особенно эффективно для доставки голосового и видеотрафика. Традиционные методы доставки трафика — это юникаст (доставка от точки к точке) и бродкаст (широковещательная посылка трафика). Мультикаст-метод позволяет доставить трафик группе узлов (мультикаст-группа). Узлы (получатели), которые хотят получать этот трафик, должны присоединиться к соответствующей мультикаст-группе. Для присоединения узлов к мультикаст-группе используется протокол Internet

Group Management Protocol (IGMP). Мультикаст-группа идентифицируется с помощью группового адреса. Для мультикастовых адресов выделена подсеть класса D со следующим диапазоном адресов для трансляций: 224.0.0.0 — 239.255.255.255.

Маршрутизаторы должны обеспечить эффективную доставку трафика от источника трансляции к получателям. Для достижения этой цели используется протокол Protocol Independent Multicast (PIM).

Маршрутизаторы в мультикастинговой среде могут иметь следующие роли:

- First Hop Router (FHR). FHR находится ближе всего к источнику трансляции и отвечает за регистрацию источника трансляции в сети.
- Rendezvous Point (RP). RP является каталогом доступных мультикаст-источников для режима Any Source Multicast (ASM).
- Last Hop Router (LHR). LHR находится ближе всего к приемнику мультикаст-трансляции. Клиенты (приемники трансляции) в локальных сетях, подключенных к LHR, используют протокол IGMP для регистрации себя в необходимой мультикаст-группе посредством отправки сообщения IGMP membership report.

UserGate NGFW может быть использован в качестве LHR для локальных сетей, подключенных к нему. Для регистрации клиентов (приемников) UserGate NGFW поддерживает протоколы IGMPv3 и IGMPv2.

Для взаимодействия с другими мультикаст-маршрутизаторами UserGate NGFW может использовать только режим работы PIM Sparse Mode (PIM-SM). Это режим, в котором мультикаст-трафик отсылается только на те приемники, которые его явно запросили. Приемники должны периодически подтверждать необходимость получать мультикаст-трафик.

UserGate NGFW поддерживает режимы работы Source Specific Multicast (SSM) и Any Source Multicast (ASM).

Режим работы SSM используется, когда приемник трафика явно указывает известный ему адрес источника трансляции. В таком режиме используется следующая адресация:

`rtp://<src_ip>@<group_address>:<port>`, где `src_ip` — адрес источника трансляции, `group_address` — мультикастовый групповой адрес, `port` — порт. Например, `rtp://10.10.10.10@239.0.0.5:4344`

В режиме работы ASM приемник трансляции указывает мультикаст-группу, от которой он будет получать трансляцию. Для работы режима необходимо

наличие маршрутизатора с ролью RP. RP определяет источник трансляции для группы приемника. Далее источник и приемник выбирают лучший сетевой путь для пересылки мультикаст-трафика. В этом режиме используется следующая адресация:

`rtp://@<group_address>:<port>`, где `group_address` — мультикастовый групповой адрес, `port` — порт. Например, `rtp://@239.0.0.5:4344`

Для настройки работы UserGate NGFW в качестве LHR мультикаст-маршрутизатора:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.
2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **Мультикаст-маршрутизатор** и установите флажок **Включено**.
3. Настройте общие параметры мультикастинга:
 - **Использовать ECMP** — распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если эта опция отключена, то весь трафик на определенный узел назначения будет пересылаться только через один из маршрутизаторов (next hop).
 - **Использовать ECMP rebalance** — если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). При отключенной опции перераспределяются только те потоки, которые передавались через отключенный интерфейс.
 - **JOIN/PRUNE интервал** — интервал в секундах для отправки сообщений PIM JOIN и PIM PRUNE для управления потоком мультикаст-трафика.
 - **Интервал register suppress** — таймер в секундах, который временно запрещает маршрутизатору-источнику инкапсулировать мультикаст-трафик в пакеты PIM Register.
 - **Keep-alive-таймер** — интервал в секундах (31–60 000), через который маршрутизатор будет посылать сообщения keealive соседям. Это же значение интервала используется маршрутизатором для принятия решения о недоступности соседа.

4. На вкладке **Интерфейсы** настройте параметры интерфейсов, на которых будет работать мультикастинг.

Параметр	Описание
Включено	Включение или отключение использования интерфейса для мультикастинга
Интерфейс	Интерфейс, который будет использоваться для работы мультикастинга. Для выбора доступны только те интерфейсы, которые входят в выбранный виртуальный маршрутизатор
Интервал отправки HELLO-сообщений	Интервал отправки PIM HELLO-сообщений в секундах (1–180). PIM Hello-сообщения отправляются периодически со всех интерфейсов, для которых включена поддержка мультикастинга. С помощью этих сообщений маршрутизатор узнает о соседних маршрутизаторах, поддерживающих мультикастинг
Приоритет выбора DR	Приоритет при выборе маршрутизатора-источника (Designated router, DR) — значение от 1 до 4294967295, с помощью которого администратор может управлять процессом выбора DR для локальной сети
Принимать IGMP	Принимать сообщения IGMP report и IGMP query на этом интерфейсе
Использовать IGMPv2	Использовать IGMPv2, по умолчанию используется IGMPv3
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга. Позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса. Подробнее — в разделе « Профили BFD »

5. На вкладке **Rendezvous points** укажите адреса RP для режима ASM.

Параметр	Описание
Включено	Включение или отключение RP
Название	Название RP
IP-адрес	IP-адрес RP
Разрешенные группы ASM	Список разрешенных групповых адресов для отправки any source multicast (ASM) с данного RP. Любые сети из диапазона 224.0.0.0/4. Если ничего не задано, ограничений нет

6. Если необходимо, на вкладке **Разрешенные группы SSM** установите необходимые ограничения на доступные мультикаст-группы для режима SSM. Укажите список разрешенных групповых адресов для SSM. Могут быть указаны любые сети из диапазона 232.0.0.0/8. Если ничего не задано, ограничений нет.

7. Если необходимо, на вкладке **Исключения из SPT** укажите список IPv4 мультикаст-групп, исключенных из переключения на Shortest Path Tree (SPT).

WCCP

Web Cache Communication Protocol (WCCP) — разработанный компанией [Cisco](#) протокол перенаправления контента. Предоставляет механизм перенаправления потоков трафика в реальном времени, имеет встроенные масштабирование, балансировку нагрузки, отказоустойчивость. При использовании WCCP, WCCP-сервер принимает HTTP-запрос от клиентского браузера и перенаправляет его на один или несколько WCCP-клиентов. WCCP-клиент получает данные из интернет и возвращает их в браузер клиента. Доставка данных клиенту может происходить как через WCCP-сервер, так и минуя его, в соответствии с правилами маршрутизации.

UserGate NGFW может выступать в качестве WCCP-клиента. В качестве WCCP-сервера обычно выступает маршрутизатор. Для трафика, полученного через WCCP, можно применять все доступные механизмы фильтрации.

Сервисная группа WCCP — это набор серверов WCCP (роутеры, коммутаторы) и клиентов WCCP (NGFW) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настройте WCCP сервер.	Произведите настройку сервера WCCP в соответствии с инструкцией на WCCP-сервер.
Шаг 2. Настроить сервисные группы WCCP.	В консоли NGFW в разделе Сеть → WCCP нажать на кнопку Добавить и создать одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает данную сервисную группу.
Название	Имя сервисной группы.
Описание	Описание сервисной группы.
Сервисная группа	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
Приоритет	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
Пароль	Пароль, необходимый для аутентификации NGFW в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
Способ перенаправления трафика	Определяет способ перенаправления трафика с серверов WCCP на NGFW. Возможны значения: • gre — используя туннель Generic Routing Encapsulation (GRE). • L2 — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес NGFW. Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2. Важно! Для трафика, полученного через WCCP-туннель, в качестве IP источника NGFW будет использовать IP-адрес компьютера клиента, а зона источника не будет определена, поэтому в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).
Способ возврата трафика	Определяет способ перенаправления трафика с NGFW на серверы WCCP. Возможны значения: • gre — используя туннель Generic Routing Encapsulation (GRE). • L2 — используя перенаправление L2. В этом случае NGFW (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер).

Наименование	Описание
	Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
Порты для перенаправления	Порты для перенаправления. Укажите здесь порты назначения трафика. При необходимости указать несколько портов, укажите их через запятую, например: 80, 442, 8080 Для перенаправления трафика на основании значений портов источника необходимо поставить флажок Порт источника. Важно! NGFW может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на NGFW с другими портами, будет отправляться в интернет без фильтрации.
Протокол	Укажите протокол — TCP или UDP.
Роутеры WCCP	Укажите IP-адреса серверов WCCP (роутеры).
Способ назначения	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможны варианты: • Хэш — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета. Альтернативный хэш — если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиента с использованием обычного хэша. Поля IP-пакета, используемые для получения хэша, должны отличаться для вычисления основного и альтернативного хэшей. • Маска — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP.

ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Пользователи и группы

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности UserGate NGFW могут быть применены к пользователям или группам пользователей. Возможность применения политик только к тем пользователям, которым это необходимо, позволяет администратору гибко настроить свою сеть в соответствии с потребностями организации.

Идентификация пользователя — это базисная функция NGFW. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. NGFW использует различные механизмы для идентификации пользователей:

- Идентификация по явно указанному IP-адресу.
- Идентификация по имени и паролю.
- Идентификация пользователей терминальных серверов Microsoft с помощью специального агента терминального сервиса.
- Идентификация пользователей с помощью агента авторизации (для Windows-систем).
- Идентификация с помощью протоколов NTLM, Kerberos.

Идентификация пользователей по имени и паролю возможна через Captive-портал, который, в свою очередь, может быть настроен на идентификацию пользователей с помощью каталогов Active Directory, Radius, TACACS+, NTLM, Kerberos или локальной базы пользователей.

NGFW определяет следующие типы пользователей:

Наименование	Описание
Пользователь Unknown	Представляет множество пользователей, не идентифицированных системой.
Пользователь Known	Представляет множество пользователей, идентифицированных системой. Методы идентификации

Наименование	Описание
	пользователей могут быть различными и более подробно будут описаны далее в этой главе.
Пользователь Any	Любой пользователь является объединением множеств пользователей Known и Unknown .
Определенный пользователь	Конкретный пользователь, определенный и идентифицированный в системе, например, пользователь DOMAIN\User, идентифицированный с помощью авторизации в домене Active Directory.

Пользователи и группы пользователей могут быть заведены на самом устройстве NGFW — это так называемые **локальные пользователи и группы** или могут быть получены с внешних каталогов, например, Microsoft Active Directory.

Группы

Группы пользователей позволяют объединить пользователей для более удобного управления политиками безопасности.

Пользователи

В данном разделе можно добавить локальных пользователей. Здесь же можно временно отключить пользователей или включить их заново.

Обязательными параметрами для создания локального пользователя являются имя пользователя и логин. Остальные параметры являются необязательными, но для корректной идентификации необходимо указать:

- Логин и пароль — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
- IP-адрес или диапазон, MAC-адрес для идентификации с помощью комбинации MAC и IP-адресов. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанных MAC и/или IP-адреса.
- VLAN ID для идентификации пользователя по тегу VLAN. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанного VLAN.

- Почтовые адреса — email пользователя. Если указан, может быть использован для отсылки пользователю информации по электронной почте, например, 2-й фактор многофакторной организации.
- Номера телефонов — телефоны пользователя. Если указан, может быть использован для отсылки пользователю информации по SMS, например, 2-й фактор многофакторной организации.

В случае, если у пользователя указан и логин, и пароль, и IP/MAC/VLAN адреса, система использует идентификацию по адресу, то есть идентификация по адресу является более приоритетной.

Учетные записи пользователей LDAP здесь не отображаются, но эти пользователи также могут быть использованы в политиках безопасности.

Серверы аутентификации

Серверы аутентификации — это внешние источники учетных записей пользователей, например LDAP-сервер, или серверы, производящие аутентификацию для NGFW, например RADIUS, TACACS+, Kerberos, SAML.

Серверы аутентификации RADIUS, TACACS+, NTLM, SAML могут осуществлять только аутентификацию пользователей, в то время как LDAP-коннектор позволяет также получать информацию о пользователях и их свойствах.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA с использованием методов аутентификации Captive-портал, Kerberos, NTLM.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то NGFW получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, NGFW будет использовать резервный. В случае недоступности части контроллеров домена с площадки, где работает NGFW, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Срок жизни LDAP-кэша	Срок жизни LDAP-кэша (от 1 до 48 часов). Новый срок жизни применяется к новым записям, добавляемым в LDAP-кэш после того, как администратор его установит. (Доступно начиная с релиза UGOS 7.1.3).
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. При наличии поддоменов, в которых может происходить авторизация пользователей, на вкладке Домены LDAP необходимо указывать все варианты таких поддоменов. Здесь же можно указать короткое netbios имя домена. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Более подробно о настройке Captive-портала смотрите раздел Настройка Captive-портала.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп.

Наименование	Описание
	Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.
Kerberos keytab	Здесь можно загрузить keytab-файл для аутентификации Kerberos. Подробно об аутентификации Kerberos и создании keytab-файла смотрите в разделе Метод аутентификации Kerberos .

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Примечание

Для авторизации пользователей с помощью LDAP-коннектора необходимо, чтобы пользователи входили в доменную группу **Domain users**.

Настройка LDAP-коннектора завершена. Для авторизации LDAP-пользователей по имени и паролю необходимо создать правила Captive-портала. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Для добавления пользователя или группы пользователей LDAP в правила фильтрации необходимо нажать на **Добавить пользователя LDAP/Добавить группу LDAP**, в поле поиска указать как минимум один символ, входящий в имена искомых объектов, после чего нажать на **Поиск** и выбрать желаемые группы/пользователей.

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть NGFW выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер NGFW посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Сервер RADIUS не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере RADIUS) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации RADIUS необходимо нажать на кнопку **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Хост	IP-адрес сервера RADIUS.
Порт	UDP-порт, на котором сервер RADIUS слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.

После создания сервера аутентификации необходимо настроить Captive-портал для использования метода RADIUS. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При авторизации через TACACS+ NGFW посылает на серверы TACACS+ информацию с именем и паролем пользователя, а сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Сервер TACACS+ не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации TACACS+ необходимо нажать на кнопку **Добавить**, выбрать **Добавить TACACS+-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.

Наименование	Описание
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	Порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт TCP 49.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+. Внимание! Чтобы данная опция работала, необходимо также настроить её на стороне сервера TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет авторизовать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю, единожды авторизовавшись в системе SSO, прозрачно проходить авторизацию на всех ресурсах, поддерживающих аутентификацию SAML. NGFW может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в NGFW поэтому, если не настроено подключение к домену AD с помощью LDAP-коннектора, в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере SAML) или **Unknown** (не прошедших аутентификацию).

Для использования авторизации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать DNS-записи для NGFW.	На контроллере домена создать DNS-запись, соответствующую NGFW, для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть Trusted .

Наименование	Описание
Шаг 2. Настроить DNS-серверы на NGFW.	В настройках NGFW в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 3. Изменить адрес Домен auth captive-портала .	Изменить адрес Домен auth captive-портала в разделе Настройки на созданную на предыдущем шаге запись DNS. Подробно об изменении адреса домена Auth Captive-портала смотрите в разделе Общие настройки .
Шаг 4. Настроить сервер SAML IDP.	Добавить на сервере SAML IDP запись о сервис-провайдере NGFW, указывая созданное на шаге 1 FQDN имя.
Шаг 5. Создать сервер аутентификации пользователей SAML IDP.	Создать в NGFW сервер аутентификации пользователей SAML IDP.

Для создания сервера аутентификации пользователей SAML IDP необходимо в разделе **Пользователи и устройства → Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку Загрузить происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера аутентификации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации.
Сертификат SAML IDP	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: Создать новый сертификат из скачанного — если при настройке был использован метод загрузки xml-файла, то сертификат автоматически создается и ему назначается роль SAML IDP (смотрите раздел Управление сертификатами).

Наименование	Описание
	- Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе Сертификаты, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP. - Не использовать сертификат.
Single sign-on URL	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single sign-on binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout URL	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect . Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Сервер аутентификации NTLM

Аутентификация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации с помощью NTLM NGFW работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в Интернет.

Сервер NTLM не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере NTLM) или **Unknown** (не прошедших аутентификацию).

Аутентификация NTLM может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан. Настройка NGFW не отличается от режима работы авторизации.

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить синхронизацию времени с контроллером домена.	В настройках NGFW включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 2. Создать DNS-запись для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть Trusted .
Шаг 3. Изменить адрес Домен Auth Captive-портала.	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки . Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала .
Шаг 4. Добавить NTLM-сервер.	В разделе Серверы аутентификации нажать на кнопку Добавить , выбрать Добавить NTLM-сервер и указать название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена.
Шаг 5. Создать правило Captive-портала с аутентификацией NTLM.	Настроить Captive-портал для использования метода аутентификации NTLM. Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 6. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM
Шаг 7. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса NGFW в качестве адреса прокси-сервера. Важно! Вместо IP-адреса можно использовать доменное имя, но для NTLM важно, чтобы это имя было не из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.

Наименование	Описание
	Важно! В настройках NGFW имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.
Шаг 8. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность, выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security, выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации Kerberos

Аутентификация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации через Kerberos NGFW работает с контроллерами домена, которые выполняют проверку пользователя, получающего доступ в Интернет.

Аутентификация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для авторизации с помощью Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW, для использования в качестве доменов для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть Trusted. Важно! Для корректной работы создайте записи типа A, не используйте CNAME-записи.
Шаг 2. Создать пользователя для NGFW.	

Наименование	Описание
	Создать пользователя в домене AD, например, <code>kerb@domain.loc</code> с опцией password never expires. Установите пароль пользователю <code>kerb</code>. Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя <code>kerb</code> или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя <code>kerb</code>. Важно! Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.
Шаг 3. Создать keytab-файл.	На контроллере домена, создать keytab файл, выполнив следующую команду из-под администратора (команда в одну строку!): <pre>ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC / mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab</pre> Введите пароль пользователя <code>kerb</code>. Важно! Команда чувствительна к регистру букв. В данном примере: <code>auth.domain.loc</code> — DNS-запись, созданная для сервера UserGate на шаге 1 <code>DOMAIN.LOC</code> — Kerberos realm domain, обязательно большими буквами! <code>kerb@DOMAIN.LOC</code> — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Шаг 4. Настроить DNS-серверы на NGFW.	В настройках NGFW в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 5. Настроить синхронизацию времени с контроллером домена.	В настройках NGFW включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 6. Изменить адрес Домен auth captive-портала.	Изменить адрес Домен auth captive-портала и опционально адрес Домен logout captive-портала в разделе Настройки на созданные на предыдущем шаге записи DNS. Подробно об изменении адресов доменов смотрите в разделе Общие настройки .
Шаг 7. Создать LDAP-коннектор и загрузить в него keytab-файл.	Создать сервер аутентификации типа LDAP-коннектор и загрузить полученный на предыдущем шаге keytab-файл. Важно! Не используйте в качестве пользователя для LDAP-коннектора, пользователя, созданного ранее для работы

Наименование	Описание
	Kerberos. Необходимо использовать отдельную учетную запись. Подробнее о настройке LDAP-коннектора смотрите раздел LDAP-коннектор.
Шаг 8. Создать правило Captive-портала с аутентификацией по Kerberos.	Настроить Captive-портал для использования метода аутентификации Kerberos. Более подробно о Captive-портале рассказывается в разделе Настройка Captive-портала .
Шаг 9. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.
Шаг 10. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени NGFW, созданного на шаге 3.
Шаг 11. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в Панель управления → Свойства браузера → Безопасность, выберите зону Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя и установите Автоматический вход в сеть с текущим именем пользователя и паролем (Control panel → Internet options → Security, выберите зону Internet → Custom level → User Authentication → Logon и установите Automatic logon with current name and password). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации HTTP Basic

Аутентификация Basic позволяет авторизовать пользователей с явно указанным прокси-сервером по базе локальных и LDAP-пользователей. Не рекомендуется использовать данный тип аутентификации поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификация HTTP Basic можно использовать для автоматической авторизации утилит командной строки, которым необходим доступ в Интернет, например:

```
curl -x 192.168.179.10:8090 -U user:password http://www.msn.com
```

Для авторизации по HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-запись для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть Trusted.
Шаг 2. Изменить адрес Домен Auth Captive-портала.	Изменить адрес домена Auth Captive-портала и опционально адрес домена Logout Captive-портала в разделе Настройки. Для домена Auth Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Для домена Logout Captive-портала необходимо указать созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 3. Создать правило Captive-портала с аутентификацией по HTTP Basic.	Настроить Captive-портал для использования метода аутентификации HTTP Basic. При настройке, помимо метода HTTP Basic, необходимо добавить базу пользователей, по которой будет проверяться аутентификация (например, добавить методы аутентификации Локальный пользователь или Сервер LDAP). Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 4. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе Зоны разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью HTTP Basic.
Шаг 5. Настроить прокси-сервер на компьютерах пользователей	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса NGFW в качестве адреса прокси-сервера.

Профили аутентификации

Профиль аутентификации позволяет указать набор способов и параметров аутентификации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах UserGate NGFW, например Captive-портал, VPN, веб-портал и т. д. Чтобы создать профиль аутентификации,

необходимо в разделе **Настройки → Пользователи и устройства → Профили аутентификации** нажать **Добавить** и указать необходимые параметры.

Параметр	Описание
Название	Название профиля
Описание	Описание профиля
Профиль MFA	Профиль многофакторной аутентификации. Должен быть предварительно создан в разделе Профили MFA, если планируется использовать многофакторную аутентификацию. Профиль определяет способ доставки одноразового пароля для дополнительного метода аутентификации. Подробнее о настройке профилей MFA — в разделе «Профили MFA» i Важно! Многофакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только с теми, где пользователь явно вводит свои учетные данные в веб-форму страницы аутентификации. В связи с этим, многофакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Этот параметр определяет, через сколько секунд UserGate NGFW переведет пользователя из состояния Known users в состояние Unknown users при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя)
Время жизни авторизованного пользователя	Этот параметр определяет, через сколько секунд UserGate NGFW переведет пользователя из состояния Known users в состояние Unknown users. По прошествии указанного времени пользователю потребуется повторно аутентифицироваться на Captive-портале
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток аутентификации через Captive-портал до блокировки учетной записи пользователя
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации

Параметр	Описание
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов аутентификации, таких как: • Локальный пользователь — аутентификация по базе данных локально заведенных пользователей. • Принять политику — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Этот тип аутентификации необходимо применять совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • HTTP Basic — аутентификация с помощью устаревшего метода HTTP Basic. • Аутентификация Kerberos — аутентификация по протоколу Kerberos

Настройка Captive-портала

Captive-портал позволяет авторизовать неизвестных пользователей (**Unknown users**) с помощью методов авторизации с использованием каталогов Active Directory, Radius, TACACS+, SAML IDP, Kerberos, NTLM или локальной базы пользователей. Кроме этого, с помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail.

Следует помнить, что:

- Идентифицированные пользователи, например, у которых в свойствах пользователя явно указан IP-адрес, идентифицированные с помощью агентов авторизации терминальных серверов или для систем Windows, не авторизуются на Captive-портале. Такие пользователи уже относятся к типу **Known users** и не требуют дополнительной идентификации.
- Авторизация с помощью Captive-портала возможна только для протокола HTTPS. Например, если вы создали правило межсетевого

экрана, разрешающее доступ в интернет по протоколу FTP только для пользователя **Known users**, то пользователи не смогут получить доступ в интернет по этому протоколу до тех пор, пока они не станут идентифицированными, то есть не запустят у себя браузер и не пройдут авторизацию на Captive-портале.

- Необходимо настроить инспектирование SSL, иначе авторизация по протоколу HTTPS работать не будет.
- Если Captive-портал использует метод авторизации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Настройка Captive-портала сводится к следующим шагам:

Наименование	Описание
Шаг 1. Создать метод авторизации, например, авторизация с помощью домена Active Directory.	В консоли NGFW в разделе Пользователи и устройства → Серверы аутентификации нажать на кнопку Добавить и создать сервер авторизации.
Шаг 2. Создать профиль аутентификации, в котором указать необходимые методы авторизации.	В консоли NGFW в разделе Пользователи и устройства → Профили аутентификации нажать на кнопку Добавить и создать профиль авторизации, используя созданный ранее метод авторизации.
Шаг 3. Создать Captive-профиль, в котором указать необходимые профили аутентификации.	В консоли NGFW в разделе Пользователи и устройства → Captive-профили нажать на кнопку Добавить и создать Captive-профиль, используя созданный ранее профиль авторизации.
Шаг 4. Создать правило Captive-портала.	Правило Captive-портала определяет трафик, к которому должны быть применены методы идентификации пользователей, указанные в Captive-профиле. В консоли NGFW в разделе Пользователи и устройства → Captive-портал нажать на кнопку Добавить и создать правило Captive-портала.

Наименование	Описание
Шаг 5. Настроить DNS для доменов auth.captive и logout.captive.	Служебные доменные имена auth.captive и logout.captive используются NGFW для авторизации пользователей. Если клиенты используют в качестве DNS-сервера NGFW то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса NGFW, который подключен в клиентскую сеть. Альтернативное решение — настроить параметры Домен auth captive-портала и Домен logout captive-портала . Более детально эти параметры описаны в разделе Общие настройки .

Создание методов авторизации подробно рассматривалось в предыдущих главах. Рассмотрим более подробно создание Captive-профиля и правил Captive-портала.

Чтобы создать Captive-профиль, необходимо в разделе **Captive-профили** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название Captive-профиля.
Описание	Описание Captive-профиля.
Шаблон страницы авторизации	Выбрать шаблон страницы авторизации. Создавать страницы авторизации можно в разделе Библиотеки → Шаблоны страниц . Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, то следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).
Метод идентификации	Метод, с помощью которого NGFW запомнит пользователя. Возможны 2 варианта: • Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал NGFW запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю. Данный метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и NGFW. Это рекомендуемое значение, устанавливаемое по умолчанию. • Запоминать cookie. После успешной авторизации пользователя через Captive-портал NGFW добавляет в

Наименование	Описание
	браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя. Данный метод позволяет авторизовать пользователей, находящихся за NAT-устройством, но авторизуется только протокол HTTP(S) и только в том браузере, в котором происходила авторизация через Captive-портал. Кроме этого, для авторизации HTTPS-сессий пользователя NGFW будет принудительно дешифровать все HTTPS-соединения. Для правил межсетевого экрана пользователь, идентифицированный по cookie, будет всегда определен как Unknown user .
Профиль аутентификации	Созданный ранее профиль авторизации, определяющий методы аутентификации.
Режим аутентификации	Аутентификация с помощью логина и пароля через RADIUS сервер (AAA) или посредством сертификатов (PKI).
Профиль сертификата пользователя	При выборе режима аутентификации посредством сертификатов PKI необходимо указать сконфигурированный ранее профиль пользовательских сертификатов.
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
Разрешить браузерам запомнить авторизацию	Включает возможность сохранить авторизацию в браузере на указанное время в часах. Для сохранения авторизационной информации используются cookie.
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется авторизация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице авторизации. Если данный параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке

Регистрация гостевых пользователей. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться 2 типа — SMS и email. Более подробно о создании профиля оповещения смотрите в главе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Тема оповещения	Тема оповещения (только для email-оповещений).
Письмо оповещения	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль.
Дата и время окончания	Время, когда учетная запись временного пользователя будет отключена.
Время жизни	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена.
Длина пароля	Определяет длину пароля для создаваемого пользователя.
Сложность пароля	Определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы.
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи. О группах для временных пользователей читайте в главе Гостевой портал .

Чтобы создать правило Captive-портала, необходимо нажать на кнопку **Добавить** в разделе **Captive-портал** и указать необходимые параметры:

Наименование	Описание
Название	Название правила Captive-портала.
Описание	Описание правила Captive-портала.

Наименование	Описание
Captive-профиль	Выбрать Captive-профиль, созданный ранее. Доступно действие Не использовать аутентификацию , при выборе которого аутентификация не будет требоваться.
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
Источник	Адреса источника. В качестве источника можно указать определенную зону, например, зону LAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Адреса назначения. В качестве адресов можно указать определенную зону, например, зону WAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Категории	Категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.
URL	Списки URL, для которых будет применяться правило.
Время	Время, когда данное правило будет активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний.

Наименование	Описание
	Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики .
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

Примечание

Условия, указанные во вкладках правила, применяются согласно логике “И”, то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику “ИЛИ”, то это достигается путем создания нескольких правил.

Примечание

Правила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил с помощью соответствующих кнопок.

Примечание

При обработке правил применяется только первое сработавшее правило.

В случае, если необходимо сменить пользователя после его авторизации в системе или выйти из системы, необходимо перейти на URL <http://logout.captive> и нажать на кнопку **Выйти**.

Пользователи терминальных серверов

Терминальный сервер служит для удаленного обслуживания пользователя с предоставлением рабочего стола или консоли. Как правило, один терминальный сервер предоставляет свой сервис нескольким пользователям, а в некоторых случаях десяткам или даже сотням пользователей. Проблема

идентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и NGFW не может корректно идентифицировать сетевые подключения пользователей. Для решения данной проблемы предлагается использование специального агента терминального сервиса. Каждому пользователю выделяется диапазон портов, с использованием которых происходит соединение пользователя, т.е. исходные порты подменяются на порты из выделенного для пользователя диапазона.

Агент терминального сервиса должен быть установлен на все терминальные серверы, пользователей которых необходимо идентифицировать. Агент представляет собой сервис, который передает на UserGate NGFW информацию о пользователях терминального сервера и об их сетевых соединениях. В силу специфики работы протокола TCP/IP, агент терминального сервиса может идентифицировать трафик пользователей, передаваемый только с помощью TCP и UDP протоколов. Протоколы, отличные от TCP/UDP, например, ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей, в случае использования на терминальных серверах авторизации Active Directory, требуется настроенный сервер Active Directory коннектор.

Чтобы начать работу с аутентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис Агент аутентификации на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис Агент Аутентификации для той зоны, со стороны которой расположены серверы терминального доступа.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажать на кнопку Настроить и задать пароль агентов терминального сервера.
Шаг 3. Установить агент терминального сервера.	Установить агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке следует задать адрес NGFW и заданный на предыдущем шаге пароль.
Шаг 4. Добавить необходимые серверы в консоли NGFW.	В разделе Пользователи и устройства → Терминальные серверы необходимо добавить агентов терминального сервера, указав имя и адрес хоста. После получения данных с указанного в настройках хоста и совпадении пароля, указанного в пункте 2, аутентификация пользователей будет включена автоматически.

Наименование	Описание
	При обновлении версии NGFW агенты терминальных серверов, которые ранее отображались в веб-консоли, будут продолжать работать.

UserGate теперь будет получать информацию о пользователях.

Агент терминального сервера позволяет аутентифицировать не только доменных, но и локальных пользователей терминального сервера. Для этого необходимо добавить в файл конфигурации (%ALLUSERSPROFILE%\Entensys\Terminal Server Agent\tsagent.cfg) следующий параметр:

LocalDomain = 1

При включении данного параметра информация о пользователях будет передаваться на NGFW в формате "имя сервера_имя пользователя" для локальных пользователей или "имя домена_имя пользователя" для доменных.

Таких пользователей также необходимо добавить в NGFW как локальных. О добавлении пользователей читайте в разделе [Пользователи](#). При добавлении необходимо указать **Логин** в приведенном выше формате; пароль указывать не нужно.

Данная опция предназначена, в основном, для терминальных серверов, не включенных в домен, вход на который осуществляется с локальными учетными данными.

После изменения файла конфигурации сервис терминального агента нужно перезапустить.



Примечание

Имя компьютера должно состоять из букв, цифр и знака подчёркивания.

Использование тире в имени компьютера возможно только в том случае, если используются только доменные пользователи.

Параметры терминального сервера могут быть изменены путём внесения изменений в файл конфигурации агента аутентификации для терминальных серверов. После внесения изменений агент аутентификации необходимо перезапустить.

Ниже представлен список параметров файла tsagent.cfg:

- **TimerUpdate**: периодичность отправки данных (указывается в секундах).

- **MaxLogSize**: максимальный размер журнала работы сервиса (указывается в Мбайт).
- **SharedKey**: пароль для подключения агента.
- **SystemAccounts**: может принимать значения **0** или **1**. При значении параметра **SystemAccounts=1** включает передачу информации о соединениях системных аккаунтов (system, local service, network service) и портах, используемых для соединения, на NGFW.
- **FQDN**: может принимать значения **0** или **1**. Значение параметра **FQDN=1** соответствует использованию FQDN (Fully Qualified Domain Name), например, «example.com» вместо «example».
- **ServerPort**: номер порта NGFW, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- **ServerAddress**: адрес устройства UserGate, принимающего соединение от агента аутентификации. Начиная с версии агента 6.2.0.49 поддерживается возможность работы с несколькими NGFW одновременно. Строка **ServerAddress** может содержать несколько элементов, разделенных символом ";". Это могут быть как IP-адреса, так и FQDN (например, *ServerAddress=testtermserver.net;15.0.0.203*). Все адреса резолвятся в момент старта и в момент изменений в настройках сетевых адаптеров. Рассылки о пользователях дублируются на все адреса.
- **UserCount**: максимальное количество пользователей.
- **BlockDNS**: может принимать значения **0** или **1**. При **BlockDNS=1** происходит замена порта источника на свободный порт из выделенного для пользователя диапазона при DNS запросе (UDP:53); при **BlockDNS=0** — отправка трафика происходит без замены порта.
- **BlockUDP**: может принимать значения **0** или **1**. Значение параметра **BlockUDP=1** соответствует замене порта источника на свободный порт из выделенного для пользователя диапазона при отправке трафика UDP; при **BlockUDP=0** — отправка трафика происходит без замены порта.
- **ExcludeIP**: в случае, если на терминальном сервере настроены несколько IP-адресов, то все они будут использованы для аутентификации пользователей. Параметр ExcludeIP позволяет ограничить

аутентификацию пользователей с определённых IP-адресов терминального сервера:

- IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
- Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
- Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
- Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP**. Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore**.
- **ExcludePorts**: диапазон, порты из которого не будут подменяться на порты из выделенного для пользователя диапазона портов (диапазон портов указывается следующим образом: **ExcludePorts=port1-port2**).
- **NAT_IP**: необходим при наличии NAT между терминальным сервером и UserGate: замена IP-адреса терминального сервера на один из адресов указанного диапазона. Адреса указываются в следующем виде: **NAT_IP="12.3.4-1.1.1.1;2.2.2.2-5.5.5.5"**.

Для исключения из рассылки определенных адресов и/или подсетей терминальным агентом помимо добавления параметра **ExcludeIP** в файл конфигурации tsagent.cfg он может быть активирован и в реестре сервера следующим образом:

- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Профили MFA (многофакторной аутентификации)

Многофакторная аутентификация — это метод идентификации и аутентификации пользователя, где используются два или более различных типа идентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

UserGate NGFW поддерживает многофакторную аутентификацию с использованием следующих методов:

- **TOTP** (Time-based One Time Password). TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром; более подробно о TOTP можно прочитать в https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. В качестве TOTP-токена могут выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например, Google Authenticator.
- **SMS** — получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в UserGate NGFW или в доменной учетной записи в Active Directory.
- **Email** — получение одноразового пароля по электронной почте. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в UserGate NGFW или в доменной учетной записи в Active Directory.

Чтобы настроить многофакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить авторизацию с помощью Captive-портала.	Многофакторная аутентификация работает только при аутентификации пользователей с помощью Captive-портала. Смотрите раздел для подробной информации.

Наименование	Описание
Шаг 2. Создать профиль многофакторной авторизации.	В разделе консоли Пользователи и устройства → Профили MFA создать профиль многофакторной авторизации. При создании профиля указать необходимые настройки доставки второго фактора авторизации. Возможно создать 3 типа доставки: • MFA через TOTP — доставка второго фактора авторизации с помощью токенов TOTP. • MFA через SMS — доставка второго фактора авторизации с помощью SMS. • MFA через email — доставка второго фактора авторизации с помощью email.

Для способа доставки **MFA через TOTP** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Инициализация TOTP	Для получения токенов TOTP необходимо произвести первоначальную инициализацию устройства или ПО клиента. Для этого требуется ввести уникальный ключ в устройство или ПО клиента. Передать первоначальный код для инициализации TOTP можно следующими средствами: • Показать на странице Captive-портала после первой успешной авторизации. Для этого варианта необходимо выбрать Показать ключ на странице Captive -портала. • Выслать с помощью SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки SMS (профиль SMPP). • Выслать с помощью email. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки email (профиль SMTP).

Наименование	Описание
Показывать QR -код	Показывать QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.

В случае, если пользователь утратил токен, администратор может потребовать повторной инициализации TOTP-токена. Для этого ему необходимо выбрать данного пользователя в списке пользователей (**Пользователи и устройства → Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей авторизации пользователю будет предложено заново проинициализировать свой токен.

Для способа доставки **MFA через SMS** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробно о настройке профилей отсылки сообщений через SMS смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Для способа доставки **MFA через email** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по

Наименование	Описание
	электронной почте смотрите в разделе Профили оповещений .
От	Указать, от имени кого будут отправляться оповещения.
Тема	Тема оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

UserID-агент

UserID — технология прозрачной аутентификации пользователей. Источниками данных для однозначной идентификации пользователей являются журналы безопасности операционных систем доменных контроллеров, данные журналов серверов приложений и доступа, в которых пользователи уже аутентифицированы.

Чтобы создавать политики, включающие пользователей и группы, межсетевому экрану необходимо сопоставить IP-адреса с пользователями, получившими эти адреса и извлечь информацию о группах, в которые они входят. UserID предоставляет несколько методов, позволяющих выполнить такое сопоставление. Например, для получения информации о пользователях UserID может просматривать журналы на серверах в поисках сообщений от служб аутентификации. Те пользователи, чьи имена не удалось сопоставить с IP-адресами, могут быть перенаправлены на специальный портал (Captive Portal) для прохождения аутентификации. Для получения информации о группах межсетевой экран подключается напрямую к серверам LDAP.

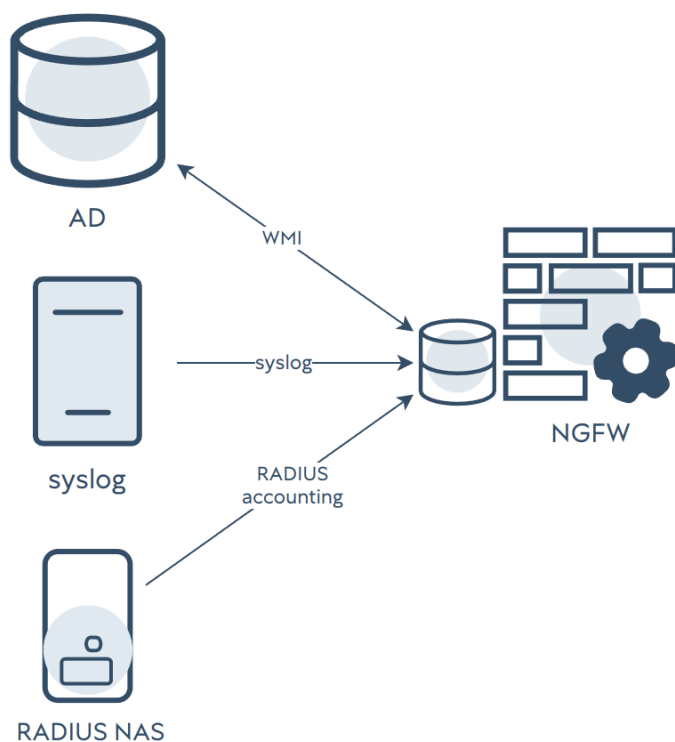
В качестве источников данных для аутентификации в UserID используются журналы Microsoft Active Directory, данные, полученные по syslog или сообщения RADIUS accounting (в версии 7.2.0 и выше).

Для конечных пользователей работа UserID полностью прозрачна, то есть пользователям нет необходимости в явном виде проходить аутентификацию на UserGate NGFW.

Принцип работы UserID

В зависимости от сценария использования и настройки UserID-агент получает данные о событиях, связанных с аутентификацией пользователей, одним из следующих способов:

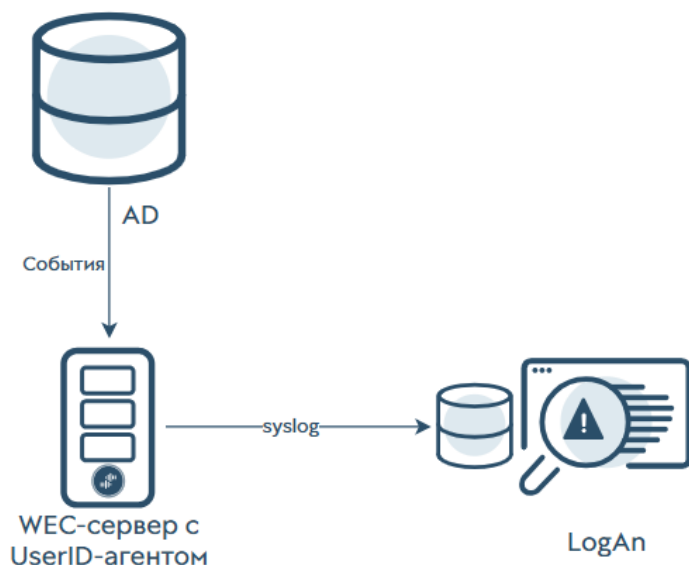
- Непосредственное получение данных узлом с UserID-агентом от источников данных аутентификации с помощью настроенных коннекторов:
 - UserID-агент может подключаться к контроллеру домена AD с помощью технологии WMI и считывать журналы событий безопасности;
 - UserID-агент может принимать со сторонних серверов сообщения по протоколу syslog;
 - UserID-агент может принимать со сторонних RADIUS NAS-серверов сообщения RADIUS accounting.



- Получение данных через посредника — специального программного агента, который устанавливается на контроллер домена или сервер-сборщик событий (WEC).

Программный агент UserID для AD- и WEC-серверов устанавливается на контроллер домена (AD) или сервер-сборщик событий домена (WEC), считывает необходимую для идентификации пользователя информацию из

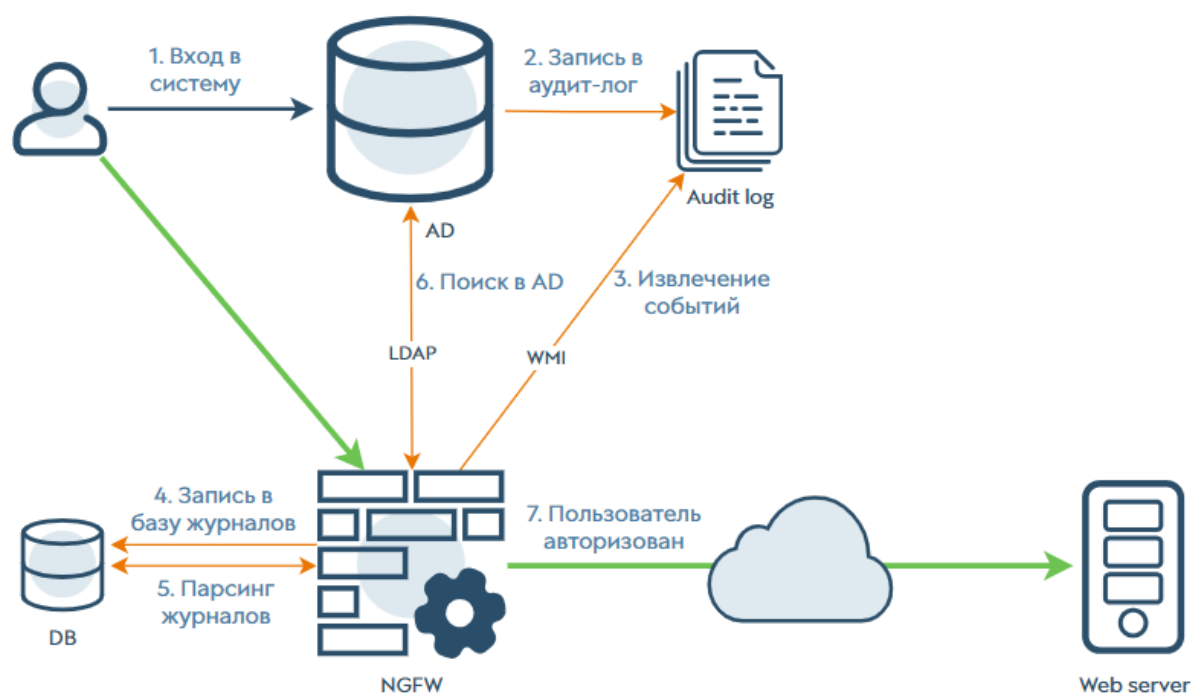
журналов безопасности Windows и пересылает ее в формате syslog на коллектор UserID на UserGate Log Analyzer или UserGate NGFW (подробнее об агенте — в разделе «[UserID-агент для AD/WEC](#)»).



Главные достоинства такого способа получения данных из домена AD:

- Не требуется предоставлять доступ извне в контроллер домена для сбора данных об аутентификации пользователей, как это требуется при доступе по технологии WMI.
- Не требуется создавать в домене специальную учетную запись с особыми привилегиями для узлов, на которых работает UserID-агент.

Рассмотрим принцип работы технологии UserID на примере сценария взаимодействия с Active Directory в качестве источника данных для аутентификации пользователей через технологию WMI.



На контроллере домена AD работает аудит событий безопасности, который записывает события по настроенным категориям в специальный журнал аудита.

После создания и настройки UserID-агента и коннектора Microsoft Active Directory на UserGate NGFW, UserID-агент начинает периодически отправлять на контроллер AD WMI-запросы для извлечения следующих событий по Event ID из журнала аудита:

- 4624 — успешный вход в систему;
- 4768 — запрос билета аутентификации Kerberos TGT;
- 4769 — запрос билета аутентификации Kerberos TGS;
- 4770 — обновление билета аутентификации Kerberos TGS;
- 4627 — сведения о членстве в группах.

Данные события позволяют UserID-агенту получать информацию о регистрации пользователей и членстве в группах. Полученная информация записывается в специальную системную базу данных на UserGate NGFW.

Информация из Microsoft AD о выходе пользователя из системы в настоящий момент не обрабатывается.

UserID-агент периодически обращается к этой базе данных, извлекает из записей имя пользователя, домен, SID, IP-адрес, список групп пользователя. Эти данные кешируются. Интервал поиска записей в базе данных можно задать в

настройках UserID-агента. Время жизни данных о пользователе в кеш-памяти устанавливается в настройках коннектора UserID-агента на UserGate NGFW.

В случае, если список групп, в которые входит пользователь, не был получен, UserID-агент обращается к контроллеру домена по протоколу LDAP в соответствии с настроенным профилем аутентификации для получения информации о группах.

При обработке сетевого трафика, в том случае, если в правилах настроены условия для определенных пользователей и групп, UserGate NGFW обращается к кеш-памяти для поиска информации о том, какие пользователи зарегистрированы с какими IP-адресами. Эта информация используется для принятия решения о том, как будут обрабатываться пакеты.

Завершение сессий пользователей может принудительно инициироваться администратором UserGate NGFW. Для этого администратор может выполнить сброс всех пользователей или сброс отдельного пользователя:

- В веб-консоли UserGate NGFW в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** на панели инструментов нажмите на панели инструментов нажмите **Сбросить аутентификацию всех пользователей**.
- В консоли CLI — выполните [команду](#):

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

В сценарии с использованием серверов-источников данных syslog в качестве источника данных аутентификации пользователей принцип работы аналогичен, только UserGate NGFW в этом случае выступает в роли syslog listener — принимает сообщения от отправителя syslog. Номер порта и протокол устанавливаются в настройках UserID-агента, по умолчанию — порт TCP 514. Нужные события фильтруются в потоке принятых данных с помощью настроенных фильтров из библиотеки Syslog фильтры UserID-агента. В этом случае в базу данных сохраняются: имя пользователя, IP-адрес, SID (опционально). Для получения информации о группах, в которых зарегистрирован пользователь, UserID-агент обращается к контроллеру домена по LDAP-протоколу в соответствии с настроенным профилем аутентификации UserID-агента.

В сценарии с использованием сообщений RADIUS accounting в качестве источника данных аутентификации пользователей принцип работы в целом схож. UserGate NGFW выступает в роли пропускного RADIUS-сервера

— принимает сообщения RADIUS accounting от серверов NAS (по порту UDP 1813) и проверяет пользователя на контроллере домена AD по LDAP в соответствии с настроенным профилем аутентификации UserID-агента.

Настройка UserID-агента на UserGate NGFW не является кластерной, а значит ее нужно производить на каждом узле отдельно. После настройки UserID-агент будет работать самостоятельно и самостоятельно получать данные о событиях логин\логаут из журналов источников.

Помимо UserGate NGFW UserID может работать на устройствах UserGate Log Analyzer. Подробнее о работе UserID на Log Analyzer читайте в руководстве администратора UserGate Log Analyzer. Использование UserGate Log Analyzer позволяет масштабировать технологию UserID на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer аналогичен принципу работы на UserGate NGFW. Найденные в собранных данных события отправляются на другие узлы UserGate NGFW в соответствии с политикой UserID Sharing, настроенной с помощью профилей редистрибуции. При необходимости можно отправлять разные данные на разные узлы UserGate NGFW. На NGFW отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate NGFW в сети.

Примечание

В инфраструктурах с серверами Active Directory и высоким потоком событий аутентификации (свыше 50 событий в секунду) для корректной работы функции UserID рекомендуется применять сценарий сбора событий через AD/WEC-агент вместо сценария с технологией WMI. Это связано с ограниченной производительностью технологии WMI, которая может вызывать ошибки при получении данных и приводить к некорректной работе правил фильтрации.

Алгоритм настройки UserID

Для настройки работы UserID необходимо выполнить ряд действий как на стороне источников данных аутентификации, так и на UserGate NGFW.

Настройка на стороне источников данных:

- При работе с Active Directory в качестве источника данных об аутентификации пользователей включите аудит событий безопасности. Потребуется следующие категории:
 - Audit LogOn;
 - Audit LogOff;
 - Audit Kerberos Authentication Service;
 - Audit Group Membership;
 - Audit Kerberos Service Ticket Operations.
- При работе с серверами-источниками данных syslog настройте отправку журналов на адрес UserID-агента (то есть на IP-адрес UserGate NGFW; номер порта и протокол устанавливаются в настройках UserID-агента, по умолчанию порт TCP 514).
- При работе с серверами RADIUS NAS настройте отправку сообщений RADIUS accounting на адрес UserID-агента (то есть на IP-адрес UserGate NGFW, порт UDP 1813).

Настройка на стороне UserGate NGFW:

- Создайте сервер аутентификации для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе «[Серверы аутентификации](#)».
- Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе «[Профили аутентификации](#)».
- Для сценария с серверами-источниками данных syslog активируйте сервис **UserID syslog collector** в параметрах контроля доступа зоны, где будет находиться отправитель syslog. Для сценария с RADIUS NAS-серверами активируйте сервис **Агент аутентификации** в настройках контроля доступа зон, где будет находиться серверы RADIUS NAS. Подробнее о создании и настройке зон — в разделе «[Настройка зон](#)».
- Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.
- Настройте общие параметры UserID-агента.

Создание коннектора UserID-агента

Коннектор UserID-агента в веб-консоли UserGate NGFW создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмите **Добавить** на панели инструментов и выберите тип создаваемого коннектора:

- Microsoft Active Directory;
- Отправитель syslog;
- RADIUS-сервер.

Microsoft Active Directory

В случае, если в качестве источника информации выступает Microsoft Active Directory:

1. Настройте источник событий.
2. Настройте параметры коннектора UserID-агента для мониторинга AD.

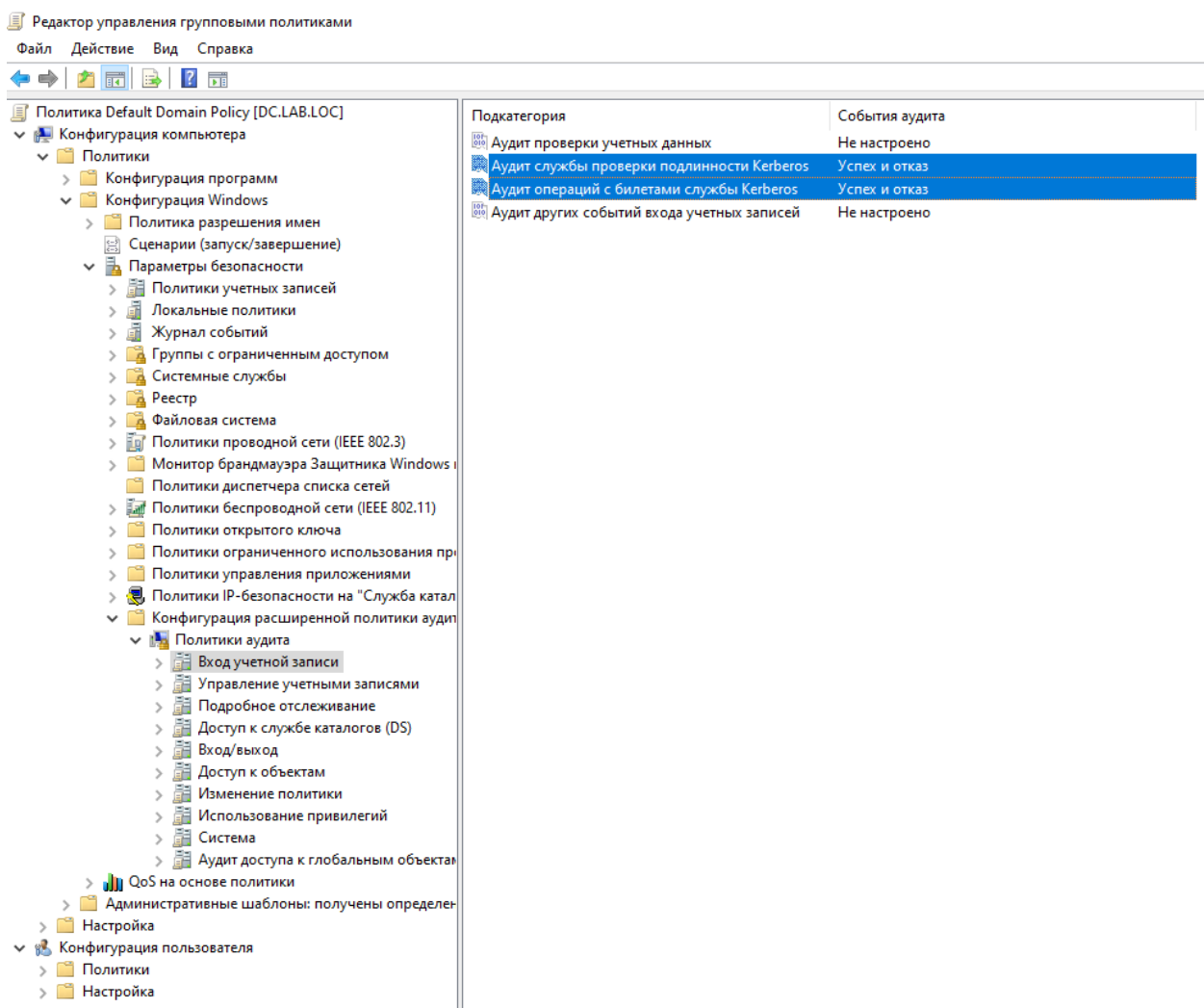
Для включения аудита событий на сервере AD отредактируйте **Политики Аудита** в **Политике домена** по умолчанию и **Конфигурацию расширенной политики**, как указано на следующих снимках экрана, используя оснастку `gpedit.msc`:

Редактор управления групповыми политиками

Файл Действие Вид Справка



Политика Default Domain Policy [DC.LAB.LOC] Конфигурация компьютера Политики Конфигурация программ Конфигурация Windows Политика разрешения имен Сценарии (запуск/завершение) Параметры безопасности Политики учетных записей Политика паролей Политика блокировки учетной записи Политика Kerberos Локальные политики Политика аудита Назначение прав пользователя Параметры безопасности Журнал событий Группы с ограниченным доступом Системные службы Реестр Файловая система Политики проводной сети (IEEE 802.3) Монитор брандмауэра Защитника Windows Политики диспетчера списка сетей Политики беспроводной сети (IEEE 802.11) Политики открытого ключа Политики ограниченного использования Политики управления приложениями Политики IP-безопасности на "Служба" Конфигурация расширенной политики Политики аудита Вход учетной записи Управление учетными записями Подробное отслеживание Доступ к службе каталогов (DS) Вход/выход Доступ к объектам Изменение политики Использование привилегий Система Аудит доступа к глобальным объектам	<table> <thead> <tr> <th>Подкатегория</th><th>События аудита</th></tr> </thead> <tbody> <tr><td>Аудит блокировки учетных записей</td><td>Не настроено</td></tr> <tr><td>Аудит заявок пользователей или устройств на доступ</td><td>Не настроено</td></tr> <tr><td>Членство в группе аудита</td><td>Успех и отказ</td></tr> <tr><td>Аудит расширенного режима IPsec</td><td>Не настроено</td></tr> <tr><td>Аудит основного режима IPsec</td><td>Не настроено</td></tr> <tr><td>Аудит быстрого режима IPsec</td><td>Не настроено</td></tr> <tr><td>Аудит выхода из системы</td><td>Успех и отказ</td></tr> <tr><td>Аудит входа в систему</td><td>Успех и отказ</td></tr> <tr><td>Аудит сервера политики сети</td><td>Не настроено</td></tr> <tr><td>Аудит других событий входа и выхода</td><td>Не настроено</td></tr> <tr><td>Аудит специального входа</td><td>Не настроено</td></tr> </tbody> </table>	Подкатегория	События аудита	Аудит блокировки учетных записей	Не настроено	Аудит заявок пользователей или устройств на доступ	Не настроено	Членство в группе аудита	Успех и отказ	Аудит расширенного режима IPsec	Не настроено	Аудит основного режима IPsec	Не настроено	Аудит быстрого режима IPsec	Не настроено	Аудит выхода из системы	Успех и отказ	Аудит входа в систему	Успех и отказ	Аудит сервера политики сети	Не настроено	Аудит других событий входа и выхода	Не настроено	Аудит специального входа	Не настроено
Подкатегория	События аудита																								
Аудит блокировки учетных записей	Не настроено																								
Аудит заявок пользователей или устройств на доступ	Не настроено																								
Членство в группе аудита	Успех и отказ																								
Аудит расширенного режима IPsec	Не настроено																								
Аудит основного режима IPsec	Не настроено																								
Аудит быстрого режима IPsec	Не настроено																								
Аудит выхода из системы	Успех и отказ																								
Аудит входа в систему	Успех и отказ																								
Аудит сервера политики сети	Не настроено																								
Аудит других событий входа и выхода	Не настроено																								
Аудит специального входа	Не настроено																								



Для выполнения WMI-запросов создайте пользователя с соответствующими привилегиями по процедуре, указанной ниже.

Внимание!

Эти настройки нужны для подключения агента по WMI посредством учетной записи с ограниченными правами.

1. Создайте учетную запись пользователя на контроллере домена:

- Перейдите в меню **Пуск → Диспетчер серверов → Средства → Active Directory — пользователи и компьютеры**.
- В соответствующем Подразделении (OU) создайте **Нового пользователя** для UserID.

2. Настройте членство в группах для новой учетной записи пользователя:

- Нажмите правой кнопкой мыши на новой учетной записи пользователя UserID и выберите **Свойства**.
- Перейдите на вкладку **Членство в группах**.
- Нажмите **Добавить → Дополнительно → Поиск**.
- Выберите следующие группы:
 - **Пользователи DCOM**;
 - **Пользователи журналов производительности**;
 - **Пользователи удаленного рабочего стола**;
 - **Читатели журнала событий**.
- Нажмите **ОК**.

3. Назначьте права Distributed Component Object Model (DCOM):

- Перейдите в меню Windows **Пуск → Администрирование → Службы компонентов**. Откроется окно **Службы компонентов**.
- Раскройте **Службы компонентов → Компьютеры → Мой компьютер**.
- Нажмите правой кнопкой мыши на **Мой компьютер** и выберите **Свойства**. Откроется окно **Свойства: Мой компьютер**.
- Перейдите на вкладку **Безопасность COM**.
- В области **Права доступа** нажмите **Изменить ограничения**.
- Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный доступ** и **Удаленный доступ**.
- Нажмите **ОК**, чтобы сохранить параметры.
- В окне **Свойства: Мой компьютер** нажмите в разделе **Разрешения на запуск и активацию** на **Изменить ограничения**.
- Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный запуск**, **Удаленный запуск**, **Локальная активация** и **Удаленная активация**.

- Нажмите **ОК**, чтобы сохранить настройки; еще раз нажмите **ОК**, чтобы закрыть окно **Свойства: Мой компьютер**.

- Выберите **Файл → Выход**, чтобы закрыть окно **Службы компонентов**.

4. Настройте назначения защиты пространства имен WMI:

- Перейдите в меню **Пуск → Выполнить**.
- Введите `wmimgmt.msc` и нажмите **ОК**.
- Нажмите правой кнопкой мыши на **Элемент управления WMI (локальный)** и выберите **Свойства**.
- Перейдите на вкладку **Безопасность**.
- Нажмите **Безопасность → Добавить → Дополнительно → Поиск**.
- Выберите новую учетную запись пользователя, нажмите **ОК**, пока вы не вернетесь в окно **Безопасность** для Root.
- Нажмите **Дополнительно** и выберите добавленную учетную запись пользователя.
- Нажмите **Изменить**.
- В меню **Применяется к:** выберите **Данное пространство и подпространство имен**.
- Убедитесь, что выбрано **Выполнение методов, Включить учетную запись, Включить удаленно** и **Прочитать безопасность**.
- Нажмите **ОК**, пока вы не вернетесь в окно `wmimgmt`.
- Выберите **Файл → Выход**, чтобы закрыть окно `wmimgmt`.

i Внимание!

Обновление Windows KB5014692 может привести к появлению ошибок доступа к WMI типа: NTSTATUS: NT_STATUS_ACCESS_DENIED. В этом случае можно попробовать добавить в реестр Windows следующую информацию:

Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat

Value Name: "RequireIntegrityActivationAuthenticationLevel"

Type: dword

Value Data: 0x00000000

При использовании серверов AD в качестве источников событий UserID-агент выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627).

В веб-консоли UserGate NGFW в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **Microsoft Active Directory**. Укажите следующие параметры:

- **Включено** — включение и отключение получения журналов с источника.
- **Название** — название источника.
- **Описание** — описание источника (опционально).
- **Адрес сервера** — адрес сервера Microsoft Active Directory.
- **Протокол** — протокол доступа к AD (WMI).
- **Пользователь** — имя пользователя для подключения к AD.
- **Пароль** — пароль пользователя для подключения к AD.
- **Профиль аутентификации** — название созданного ранее профиля аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.

- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate NGFW. Значение по умолчанию – 2700 секунд (45 минут).

Syslog

В случае, если в качестве источника информации выступает отправитель syslog:

1. Настройте источник событий.

Для корректной работы коннектора UserID-агента syslog, настройте сервер-источник данных syslog для отправки журналов на адрес UserID-агента. Подробнее см. документацию на отправитель syslog.

Параметры сервера syslog на UserGate NGFW можно посмотреть или изменить [в общих параметрах UserID-агента](#).

2. Разрешите сбор информации с удаленных устройств по протоколу syslog.

В параметрах контроля доступа зоны, в которой находится отправитель syslog, разрешите сервис **UserID syslog коллектор**.

3. Настройте параметры коннектора UserID-агента для отправителя syslog.

В веб-консоли UserGate NGFW в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора **Отправитель syslog**. Далее укажите следующие данные:

- **Включено** — включение или отключение получения журналов с источника.
- **Название** — название источника.
- **Описание** — описание источника (опционально).
- **Адрес сервера** — адрес хоста, с которого UserGate NGFW будет получать события по протоколу syslog.
- **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
- **Часовой пояс** — часовой пояс, установленный на источнике. При использовании UserID-агента для AD/WEC в syslog-коннекторе всегда

должно быть время в UTC независимо от настроек времени на контроллере домена.

- **Профиль аутентификации** — профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах syslog.
- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеша на UserGate NGFW. Значение по умолчанию: 2700 секунд (45 минут).

На вкладке **Фильтры** выбираются фильтры для поиска необходимых записей журнала.

Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «[Syslog фильтры UserID-агента](#)».

RADIUS accounting

В случае, если источником информации выступают сообщения RADIUS accounting (доступно в версии 7.2.0 и выше):

1. Настройте источник событий.

Для корректной работы коннектора UserID-агента, настройте NAS-сервер для отправки сообщений RADIUS accounting на адрес UserID-агента (порт UDP 1813). Подробнее см. документацию на NAS-сервер.

2. Разрешите получение запросов RADIUS accounting от удаленных устройств.

В параметрах контроля доступа зон, в которых находятся NAS-серверы, разрешите сервис **Агент аутентификации**.

3. Настройте параметры коннектора UserID-агента для RADIUS-сервера.

В веб-консоли UserGate NGFW в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **RADIUS-сервер**. Укажите следующие данные:

- **Включено** — включение и отключение получения журналов с источника.
- **Название** — название источника.

- **Описание** — описание источника (опционально).
- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти. Значение по умолчанию – 2700 секунд (45 минут).
- **Профиль аутентификации** — профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах RADIUS accounting.
- **Атрибут для имени** — номер radius attribute type, в котором находится имя пользователя. Значение по умолчанию: 1.
- **Атрибут для групп** — номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
- **Домен по умолчанию** — имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
- **Секретный код** — общий ключ, используемый протоколом RADIUS для аутентификации.

На вкладке **Адреса** указываются адреса хостов (NAS-серверов), с которых UserID-агент будет получать события RADIUS accounting:

Настройка UserID-агента

Настройка общих параметров UserID-агента производится в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**. Нажмите **Редактировать** на панели инструментов.

На вкладке **Общие** настраиваются интервалы опроса данных:

- **Интервал опроса WMI** — период опроса серверов Active Directory. Значение по умолчанию: 120 секунд.
- **Интервал опроса syslog** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей syslog-источников. Значение по умолчанию: 60 секунд.
- **Интервал опроса RADIUS** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей по RADIUS-логу (доступно в версии 7.2.0 и выше). Значение по умолчанию: 120 секунд.

На вкладке **Протоколы syslog** настраиваются параметры соединения с сервером syslog.

Для протокола TCP:

- **Включено** — включение и отключение протокола TCP для приема журналов syslog.
- **Порт** — номер порта, используемого для сбора syslog-событий. По умолчанию: порт 514.
- **Максимальное количество сессий** — максимальное количество устройств, подключенных одновременно с целью отправки сообщений.
- **Безопасное соединение** — включение и отключение шифрования потока данных.
- **Файл сертификата УЦ** — сертификат удостоверяющего центра, который используется для установления безопасного соединения.
- **Файл сертификата** — сертификат, созданный пользователем и подписанный удостоверяющим центром.

Для протокола UDP:

- **Включено** — включение и отключение протокола UDP для приема журналов syslog.
- **Порт** — номер порта, используемого для сбора syslog-событий. По умолчанию: порт 514.

На вкладке **Списки Ignore server** указываются списки IP-адресов, события от которых будут проигнорированы UserID-агентом. Запись об игнорировании источника появится в журнале UserID:

Список может быть создан в разделе **Библиотеки → IP-адреса**, или при настройке UserID-агента (нажмите **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов — в разделе «[IP-адреса](#)».

Этот параметр является глобальным и относится ко всем источникам.

На вкладке **Списки Ignore user** указываются имена пользователей, события от которых будут проигнорированы UserID-агентом. Поиск производится по Common Name (CN) пользователя AD.

Этот параметр является глобальным и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.

Важно!

При задании имени допустимо использовать символ астериск (*) только в конце строки.

Примечание

При подключении UserGate NGFW к UserGate Log Analyzer возможна одновременная работа UserID-агентов, настроенных на обоих устройствах. Агенты устройств будут работать независимо друг от друга. События журналов UserID-агента, полученные UserGate NGFW, как и события других журналов, будут переданы на UserGate Log Analyzer.

Журналирование

UserID-агент периодически обращается к настроенным источникам данных. Полученные события сохраняются в служебной базе данных без каких-либо изменений. Содержимое этой базы можно посмотреть в соответствующих журналах:

- Журнал Windows AD коннектора;
- Syslog коннектор;
- RADIUS коннектор.

В веб-консоли UserGate NGFW журналы доступны в разделе **Журналы и отчеты → Журналы → Агент UserID**:

UserID-агент периодически обращается к служебной базе данных и извлекает из записей событий имя пользователя, SID, домен, IP-адрес, списки групп. Результаты обработки записей событий заносятся в журнал UserID-агент события аутентификации. Посмотр журнала доступен в том же разделе: **Журналы и отчеты → Журналы → Агент UserID**.

О журналах источников данных и UserID-агента — в разделе «[Агент UserID](#)» документации.

Описание форматов экспорта журналов UserID доступно в Приложении в разделе «[Описание форматов журналов](#)».

Radius accounting

NGFW может прозрачно аутентифицировать пользователей, уже прошедших аутентификацию на внешнем сервере RADIUS. NGFW не взаимодействует с сервером RADIUS, а только отслеживает информацию RADIUS accounting, перенаправленную от RADIUS клиента. RADIUS accounting содержит информацию об имени и IP-адресе пользователя. Для настройки нужно выполнить следующие шаги:

Наименование	Описание
Шаг 1. Завести пользователя в NGFW.	Завести необходимых локальных пользователей в NGFW. Смотрите раздел Пользователи .
Шаг 2. Разрешить сервис Агент авторизации на требуемой зоне.	В разделе Сеть → Зоны , выберите зону, на интерфейс которой планируется отсылать RADIUS-accounting. Разрешите сервис Агент авторизации .
Шаг 3. Настроить пароль агентов терминального сервиса.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажмите на кнопку Настроить и укажите пароль агента терминального сервиса. Данный пароль будет использоваться в качестве RADIUS secret при настройке сервера RADIUS.
Шаг 4. Добавить источник RADIUS accounting в веб-консоли NGFW.	В разделе Пользователи и устройства → Терминальные серверы необходимо добавить источник информации RADIUS accounting, указав имя и IP-адрес хоста.
Шаг 5. Настроить RADIUS accounting.	Настроить отсылку информации RADIUS accounting на NGFW, указав в качестве IP-адреса сервера IP-адрес NGFW, порт — UDP 1813. Указать RADIUS secret, совпадающий с паролем агента для терминального сервера, указанным на шаге 3. Имя пользователя необходимо передавать в атрибуте RADIUS User-Name (type=1), IP-адрес пользователя — в атрибуте RADIUS Framed-IP-Address (type=8), а IP-адрес сервера RADIUS — в атрибуте RADIUS NAS_IP_Address (type=4). Более подробно о настройке сервера RADIUS смотрите в руководстве на используемый вами сервер RADIUS и RADIUS клиент. Важно! Период обновления информации RADIUS accounting должен быть не более 120 секунд.

После выполнения данной настройки, NGFW будет сопоставлять имя пользователя и присылаемый сервером RADIUS accounting IP-адрес пользователя. В зависимости от передаваемой информации NGFW будет вести себя следующим образом:

Наименование	Описание
RADIUS сервер прислал имя пользователя, который не заведен на NGFW.	На Accounting-запрос будет ответ Accounting reject. Данные о пользователях не изменятся.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Start или Interim-Update.	Указанному пользователю присвоится переданный IP-адрес. Имя пользователя начнет отображаться в журналах для данного IP-адреса. Пользовательские правила начнут применяться для трафика данного IP-адреса. Если у пользователя уже был IP-адрес, отличный от переданного, то пользователю будет присвоено 2 и более IP-адресов. Если пользователю уже присвоен данный IP-адрес, то ничего не происходит. Если этот IP-адрес присвоен другому пользователю, то он будет удален у того пользователя и будет присвоен пользователю, указанному в запросе.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Stop.	У указанного пользователя удалится переданный IP-адрес. Имя пользователя перестанет отображаться в журналах для данного IP адреса. Пользовательские правила перестанут применяться для трафика данного IP-адреса.

Агент аутентификации для Windows

Для пользователей, работающих на операционной системе Windows, входящих в домен Active Directory, существует еще один способ аутентификации — использовать специальный агент аутентификации. Агент представляет собой сервис, который передает на NGFW информацию о пользователе, его имя и IP-адрес, соответственно, NGFW будет однозначно определять все сетевые подключения данного пользователя, и аутентификация другими методами не требуется. Чтобы начать работу с идентификацией пользователей с помощью агента аутентификации, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис Агент аутентификации на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис Агент аутентификации для той зоны, со стороны которой находятся пользователи.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе UserGate → Настройки → Модули напротив записи Пароль агентов терминального сервиса нажать на кнопку Настроить и задать пароль агентов терминального сервера.
Шаг 3. Установить агент аутентификации.	Установить агент аутентификации на все компьютеры, для которых необходимо идентифицировать пользователей. Агент может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 ГБ оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске. Агент аутентификации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. С помощью административного шаблона администратор может задать IP-адрес и порт UserGate NGFW, и заданный на предыдущем шаге пароль. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft. Агент может быть установлен и без использования групповых политик. Для этого необходимо установить агент из инсталлятора и указать необходимые параметры для подключения к UserGate NGFW в следующих ключах реестра: <pre>[HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""</pre>

NGFW теперь будет получать информацию о пользователях. В политиках безопасности можно использовать имена пользователей, как они указаны в Active Directory, для этого необходим настроенный LDAP-коннектор. Если коннектор не настроен, то можно использовать пользователей **Known** и **Unknown**.

i Примечание

В параметрах агента в качестве адреса назначения «ServerIP» следует указывать IP-адрес интерфейса UserGate NGFW, на который поступают запросы агента, или FQDN, разрешающийся в этот IP-адрес.

Установленный агент аутентификации отправляет информацию обо всех IP-адресах, назначенных на интерфейсы устройства. В некоторых сценариях может возникнуть необходимость исключать из этой информации определенные IP-адреса с помощью указания сети или диапазона в настройках агента.

Исключить рассылку определенных адресов и/или подсетей агентом аутентификации можно с помощью параметра **ExcludeIP**. Параметр ExcludeIP может иметь следующие настройки:

- IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n, указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
- Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
- Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
- Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP**. Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore**.

Параметр ExcludeIP может быть активирован в системе несколькими способами:

- Добавлен в файл конфигурации агента tsagent.cfg, который создается в разделе: \users\<username>..ApplicationData\Entensys. После внесения изменений агент аутентификации необходимо перезапустить. В этом случае настройки параметра будут действовать только для пользователя, под учетной записью которого создан файл.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом

случае настройки параметра будут действовать только для данного пользователя.

- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Прокси-агент для Windows

Для пользователей, работающих на операционной системе Windows, существует возможность предоставить доступ в интернет через явно указанный прокси-сервер программам, которые не поддерживают работу через прокси-сервер. Иногда также возникает необходимость предоставить таким программам доступ в интернет в случае, когда NGFW не является шлюзом в интернет по умолчанию для пользовательских компьютеров. Для подобных случаев можно использовать прокси-агент. Прокси-агент пересылает все TCP-запросы, идущие не на локальные адреса, на NGFW, который выступает для них прокси-сервером.

Примечание

Прокси-агент не авторизует пользователя на NGFW, таким образом, если необходима авторизация, то потребуются настроить один из способов авторизации пользователей, например, установить агент авторизации для Windows.

Установить прокси-агент возможно вручную либо с использованием политик Active Directory.

Прокси-клиент может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 ГБ оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске.

Если устанавливаете не политикой, то для настройки агента необходимо создать текстовый файл `utmagent.cfg` в директории `%ALLUSERSPROFILE%\Entensys\UTMAgent\`. В файле конфигурации следует указать:

`ServerName=10.255.1.1`

`ServerHttpPort=8090`

`LocalNetwork=192.168.1.0/24; 192.168.0.0/24; 192.168.30.0/24;`

где `ServerName` и `ServerHttpPort` — IP-адрес и порт прокси-сервера на NGFW, по умолчанию это порт 8090.

Примечание

LocalNetwork — список сетей, которые не нужно направлять в прокси. Сеть интерфейсов машины не направляется в прокси по умолчанию.

Если запрос от программы, установленной на компьютере, происходит на адрес, находящийся в одной подсети с адресом интерфейса компьютера, то этот запрос не перехватывается прокси-агентом и не перенаправляется на адрес прокси-сервера. Аналогично, если какая-либо программа, установленная на этом компьютере, обращается на адрес из подсети, указанной в параметре `LocalNetwork`, то этот запрос также не перенаправляется агентом на прокси-сервер.

Сервис прокси-агента слушает локальный порт 8080.

После создания или изменения файла конфигурации необходимо перезапустить сервис прокси-агента.

Если вы устанавливаете через GPO, прокси-агент поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft

Все необходимые параметры для корректной работы прокси-агента задаются при настройке групповой политики. При установке параметры вносятся в реестр пользовательского компьютера и имеют приоритет перед файлом `.cfg`. При удалении агента политикой значения реестра не удаляются, сохраняясь в ветке реестра:

`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Entensys\UTMAgent`

Управление гостевыми пользователями

UserGate NGFW позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или email.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать администратора гостевых пользователей (опционально).	- В разделе Администраторы нажать кнопку Добавить и создать профиль администратора, разрешающий Гостевой портал для чтения и записи в закладке Разрешения для веб-консоли. Данный профиль дает доступ в консоль управления временными пользователями. - Создать учетную запись администратора и назначить ей созданную роль. Более подробно о создании администраторов NGFW смотрите соответствующий раздел руководства.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Подключиться к консоли управления Гостевого портала.	В браузере перейти на адрес https://IP_NGFW:8001/ta Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1.
Шаг 4. Создать список пользователей.	В консоли нажать на кнопку Добавить и заполнить поля: - Количество пользователей. - Комментарий. Дата и время окончания — время, когда учетная запись гостевого пользователя будет отключена.

Наименование	Описание
	• Длина пароля — определяет длину пароля для создаваемого пользователя. • Сложность пароля — определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спецсимволы. • Время жизни — продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена. • Группа — созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи.

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через email).	В разделе Библиотеки → Профили оповещений нажать кнопку Добавить и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений .
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи.	В разделе Пользователи и устройства в подразделе Captive-профили создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон Captive portal: email auth или Captive portal: SMS auth , в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времена действия учетной записи. Более

Наименование	Описание
	подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений .
Шаг 4. Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль.	В разделе Пользователи и устройства → Captive-портал создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства Настройка Captive-портала .

Конечные устройства UserGate Client

Под конечными устройствами подразумеваются пользовательские компьютеры с установленным ПО UserGate Client.

ПО UserGate Client (UGC) является компонентом экосистемы UserGate SUMMA. С помощью UserGate Client вы можете централизованно управлять парком конечных устройств. Установка UGC на компьютеры пользователей позволяет получать информацию о состоянии устройств, например, такую как, загрузка процессора, критические события, произошедшие на устройстве, журналы различных сервисов, журналы и оповещения от антивирусных продуктов и т. п. Объем информации, получаемой с конечных устройств UGC, будет постоянно расширяться.

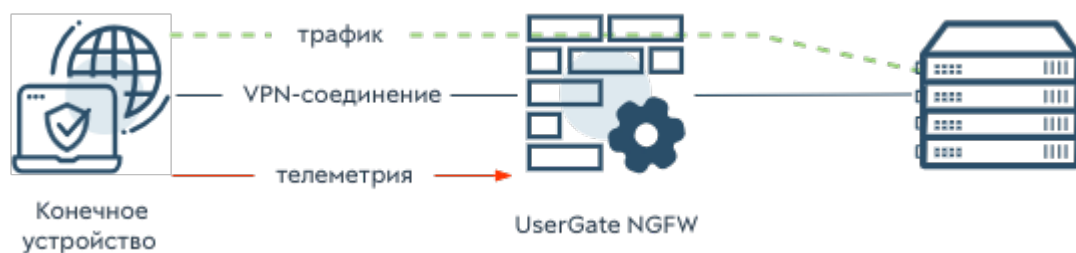
Телеметрическая информация, журналы ОС и другие данные о безопасности конечных устройств передаются в системы сбора и анализа событий (UserGate LogAn и UserGate SIEM) и могут быть использованы для автоматического реагирования на угрозы безопасности.

ПО UserGate Client разработано для операционных систем [Windows](#), [Linux](#), [macOS](#).

Работа UserGate Client в связке с UserGate NGFW

Регистрация конечных устройств и проверка на соответствие требованиям безопасности на UserGate NGFW возможна только с версией [UserGate Client для Windows](#).

Взаимодействие между конечными устройствами и UserGate NGFW происходит по порту 4045 с использованием протокола HTTPS.



Регистрация конечного устройства происходит после подключения устройства к UserGate NGFW по VPN. При первом подключении конечное устройство проверяет корректность сертификата, указанного на UserGate NGFW для установки SSL-соединения, запоминает сертификат и далее использует его для проверки.

Примечание

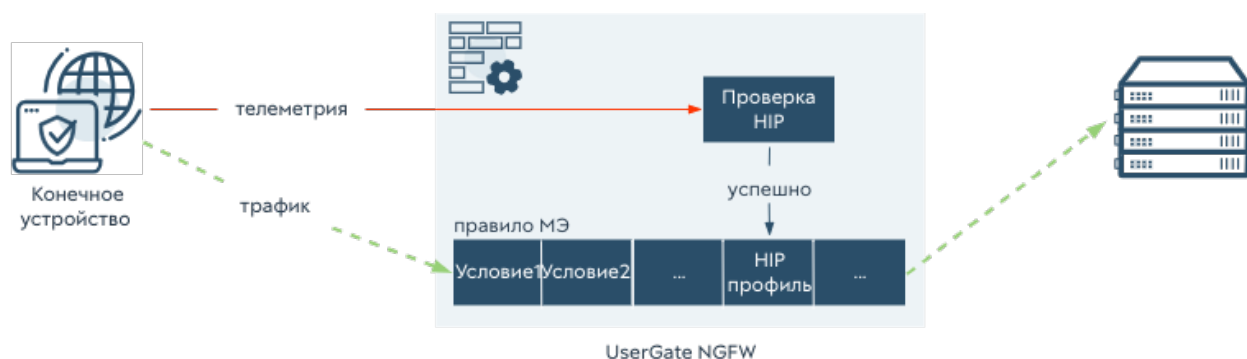
Если сертификат был изменен, то необходимо распространить корневой сертификат удостоверяющего центра (Root CA) на подключенные конечные устройства; сертификат должен быть установлен в хранилище доверенных корневых центров сертификации локального компьютера.

После регистрации каждому новому конечному устройству присваивается уникальный идентификатор, который хранится в базе UserGate NGFW. Тайм-аут активности конечных устройств составляет 2 минуты, т.е., если в течение 2-х минут на UserGate NGFW не поступает информация от конечного устройства, то оно считается неактивным. После истечения трёх периодов неактивности запись о конечном устройстве удаляется из базы; при повторном подключении конечное устройство будет зарегистрировано. Если конечное устройство будет подключено до истечения этого времени, то его запись будет обновлена.

После подключения к другому VPN-серверу, конечное устройство будет зарегистрировано на новом UserGate NGFW.

Проверка HIP на UserGate NGFW

Проверка на соответствие требованиям безопасности (комплаенса) происходит по следующей схеме:



Конечное устройство отправляет на UserGate NGFW:

- информацию о пользователях;
- данные о системе (версия, издание, netbios-имя);
- список запущенных процессов;
- список запущенных служб;
- список установленного программного обеспечения (название, вендор, версия);
- ключи реестра, которые используются в НИР объектах;
- список обновлений системы;
- элементы автозагрузки;
- информацию о защищенности системы (антивирус, межсетевой экран, BitLocker и т.п.);
- информацию о точках восстановления системы.

Полученные от конечного устройства данные расшифровываются и передаются для сравнения с НИР-профилями. Информация о результате проверки передается далее для использования в правилах межсетевого экрана. Если конечное устройство подходит под все условия правила межсетевого экрана, то это правило становится активным для данного конечного устройства.

i Примечание

Если ОС конечного устройства присылает некорректную задвоенную информацию об установленном одинаковом антивирусном ПО с различными статусами (один со статусом включен, другой — выключен), то при проверке HIP учитывается наихудший случай (антивирус выключен). Статус обновления баз антивирусного ПО проверяется только для включенного антивируса.

Регистрация конечного устройства на UserGate NGFW

Подключение конечного устройства к UserGate NGFW происходит в автоматическом режиме после подключения к VPN-серверу, данные которого вводятся в начальном окне графического интерфейса приложения. Встроенный в ПО UserGate Client VPN-клиент использует следующие настройки для установки соединения VPN:

- режим IKE (при использовании IKEv1): основной;
- Dead Peer Detection (DPD): режим On idle.
- группы Диффи-Хеллмана: группа 2 Prime 1024, группа 14 Prime 2048, группа 16 Prime 4096;
- пары алгоритмов аутентификации и шифрования (фазы 1 и 2): SHA1/AES128, SHA256/AES128, SHA384/AES128, SHA1/AES256, SHA256/AES256, SHA384/AES256, SHA1/3DES, SHA256/3DES, SHA384/3DES;
- максимальный размер данных, шифруемых одним ключом (фаза 2): не ограничен.

i Примечание

Если конечное устройство подключено к UserGate MC, перерегистрации на UserGate NGFW после установки VPN-соединения не произойдет.

i Примечание

Для работы с конечными устройствами UserGate Client необходимо наличие лицензии. В случае отсутствия соответствующей лицензии регистрации конечного устройства на UserGate NGFW не произойдет; будет установлено только VPN-соединение.

i Примечание

В режиме ожидания (idle), активируется проверка доступности соседнего узла при отсутствии трафика IPsec в туннеле. Согласно настройке по умолчанию DPD будет выполняться каждые 15 секунд, 5 раз. В общей сложности через полторы минуты без ответов DPD вторая сторона будет считаться недоступной и соединение будет разорвано.

Для подключения конечного устройства необходимо:

Наименование	Описание
Шаг 1. Разрешить подключение конечных устройств на зоне.	На зоне, используемой для VPN-подключений разрешить сервис Подключение конечных устройств .
Шаг 2. Указать данные для установки SSL-соединения между конечным устройством и UserGate NGFW.	В разделе UserGate → Настройки укажите сертификат и профиль для установки SSL-соединения. При подключении конечное устройство будет проверять валидность сертификата. В случае смены сертификата на UserGate NGFW при наличии уже подключенных конечных устройств необходимо распространить корневой сертификат удостоверяющего центра (Root CA); сертификат необходимо поместить в хранилище локального компьютера Доверенные корневые центры сертификации . Для взаимодействия конечного устройства и UserGate NGFW используется порт TCP 4045.
Шаг 3. Настроить UserGate NGFW в качестве VPN-сервера.	Настройте VPN на UserGate NGFW, к которому будет подключено конечное устройство. После установки VPN-соединения регистрация конечного устройства произойдет автоматически. Политики безопасности, настроенные на UserGate NGFW, также будут применены к конечным устройствам. Важно! Для проверки на соответствие требованиям безопасности (комплаенса) конечное устройство будет отправлять телеметрию на UserGate NGFW с периодичностью в 1 минуту.

Конечное устройство будет производить попытку регистрации каждый раз после подключения к новому VPN-серверу.

Примечание

Встроенный в ПО UserGate Client VPN-клиент предполагает подключение только к серверам, настроенным на UserGate NGFW.

Примечание

Для подключения по IKEv2 не заполняйте поле *Passphrase*. При установке соединения приложение выполнит запрос к VPN-серверу и, в случае его корректной настройки, автоматически определит способ подключения (по сертификату или логину/паролю).

UserID-агент для серверов AD, WEC

UserID-агент для AD- и WEC-серверов — это программный компонент, который устанавливается на сервере — контроллере домена или на сервере WEC (Windows Event Collector). Агент считывает необходимую для идентификации пользователя информацию из журналов безопасности Windows и пересылает ее в формате `syslog` в коллектор UserID на устройствах UserGate Log Analyzer или UserGate NGFW.

Основные функции UserID-агента для AD- и WEC-серверов:

- Работа в качестве сервиса.
- Настройка параметров работы через файл конфигурации.
- Чтение журналов безопасности Windows и отправка событий на UserID-коллектор через `syslog`.
- Ведение файла журнала и его ротация. Возможность включить режим отладки журналирования.

Для работы агента в качестве источника данных в сценарии аутентификации с помощью UserID необходимо:

1. Установить и настроить UserID-агент для AD- и WEC-серверов.

2. Настроить сбор информации об аутентификации пользователей [на UserGate Log Analyzer](#) или [на UserGate NGFW](#) с помощью коннектора с типом syslog.
3. Настроить работу функции UserID [на UserGate Log Analyzer](#) или [на UserGate NGFW](#).

Установка и настройка агента

UserID-агент для AD- и WEC-серверов поставляется в формате установочного файла.

Для установки агента:

1. Скачайте последнюю версию агента [с официального сайта UserGate](#).
2. Распакуйте архив и запустите установочный MSI-файл.
3. По завершении установки перейдите в рабочую папку агента (по умолчанию: `C:\Program Files (x86)\UserGate\useridagent`) и отредактируйте файл конфигурации `useridagent.cfg`, добавив параметры вашей сети. Подробнее о параметрах и формате файла конфигурации — в разделе «[Настройка](#)».
4. Перезапустите сервис **UserIDAgent** через встроенное приложение **Windows Services** («Службы»).

Удалить агент можно через панель управления:

1. Нажмите комбинацию клавиш **Win + R** и выполните команду `control`.
2. В панели управления перейдите в раздел **Программы → Программы и компоненты**.
3. Найдите в списке нужное приложение и нажмите **Удалить**.

Настройка

Чтобы настроить агент, отредактируйте его конфигурационный файл. Вы можете изменить или добавить следующие параметры:

- **EventFileNames** — имена журналов для чтения. Значение по умолчанию: **Security**.
- **MaxLogSize** — максимальный размер файла журнала в МБ. Значение по умолчанию: **10**.

- **EventIDs** — номера событий для пересылки. Например, 4624,4634 (ID событий входа в сеть и выхода из сети).
- **DebugLogs** — включение или отключение режима отладки. 0 — журналируются основные события, 1 — журналируется расширенный список событий. Значение по умолчанию: 1.
- **UserExclude** — список пользователей, для которых события не должны собираться.
- **NetworkList** — список подсетей, в которых собираются события UserID.
- **GatewayList** — список шлюзов (узлы UserGate Log Analyzer, UserGate NGFW), на которые отправляются найденные события.

Синтаксис конфигурационного файла:

- Разделителем между параметрами в списках является символ запятой, пробелы после запятой игнорируются.
- Строки, начинающиеся с символов: «;» и «#», являются комментариями.
- Раздел [default] является необязательным, при использовании раздел должен сохранять указанное название. Перечень подсетей и шлюзов следует указывать в других разделах, названия которых могут быть произвольными. Названия разделов указываются в квадратных скобках.
- В файле конфигурации должен быть минимум один раздел с одной подсетью и одним шлюзом.

Пример конфигурации:

```
[default]
MaxLogSize=10
EventIDs=4634, 4624
EventFileNames=Security
DebugLogs=1
UserExclude=adm_, sys_
[net1]
NetworkList=192.168.30.0/24,172.30.250.0/24
GatewayList=192.168.45.1:514,192.168.45.2:514
[net2]
NetworkList=192.168.200.0/24,10.10.0.0/16
GatewayList=192.168.45.4:514,192.168.45.5:514
```

Пример минимальной конфигурации:

```
[net1]
NetworkList=192.168.30.0/24
GatewayList=192.168.45.1
```

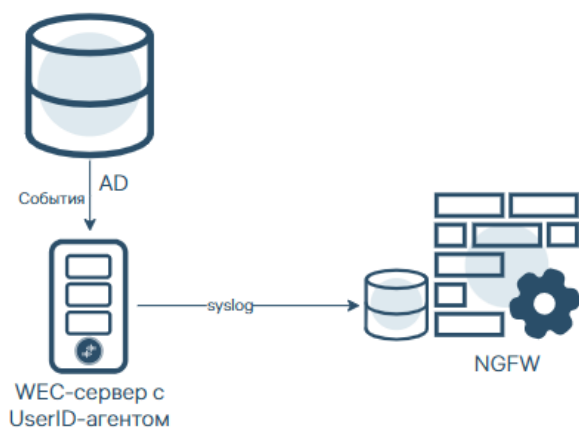
Журналирование

UserID-агент записывает информацию о событиях в файл `uidagent.log`, размер которого контролируется параметром `MaxLogSize`. При достижении лимита:

- текущий файл журнала сохраняется с расширением `.bak`, заменяя предыдущую версию файла;
- начинается запись нового файла журнала.

Для хранения всех записей работы сервиса рекомендуется настроить внешнее копирование файлов журнала с помощью специализированных сервисов.

Интеграция с UserGate NGFW



Для получения информации об аутентификации пользователей выполните настройку следующих параметров на UserGate NGFW:

1. Активируйте сервис `UserID syslog collector` в параметрах контроля доступа зоны, в которой находится UserID-агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе [«Настройка зон»](#).

2. Настройте параметры аутентификации для UserID-агента в домене для получения информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь:

- Создайте сервер аутентификации на основе LDAP-коннектора для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе [«Серверы аутентификации»](#).
- Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе [«Профили аутентификации»](#).

3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

Коннектор UserID-агента в веб-консоли UserGate NGFW создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмите **Добавить** и выберите тип создаваемого коннектора и выберите тип создаваемого коннектора **Отправитель syslog**. Укажите параметры коннектора:

- На вкладке **Общие**:
 - **Включено** — включение или отключение получения журналов от источника данных.
 - **Название** — название источника данных.
 - **Описание** — описание источника данных.
 - **Адрес сервера** — адрес узла, с которого UserGate NGFW будет получать события по протоколу **syslog**.
 - **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
 - **Часовой пояс** — часовой пояс, установленный на источнике. При работе с AD- и WEC-серверами через UserID-агент в syslog-коннекторе всегда указывается время в формате UTC+0. Этот параметр не зависит от часового пояса, установленного на контроллере домена.
 - **Профиль аутентификации** — профиль аутентификации, с помощью которого UserID-агент обращается к контроллеру домена по LDAP-протоколу для получения

информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь.

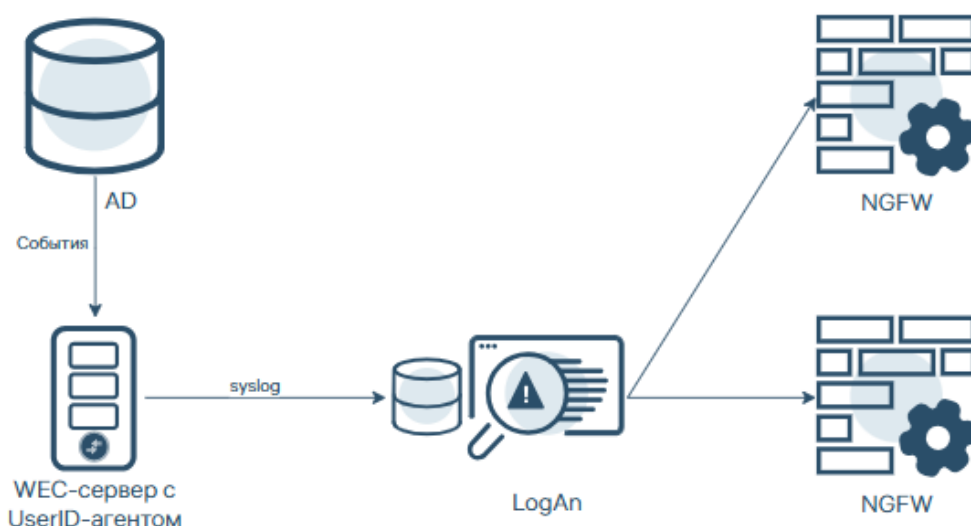
- **Время жизни аутентифицированного пользователя (сек.)**
— период времени, по истечении которого сессия пользователя будет завершена (то есть информация о нем будет удалена из кэш-памяти на UserGate NGFW). Значение по умолчанию: 2700 секунд (45 минут).
- На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «[Syslog-фильтры UserID-агента](#)».

Параметры сервера syslog на UserGate NGFW можно посмотреть или изменить в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**.

О настройке функции UserID на UserGate NGFW — в разделе «[UserID-агент](#)».

Интеграция с UserGate Log Analyzer

Благодаря интеграции источника данных об аутентификации пользователей с UserGate Log Analyzer функцию UserID можно масштабировать на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer аналогичен принципу работы на UserGate NGFW. Найденные в собранных данных события отправляются на другие UserGate NGFW в соответствии с политикой UserID Sharing на основании настроенных профилей редистрибуции. На NGFW отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate NGFW в корпоративной сети.



Для получения информации об аутентификации пользователей выполните настройку следующих параметров на на UserGate Log Analyzer:

1. Активируйте сервис **Сборщик логов** в параметрах контроля доступа зоны, в которой находится UserID агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе [«Настройка зон»](#).
2. Создайте каталог пользователей для организации доступа UserGate LogAn к серверу AD. Доступ к AD позволяет при необходимости обновлять информацию об имени пользователя в журналах, импортированных из различных сенсоров. Подробнее о создании и настройке серверов аутентификации — в разделе [«Каталоги пользователей»](#).
3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

Коннектор UserID-агента в веб-консоли UserGate Log Analyzer создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмите **Добавить** и выберите тип создаваемого коннектора и выберите тип создаваемого коннектора **Отправитель syslog**. Укажите параметры коннектора:

- На вкладке **Общие**:
 - **Включено** — включение или отключение получения журналов от источника данных.
 - **Название** — название источника данных.
 - **Описание** — описание источника данных.

- **Адрес сервера** — адрес узла, с которого UserGate Log Analyzer будет получать события по протоколу **syslog**.
 - **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
 - **Часовой пояс** — часовой пояс, установленный на источнике. При использовании UserID-агента для AD- и WEC-серверов в syslog-коннекторе всегда указывается время в формате UTC+0. Этот параметр не зависит от часового пояса, установленного на контроллере домена.
 - **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена (то есть информация о нем будет удалена из кэш-памяти на UserGate NGFW). Значение по умолчанию: 2700 секунд (45 минут).
 - **Профиль редистрибуции UserID** — профиль для определения круга устройств UserGate NGFW, на которые отправляется информация о найденных UserID-агентом пользователях.
- На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «[Syslog-фильтры UserID-агента](#)».
 - На вкладке **Каталоги пользователей** выбираются каталоги, в которых происходит поиск пользователя, найденного в журналах syslog.

Общие параметры syslog-сервера на UserGate Log Analyzer можно посмотреть или изменить в разделе **Настройки → Сборщик логов → Syslog**.

О настройке функции UserID на UserGate Log Analyzer — в разделе «[UserID](#)».

ПОЛИТИКИ СЕТИ

Общие сведения

Раздел «Политики сети» содержит настройки ключевых механизмов управления трафиком UserGate NGFW.

В этом разделе вы можете:

- Управлять прохождением трафика с помощью [правил межсетевого экрана](#). В условиях фильтрации могут использоваться зоны, адреса источника и назначения, пользователи и группы пользователей, сервисы.
- Выполнять трансляцию IP-адресов и портов сетевых пакетов с помощью [правил NAT и маршрутизации](#) для решения задач защиты внутренней сети, публикации внутренних ресурсов в интернете и объединения сетей.
- Распределять входящий трафик между публикуемыми ресурсами с помощью [правил балансировки нагрузки](#).
- Контролировать использование пропускной способности пользователями, узлами, сервисами и приложениями с помощью [правил управления пропускной способностью](#).

События срабатывания правил регистрируются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включенной опции журналирования в свойствах правил.

Межсетевой экран

С помощью правил межсетевого экрана вы можете разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate NGFW. В качестве условий правила могут выступать зоны и IP-адреса источника или назначения, пользователи, группы, сервисы.

События срабатывания правил межсетевого экрана отображаются в журнале трафика (**Журналы и отчеты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок *Инvertировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

i Примечание

Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещен.

В разрешающих правилах межсетевого экрана могут быть использованы [профили COB](#) или [профили приложений](#) (L7), содержащие настроенные наборы сигнатур. После того, как трафик попадает в первое сработавшее разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей COB или L7. При срабатывании сигнатур к трафику применяется действие, настроенное в профиле, и производится соответствующая запись в журналах (в **Журнале трафика** – для приложений и в **Журнале COB** – для COB), если в профилях была включена опция **Журналирование**.

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Чтобы создать правило межсетевого экрана, перейдите в раздел **Настройки → Политики сети → Межсетевой экран**, нажмите **Добавить** и укажите необходимые параметры правила.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила

Параметр	Описание
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Опция доступна в версии 7.3.0 и выше
Описание	Описание правила
Действие	Возможные действия правила: • Запретить — блокировать прохождение трафика; • Разрешить — разрешить прохождение трафика
Профиль приложений	Профиль приложений, созданный заранее в разделе Библиотеки → Профили приложений. Профиль приложений содержит набор сигнатур приложений, предназначенный для анализа трафика на 7 уровне модели OSI. Подробнее о создании и настройке профилей приложений — в разделе «Профили приложений» i Важно! Профиль приложений является дополнительным параметром для активации механизма анализа трафика. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.

Параметр	Описание
Профиль COB	Профиль COB, созданный заранее в разделе Библиотеки → Профили COB. Профиль COB содержит набор сигнатур, предназначенный для защиты определенных сервисов. Подробнее о создании и настройке профилей COB — в разделе «Профили COB» Важно! Профиль COB является дополнительным параметром для активации механизма анализа трафика. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.
Отбросить и	Настройка этого параметра доступна для правил, блокирующих трафик (выбрано действие Запретить). Параметр может принимать одно из следующих значений: • Не выбран. • Посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • Посылать TCP reset — блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указание сервиса (вкладка Сервис), использующего протокол TCP. • Посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
Сценарий	Выбор сценария для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии» Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.

Параметр	Описание
Журналирование	Управление записью в журнал информации о трафике при срабатывании правила. Возможные значения параметра: • Журналировать начало сессии. В журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет. В журнал трафика будет записываться информация о каждом передаваемом сетевом пакете. С этим режимом рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет. В этом случае информация в журнал не будет записываться
Источник	Указание зоны, списков IP-адресов, списков GeoIP-адресов, списков URL источника трафика. Списки URL должны включать только имена доменов.  Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate NGFW выполняет разрешение доменных имен в IP-адреса и хранит полученный результат в кэш-памяти на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Указание списка пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»

Параметр	Описание
Назначение	Указание зоны, списков IP-адресов, списков GeoIP-адресов, списков URL назначения трафика. Списки URL должны включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate NGFW выполняет разрешение доменных имен в IP-адреса и хранит полученный результат в кэш-памяти на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Указание типа сервиса, например, HTTP или HTTPS
Время	Выбор интервала времени, когда правило активно
НIP-профили	Выбор НIP-профилей, созданных в разделе Библиотеки → НIP профили. НIP-профили содержат набор НIP-объектов и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). Подробнее о создании и настройке НIP-профилей — в разделе «НIP профили» Важно! В случае выключения НIP-профиля, он будет помечен серым цветом, а правило межсетевого экрана продолжит работать без условия проверки комплаенса.
Использование	

Параметр	Описание
	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний, таблица срабатываний по приложениям. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т. п.

Расширенный поиск в разделе **Настройки → Политики сети → Межсетевой экран** доступен по следующим параметрам.

Параметр	Описание
enabled	Фильтр по состоянию правил (включены или отключены): • true — показывает только включенные правила; • false — показывает только отключенные правила
pos	Поиск по позиции правила в списке (1, 2 и т. д.)
log	Поиск правила по включенной или выключенной функции журналирования. Возможны следующие значения: • true или enabled — отображение правил, в которых включена функция журналирования (журналировать начало сессии или журналировать все сетевые пакеты). • false или disabled — отображение правил, в которых журналирование отключено. • all — отображение правил, в которых настроено журналирование всех сетевых пакетов. • start — отображение правил, в которых настроено журналирование начала сессии
name	Поиск правил по названию
action	Поиск правил по действию, настроенному в правилах межсетевого экрана: • Разрешить (allow) — разрешает трафик. • Запретить (deny) — блокирует трафик

Параметр	Описание
<code>applicationProfile</code>	Поиск правил межсетевого экрана по указанному при настройке профилю приложений. Поиск производится по правилам с действием «Разрешить»
<code>ipsProfile</code>	Поиск правил межсетевого экрана по указанному при настройке профилю СОВ. Поиск производится по правилам с действием «Разрешить»
<code>zoneSource</code>	Поиск правил по зоне источника трафика
<code>ipSource</code>	Поиск правил по IP-адресу источника трафика. Адрес должен входить в список IP-адресов, созданный в разделе Настройки → Библиотеки → IP-адреса или в свойствах правила
<code>ipSourceName</code>	Поиск правил по названию IP-листа источника трафика
<code>countrySource</code>	Поиск правил по названию страны источника трафика (Russia, Austria и т. п.). Страна источника может быть добавлена в свойства правила на вкладке Источник (Добавить GeoIP) . Например, поисковый запрос <code>countrySource = russia</code> отобразит список правил, в которых в качестве страны источника указана Россия (Russia) или GeoIP не указан (т. е. любой GeoIP)
<code>portSource</code>	Поиск правил по порту источника трафика. Порты, которые используются сервисами, можно настроить в разделе Настройки → Библиотеки → Сервисы
<code>zoneDest</code>	Поиск правил по зоне назначения трафика
<code>ipDest</code>	Поиск правил межсетевого экрана по IP-адресу назначения. Адрес должен входить в список IP-адресов, созданный в разделе Настройки → Библиотеки → IP-адреса или в свойствах правила
<code>ipDestName</code>	Поиск правил по названию IP-листа назначения трафика

Параметр	Описание
countryDest	Поиск правил по названию страны назначения трафика (Russia, Austria и т. п.). Страна назначения может быть добавлена в свойства правила на вкладке Назначение (Добавить GeoIP). Например, поисковый запрос <code>countryDest = russia</code> отобразит список правил, в которых в качестве страны назначения указана Россия (Russia) или GeoIP не указан (т.е. любой GeoIP)
portDest	Поиск правил по порту назначения трафика. Порты, которые используются сервисами, можно настроить в разделе Настройки → Библиотеки → Сервисы
user	Поиск правил по пользователям, для которых они применяются. Правило может быть применено для следующих типов пользователей: • Unknown — пользователи, не идентифицированные системой. • Known — пользователи, идентифицированные системой с помощью серверов авторизации. • Any — любой пользователь (Known или Unknown). • Определенный пользователь — конкретный пользователь, идентифицированный в системе. Пользователи могут быть созданы локально (локальные пользователи) или получены с внешних каталогов (например, Microsoft Active Directory). При поиске, требующем полного совпадения логина пользователя (с операторами «=» или «!=») также будет производиться поиск по группам пользователей
userId	Поиск правил по ID пользователя; также будут отображены правила, в которых указаны группы пользователя
group	Поиск по группам пользователей, для которых применено правило межсетевого экрана. Группы пользователей могут быть созданы локально или получены с внешних каталогов (например, Microsoft Active Directory)
groupId	Поиск правила по идентификатору группы пользователей
service	Поиск правила по указанному типу сервиса (например, HTTP или HTTPS)
active	

Параметр	Описание
	Фильтр по статусу активности правил на момент выполнения запроса: • true — показывает правила, чей интервал активности включает текущее время; • false — показывает правила, чей интервал активности не включает текущее время Время работы правила может быть задано в свойствах на вкладке Время. Для этого используются календари, которые могут быть созданы и настроены в разделе Настройки → Библиотеки → Календари или в свойствах правила
scenario	Поиск правил по названию сценария, который должен быть активным для срабатывания правила (добавление и настройка сценариев доступна в разделе Настройки → Библиотеки → Сценарии)
description	Поиск правил по описанию правила

Примечание

Поисковый запрос не распространяется на правило «Default block». Т. е., даже если поиск правил происходит по запросу `action = allow`, правило «Default block», настроенное на блокировку трафика, будет отражено в конце списка.

NAT и маршрутизация

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, NoNAT, DNAT, NoDNAT, трансляции портов, маршрутизации на основе политик и трансляции адресов сетей. UserGate NGFW поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил отображаются в журнале трафика (**Журналы и отчеты → Журнал трафика**), если в правиле включена опция журналирования.

i Примечание

GeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и трансляции портов.

Правила NAT

Как правило, для предоставления пользователям доступа в интернет необходимо создать хотя бы одно правило NAT из зоны Trusted в зону Untrusted.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило NAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила

Параметр	Описание
Тип	Тип правила. Выберите NAT
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменен адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, система будет использовать произвольный адрес из списка доступных IP-адресов, назначенных интерфейсам зоны назначения. Допускается указание диапазона IP-адресов. Например, 192.168.10.10-192.168.10.20. В этом случае UserGate NGFW будет использовать все указанные адреса для Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL источника трафика, MAC-адреса источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса.

Параметр	Описание
	 Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Пользователи	Доступно начиная в версии 7.3.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний.

Параметр	Описание
	Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Примечание

Рекомендуется создавать общие правила NAT, например правило NAT из локальной сети (обычно зона Trusted) в интернет (обычно зона Untrusted), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

Правила NoNAT

Правила NoNAT (доступно в версии 7.4.0 и выше) используются, когда из работающих в системе правил NAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги »
Описание	Описание правила
Тип	Тип правила. Выберите NoNAT
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале

Параметр	Описание
	сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL, MAC-адреса источника трафика. Списки URL должны включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля

Параметр	Описание
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу.

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Подробнее о публикации ресурсов с помощью правил reverse-прокси — в разделе [«Публикация ресурсов с помощью reverse-прокси»](#). Для публикации серверов, работающих по протоколам, отличным от HTTP/HTTPS, необходимо использовать публикацию DNAT.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило DNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите DNAT

Параметр	Описание
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменен адрес источника. Если SNAT IP не указан, то адрес источника будет заменен на адрес интерфейса UserGate NGFW, с которого отправлен пакет. Допускается указание диапазона IP-адресов. Например, 192.168.10.10-192.168.10.20. Важно! Для замены адреса источника на указанный адрес необходимо на вкладке «DNAT» активировать Флажок «Включить SNAT»
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP-адреса, MAC-адреса источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса.

Параметр	Описание
	 Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Доступно в версии 7.4.0 и выше. Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate NGFW, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов

Параметр	Описание
Сервис	Тип сервиса, который необходимо опубликовать. Если не указан сервис, будут опубликованы все сервисы i Важно! Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет
Включить SNAT	При включении данной опции UserGate NGFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

i Примечание

При использовании нескольких правил DNAT с SNAT, отличающихся только условиями адреса назначения, действие SNAT будет выполняться только по первому правилу DNAT. Это обусловлено тем, что пакет, попавший под любое из этих правил, после изменения IP-адреса назначения не будет отличаться на сетевом и транспортном уровне модели OSI. При одинаковых DNAT IP необходимо в правилах DNAT иметь уникальные условия в зонах, сервисах, адресах источника.

i Примечание

Трафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила NoDNAT

Правила NoDNAT (доступно в версии 7.4.0 и выше) используются, когда из работающих в системе правил DNAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoDNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoDNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги »
Описание	Описание правила
Тип	Тип правила. Выберите NoDNAT
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются).

Параметр	Описание
	Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса.  Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate NGFW, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Сервис	Тип сервиса, который необходимо опубликовать. Если не указан сервис, будут опубликованы все сервисы

Параметр	Описание
	 Важно! Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100.
Использование	Статистика срабатывания о правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции портов

Правила трансляции портов (port forwarding) работают аналогично правилам DNAT, за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

Примечание

Флажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило трансляции портов, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите Порт-форвардинг
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов.

Параметр	Описание
	Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Доступно в версии 7.4.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Порт-форвардинг	Трансляция портов публикуемых сервисов: • Оригинальный порт назначения — номер TCP- или UDP-порта, на который приходят запросы; следующие порты не могут быть использованы для переназначения, поскольку они уже используются

Параметр	Описание
	внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100; • Новый порт назначения — номер TCP- или UDP-порта, на который будут пересылаться запросы на внутренний публикуемый сервер
Адрес назначения DNAT	IP-адрес узла в локальной сети, который публикуется в интернет
Включить SNAT	При включении этой опции UserGate NGFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Примечание

Трафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила маршрутизации на основе политик

Правила маршрутизации на основе политик (policy-based routing, PBR) используются для указания определенного маршрута в интернет для выбранных узлов или сервисов. Например, в организации используются два провайдера и необходимо весь HTTP-трафик пересылать через провайдера 1, а весь остальной — через провайдера 2. Для этого необходимо указать в качестве шлюза по умолчанию интернет-шлюз провайдера 2 и настроить правило PBR для HTTPS-трафика через шлюз провайдера 1.

Примечание

Правила PBR не заменяют и не влияют на работу правил NAT. Для трансляции адресов после правила PBR необходимо поставить соответствующее правило NAT.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок «Инвертировать» меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило PBR, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите Policy-based routing
Шлюз	Выбор одного из существующих шлюзов. Шлюз может быть добавлен в разделе Настройки → Сеть → Шлюзы i Важно! Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
Сценарий	Указание сценария, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе « Сценарии »

Параметр	Описание
	 Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), правило не сработает.
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Параметр	Описание
Пользователи	Доступно в версии 7.3.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции адресов сетей

Правила трансляции адресов сетей (network mapping) позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес узла без изменений. Например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 узел 192.168.1.1 будет изменен на 192.168.2.1.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, в котором совпали все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки «Выше», «Ниже», «Наверх», «Вниз» или перетаскивание мышью для изменения порядка применения правил.

Чтобы создать правило **Network mapping**, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе « Теги ». Доступно в версии 7.3.0 и выше
Описание	Описание правила
Тип	Тип правила. Выберите Network mapping
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • Журналировать начало сессии — в журнал трафика будет записываться только информация о начале

Параметр	Описание
	сессии (первый пакет). Это рекомендуемый вариант журналирования. • Нет — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Важно! Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Доступно в версии 7.4.0 и выше. Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают

Параметр	Описание
	доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов.  Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Network mapping	Указание параметров подмены сетей. • Новая IP-сеть/маска — адрес сети, на которую будет производится замена. • Направление: ◦ Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска. ◦ Исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле Новая IP-сеть/маска
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите Сбросить счетчики

Параметр	Описание
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Балансировка нагрузки

UserGate NGFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена:

- Для внутренних серверов, публикуемых в интернете (DNAT).
- Для внутренних серверов без публикации.
- Для балансировки трафика, пересылаемого на внешние серверы (ферму) ICAP-серверов.
- Для балансировки трафика на серверы, публикуемые через reverse-прокси.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов, используя при этом различные методы балансировки. Чтобы настроить балансировку, необходимо в разделе **Политики сети → Балансировка нагрузки** создать правила балансировки.

Для создания правила балансировки для серверов TCP/UDP необходимо выбрать пункт **Добавить балансировщик TCP/UDP** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
IP-адрес виртуального сервера	Необходимо выбрать из списка IP-адресов, назначенных на сетевые интерфейсы. При необходимости администратор может добавить дополнительные IP-адреса на желаемый интерфейс.

Наименование	Описание
Порт	Порт, для которого необходимо производить балансировку нагрузки.
Протокол	Протокол — TCP или UDP — для которого необходимо производить балансировку нагрузки.
Метод балансировки	Возможны 4 различных метода распределения нагрузки на реальные серверы: • Round robin: каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • Weighted round robin: работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • Least connections: новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. • Weighted least connections: работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.
Реальные серверы	Добавляется пул реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать: • IP-адрес сервера. • Порт сервера. Порт, на который пересылать запросы пользователей. • Вес. Данный коэффициент используется для неравномерного распределения нагрузки на реальные серверы для режимов балансировки weighted round robin и weighted least connections. Чем больше вес, тем больше будет нагрузка на сервер. • Режим. Может быть три варианта: ◦ Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT ◦ Маскарадинг с подменой IP-источника (SNAT): аналогично маскарадингу, но при этом NGFW подменяет IP-адрес источника на свой.

Наименование	Описание
	Внимание! Поскольку в режиме <u>Шлюз</u> балансировщик не изменяет заголовки пакетов, то обратный трафик от реального сервера должен обеспечиваться средствами маршрутизации. Т.е. шлюз для обратного трафика должен отличаться от адреса NGFW.

Наименование	Описание
	выбрать тип сервиса (HTTP или DNS), строки Запрос и Ожидаемый ответ. Например, для HTTP-запроса: - Запрос: /robots.txt - Ожидаемый ответ: Disallow: /bin/ Строка запроса тут указывает на путь на реальных серверах, который будет использован в HTTP-запросе. Строка ожидаемого ответа содержит фрагмент возвращаемой веб-страницы.
Интервал проверки	Интервал времени, через который должна выполняться проверка.
Время ожидания	Интервал времени ожидания ответа на проверку.
Число неудачных попыток	Количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки.



Примечание

Правила балансировки имеют более высокий приоритет и применяются до правил NAT/DNAT/Маршрутизации.

Балансировщик серверов reverse-прокси позволяет распределить нагрузку на внутренние серверы или ферму серверов, публикуемую с помощью правил reverse-прокси. Данный балансировщик затем может быть использован в правилах reverse-прокси. Для создания балансировщика reverse-прокси необходимо выбрать пункт **Добавить балансировщик reverse-прокси** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
Reverse-прокси профили	Выбрать reverse-прокси профили серверов, на которые будет распределяться нагрузка. Более подробно о публикации с помощью reverse-прокси читайте в разделе Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси .

Пропускная способность

Правила управления пропускной способностью используются для ограничения канала для определенных пользователей, хостов, сервисов, приложений.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

Примечание

Чекбокс **Инвертировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило пропускной способности, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Пропускная способность** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила.
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе Полосы пропускания .
Сценарий	

Наименование	Описание
	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • Нет. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Пользователи или группы пользователей, к которым применится правило.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.

Наименование	Описание
	Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Приложения	Список приложений, для которых необходимо ограничить полосу пропускания.
Время	Время, когда данное правило активно.

ПОЛИТИКИ БЕЗОПАСНОСТИ

Общие сведения

С помощью политик безопасности администратор может:

- Настроить фильтрацию HTTP-контента, например запретить некоторым пользователям доступ к определенным категориям сайтов в заданное время или настроить антивирусную проверку веб-контента.
- Настроить опции веб-безопасности, например включить принудительный безопасный поиск и блокировку рекламы.
- Настроить правила инспектирования SSL, например для всех пользователей расшифровывать HTTPS для категории «Форумы», а для определенной группы — «Социальные сети». После того, как HTTPS

расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.

- Настроить проверку почтовых протоколов SMTP и POP3 на наличие спама.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP, например, на DLP-системы.
- Настроить публикацию HTTP/HTTPS-серверов.

События срабатывания данных правил регистрируются в соответствующих журналах статистики.

Правила фильтрации контента, веб-безопасности и инспектирования SSL доступны в журнале веб-доступа (**Журналы и отчёты → Журнал веб-доступа**).

Правила Защита от DoS атак — в журнале трафика (**Журналы и отчёты → Журнал трафика**).

Все правила журналируются только при включении опции «Журналирование» в параметрах правил.

Фильтрация контента

С помощью правил фильтрации контента администратор может разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS, если настроено инспектирование HTTPS. Более того, NGFW может блокировать HTTPS-трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации NGFW URL filtering или по спискам URL, в которых указаны только имена хостов. В этих случаях NGFW использует SNI (Server Name Indication), а при отсутствии SNI — значения хоста из SSL-сертификата из пользовательских запросов для определения домена.

В качестве условий правила могут выступать:

- Пользователи и группы.
- Наличие на веб-страницах определенных слов и выражений (морфология).
- Принадлежность сайтов категориям.
- URL.

- Зона и IP-адрес источника.
- Зона и IP-адрес назначения.
- Тип контента.
- Информация о реферере.
- Время.
- Useragent браузера пользователя.
- HTTP-метод.

Примечание

Чекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Примечание

Если запрещающее правило является более общим по сравнению с разрешающими правилами, то запрещающее правило отработает вперед разрешающих, несмотря на порядок расположения. В итоге, запрещающее правило нужно делать более специфичным, чтобы порядок отработывал корректно.

Примечание

Если не создано ни одного правила, то передача любого контента разрешена.

Чтобы создать правило контентной фильтрации, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Фильтрация контента** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна в версии ПО 7.3.0 и выше.
Описание	Описание правила.
Действие	Запретить — блокирует веб-страницу. Предупредить — предупреждает пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал. Разрешить — разрешает посещение.
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
Проверять потоковым антивирусом UserGate	Доступно только для правил с действием Запретить , т.е. при наличии вируса на странице ресурс будет запрещен. Если в правиле присутствуют другие условия (категории, время, и т.д.), то антивирусная проверка будет выполняться только при совпадении всех условий правила.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.
Страница блокировки	Указывает страницу блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Можно использовать внешнюю страницу, указав Использовать внешний URL , либо указать страницу блокировки NGFW. В этом случае можно выбрать желаемый шаблон страницы блокировки, который можно создать в разделе Шаблоны страниц .
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются).

Наименование	Описание
	Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, GeoIP-адресов (не более 15 адресов) или доменов назначения трафика. Важно! Не добавляйте в списки строки с символом «*», они будут игнорироваться. Важно! Обработка трафика происходит по следующей логике: условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов и/или доменов; условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов. Для добавления списков доменов назначения используются списки из библиотеки URL. Эта же библиотека применяется при добавлении списков на вкладке URL. Следует различать эти два способа использования списков URL. Когда список URL используется как список доменов назначения, выполняется преобразование URL в доменные имена. После этого UserGate NGFW каждые 5 минут выполняет разрешение доменных имен из списка в IP-адреса и хранит полученный результат во внутреннем кэше в течение времени жизни DNS-записи. По истечении времени жизни записи UserGate NGFW автоматически обновляет IP-адрес. Таким образом, блокирующее или разрешающее правило с настроенным адресом назначения срабатывает по IP-адресам, связанным с доменными именами из списка. Когда список URL выбран на вкладке URL, фильтрация контента выполняется по URL, указанным в списке. Подробнее о работе со списками URL — в разделе «Списки URL». Важно! При настройке правила контентной фильтрации не рекомендуется использовать один список для адресов назначения и URL.

Наименование	Описание
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Категории	Списки категорий UserGate URL filtering 4.0. Использование категорий требует наличия специальной лицензии. UserGate URL filtering 4.0 — это крупнейшая база электронных ресурсов, разделенных для удобства оперирования на 72 категории. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие. Администратор может переопределить категорию на любой сайт, на который, по его мнению, категория назначена неверно или не назначена совсем. Более подробно процедура изменения категории сайта описана в разделе Запросы в белый список. Важно! Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования, но без показа страницы блокировки.
URL	Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate, такие, как «Черный список UserGate», «Белый список UserGate», «Черный список Роскомнадзора», «Черный список фишинговых сайтов», «Поисковые системы без безопасного поиска». Администраторы также могут создавать собственные списки URL. Более подробно о работе со списками URL читайте в главе Списки URL. Важно! Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена хостов (доменов), но без показа страницы блокировки.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента.
Морфология	Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари,

Наименование	Описание
	обновляемые компанией UserGate, в том числе список материалов, запрещенных Министерством Юстиции Российской Федерации, словари по темам «Суицид», «Терроризм», «Порнография», «Нецензурные выражения», «Азартные игры», «Наркотики», «Защита детей ФЗ-436». Словари доступны на русском, английском, немецком, японском и арабском языках. Администраторы также могут создавать собственные словари. Более подробно о работе с морфологическими словарями читайте в главе Морфология.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари .
Useragent	Useragent пользовательских браузеров, для которых будет применено данное правило. Администратор может добавить необходимые ему Useragent в разделе Useragent браузеров .
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET.
Рефереры	Список URL, в котором указаны рефереры для текущей страницы, таким образом правило сработает, если для данной страницы реферер совпадет со списком указанных URL. Данный функционал удобно использовать, чтобы, например, разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Важно! При настроенном инспектировании данных, передаваемых по протоколу TLS/SSL, и срабатывании правила контентной фильтрации Default allow, созданного по умолчанию, счётчик будет срабатывать только для правила инспектирования SSL. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Веб-безопасность

С помощью раздела **Веб-безопасность** администратор может включить дополнительные параметры веб-безопасности для протоколов HTTP и HTTPS, если настроено инспектирование HTTPS. Доступны следующие параметры:

- Блокировка рекламы. Посещение безопасного сайта может быть связано с принудительным просмотром изображений нежелательного характера, размещенных, например, сбоку на странице. NGFW решает эту проблему, блокируя рекламные баннеры.
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. Инжектируемый скрипт будет вставлен в веб-страницы перед тегом `</head>`.
- Принудительное включение безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. С помощью данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.
- Включение журналирования поисковых запросов пользователей.
- Блокировка приложений социальных сетей. Социальные сети играют большую роль в нашей повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. NGFW может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

- Источник трафика.
- Пользователи и группы.
- Время.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Чекбокс **Инвертировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

i Примечание

Если не создано ни одного правила, то дополнительные функции веб-безопасности не применяются.

Чтобы создать правило веб-безопасности необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Веб-безопасность** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики.
Блокировать рекламу	Активирует блокировку рекламы. Нажав на Исключения , администратор может выбрать URL-список сайтов, для которых блокировать рекламу не требуется.

Наименование	Описание
Инжектор	Позволяет вставить произвольный код во все веб-страницы. Для редактирования вставляемого кода необходимо нажать на кнопку Код инжектора .
Безопасный поиск	Принудительно включает функцию безопасного поиска.
История поиска	Активирует запись поисковых запросов пользователей в журнал.
Блокировать приложения социальных сетей	Блокирует приложения в популярных социальных сетях.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства .
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари .

Наименование	Описание
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики .
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Инспектирование туннелей

Раздел позволяет администратору настроить инспекцию данных, передающихся с использованием следующих протоколов туннелирования:

- **GRE** (Generic Routing Encapsulation) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты.
- **GTP-U** (General Packet Radio Service (GPRS) Tunneling Protocol for User Data) — протокол, используемый для переноса пользовательских данных в базовой сети GPRS и между сетью радиодоступа и базовой сетью.
- **Нешифрованный IPsec** (IPsec Null Encryption) — протокол туннелирования для передачи по IPsec-туннелю нешифрованного трафика.

После включения данной функции, все туннели, соответствующие правилам инспектирования, будут деинкапсулированы. Трафик, передаваемый внутри этих туннелей, будет обрабатываться с помощью правил межсетевого экрана и политик безопасности. После фильтрации трафик будет инкапсулирован обратно в туннель и передан по оригинальному адресу назначения.

По умолчанию, в NGFW создана зона для инспектирования туннелей — **Tunnel inspection zone**. Данной зоне будут принадлежать все адреса источников и назначения инкапсулированных в туннель пакетов.

i Примечание

Все адреса источников и назначений инкапсулированных в туннель пакетов могут принадлежать только одной зоне.

Включить инспектирование и назначить другую зону для инспектируемых туннелей можно в разделе **UserGate → Настройки** модуль **Зона для инспектируемых туннелей**.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

Чтобы создать правило инспектирования туннелей, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование туннелей** и указать необходимые параметры; будут проверяться все туннели, подходящие под заданные условия.

Наименование	Описание
Включено	Включение/отключение правила инспектирования туннелей.
Название	Название правила инспектирования.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила инспектирования.
Действие	Действия правила инспектирования: • Инспектировать. • Не расшифровывать.
Инспектирование туннелей	

Наименование	Описание
	Выбор типа туннеля, который необходимо инспектировать: • GRE. • GTP-U. • Нешифрованный IPsec.
Вставить	Место создаваемого правила в списке правил — наверх, вниз или выше выбранного существующего правила.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.

Примечание

Флажок Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Инспектирование SSL

В этом разделе администратор может настроить инспекцию данных, передаваемых по протоколу TLS/SSL. Это в первую очередь HTTPS, а также почтовые протоколы SMTPS и POP3S. UserGate NGFW с функцией SSL-инспектирования выступает в роли доверенного посредника (Man-in-the-Middle, MitM).

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности. Дешифрование SMTPS и POP3S необходимо для блокирования спама.

С помощью правил раздела можно настроить инспектирование HTTPS только для определенных категорий, например «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и при этом не расшифровывать другие категории, например «Финансы», «Правительство» и т. п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе — SNI (Server Name Indication), а если SNI отсутствует, то поле Subject Name в сертификате сервера. Содержимое поля Subject Alternative Name игнорируется.

NGFW перехватывает исходящий запрос на установление SSL-соединения и производит подмену сертификата сервера на свой, выписанный внутренним корневым центром сертификации. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить корневой сертификат центра сертификации в доверенные корневые сертификаты. Подробнее — в разделе «[Установка сертификата локального удостоверяющего центра](#)».

Если корневой сертификат доверен, браузер считает полученный сертификат легитимным и устанавливает безопасное SSL-соединение между пользователем и NGFW.

Далее NGFW устанавливает новое, отдельное SSL-соединение с конечным сервером. В итоге NGFW работает как посредник: получает данные от пользователя, проверяет их, перешифровывает и отправляет на внешний сервер, и наоборот.

Аналогично браузерам пользователя некоторые почтовые серверы и пользовательские почтовые программы не принимают почту, если сертификат был подменен. В этом случае необходимо произвести в почтовых программах настройки, отключающие проверку сертификатов, или добавить исключения для сертификата UserGate. Подробно о том, как это сделать, смотрите в документации на почтовое ПО.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, в котором совпали все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок **Инвертировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

i Примечание

Если не создано ни одного правила, SSL не перехватывается и не дешифруются. При этом контент, передаваемый по SSL, не фильтруется.

Чтобы создать правило инспектирования SSL, необходимо в разделе **Настройки** → **Политики безопасности** → **Инспектирование SSL** нажать **Добавить** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе Теги руководства администратора. Опция доступна в версии ПО 7.3.0 и выше
Описание	Описание правила
Записывать в журнал правил	При активации данной опции информация о срабатывании правила будет регистрироваться в « Журнале веб-доступа »
Действие	- Расшифровать. - Не расшифровывать. - Расшифровать и переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL. При выборе данного действия

Параметр	Описание
	необходимо указать профиль пересылки SSL. Подробнее о настройке профилей пересылки — в разделе « Профили пересылки SSL »
Профиль SSL	Выбор профиля SSL. Параметры, указанные в данном профиле, будут использованы как для установки SSL-соединения от браузера пользователя к NGFW, так и при построении SSL-соединения от NGFW к запрашиваемому веб-ресурсу. Подробнее о профилях SSL — в разделе « Профили SSL »
Блокировать сайты с некорректными сертификатами	Позволяет блокировать доступ к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или не доверяемым центром сертификации
Проверять по списку отозванных сертификатов	Проверять сертификат сайта в списке отозванных сертификатов (CRL) и блокировать, если он там найден
Блокировать сертификаты с истекшим сроком действия	Блокировать сертификаты, срок действия которых истек
Блокировать самоподписанные сертификаты	Блокировать самоподписанные сертификаты
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа «Any», «Unknown», «Known». Для применения правил к конкретным пользователям или к пользователям типа «Known» необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе « Пользователи и устройства »
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом «*» в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во

Параметр	Описание
	внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.  Важно! Количество указанных GeoIP не может быть больше 15. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Адрес назначения	Списки IP-адресов назначения трафика.  Важно! Количество указанных GeoIP не может быть больше 15. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Подробнее о работе со списками IP-адресов — в разделе «IP-адреса»
Сервисы	Сервис, для которого необходимо дешифровать трафик. Может быть HTTPS, SMTPS, POP3S
Категории	Списки категорий UserGate URL filtering 4.0
Домены	Списки доменов. Доменные имена, для которых применяется данное правило. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена (www.example.com, а не http://www.example.com/home/). Подробнее о работе со списками URL — в разделе « Списки URL »

Параметр	Описание
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе « Календари »
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т. п.

По умолчанию создано правило инспектирования «SSL Decrypt all for unknown users», которое необходимо для авторизации неизвестных пользователей через Captive-портал.

Инспектирование SSH

При помощи данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу SSH (Secure Shell). SSH также позволяет создавать зашифрованные туннели для практически любых сетевых протоколов.

Правила данного раздела могут инспектировать SSH-трафик для определённых пользователей и/или их групп, зон и адресов источников и получателей данных, а также типов сервисов, передаваемых через SSH-туннель. Имеется календарь для применения каждого правила в выбранные дни недели и время суток.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Флажок Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

i Примечание

Если не создано ни одного правила или все правила отключены, то SSH не перехватывается и не дешифруется, то есть передаваемые по SSH данные не инспектируются.

Чтобы включить возможность инспектирования контента SSH необходимо:

Наименование	Описание
Шаг 1. Разрешить сервис SSH-прокси на необходимой зоне.	В разделе Сеть → Зоны разрешить сервис SSH-прокси для той зоны, со стороны которой будет инициирован трафик SSH.
Шаг 2. Создать необходимые правила инспектирования SSH.	Правило инспектирования SSH определяет критерии и действия, применяемые к трафику SSH.

Чтобы создать правило инспектирования SSH, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование SSH** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила.
Действие	Расшифровывать или не расшифровывать передаваемые данные.
Записывать в журнал правил	Информация о срабатывании правила будет регистрироваться в Журнале инспектирования SSH .

Наименование	Описание
Блокировать удаленный запуск shell	Запрет запуска командного интерпретатора на SSH-сервере. Пользователю будет разрешено запускать только команды на удаленном сервере, например: <pre>ssh user@host command</pre>
Блокировать удаленное выполнение по SSH	Запрет удаленного выполнения любых команд на SSH-сервере.
Редактировать команду SSH	Опционально для блокировки удаленного выполнения команд по SSH можно указать список конкретных команд, удаленный запуск которых будет заблокирован.
Блокировать SFTP	Блокировать соединение SFTP (Secure File Transfer Protocol).
Вставить	Место вставки создаваемого правила в списке правил – наверх, вниз или выше выбранного существующего правила.
Пользователи	Список пользователей и групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей читайте в главе Пользователи и устройства.
Источник	Зоны и/или списки IP-адресов источника трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Адрес назначения	Списки IP-адресов назначения трафика. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Наименование	Описание
	Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Сервис	Сервис, для которого необходимо дешифровать трафик. Поле обязательно для заполнения.
Время	Временной интервал, в течение которого правило активно. Можно добавить разнообразные периоды в разделе Календари .
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать Сбросить счётчики.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Защита почтового трафика

При наличии настроенной проверки почтового трафика UserGate NGFW может проверять трафик по протоколам SMTP и POP3. IMAP не поддерживается, в том числе, и при настройке SSL инспектирования.

Проверяться может и зашифрованный трафик этих протоколов.

Поддерживается 2 типа проверки:

- блокировка SMTP по наличию IP адреса сервера-отправителя в одной из баз DNSBL; наиболее эффективный метод быстро и с минимальными затратами ресурсов отсеять сообщения от очевидных и явных спамеров;
- маркировка сообщений по результатам проверки на спам; требует наличия также лицензии на модуль Mail security.

i Внимание!

Блокировка по результатам антиспам-проверки НЕ рекомендуется. Рекомендуется принятие решения "спам/не спам" на стороне почтового сервера (или дополнительного антиспам-приложения), где маркировка, выставляемая UserGate NGFW, была бы одним из критериев, с большим весом.

Посмотреть статистику работы антиспам модуля можно в дашборде, подключив соответствующие виджеты "Сводные показатели защиты почты" или "Графики защиты почты".

В настройках антиспам можно задать как белый, так и черный список IP адресов. Здесь речь идет именно об IP адресах, от которых сразу не будет приниматься соединение (для черных списков) без анализа каких-то дополнительных данных. В самих правилах можно добавлять списки адресов на вкладках envelope from / envelope to. Если в правиле будет стоять действие Блокировать, то это правило будет работать как черный список, если Пропустить — как белый.

В этих списках можно использовать символ * в значении "любой". То есть *@domain.com обозначает все адреса этого домена.

Раздел **Защита почтового трафика** позволяет настроить проверку транзитного почтового трафика на предмет наличия в нем спам-сообщений.

Поддерживается работа с почтовыми протоколами POP3(S) и SMTP(S). Защита почтового трафика требует наличия соответствующего модуля в лицензии NGFW.

Как правило, необходимо защищать почтовый трафик, входящий из интернета на внутренние почтовые серверы компании, и, в некоторых случаях, защищать исходящий почтовый трафик от серверов или пользовательских компьютеров.

Для защиты почтового трафика, приходящего из интернета на внутренние почтовые серверы, необходимо:

Наименование	Описание
Шаг 1. Опубликовать почтовый сервер в сеть Интернет.	Смотрите раздел Правила DNAT . Рекомендуется создать отдельные правила DNAT для SMTP и POP3 протоколов, а не публиковать оба протокола в одном правиле. Обязательно укажите в качестве сервиса протокол SMTP, а не TCP.
Шаг 2. Включить поддержку сервисов SMTP(S) и POP3(S) в зоне,	Смотрите раздел Настройка зон .

Наименование	Описание
подключенной к сети Интернет.	
Шаг 3. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для защиты почтового трафика в случаях, когда не требуется публиковать почтовый сервер, действия сводятся к следующим шагам:

Наименование	Описание
Шаг 1. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для настройки правил фильтрации почтового трафика необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Защита почтового трафика** и заполнить поля правила.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

Примечание

Если не создано ни одного правила, то почтовый трафик не проверяется.

Примечание

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.

Наименование	Описание
Название	Название правила.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила.
Действие	Действие, применяемое к почтовому трафику при совпадении всех условий правила: • Пропустить — пропускает трафик без изменений; • Маркировать — маркирует почтовые сообщения специальным тэгом в теме письма или дополнительном поле; • Блокировать с ошибкой — блокирует письмо, при этом сообщает об ошибке доставки письма серверу SMTP для SMTP(S)-трафика или клиенту POP3 для POP3(S)-трафика; • Блокировать без ошибки — блокирует письмо без уведомления о блокировке.
Записывать в журнал правил	Включить журналирование информации о срабатывании правила в журнал защиты почтового трафика.
Проверка	Метод проверки почтового трафика: • Проверка антиспамом UserGate — проверяет почтовый трафик на наличие спама; • DNSBL проверка — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам.
Заголовок	Поле, куда помещать тег маркировки.
Маркировка	Текст тега, который маркирует письмо.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются).

Наименование	Описание
	Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Пользователи или группы пользователей, к которым применяется данное правило.
Сервис	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило.
Envelop from	Почтовый адрес отправителя письма, указанный в поле Envelope from . Только для протокола SMTP.
Envelop to	Почтовый адрес адресата письма, указанный в поле Envelope to . Только для протокола SMTP.

Рекомендуемые настройки защиты от спама следующие.

Для протокола SMTP(S):

1. Первое правило в списке — **блокировка с помощью DNSBL**. Рекомендуется оставить списки **Envelope from/Envelope to** пустыми. В этом случае DNSBL будет отбрасывать подключения SMTP-серверов, замеченных в распространении спама, еще на этапе коннекта. При наличии email адресатов в этих списках система будет вынуждена принимать сообщения целиком для анализа этих полей, что увеличит нагрузку на сервер и ухудшит производительность проверки почтового трафика.
2. Второе правило — **маркировка** писем с помощью антиспама UserGate. Здесь можно использовать любые исключения, в том числе и по **Envelope from/Envelope to**.

Для протокола POP3(S):

- действие — **Маркировать**;
- проверка — **Антиспам UserGate**.

НАСТРОЙКИ АНТИСПАМА

Настройки BATV

BATV (Bounce Address Tag Validation) — технология, помогающая различать реальные возвраты писем от возвратов спама.

Подделка адресов отправителей (особенно тех, кто не использует SenderPolicyFramework и YahooDomainKeys для защиты от подделки своих адресов) широко применяется спамерами. Часть спама принимается MX'ами получателей, но при недоставке на следующий сервер — relay может возвращаться отправителю. А так как адрес отправителя поддельный, реальные невинные владельцы адресов получают возврат спама, который не посылали. Также часть писем спам-рассылок маскируется под возвращаемые письма, поскольку некоторые антиспам-проверки предполагают, что возвращаемые письма не могут содержать спам-сообщения, чем и пользуются злоумышленники. Для отличия реальных возвращаемых писем от поддельных и применяется технология BATV.

Отключать прием возвращаемых писем нельзя, т.к. это нарушает связность сети (нормальные письма тоже иногда не доставляются и возвращаются), поэтому требуется как-то отличать нормальные возвраты от возвращаемого чужого

спама. Тогда и была предложена технология BATV. Использование BATV может быть полезно в тех системах, где контентные фильтры спама не справляются с детектированием спама в возвращаемых письмах.

Может быть включена, либо выключена. Других настроек не предполагается.

Серверы DNSBL

DNSBL проверка — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам.

DNSBL или спам-база — это черный список доменных имен и ip-адресов, замеченных в распространении спам сообщений.

Внимание!

Появление в этом списке того или иного сервера, не является однозначным признаком принадлежности писем с этого сервера к спам-рассылкам. Частота ложных срабатываний в этой технологии зависит от используемых списков DNSBL и определяется индивидуально. В любом случае, появление сервера в списках DNSBL должно квалифицироваться как дополнительный, но не основной признак спам-рассылки.

В сети существуют десятки различных DNSBL, каждый из которых использует свои собственные критерии для добавления и исключения из своего списка IP адреса или домена. Большинство спам-фильтров используют различные DNSBL для проверки того, чтобы входящие электронные письма не отправлялись с сайтов, доменные имена которых занесены в черный список. Как правило, DNSBL являются первой линией защиты от спама.

Например, в список серверов добавляются адреса серверов DNSBL: cbl.abuseat.org, zen.spamhaus.org и т.д. Белый и черный список добавляет или убирает определенные адреса из этой проверки.

Белый список DNSBL

Список серверов исключенных из DNSBL проверки.

Черный список DNSBL

Список запрещенных серверов в дополнение к тем, что есть списках DNSBL.

Работа с внешними ICAP-серверами

UserGate NGFW позволяет передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. В данном случае UserGate NGFW будет выступать в роли ICAP-клиента.

UserGate NGFW поддерживает гибкие настройки при работе с ICAP-серверами, например, администратор может задать правила, согласно которым на ICAP-серверы будет направляться только выборочный трафик, или настроить работу с фермой ICAP-серверов.

Общие настройки

Для того, чтобы настроить работу NGFW с внешними серверами ICAP, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать ICAP-сервер.	В разделе Политики безопасности → ICAP-серверы нажать на кнопку Добавить и создать один или более ICAP-серверов.
Шаг 2. Создать правило ICAP.	В разделе Политики безопасности → Правила ICAP создать правило, которое будет задавать условия пересылки трафика на ICAP-серверы или фермы серверов. Важно! Правила ICAP применяются сверху вниз в списке правил. Срабатывает только первое правило, для которого совпали все условия, указанные в настройках правила.

Для создания ICAP-сервера в разделе **Политики безопасности → ICAP-серверы** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название ICAP-сервера.
Описание	Описание ICAP-сервера.

Наименование	Описание
Адрес сервера	IP-адрес ICAP-сервера.
Порт	TCP-порт ICAP-сервера, значение по умолчанию 1344.
Максимальный размер сообщения	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу.
Период проверки доступности сервера ICAP	Устанавливает время в секундах, через которое NGFW посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.
Пропускать при ошибках	Если эта опция включена, то NGFW не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен (не отвечает на запрос OPTIONS).
Reqmod путь	• Включено — включает использование режима Reqmod; • Путь на сервере ICAP для работы в режиме Reqmod. Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима reqmod.
Respmod путь	• Включено — включает использование режима Respmod; • Путь на сервере ICAP для работы в режиме Respmod. Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима respmod.
Посылать имя пользователя	• Включено — включает отсылку имени пользователя на ICAP-сервер; • Кодировать в base64 — кодировать имя пользователя в base64, это может потребоваться, если имена пользователей содержат символы национальных алфавитов;

Наименование	Описание
	• Название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — X-Authenticated-User.
Посылать IP-адрес	• Включено — включает отсылку IP-адреса пользователя на ICAP-сервер; • Название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Ip.
Посылать MAC-адрес	• Включено — включает отсылку MAC-адреса пользователя на ICAP-сервер; • Название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Mac.

Для создания ICAP-правила необходимо нажать **Добавить** в разделе **Политики безопасности** → **ICAP-правила** и заполнить необходимые поля.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

Примечание

Чекбокс **Инвертировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Теги	

Наименование	Описание
	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание правила.
Действие	Возможны следующие варианты: • Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • Переслать — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Это стандартный режим работы большинства ICAP-серверов. • Переслать и игнорировать — переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика.
ICAP-серверы	ICAP-сервер или балансировщик серверов ICAP, куда NGFW будет пересылать запросы.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Наименование	Описание
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known . Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей.
Адрес назначения	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента .
Категории	Списки категорий UserGate URL filtering.
URL	Списки URL.
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET. Если не используется SSL Inspection, то возможно применение метода CONNECT.
Сервис	Возможны варианты: • HTTP — веб-трафик; • SMTP — почтовый трафик; письма будут переданы на сервер ICAP в виде соответствующего MIME-типа; • POP3 — почтовый трафик; письма будут переданы на сервер ICAP в виде соответствующего MIME-типа. Важно! Перед использованием сервисов SMTP и POP3 в правилах ICAP необходимо создать правило защиты почтового трафика для данных сервисов. Подробнее о

Наименование	Описание
	защите почтового трафика смотрите в разделе Защита почтового трафика .

Работа с несколькими серверами ICAP

NGFW поддерживает работу с несколькими серверами ICAP. В общем случае без балансировки данные передаются на ICAP сервера по порядку их перечисления, в случае если сервер ICAP не отвечает: поведение NGFW зависит от настройки **Действие** в правилах ICAP:

- **Пропустить** — запрос не передаются на ICAP сервер;
- **Переслать** — запрос передается на сервер и ожидается ответ, если ответ не поступает, запрос отправляется следующему по списку ICAP серверу;
- **Переслать и игнорировать** — запрос передается на сервер, ответ не ожидается.

Защита от DoS атак

UserGate NGFW позволяет гранулированно настроить параметры защиты сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP). Грубая настройка производится в свойствах зон (смотрите раздел [Настройка зон](#)), более точная настройка производится в данном разделе. Используя правила защиты DoS, администратор может указать специфические настройки защиты от DoS атак для определенного сервиса, протокола, приложения и т.п. Чтобы создать правила защиты DoS администратору необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профили DoS защиты.	В разделе Политики безопасности → Профили DoS нажать на кнопку Добавить и создать один или более профилей DoS защиты.
Шаг 2. Создать правила защиты DoS.	В разделе Политики безопасности → Правила защиты DoS создайте правила, используя профили защиты, созданные на предыдущем шаге.

Настройка профиля защиты DoS подобна настройке защиты от DoS на зонах NGFW. При создании профиля необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Теги	Указание опционального тега для маркировки правила. Подробнее читайте в статье Теги руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.
Описание	Описание профиля.
Агрегировать	Данная настройка регулирует, будет ли NGFW суммировать количество пакетов, проходящих в секунду, для всех IP-адресов источника трафика, или будет производить подсчет индивидуально для каждого IP-адреса. В случае активации данной настройки необходимо устанавливать достаточно высокие значения количества пакетов/сек в настройках закладки Защита DoS и в закладке Защита ресурсов .
Защита DoS	Данная настройка позволяет указать параметры защиты от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • Порог уведомления — при превышении количества запросов над указанным значением происходит запись события в системный журнал. • Порог отбрасывания пакетов — при превышении количества запросов над указанным значением NGFW начинает отбрасывать пакеты, и записывает данное событие в системный журнал.
Защита ресурсов	Данная настройка позволяет ограничить количество сессий, которые будут разрешены для защищаемого ресурса, например, опубликованного сервера: • Включено: включает ограничение количества сессий. • Ограничить число сессий: задается число сессий.

Чтобы создать правило защиты DoS, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Правила защиты DoS** и указать необходимые параметры.

i Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Выше/Ниже**, **Наверх/Вниз** или перетаскивание мышью для изменения порядка применения правил.

i Примечание

Чекбокс **Инвертировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Запретить — безусловно блокирует трафик подобно действию правил Межсетевого экрана. Разрешить — разрешает трафик, защита от DoS не применяется. Может быть использовано для создания исключений. Защитить — применить профиль защиты от DoS атак.
Профиль DoS	В случае, если выбрано действие Защитить, необходимо указать профиль защиты DoS. Если при использовании профиля DoS с защитой ресурсов не использовать дополнительные условия, например адрес назначения, то будут учитываться все транзитные соединения.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. Важно! Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не работает.

Наименование	Описание
Записывать в журнал правил	Записывает в журнал трафика информацию о трафике при срабатывании правила. Возможны варианты: • Журналировать начало сессии. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • Журналировать каждый пакет. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. Важно! Строки с символом '*' в таких списках не работают (игнорируются).

Наименование	Описание
	Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Важно! Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP или HTTPS.
Время	Интервалы времени, когда правило активно.

Система обнаружения и предотвращения вторжений

Система обнаружения и предотвращения вторжений (COB) позволяет распознавать вредоносную активность в сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз, а также предоставление отчетов.

Выявление проблем безопасности происходит с помощью использования эвристических правил и анализа сигнатур известных атак. COB отслеживает и блокирует подобные атаки в режиме реального времени. Возможными мерами превентивной защиты являются обрыв соединения, блокирование адреса источника, оповещение администратора сети и запись в журнал.

Принцип работы с системой COB

Сигнатуры COB создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. Пользователь также имеет возможность создавать собственные сигнатуры. Описание характерных признаков сетевых уязвимостей в таких сигнатурах выполняется с помощью языка [UASL](#) (UserGate Application and Security

Language). Для каждой сигнатуры можно отдельно настроить свое действие, журналирование, запись в файл pcap, включение/отключение сигнатур. Подробнее о сигнатурах COB читайте в разделе [Сигнатуры COB](#).

С помощью гибко настраиваемых фильтров наборы сигнатур добавляются в профили COB. Администратор может создать необходимое количество профилей COB для защиты различных сервисов. Подробнее о профилях COB читайте в разделе [Профили COB](#).

Для активации системы обнаружения и предотвращения вторжений профиль COB добавляется в разрешающее правило [межсетевого экрана](#). Таким образом, системой будут обрабатываться только те сигнатуры, которые попали в добавленные профили.

Правила межсетевого экрана применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Если в правиле определен профиль COB, трафик начинает анализироваться с помощью набора сигнатур профиля. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в профиле и произведена соответствующая запись в [Журнале COB](#), если была включена опция журналирования. Если ни одна из сигнатур не была найдена, то трафик пропускается дальше.

Важно!

Для работы системы COB через NGFW должен проходить как прямой, так и обратный трафик. На асимметричном трафике COB работать не будет..

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные COB/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

Flow control и intelligent mode

Функция flow control предназначена для отслеживания загрузки процессора устройства. Flow control производит анализ всех пакетов сессии COB до достижения контролируемой границы. После достижения границы новые

сессии будут пропускаться и не будут подвержены сканированию при помощи системы COB. По умолчанию данная функциональность всегда включена.

Одним из режимов работы функции flow control системы обнаружения и предотвращения вторжений является интеллектуальный режим сканирования пакетов, intelligent mode. Для уменьшения загрузки системой COB сканируется часть проходящих пакетов TCP-сессии в пределах установленного лимита, остальные пакеты пропускаются без обработки. Администратор может установить, сколько байт от начала сессии необходимо сканировать в этом режиме.

При увеличении загрузки ядер процессора алгоритм уменьшает объем сканирования трафика, снижая тем самым нагрузку на процессор.

По умолчанию режим intelligent mode всегда активирован в системе.

При необходимости администратор системы может отключить/включить функцию flow control и режим intelligent mode через интерфейс командной строки (CLI). При отключении функции flow control параметры режима intelligent mode изменять нельзя. Останутся значения параметров, которые были назначены до отключения функции flow-control.

Команда включения/отключения функции flow control (доступно в версии ПО 7.4.0 и выше):

```
Admin@nodename# set security-policy intrusion-prevention flow-control
+ on      Enable
+ off     Disable
```

Команда включения/отключения режима intelligent mode:

```
Admin@nodename# set security-policy intrusion-prevention mode
+ on      Enable
+ off     Disable
```

Команда для изменения лимита сканирования в сессии:

```
Admin@einmanediard# set security-policy intrusion-prevention limit
+ <num>      Enter kbytes between 50-200 (e.g. 100)
```

Посмотреть текущее состояние функции flow control и режима intelligent mode можно командой:

```
Admin@nodename# show security-policy intrusion-prevention
```

```
mode           : on
limit          : 200
flow-control   : on
```

Защита АСУ ТП

Администратор может контролировать прохождение трафика автоматизированных систем управления технологическими процессами (АСУ ТП) через UserGate NGFW с помощью профилей COB и приложений.

В профили с помощью гибко настраиваемых фильтров набираются сигнатуры, предназначенные для защиты различных сервисов. Подробнее о профилях COB — в разделе [Профили COB](#), о профилях приложений — в разделе [Профили приложений](#).

Сигнатуры COB или приложений создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. Пользователь также имеет возможность создавать собственные кастомизированные сигнатуры. Описание характерных признаков сетевых уязвимостей в таких сигнатурах выполняется с помощью языка [UASL](#) (UserGate Application and Security Language). Для каждой сигнатуры можно отдельно настроить своё действие, журналирование, запись в файл pcap, включение/отключение сигнатуры. Подробнее о сигнатурах COB — в разделе [Сигнатуры COB](#), о сигнатурах приложений — в разделе [Приложения](#).

Профили добавляются в разрешающее правило межсетевого экрана. Таким образом, системой будут обрабатываться только те сигнатуры, которые попали в добавленные профили. Подробнее о работе правил межсетевого экрана — в разделе [Межсетевой экран](#).

С помощью сигнатур приложений можно определять типы протоколов АСУ ТП. Доступно более 40 протоколов, включая OPC UA, Modbus, Profinet, DNP3, Omron, DeltaV, Siemens S7, HART-IP, IEC-104, IEC-61850.

Для поиска таких сигнатур в библиотеке сигнатур приложений используйте фильтр: `category = ICS/IoT`.

Библиотеки

- Приложения
- Профили приложений
- Сигнатуры COB
- Профили COB

Приложения

Добавить
Редактировать
Удалить

category = ICS/IoT

	Id	Тип	Название ↑	Категории приложения	Технология приложения	Владелец
1	9779	Протокол	ADDP	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
4	1227	Протокол	BACnet	☐ ICS/IoT ☐ Business	Network-protocol	© UserGate
1	9797	Протокол	CC-Link IE Field Basic	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
3	11028	Протокол	CoAP	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
1	9790	Протокол	CodeSys	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
1	9780	Приложен...	Component Network over IP (CN/IP) (CEA 852)	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
1	9794	Протокол	Delta-V (Emerson protocol)	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate
1	9786	Протокол	DLMS/COSEM	☐ ICS/IoT ☐ Standard networks	Network-protocol	© UserGate

В библиотеке сигнатур COB, поставляемых UserGate, имеется набор сигнатур, которые идентифицируют известные уязвимости протоколов АСУ ТП по CVE/BDU. Сигнатуры закрывают известные уязвимости основных производителей контроллеров — Yokogawa, Siemens, Schneider Electric, ABB, Advantech, AVEVA, Honeywell, Beckhoff, GE, Delta, Eaton, Allen Bradley, Rockwell и других.

Для поиска таких сигнатур в библиотеке сигнатур COB используйте фильтр: `category = scada and classtype != protocol-command`.

Библиотеки

- Приложения
- Профили прилож...
- Сигнатуры COB
- Профили COB

Сигнатуры COB

Добавить
Редактировать
Удалить
Включить
Отключить
Восстановить по умолчанию

category = scada and classtype != protocol-command

	Id ↑	Журналиро...	Название сигнатуры	Действие	Протокол	Категория	Класс	References
5	158	Журна...	DATAC RealWin SCADA Server Remote Stack Buffer Overflow Vulnerability	Пропустить	tcp	scada	arbitrary-code-execution	CVE: 2008-4322
4	159	Журна...	Advantech WebAccess Multiple Remote Code Execution Vulnerabilities	Пропустить	tcp	scada	arbitrary-code-execution	CVE: 2017-14016
5	160	Журна...	Multiple Schneider Electric Products Stack Based Buffer Overflow Vulnera...	Пропустить	tcp	scada	arbitrary-code-execution	CVE: 2018-8840 BDU: 2018-00788
4	161	Журна...	CitectSCADA/CitectFacilities ODBC Server Remote Stack Based Buffer Ov...	Пропустить	tcp	scada	arbitrary-code-execution	CVE: 2008-2639
4	162	Журна...	7T Interactive Graphical SCADA System Multiple Security Vulnerabilities	Пропустить	tcp	scada	misc-attack	CVE: 2011-1565
5	163	Журна...	7T Interactive Graphical SCADA System Remote Command Injection	Пропустить	tcp	scada	arbitrary-code-execution	CVE: 2011-1566

С помощью сигнатур COB можно определять команды управления, передаваемые по протоколам АСУ ТП. В библиотеке сигнатур имеются сигнатуры для определения команд управления протоколов DNP3, IEC-104, OPC UA, MODBUS TCP, UMAS и других.

Для поиска таких сигнатур в библиотеке сигнатур COB используйте фильтр: `classtype = protocol-command`.

Библиотеки

Приложения

Профили прилож...

Сигнатуры COB

Профили COB

Сигнатуры COB

Добавить

Редактировать

Удалить

Включить

Отключить

Восстановить по умолчанию

classType = protocol-command

	Id ↑	Журналиро...	Название сигнатуры	Действие	Протокол	Категория	Класс
2	80000000	Журна...	Modbus TCP Read Coils(1)	Пропустить	tcp	scada	protocol-command
2	80000001	Журна...	Modbus TCP Read Coils(1) Error	Пропустить	tcp	scada	protocol-command
2	80000002	Журна...	Modbus TCP Read Discrete Inputs(2)	Пропустить	tcp	scada	protocol-command
2	80000003	Журна...	Modbus TCP Read Discrete Inputs(2) Error	Пропустить	tcp	scada	protocol-command
2	80000004	Журна...	Modbus TCP Read Holding Registers(3)	Пропустить	tcp	scada	protocol-command
2	80000005	Журна...	Modbus TCP Read Holding Registers(3) Error	Пропустить	tcp	scada	protocol-command
2	80000006	Журна...	Modbus TCP Read Input Registers(4)	Пропустить	tcp	scada	protocol-command

ГЛОБАЛЬНЫЙ ПОРТАЛ

Общие сведения

Веб-портал и reverse-прокси, наряду с правилами DNAT/Порт-форвардинга, позволяют опубликовать ресурсы, находящиеся внутри компании, пользователям из интернета.

При наличии публикаций внутренних ресурсов с помощью DNAT/Порт-форвардинга, reverse-прокси и веб-портала порядок обработки правил следующий:

1. Правила DNAT/Порт-форвардинга.
2. Правила веб-портала. Если имя хоста в запросе совпало с именем хоста веб-портала, и номер порта в запросе совпал с номером порта, указанного для работы веб-портала, то отрабатывают правила веб-портала.
3. Правила Reverse-прокси.

Веб-портал (SSL VPN)

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удаленных или мобильных пользователей, используя при этом только протокол HTTPS. Данная технология не требует установки специального клиента VPN, достаточно обычного браузера.

i Примечание

Если на целевых HTTP-ресурсах настроена аутентификация Kerberos или NTLM, то NGFW может производить аутентификацию по технологии SSO (необходим настроенный LDAP-коннектор с загруженным keytab-файлом). При этом аутентификация на самом NGFW также должна быть настроена через Kerberos/NTLM, так как NGFW передаёт данные прозрачно, форма аутентификации при ответе сайта с ошибкой 401 (Unauthorized) не передается клиенту веб-портала.

i Примечание

Начиная с версии 7.4.0 для создания защищенного соединения с веб-серверами UserGate NGFW использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. Поэтому, перед тем как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях «server hello» при установлении соединения.

Для настройки веб-портала необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Включить и настроить веб-портал.	В разделе Настройки → Веб-портал включить и настроить параметры веб-портала. Подробные значения настроек будут описаны далее в этой главе
Шаг 2. Разрешить доступ к сервису веб-портала на необходимых зонах.	В разделе Сеть → Зоны разрешить сервис веб-портала для выбранных зон (обычно зона Untrusted). Данное разрешение откроет доступ к порту сервиса, который был указан в настройках веб-портала на предыдущем шаге
Шаг 3. Добавить внутренние ресурсы в веб-портал.	В разделе Глобальный портал → Веб-портал добавить URL внутренних ресурсов, к которым необходим доступ пользователей. Подробные значения настроек будут описаны далее в этой главе

При настройке веб-портала (раздел **Настройки → Веб-портал**) необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает/Выключает веб-портал
Имя хоста	

Наименование	Описание
	Имя хоста, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. Данное имя должно резолвиться службами DNS в IP-адрес интерфейса NGFW, входящего в зону, на которой разрешен сервис веб-портала
Порт	Порт TCP, который будет использоваться сервисом веб-портала. Порт вместе с именем хоста образуют URL для подключения пользователей в виде: <code>https://имя_хоста:порт</code>
Профиль аутентификации	Профиль аутентификации пользователей, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Профиль аутентификации задает метод аутентификации, например, AD-коннектор или локальный пользователь. Также в профиле аутентификации можно указать требование использовать мультифакторную аутентификацию для доступа к веб-порталу. Подробнее о профилях аутентификации — в разделе « Профили аутентификации »
Шаблон страницы аутентификации	Выбрать шаблон страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Вы также можете создать свою страницу аутентификации. Подробнее об этом — в разделе « Шаблоны страниц »
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Вы также можете создать свой шаблон веб-портала. Подробнее об этом — в разделе « Шаблоны страниц »
Предлагать выбор домена AD/LDAP на странице аутентификации	Показывать выбор домена на странице аутентификации веб-портала.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации веб-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе « Профили SSL »

Наименование	Описание
Сертификат	Сертификат, который будет использоваться для создания HTTPS-соединения. Если выбран режим Автоматически , то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе « Управление сертификатами »
Аутентификация пользователя по сертификату	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов NGFW, ему должна быть назначена роль Пользовательский сертификат и назначен соответствующий пользователь NGFW. Подробнее о пользовательских сертификатах — в разделе « Управление сертификатами »

Настройка веб-портала (раздел **Глобальный портал → Веб портал**) сводится к тому, что необходимо создать записи публикации URL внутренних веб-ресурсов. Для каждого URL необходимо создать закладку и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает закладку
Название	Название закладки
Описание	Описание закладки
URL	URL ресурса, который необходимо опубликовать через веб-портал. Указывайте полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. Важно! Для публикации терминальных серверов необходимо отключить опцию, требующую Network Level Authentication в свойствах RDP доступа на серверах терминального доступа. Аутентификацию пользователей для доступа к серверам в данном случае будет выполнять веб-портал в соответствии со своими настройками

Наименование	Описание
Домен прямого доступа	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Домены прямого доступа должны быть локальными, и их разрешение должно происходить через DNS-сервер, установленный внутри локальной сети. При указании домена прямого доступа нужно выбрать профиль SSL. Выбор сертификата в этом случае не является обязательным. Если сертификат не выбран, он будет сгенерирован UG NGFW
Проверять авторизацию для RDP-сессий	Разрывать сессию RDP по завершению аутентификации на веб-портале на стороне сервера
Включить прозрачную аутентификацию	Прозрачная аутентификация позволяет аутентифицировать пользователя на опубликованном для него приложении. Для аутентификации будут использованы те же данные, что пользователь ввел при входе на веб-портал. Для успешной работы этой опции необходимо, чтобы опубликованное приложение поддерживало прозрачную аутентификацию
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе « Профили SSL »
Сертификат	Сертификат, который будет использоваться для создания HTTPS-соединения между NGFW и сервером. Если выбран режим Выбрать сертификат , то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе « Управление сертификатами »
Иконка	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из predefined иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку
Вспомогательные URL	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Например, основной URL http://www.example.com получает часть медиаконтента со вспомогательного URL http://cdn.example.com
Пользователи	Список пользователей и/или групп пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL

Очередность закладок веб-портала определяет порядок отображения их пользователю. Администратор может менять очередность закладок с помощью кнопок **Выше/Ниже**, **Наверх/Вниз** или перетаскивая закладки с помощью мыши.

Публикация ресурсов с помощью reverse-прокси

UserGate NGFW поддерживает публикацию веб-серверов удаленных приложений в режиме сервера reverse-прокси. Доступ к веб-серверам и безопасность соединений с ними контролируются настраиваемыми правилами reverse-прокси.

Режим сервера reverse-прокси предоставляет следующие возможности:

- **Балансировка нагрузки.** Если обработку запросов к удаленному приложению выполняют несколько веб-серверов, сервер reverse-прокси может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- **Переопределение URL-адресов.** Сервер reverse-прокси может выполнять подмену путей и доменных имен в запросах, чтобы перенаправить их на разные веб-серверы, помогая таким образом разделить трафик для разных приложений.
- **Управление доступом к веб-серверам.** Сервер reverse-прокси может блокировать попытки доступа по идентификационной строке клиентского приложения (useragent) и нежелательным адресам.
- **Поддержка SSL-подключения.** Сервер reverse-прокси может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.

Чтобы опубликовать веб-сервер:

1. Создайте один или несколько серверов reverse-прокси.
2. Если для доступа к удаленному приложению развернуто несколько веб-серверов, создайте для них правило балансировки.
3. Создайте правила reverse-прокси, которые будут определять условия публикации веб-сервера или группы веб-серверов.

i Важно!

Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в параметрах правила.

4. В разделе **Настройки → Сеть → Зоны** в параметрах контроля доступа той зоны, в которой необходимо разрешить доступ к внутренним ресурсам, разрешите сервис **Reverse-прокси**.

Создание сервера reverse-прокси

Чтобы создать сервер reverse-прокси:

1. В разделе **Глобальный портал → Серверы reverse-прокси** нажмите **Добавить**.
2. В окне **Настройка сервера reverse-прокси** укажите название, IP-адрес или FQDN и TCP-порт публикуемого веб-сервера, .
3. Если необходимо, настройте остальные параметры:
 - Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate NGFW до публикуемого веб-сервера. Если этот флажок установлен, убедитесь, что на шаге 2 вы указали порт для защищенного соединения.

i Примечание

Начиная с версии 7.4.0 для создания защищенного соединения с веб-серверами UserGate NGFW использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. Поэтому, перед тем как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях «server hello» при установлении соединения.

- Установите флажок **Проверять SSL-сертификат**, чтобы включить проверку подлинности SSL-сертификата, установленного на публикуемом веб-сервере. Доступно, если установлен флажок **HTTPS до сервера**.

- Установите флажок **Не изменять IP-адрес источника**, чтобы сохранять
- оригинальный IP-адрес источника в запросах. Если флажок снят, IP-адрес источника заменяется на IP-адрес UserGate NGFW.

Важно!

Если установлен флажок «Не изменять IP-адрес источника», для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UG NGFW, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UG NGFW или можно настроить статические маршруты через UG NGFW для «белых» IP-адресов источников.

4. Сохраните изменения.

Балансировка серверов reverse-прокси

Если для доступа к удаленному приложению развернуто несколько веб-серверов, вы можете распределять клиентские запросы между ними с помощью правил балансировки нагрузки.

Чтобы создать правило балансировки серверов reverse-прокси:

1. В разделе **Глобальный портал** создайте серверы reverse-прокси для удаленного приложения. Убедитесь, что в окне **Настройка сервера reverse-прокси** для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.
2. В разделе **Настройки → Политики сети → Балансировка нагрузки** нажмите **Добавить** и выберите **Добавить балансировщик reverse-прокси**.
3. В окне **Настройка правила балансировки reverse-прокси** на вкладке **Общие** укажите название правила и включите его.
4. На вкладке **Серверы reverse-прокси** добавьте серверы, на которые будет распределяться нагрузка.
5. Сохраните изменения.

Создание правила публикации reverse-прокси

Правила публикации reverse-прокси позволяют фильтровать запросы к веб-серверам, контролировать доступ к ним и обеспечивать безопасное соединение.

Созданные правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете мышью перетаскивать правила в списке для изменения порядка применения правил.

Чтобы создать правило reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** нажмите **Добавить**.
2. В окне **Настройка правила reverse-прокси** на вкладке **Общие**:
 - Включите правило и укажите его название.
 - Если необходимо, укажите теги для маркировки правила. Подробнее — см. в разделе «[Теги](#)». Параметр доступен в версии ПО 7.3.0 и выше.
 - В списке **Сервер reverse-прокси** выберите сервер или балансировщик reverse-прокси, которому UserGate NGFW будет пересылать запросы.
 - Укажите порты, на которых UserGate NGFW будет слушать входящие запросы.
 - Установите флажок **Использовать HTTPS**, если необходимо, чтобы обмен трафиком с клиентом проходил по защищенному соединению.
 - Если флажок **Использовать HTTPS** установлен:
 - Выберите профиль SSL, поддерживающий нужные протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи.
 - Укажите сертификат веб-сервера для поддержки HTTPS-соединения.
 - Если необходимо, включите авторизацию пользователя по сертификату, выбрав значение **PKI**, и затем укажите предварительно созданный профиль клиентских сертификатов.

Подробнее — см. в разделе «[Профили клиентских сертификатов](#)».

- С помощью параметра **Вставить** настройте расположение правила в списке.

i Примечание

Параметр доступен, если в списке уже есть другие правила.

3. На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса (не более 15 адресов), для которых будет разрешен обмен трафиком с веб-серверами.

i Важно!

Не добавляйте в списки строки с символом «*», они будут игнорироваться.

i Примечание

Вы также можете настроить правило, игнорирующее источники трафика в указанных зонах и с выбранными адресами. Для этого на вкладке «Источник» нужно сформировать список нежелательных зон и/или адресов и в соответствующих блоках параметров включить «Инвертировать».

i Примечание

Каждые пять минут UserGate NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate NGFW автоматически обновляет значение IP-адреса.

i Важно!

Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменных имен; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

4. Если на шаге 2 выбраны использование HTTPS и авторизация по клиентскому сертификату, на вкладке **Пользователи**, если необходимо, сформируйте список пользователей и групп, для которых будет применяться это правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Подробнее — см. в разделе «[Пользователи и группы](#)».

5. На вкладке **Назначение** укажите IP-адреса, назначенные на интерфейсы, которые принимают входящие соединения. Этот параметр следует настраивать, когда на один интерфейс UserGate NGFW назначено несколько IP-адресов либо несколько интерфейсов подключены к сети.

i Примечание

Вы также можете настроить правило, игнорирующее входящие соединения на указанные адреса. Для этого на вкладке «Назначение» укажите адреса и включите «Инвертировать».

i Важно!

Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

6. На вкладке **Useragent**, если необходимо, добавьте идентификационные строки клиентских браузеров, для которых будет разрешен обмен трафиком с веб-серверами.

i Примечание

Вы также можете настроить правило, игнорирующее определенные браузеры, запрашивающие доступ к веб-серверу. Для этого на вкладке «Useragent» нужно сформировать список нежелательных браузеров и включить «Инвертировать».

7. На вкладке **Подмена путей** настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

8. Сохраните изменения.

Подмена путей в правилах reverse-прокси

В этом разделе описан порядок работы функции подмены путей в правилах reverse-прокси для версии 7.2.0 и выше.

Подмена путей в правилах reverse-прокси используется для перенаправления HTTP-запроса пользователя на иной путь. Таким образом вы можете управлять разделением трафика для разных сервисов. Например, пользователь выполнил запрос на `example.com/path1`, а сервер reverse-прокси перенаправляет запрос на `example.local/path2`.

Чтобы настроить подмену путей в правиле reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** создайте или выберите правило.
2. В окне **Настройка правила reverse-прокси** на вкладке **Подмена путей** нажмите **Добавить** и заполните поля:
 - **Изменить с** — домен и/или путь URL, которые требуется изменить. Если в поле **Изменить с** указан домен, то правило reverse-прокси будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.
 - **Изменить на** — домен и/или путь URL, на которые требуется заменить старый.

Примечание

Начиная с версии 7.5.0 вы можете настраивать подмену путей и для кириллических доменов.

Настройка правила reverse-прокси

Общие
Источник
WAF
Пользователи
Назначение
Useragent
Подмена путей

+ Добавить
✎ Редактировать
✖ Удалить
⬆ Выше
⬆ Ниже
Копировать

Изменить с	Изменить на
example.com/path1	example.local/path2

Сохранить
Отмена

3. Сохраните правило.

При обработке HTTP-запроса сработает правило reverse-прокси, паттерн которого в поле **Изменить с** совпадет с путем URL в запросе. При срабатывании правила reverse-прокси происходит подмена пути в HTTP-запросе: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос пользователя не попадет ни под одно правило reverse-прокси, в ответ на него будет получена ошибка: 403 Forbidden.

Условия проверки соответствия

Синтаксис HTTP-запроса представляет собой следующую последовательность: `<scheme>://<host>:<port>/<path>`.

Паттерн в поле **Изменить с** состоит из последовательности `<host>/<path>` и должен удовлетворять следующим условиям:

- `<host>` — обязательный параметр. Совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно. Все названия узлов приводятся к нижнему регистру.
- `<path>` — необязательный параметр. Без него будет выбираться любой путь. Совпадение префиксное (не строгое).
- Паттерн из поля **Изменить с** и паттерн из поля **Изменить на** должны оба либо заканчиваться символом «/», либо не содержать его в конце. В противном случае подмена путей сработает некорректно.
- Схема (`<scheme>`) запроса игнорируется и не изменяется.
- Порт (`<port>`) запроса игнорируется и не изменяется.

При совпадении запроса и исходного паттерна правило считается сработавшим.

В таблице ниже приведены примеры срабатываний паттернов.

Исходный паттерн в правиле reverse-прокси	Примеры запросов, на которые правило сработает	Примеры запросов, на которые правило не сработает
test.dev	• test.dev • test.dev/ • test.dev/* • http://test.dev • test.dev:<любой порт>	• abc.com • test.develop • test.dev.lol
tesT.dev	• test.dev • tesT.dev/ • TEST.dev	• abc.com • test.develop • test.dev.lol
test.dev/co	• test.dev/co* • http://test.dev/co* • test.dev:<любой порт>/co*	• test.dev.lol/co* • test.dev/kool*
http://test.dev	• http://test.dev • http://test.dev/*	• http://test.develop

Исходный паттерн в правиле reverse-прокси	Примеры запросов, на которые правило работает	Примеры запросов, на которые правило не работает
	• <code>http://test.dev:<любой порт></code> • <code>http://test.dev:<любой порт>/</code> • <code>http://test.dev:<любой порт>/*</code>	
<code>http://test.dev/co</code>	• <code>http://test.dev/co*</code> • <code>http://test.dev:<любой порт>/co</code>	• <code>http://test.dev/cool*</code>

Правила подмены путей

Рассмотрим детальнее логику работы подмены путей.

Для этого создадим правило `test.dev/exa → test.dev/ad/test` и сделаем несколько запросов.

Настройка правила reverse-прокси

Общие Источник WAF Пользователи Назначение Useragent Подмена путей

+ Добавить
 Редактировать
 ✖ Удалить
 ⬆ Выше
 ⬆ Ниже
 Копировать

Изменить с	Изменить на
test.dev/exa	test.dev/ad/test

Сохранить Отмена

1) Запрос на **test.dev/exalala**.

Параметр path = **/exalala**. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается **/exa**. Оставшаяся часть: **lala**.

При дальнейшей конвертации берется полученный остаток **lala** и добавляется к концу path паттерна из поля **Изменить на**, то есть: **/ad/test** + **lala**. В итоге, после преобразования, параметр path получает значение **/ad/testlala**.

Таким образом, конечный запрос будет отправлен по адресу **test.dev/ad/testlala**.

2) Запрос на **test.dev/exa/vvv**.

Параметр path = **/exa/vvv**. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается **/exa**. Оставшаяся часть: **/vvv**.

При дальнейшей конвертации берется полученный остаток `/vvv` и добавляется к концу path паттерна из поля **Изменить на**, то есть: `/ad/test` + `/vvv`. В итоге, после преобразования, параметр path получает значение `ad/test/vvv`.

Таким образом, конечный запрос будет отправлен по адресу `test.dev/ad/test/vvv`.

НАСТРОЙКА VPN

Общие сведения

VPN (Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих создавать логические сети (туннели) поверх открытых публичных сетей для обеспечения безопасности коммуникаций.

Для создания VPN необходимо как минимум два сетевых устройства, которые могут идентифицировать друг друга и зашифровать поток данных между собой.

Типы VPN-подключений

UserGate NGFW позволяет создавать VPN-подключения следующих типов:

- VPN для защищенного соединения офисов (Site-to-Site VPN). В этом сценарии один узел выступает в роли VPN-сервера, а другой — в роли VPN-клиента. Подключение сервер-сервер позволяет объединить офисы компании в единую логическую сеть.
- VPN для удаленного доступа клиентов в сеть (Remote access VPN). В этом сценарии NGFW UserGate выступает в роли VPN-сервера, а устройства пользователей — в роли VPN-клиентов. В качестве клиентского ПО на устройствах пользователей может использоваться ПО UserGate Client (для операционных систем [Windows](#), [Linux](#) и [macOS](#)), также поддерживаются стандартные клиенты большинства популярных операционных систем, таких как Windows, Linux, Mac OS X, iOS, Android.

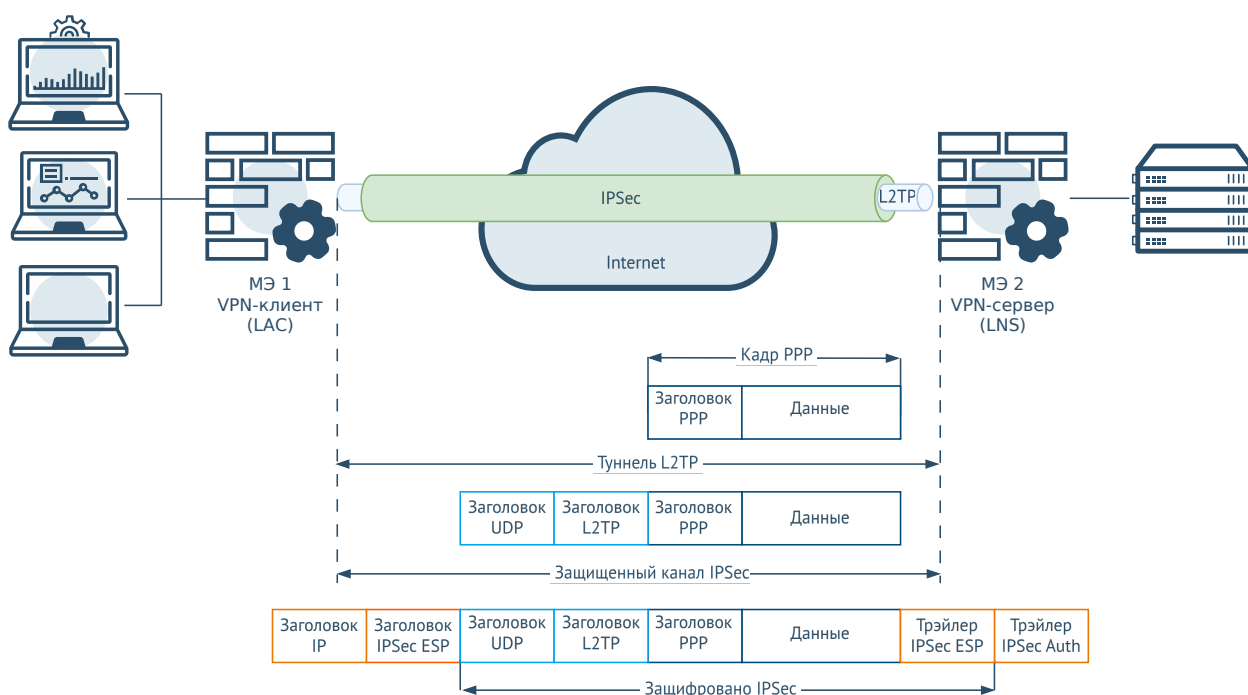
Варианты организации защищенных VPN-туннелей

Для создания защищенных VPN-туннелей могут использоваться протоколы L2TP/IPsec(IKEv1), IPsec(IKEv2), IPsec(IKEv1), GRE/IPsec.

L2TP/IPsec VPN

При создании VPN с помощью L2TP/IPsec, протокол L2TP ([RFC 3931](#)) создает туннель, в котором пакеты сетевого уровня передаются в кадрах PPP. Поскольку L2TP сам по себе не обеспечивает строгую аутентификацию, конфиденциальность и целостность передаваемых данных, для этих целей используется группа протоколов IPsec ([RFC 6071](#)).

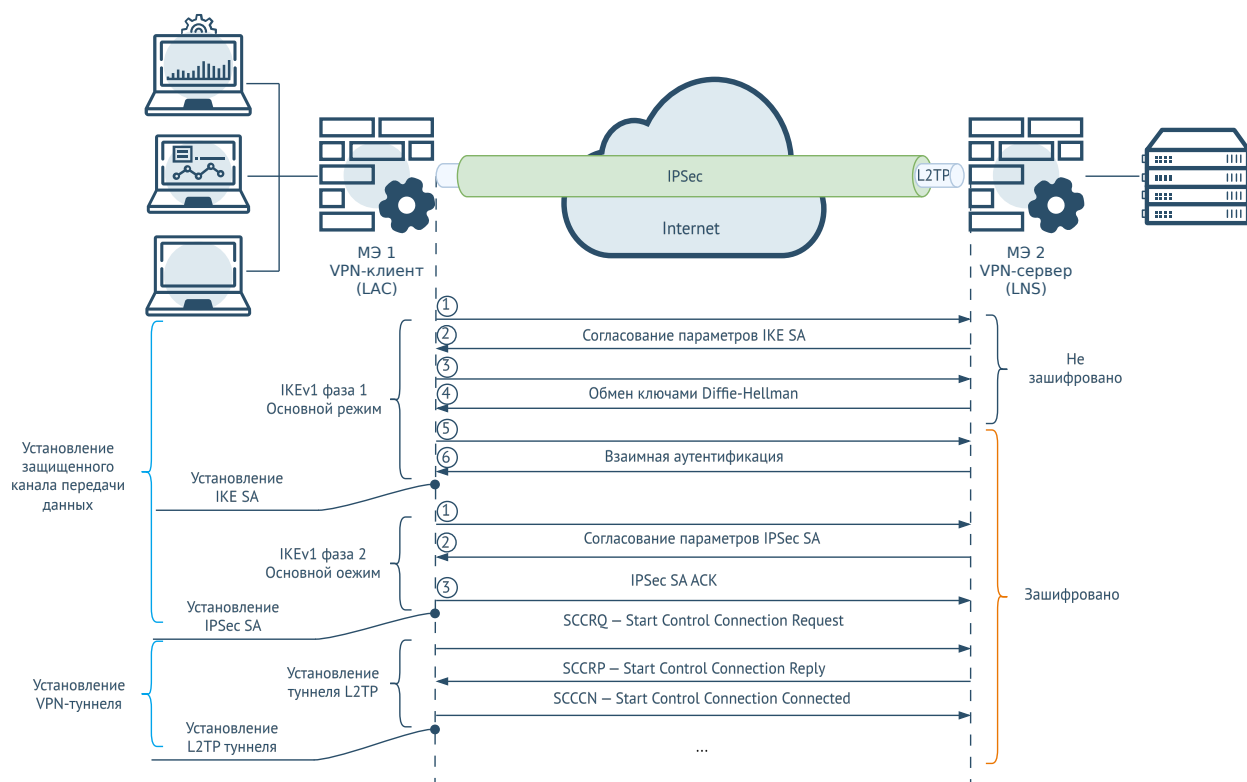
L2TP-туннель создается внутри защищенного IPsec-канала и для его установления необходимо сначала создать защищенное IPsec-соединение между узлами. IPsec в данном случае работает в транспортном режиме и использует протокол ESP (Encapsulating Security Payload) для шифрования L2TP-пакетов.



VPN имеет два уровня инкапсуляции — внутреннюю инкапсуляцию L2TP и внешнюю инкапсуляцию IPsec. Внутренний уровень имеет заголовки L2TP и UDP дополнительно к кадру PPP. Внешний уровень добавляет заголовок и трейлер IPsec ESP. Трейлер проверки подлинности IPsec Auth обеспечивает проверку целостности сообщений и аутентификацию.

Процесс создания VPN состоит из следующих основных этапов:

1. Установление защищенного канала передачи данных.
2. Установление VPN-туннеля.



Установка защищенного канала передачи данных

Для установления защищенного канала передачи данных используется группа протоколов IPsec.

В основе IPsec лежат три протокола:

- Authentication Header (AH),
- Encapsulating security payload (ESP),
- Internet Key Exchange (IKE).

Authentication Header (AH) обеспечивает целостность передаваемых данных, аутентификацию источника информации и защиту от повторной передачи данных. AH не обеспечивает конфиденциальность передаваемых данных, поскольку не осуществляет шифрование. Номер IP-протокола для AH — 51.

Encapsulating security payload (ESP) обеспечивает конфиденциальность передаваемых данных с помощью шифрования, также поддерживается целостность передаваемых данных и аутентификация источника информации. Номер IP-протокола для ESP — 50.

Internet Key Exchange (IKE) — это протокол обмена служебной информацией для согласования и установления ассоциации безопасности (Security Association — SA). Ассоциация безопасности содержит набор параметров

защищенного соединения, которые могут использоваться обеими сторонами соединения для взаимной аутентификации и шифрования передаваемых данных. IKE работает по UDP-порту 500.

IPsec может работать в двух режимах:

- туннельный режим,
- транспортный режим.

В туннельном режиме протоколом IPsec шифруется весь исходный IP-пакет вместе со своим заголовком. Далее он инкапсулируется внутри дополнительного пакета, который имеет собственный заголовок. Туннельный режим применяется, когда две частные сети передают данные через публичную незащищенную сеть.

В транспортном режиме шифруется только полезная нагрузка IP-пакета, при этом исходный заголовок остается, в него добавляется дополнительная информация. Транспортный режим используется, когда между двумя узлами уже существует IP-связь, но она не обеспечивает защиту передаваемых данных.

В сценарии установления VPN с помощью протоколов L2TP/IPsec туннель между узлами создается протоколом L2TP, при этом IPsec должен обеспечивать безопасность канала. В этом случае IPsec работает в транспортном режиме, а согласование ассоциаций безопасности и установление защищенного канала осуществляется с помощью протокола IKE версии IKEv1 в двух фазах.

В фазе 1 происходит аутентификация соседних узлов, согласование ассоциации безопасности IKE SA и установление служебного защищенного канала между узлами для обеспечения обмена данными IKE.

Согласуемыми параметрами IKE SA являются:

- хэш-алгоритмы (MD5, SHA),
- алгоритмы шифрования (DES, 3DES, AES),
- параметры времени жизни туннеля,
- группы Diffie-Hellman.

Для аутентификации узлов канала используется метод общих ключей — pre-shared keys.

Согласование фазы 1 IKEv1 может происходить в двух режимах:

- основной (Main) режим;

- агрессивный (Aggressive) режим.

В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации для IKE SA. Вторым обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее.

В агрессивном режиме происходит два обмена сообщениями (всего три сообщения). В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации, и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.

Меньшее количество передаваемых сообщений в агрессивном режиме позволяет достичь более быстрого установления соединения, однако обмен идентификаторами узлов канала осуществляется открытым текстом. Основным режим считается более безопасным, поскольку данные идентификации в основном режиме зашифрованы.

Результатом фазы 1 является согласование двунаправленной ассоциации безопасности IKE SA и установление защищенного служебного канала. Данный канал будет использоваться в фазе 2 для согласования параметров IPsec SA основного канала передачи данных.

В фазе 2 по защищенному служебному каналу, установленному в фазе 1, происходит согласование IPsec SA для защиты данных, проходящих через канал IPsec.

IKEv1 в фазе 2 имеет один режим, называемый быстрым режимом (Quick mode).

Согласуемыми параметрами IPsec SA являются:

- Алгоритмы шифрования (DES, 3DES, AES);
- Хэш-алгоритмы (MD5, SHA-1, SHA-2);
- Параметры времени жизни SA.

По результатам согласования IPsec SA создается защищенный канал для передачи данных, работающий в транспортном режиме IPsec с инкапсуляцией ESP, имеющий два однонаправленных SA в обе стороны канала.

После его установления служебный канал, созданный в фазе 1, не пропадает – он используется для обновления SA основного.

IPsec SA завершает работу при выключении VPN с одной из сторон соединения или по истечении времени жизни. Тайм-аут по времени жизни возникает при истечении времени жизни ключа или при достижении установленного порога байт данных, прошедших через канал. Когда SA завершает работу, ключи удаляются. Если для передачи данных требуются дополнительные IPsec SA, выполняется новая фаза согласования IKE.

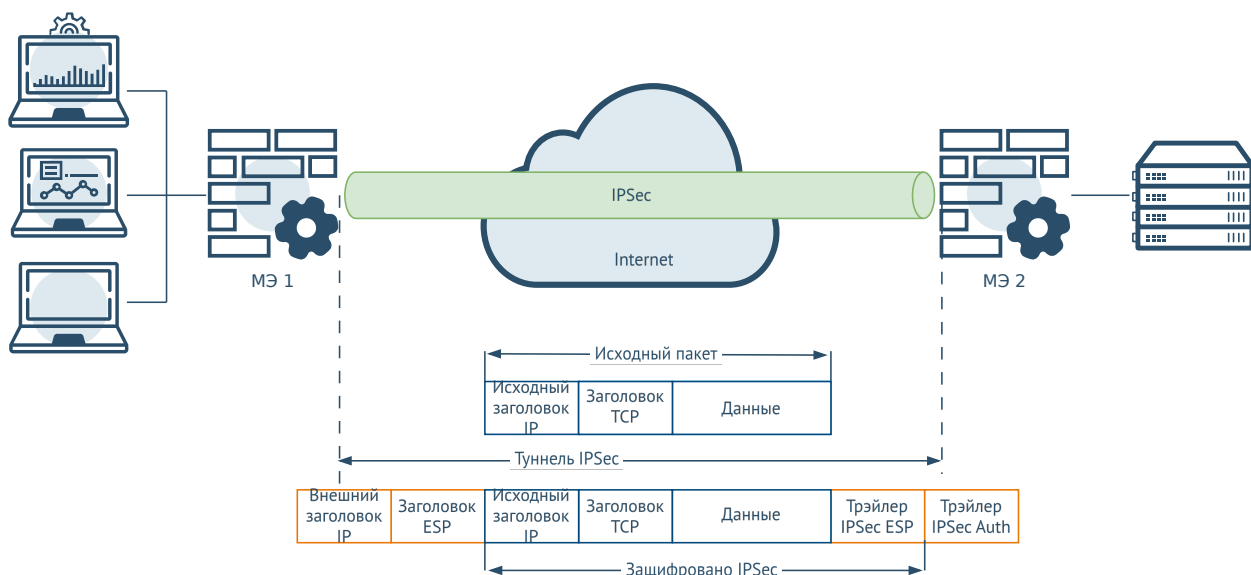
Установление VPN-туннеля

На этом этапе происходит согласование и установление туннеля L2TP между конечными точками SA. Фактическое согласование параметров происходит по защищенному каналу IPsec SA. Протокол L2TP использует UDP-порт 1701.

Когда процесс установления VPN туннеля завершен, пакеты L2TP между конечными точками инкапсулируются с помощью IPsec. Поскольку сам пакет L2TP скрыт внутри пакета IPsec, исходный IP-адрес источника и назначения зашифрован внутри пакета. Кроме того, нет необходимости открывать UDP-порт 1701 на FW между конечными точками, поскольку внутренние пакеты не обрабатываются до тех пор, пока данные IPsec не будут расшифрованы, что происходит только на конечных точках туннеля.

IPsec(IKEv2) VPN

При создании VPN с помощью **IPsec(IKEv2)** защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии IKEv2 ([RFC 7296](#), [RFC 7427](#)).



В этом сценарии IPsec работает в туннельном режиме, исходные IP-пакеты целиком инкапсулируются и шифруются внутри нового пакета, который имеет свой собственный заголовок и трэйлеры.

Подобно IKEv1, IKEv2 также имеет двухэтапный процесс установления защищенного соединения, но при этом происходит меньше обменов сообщениями.



Первый этап известен, как IKE_SA_INIT. В двух сообщениях обмена IKE_SA_INIT между соседними узлами происходит согласование параметров ассоциации безопасности IKE SA и установление защищенного служебного канала. Согласуемые параметры IKE SA:

- хэш-алгоритмы,
- алгоритмы шифрования,

• ключи Diffie-Hellman

Каждый узел генерирует seed-key (SKEYSEED) — ключ, который используется для последующей генерации ключей, используемых в IKE SA. Все будущие ключи IKE создаются с помощью SKEYSEED.

Второй этап называется IKE_AUTH. На этом этапе происходит проверка подлинности соседних узлов. Два сообщения обмена IKE_AUTH аутентифицируются и шифруются в рамках ассоциации безопасности IKE SA, созданной в обмене сообщениями этапа IKE_SA_INIT.

В конце второго этапа согласования через IKE SA создается дочерняя ассоциация безопасности (CHILD SA) для защищенной передачи данных. CHILD SA — это термин IKEv2, подобный IPsec SA для IKEv1. IKEv2 работает через UDP-порты 500 и 4500 (IPsec NAT Traversal).

Дополнительные CHILD SA могут создаваться для организации нового туннеля. Этот обмен называется CREATE_CHILD_SA, в нем могут быть согласованы новые значения групп Diffie-Hellman, новые комбинации алгоритмов шифрования и хэширования.

Аутентификация узлов IPsec туннеля может происходить посредством сертификатов, использующих инфраструктуры открытых ключей (PKI) или с помощью протокола EAP (Extensible Authentication Protocol).

IPsec(IKEv1) VPN

При создании VPN с помощью IPsec(IKEv1) защищенный VPN-туннель создается протоколами группы IPsec с протоколом IKE версии IKEv1.

UserGate NGFW в таком сценарии может работать в качестве VPN-клиента и в качестве VPN-сервера.

GRE/IPsec VPN

GRE ([RFC 2784](#)) — это протокол туннелирования, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей, благодаря чему создается виртуальный канал «точка-точка» поверх IP-сети. GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. При этом GRE не обеспечивает конфиденциальность и целостность передаваемых данных. Для этих целей совместно с GRE используются протоколы группы IPsec.

При совместном использовании GRE и IPsec могут быть созданы 2 типа соединений: IPsec over GRE и GRE over IPsec.

При использовании соединения IPsec over GRE происходит передача зашифрованного трафика по незащищённому GRE-туннелю, т.е. сначала происходит инкапсуляция IPsec, а затем инкапсуляция GRE. Недостаток IPsec over GRE заключается в том, что не поддерживается передача многоадресных и широковещательных пакетов.

Соединение GRE over IPsec позволяет использовать преимущества GRE (поддержка многоадресной и широковещательной рассылки) и IPsec (передача трафика в зашифрованном виде). При использовании соединения GRE over IPsec происходит инкапсуляция пакетов в GRE, а затем их передача по зашифрованному каналу связи (инкапсуляция IPsec).

Для настройки GRE over IPsec необходимо выполнить следующие шаги:

Параметр	Описание
Шаг 1. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте далее в разделе VPN для защищенного соединения офисов (Site-to-Site VPN).
Шаг 2. Настройка туннеля GRE.	Подробнее о настройке туннельного интерфейса GRE читайте в разделе Интерфейс туннель. i Важно! При настройке туннельного интерфейса GRE в качестве адресов источника (локальный IP) и назначения (удалённый IP) должны быть указаны IP-адреса VPN-интерфейсов.

VPN для защищенного соединения офисов (Site-to-Site VPN)

Важно!

Алгоритм настройки параметров VPN, описанный в этом разделе, относится к версиям ПО ниже 7.5.0. Для версии 7.5.0 и выше — смотрите в разделе «[Настройка VPN для защищенного соединения офисов](#)».

VPN-подключение, позволяющее соединить локальные сети удаленных офисов, называется Site-to-Site VPN.

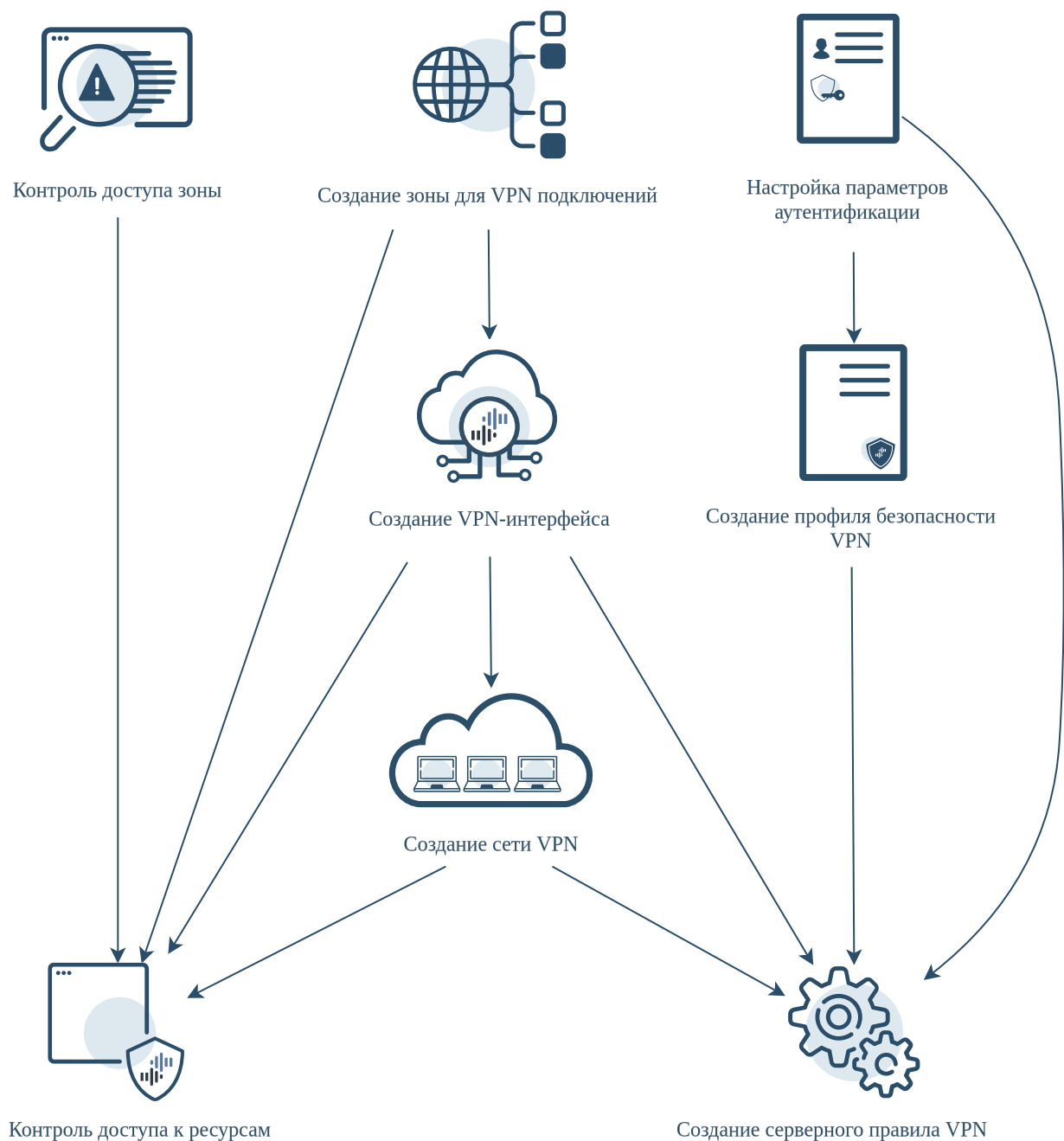
В этом подключении один межсетевой экран выступает в роли VPN-сервера, а другой — в роли VPN-клиента. Клиент инициирует соединение с сервером. Site-to-Site VPN может быть создан между двумя межсетевыми экранами UserGate, либо между межсетевым экраном UserGate и устройством другого производителя.

При создании Site-to-Site VPN-туннелей используются протоколы L2TP/IPsec(IKEv1), IPsec(IKEv2), IPsec(IKEv1).

Необходимо произвести настройки соответствующих параметров на обоих граничных узлах защищенного соединения — на VPN-сервере, и на VPN-клиенте.

Алгоритм настройки VPN-сервера

Для работы NGFW в качестве VPN-сервера необходимо настроить следующие параметры:



- [Контроль доступа зоны.](#)
- [Создание зоны для VPN подключений.](#)
- [Настройка параметров аутентификации.](#)
- [Создание профиля безопасности VPN.](#)
- [Создание VPN-интерфейса.](#)
- [Создание сети VPN.](#)
- [Создание серверного правила VPN.](#)

[Контроль доступа к ресурсам.](#)

Контроль доступа зоны

Необходимо разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Это можно сделать в веб-консоли администратора, перейдя в раздел **Сеть → Зоны**. Далее в настройках контроля доступа для той зоны, с которой будут подключаться VPN-клиенты, нужно разрешить сервис VPN. Как правило, это зона **Untrusted**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены подключаемые по VPN узлы.

В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Настройка параметров аутентификации

При организации VPN-туннеля с протоколом **L2TP** необходимо на VPN-сервере создать локальную учетную запись, которая будет использоваться для аутентификации узла, выполняющего роль VPN-клиента. Локальная учетная запись создается в разделе **Пользователи и устройства → Пользователи**. Для удобства использования все созданные подобные пользователи могут быть помещены в имеющуюся группу **VPN servers**, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп читайте в разделе руководства [Пользователи и группы](#).

При создании защищенного соединения **IPsec** возможны следующие методы аутентификация удаленного узла:

- Аутентификация посредством **общего ключа** (Pre-shared key).
Используется при выборе протокола **IKEv1** для организации защищенного соединения. Общий ключ задается в настройках профилей безопасности VPN. Он должен совпадать на [VPN-сервере](#) и [VPN-клиенте](#) для успешного подключения.
- Аутентификация посредством **сертификатов**,
использующих инфраструктуру открытых ключей (PKI). Используется при выборе протокола **IKEv2** для организации защищенного соединения.

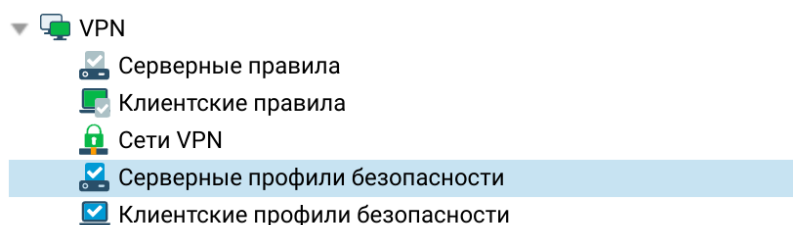
Необходимо заранее создать сертификаты сервера и клиента и импортировать их в NGFW. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).

При необходимости аутентификации **пользователей VPN** нужно создать соответствующий профиль аутентификации. Профили аутентификации создаются в разделе **Пользователи и устройства → Профили аутентификации**. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Подробнее о профилях аутентификации читайте в разделе руководства [Профили аутентификации](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов.

В веб-консоли администратора в разделе **VPN** профили безопасности для узлов, выступающих в роли VPN-сервера и VPN-клиента, настраиваются отдельно:



Для создания профиля безопасности **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**, нажать кнопку **Добавить** и заполнить необходимые поля в свойствах профиля безопасности:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

Название: Site-to-Site VPN profile

Описание: Example VPN security profile for Site-to-Site VPN. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

1. Протокол: IPSEC/L2TP → IPSEC only/IKEv1 → IKEv2

2. Режим IKE: Основной

3. Тип идентификации: отсутствует

Значение идентификации:

4. Общий ключ: *****

Общий ключ (повтор): *****

Сертификат сервера: Сертификат не выбран

Режим аутентификации: Любой

Профиль клиентского сертификата: Не выбран профиль клиентского сертификата

Подсети для VPN

5. + Добавить ✎ Редактировать ✖ Удалить

Локальная подсеть	Удалённая подсеть

Сохранить Отмена

Вкладка **Общие** предназначена для выбора версии протокола VPN и задания параметров аутентификации узлов при установлении защищенного соединения.

1. **Протокол.** Возможны следующие варианты выбора поля:

- IPsec/L2TP.
- IPsec only/IKEV1.
- IKEv2.

2. **Режим работы IKE** (доступно только для IKEv1). Возможны следующие варианты выбора поля:

- **Основной.**

Агрессивный.

3. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации NGFW на соседнем узле при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:

- **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate.
- **IPv4** — IP-адрес узла.
- **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
- **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
- **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.

4. Тип аутентификация удаленного узла при установлении защищенного соединения.

- При выборе протокола IKEv1 используется аутентификация с **общим ключом** (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- При выборе протокола IKEv2 для организации туннеля Site-to-Site возможна аутентификация с помощью сертификатов, использующих инфраструктуру открытых ключей (PKI). Необходимо указать заранее созданные сертификат сервера и профиль клиентских сертификатов. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#). О создании профилей клиентских сертификатов читайте в разделе [Профили клиентских сертификатов](#).

5. **Подсети для VPN**. Задается при выборе протокола организации VPN-туннеля IPsec only/IKEV1:

- **Локальная подсеть** — IP-адрес разрешенной локальной подсети.
- **Удаленная подсеть** — IP-адрес разрешенной подсети со стороны удаленного узла.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

Свойства серверного профиля безопасности

Общие **Фаза 1** Фаза 2

6. время жизни ключа: 24 часов

7. Dead peer detection: Отключена 60 (в сек)
Неудачных попыток: 5

8. Diffie-Hellman группы

+ Добавить - Удалить

Группа 2 Prime 1024 бит
Группа 14 Prime 2048 бит

9. Безопасность

+ Добавить Редактировать - Удалить Выше Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

6. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

7. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения

R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 режима работы механизма:

- **Отключено** — Механизм отключен. DPD запросы не отсылаются.
- **Всегда включено** — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.
- **При отсутствии трафика** — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.

8. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будут использоваться для обмена ключами.

9. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

10. Время жизни ключа: 12 часов

11. Максимальный размер данных, шифруемых одним ключом: Отключено

4500 МБ

12. Включить NAT keepalive: ☐

Время жизни NAT: 0 (в секундах)

Безопасность

+ Добавить Редактировать Удалить Выше Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить Отмена

10. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

11. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

12. **NAT keepalive** — применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически

отправляет пакеты keeralive в сторону реер-узла для поддержания сессии NAT активной.

13. **Безопасность** — алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

Настройка VPN-адаптера

Общие Сеть

1 Включено: ☒

2 Название: tunnel2

Описание: Example VPN interface to be used in Site-to-Site VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for Site-to-Site

4 Профиль netflow: Не выбран

5 Алиас/Псевдоним:

Сохранить Отмена

1. **Включено** — включение/отключение интерфейса.
2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса.
3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).
4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#). Опциональный параметр.
5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

Настройка VPN-адаптера

Общие Сеть

6 Режим: Статический

7 MTU: 1420

IP интерфейса

+ Добавить ✎ Редактировать ✕ Удалить

IP интерфейса	Маска
172.30.255.1	255.255.255.0

Сохранить Отмена

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN), то необходимо использовать статический IP-адрес.

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

8. Поле добавления **IP-адреса** VPN-интерфейса в случае, если выбран статический режим присвоения адреса.

Создание сети VPN

Сеть VPN определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов

клиентам внутри туннеля, настройки DNS и маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.

Сеть VPN в веб-консоли администратора создается в разделе **VPN → Сети VPN**, Необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах VPN-сети:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

1 Название: Site-to-Site VPN network

2 Описание: Example VPN network for Site-to-Site VPN. It can be changed or deleted if necessary.

Сохранить Отмена

1. **Название** сети VPN.

2. **Описание** сети VP. Опциональный параметр.

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

3 Диапазон IP: 172.30.255.2-172.30.255.2

4 Маска: 255.255.255.0

5 ☒ Использовать системные DNS-серверы

Серверы DNS:

IP-адрес	Действия
	Добавить Редактировать Удалить

Сохранить Отмена

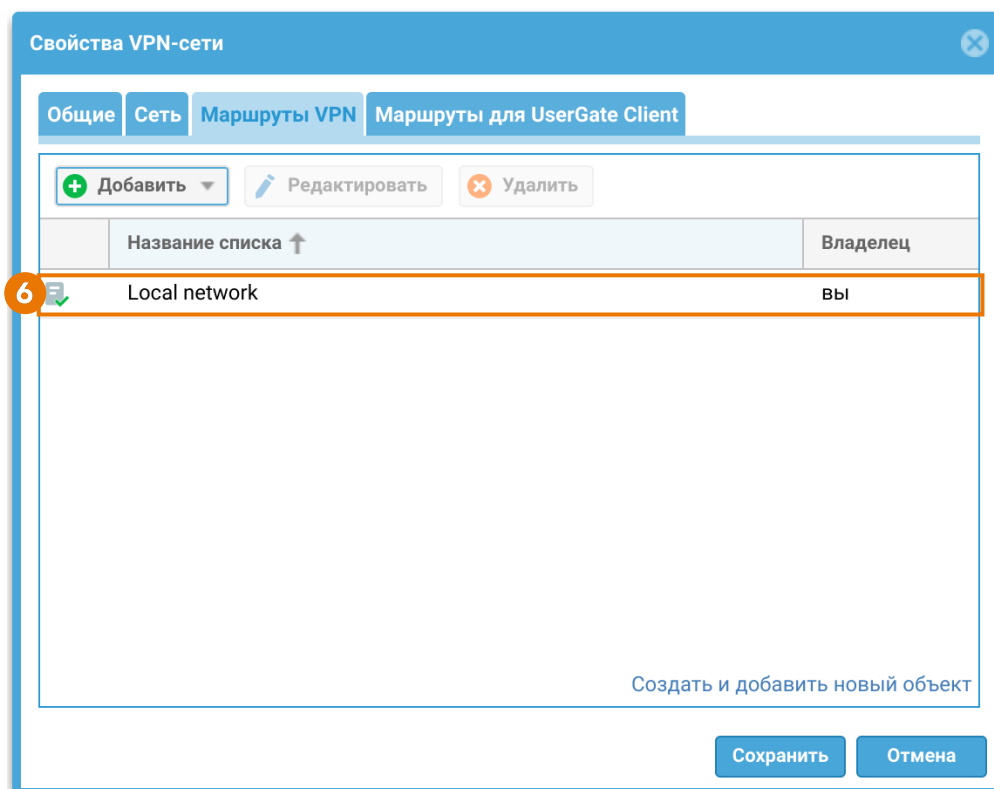
3. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен **VPN-интерфейсу** NGFW, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.

4. **Маска** сети VPN.

5. Указать **DNS-серверы**, которые будут переданы клиенту, или поставить флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

Важно!

Можно указать не более двух DNS-серверов.



6. **Маршруты VPN** — маршруты, передаваемые VPN-клиенту в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.

Вкладка **Маршруты для UserGate client** не используется в сценарии настройки VPN для защищенного соединения офисов (Site-to-Site VPN). Она предназначена для [настройки функции раздельного туннелирования для UserGate Client](#) в сценарии [удаленного доступа в сеть](#).

Создание серверного правила VPN

Серверные правила VPN в веб-консоли администратора создаются в разделе **VPN → Серверные правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

Свойства

Общие Источник Пользователи Назначение

1 Включено: ☒

2 Название: Site-to-Site VPN rule

3 Описание: Example VPN server rule which allows access for Site-to-Site VPN clients connections from Untrusted zone and places them to VPN for Site-to-Site zone (zone assigned to VPN interface). This rule can be changed or deleted if necessary.

4 Профиль безопасности VPN: Site-to-Site VPN profile

5 Сеть VPN: Site-to-Site VPN network

6 Профиль аутентификации: local URL инициализации TOTP

7 Интерфейс: tunnel2

Сохранить Отмена

1. **Включено** — включение/отключение правила VPN.

2. **Название** серверного правила VPN.

Теги — указание опционального тега для маркировки правила. Подробнее читайте в статье [Теги](#) руководства администратора. Опция доступна начиная с релиза ПО 7.3.0.

3. **Описание** серверного правила VPN. Опциональный параметр.

4. **Профиль безопасности VPN** — профиль безопасности, созданный [ранее](#).

5. **Сеть VPN** — сеть, созданная ранее на этапе [создания сети VPN](#). При настройке серверного правила для IPsec-туннеля, когда UserGate является VPN-сервером (указан протокол VPN **IPsec only/IKEV1** в свойствах серверного профиля безопасности) необходимо в данном поле выбрать опцию **Не использовать**.

6. **Профиль аутентификации** — профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы

прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. При необходимости в разделе **Пользователи и устройства → Профили аутентификации** можно создать профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации смотрите в разделе [Профили аутентификации](#).

При настройке серверного правила для IPsec-туннеля, когда UserGate является VPN-сервером (указан протокол VPN **IPsec only/IKEV1** в свойствах серверного профиля безопасности) необходимо в данном поле выбрать опцию **Не использовать**.

7. **Интерфейс** — созданный ранее [VPN-интерфейс](#).

Свойства

Общие **Источник** Пользователи Назначение

Зона источника

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☐ Trusted
- ☐ Tunnel inspection zone
- ☒ Untrusted
- ☐ VPN for remote access
- ☐ VPN for Site-to-Site

Адрес источника

+ Добавить Редактировать

Название списка ↑	Владелец

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Создать и добавить новый объект

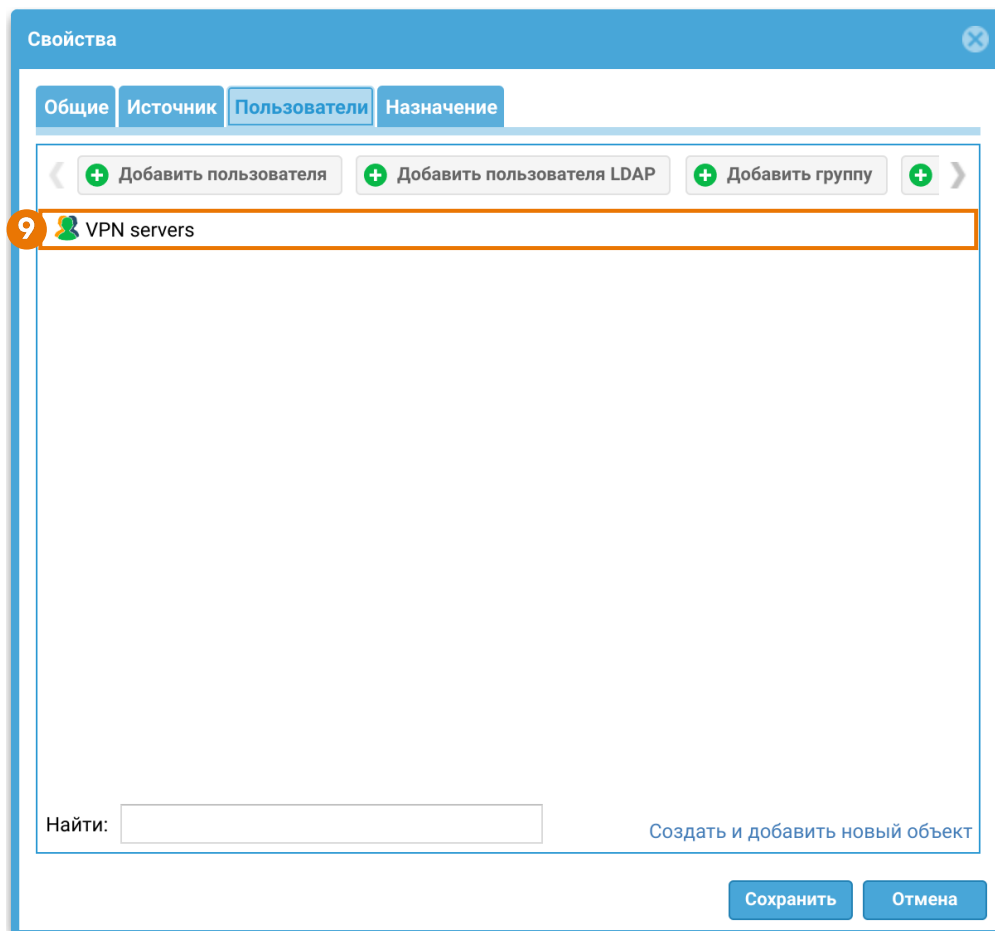
Сохранить Отмена

8. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

Важно!

Обработка трафика происходит по следующей логике:

- условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;
- условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.



9. **Пользователи** — группа учетных записей серверов или отдельные учетные записи серверов, которым разрешено подключаться по VPN.

Свойства

Общие Источник Пользователи **Назначение**

Адрес назначения

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Ext. address	Вы

Создать и добавить новый объект

Сохранить Отмена

10 **Назначение** — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

Важно!

Для применения различных серверных правил к разным клиентам необходимо использовать параметры Зона источника и Адрес источника. Параметр Пользователи не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

Примечание

При изменении настроек VPN-сервера (изменение серверных правил, изменение профилей безопасности, добавление новых VPN-сетей) не происходит перезагрузка VPN-сервера, благодаря чему ранее установленные активные сессии VPN-клиентов не обрываются. Перезагрузка VPN-сервера и переподключение активных сессий VPN-клиентов может произойти в случае смены IP-адреса туннельного интерфейса VPN-сервера.

i Примечание

Начиная с версии ПО 7.2.0 трафик, проходящий через VPN-соединение между офисами, маркируется в журналах логинами конкретных пользователей, если они известны, иначе — именем "Unknown".

Контроль доступа к ресурсам

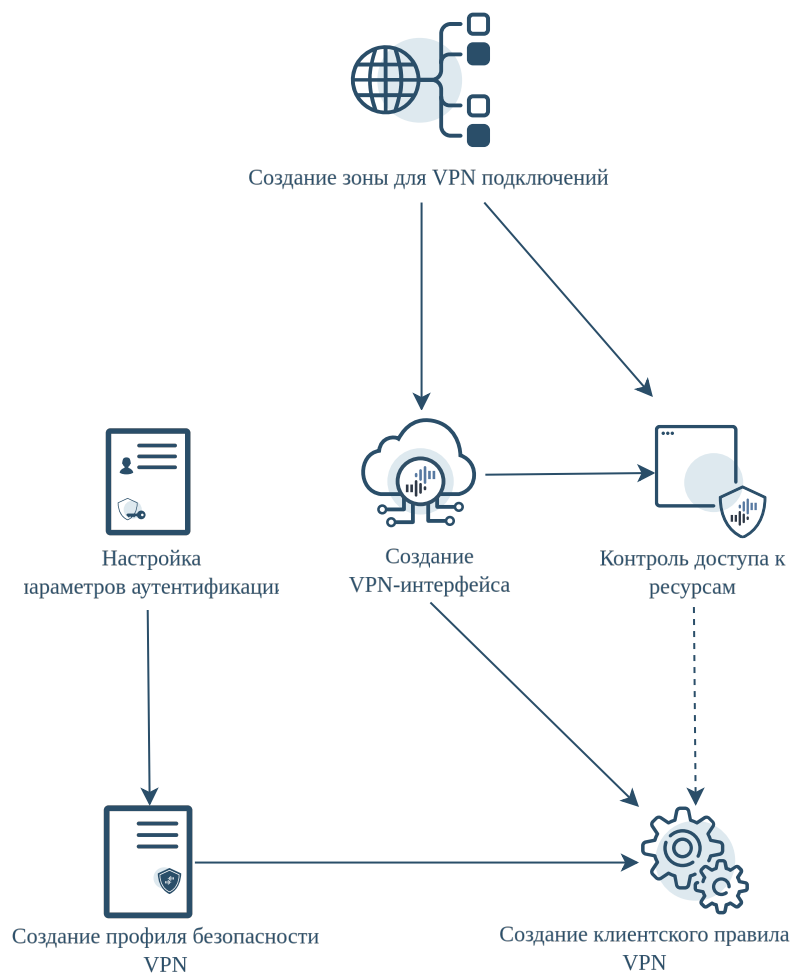
При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из [зоны для VPN-подключений](#) в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства [Межсетевой экран](#).

Чтобы трафик передавался обратно клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, сконфигурированную ранее [зону для VPN-подключений](#).

На VPN-сервере необходимо настроить маршрутизацию для возвратного трафика. Например, для того чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте. Подробнее о настройках виртуального маршрутизатора читайте в разделе руководства [Виртуальные маршрутизаторы](#).

Алгоритм настройки VPN-клиента

Для работы NGFW в качестве VPN-клиента необходимо настроить следующие параметры:



- [Создание зоны для VPN подключений.](#)
- [Создание VPN-интерфейса.](#)
- [Контроль доступа к ресурсам.](#)
- [Настройки параметров аутентификации.](#)
- [Создание профиля безопасности VPN.](#)
- [Создание клиентского правила VPN.](#)

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены интерфейсы, используемые для подключения по VPN. В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения по VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

Настройка VPN-адаптера

Общие Сеть

1 Включено: ☒

2 Название: tunnel3

Описание: Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for Site-to-Site

4 Профиль netflow: Не выбран

5 Алиас/Псевдоним:

Сохранить Отмена

1. **Включено** — включение/отключение интерфейса.

2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса. Расположенное ниже поле

Описание является опциональным.

3. **Зона**, к которой будет относиться данный интерфейс. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).

4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#). Опциональный параметр.

5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

Настройка VPN-адаптера

Общие Сеть

6 Режим: Динамический

7 MTU: 1420

IP интерфейса

+ Добавить ✎ Редактировать ✖ Удалить

IP интерфейса	Маска

Сохранить Отмена

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — **Динамический**. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, сконфигурированной в настройках VPN-сервера на этапе [создания сети VPN](#).

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем

установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

Важно!

Если при настройке туннельного интерфейса на стороне VPN-сервера и VPN-клиента был выбран уже созданный для примера один и тот же туннельный интерфейс с настройками по умолчанию, то при подключении клиента к серверу возникнет конфликт IP-адресов. Для корректной работы диапазоны адресов туннельных интерфейсов не должны пересекаться. Необходимо изменить диапазоны адресов на клиенте и сервере на уникальные.

Контроль доступа к ресурсам

При необходимости в разделе **Политики сети** → **Межсетевой экран** создать разрешающее правило межсетевого экрана, разрешающее трафик между зоной для VPN-подключений и зонами назначения.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, зону VPN-подключений. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства [Межсетевой экран](#).

Настройки параметров аутентификации

При создании защищенного соединения **IPsec** с **IKEv2** используется аутентификация посредством **сертификатов**, использующих инфраструктуру открытых ключей (PKI). Созданный ранее сертификат VPN-клиента необходимо импортировать в разделе **UserGate** → **Сертификаты** на устройстве, исполняющем роль VPN-клиента.

О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. В разделе **VPN** веб-консоли администратора профили безопасности для узлов, выступающих в роли VPN-сервера и VPN-клиента, настраиваются отдельно:

- ▼ VPN
 - Серверные правила
 - Клиентские правила
 - Сети VPN
 - Серверные профили безопасности
 - Клиентские профили безопасности**

Для создания профиля безопасности **VPN-клиента** необходимо перейти в раздел **VPN → Клиентские профили безопасности**, нажать кнопку **Добавить** и заполнить необходимые поля в свойствах клиентского профиля безопасности:

Свойства клиентского профиля безопасности

Общие

Фаза 1

Фаза 2

1

Название:

Client VPN profile

2

Описание:

Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

3

Протокол:

IPsec L2TP → IPsec → IKEv2 с сертификатом

4

Режим IKE:

Основной

5

Тип идентификации:

отсутствует

Значение идентификации:

6

Общий ключ:

.....

Общий ключ (повтор):

.....

Сертификат клиента:

Сертификат не выбран

Подсети для VPN

8

Локальная подсеть:

100.100.0.0/24

Удалённая подсеть:

10.10.1.0/24

Аутентификация

7

Логин:

vpncInt1

Пароль:

.....

Сохранить

Отмена

Вкладка **Общие** предназначена для выбора версии протокола IKE и задания параметров аутентификации узлов при установлении защищенного соединения.

1. **Название** клиентского профиля безопасности.

2. **Описание** клиентского профиля безопасности. Опциональный параметр.

3. **Протокол** — протокол установления VPN канала между двумя сетями. Возможны следующие варианты выбора поля:

- **IPsec L2TP** — для создания защищенного VPN канала с использованием L2TP и IPsec/IKEv1.
- **IPsec** — для создания защищенного VPN канала с VPN-сервером с использованием IPsec/IKEv1.
- **IKEv2 с сертификатом** — для создания защищенного VPN канала с использованием IKEv2 и аутентификацией с помощью сертификата, использующего инфраструктуру открытых ключей (PKI).

4. **Режим работы IKE**. Возможны следующие варианты выбора поля:

- **Основной**.
- **Агрессивный**.

5. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации соседнего узла при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:

- **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate.
- **IPv4** — IP-адрес узла.
- **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
- **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
- **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.

6. Тип аутентификация удаленного узла при установлении защищенного соединения.

- При выборе протокола **IPsec/L2TP** и **IPsec** используется аутентификация с общим ключом (Pre-shared key). Необходимо задать общий ключ.

Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.

- При выборе протокола **IKEv2 с сертификатом** для организации туннеля Site-to-Site используется аутентификация с помощью сертификатов, использующих инфраструктуру открытых ключей (PKI). Необходимо указать заранее созданный сертификат клиента. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#).

7. **Аутентификация** — логин и пароль локальной учетной записи, [созданной](#) на VPN-сервере для аутентификации узла, выступающего в роли VPN-клиента при установлении **L2TP** туннеля.

8. Подсети для VPN:

- **Локальная подсеть** — IP-адрес разрешенной локальной подсети.
- **Удаленная подсеть** — IP-адрес разрешенной подсети со стороны удаленного VPN-сервера.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

Свойства клиентского профиля безопасности

Общие Фаза 1 Фаза 2

9. Время жизни ключа: 24 часов

10. Dead peer detection: Отключена 60 (в сек)

Неудачных попыток: 5

Diffie-Hellman группы

11. + Добавить - Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

12. + Добавить Редактировать - Удалить Выше Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

9. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

10. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 режима работы механизма:

- **Отключено** — Механизм отключен. DPD запросы не отсылаются.
- **Всегда включено** — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ есть, работа механизма

возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.

- **При отсутствии трафика** — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.

11. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будут использоваться для обмена ключами.

12. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

Свойства клиентского профиля безопасности

Общие Фаза 1 Фаза 2

13. Время жизни ключа: 12 часов

14. Максимальный размер данных, шифруемых одним ключом: Отключено

4500 МБ

Безопасность

+ Добавить ✎ Редактировать ✖ Удалить ⬆ Выше ⬇ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

13. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

14. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

15. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Низе**.

Создание клиентского правила VPN

Клиентское правило VPN будет инициировать подключение к VPN-серверу. Клиентские правила VPN в веб-консоли администратора создаются в разделе **VPN → Клиентские правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

Свойства	
Общие	
1 Включено:	☒
2 Название:	Client VPN rule
3 Описание:	Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.
4 Профиль безопасности VPN:	Client VPN profile
5 Интерфейс:	tunnel3
6 Адрес сервера:	192.168.1.101
Сохранить Отмена	

1. **Включено** — включение/отключение данного правила.

2. **Название** клиентского правила.

Теги — указание опционального тега для маркировки правила. Подробнее читайте в статье [Теги](#) руководства администратора. Опция доступна в версии 7.3.0 и выше.

3. **Описание** клиентского правила. Опциональный параметр.

4. **Профиль безопасности VPN** — созданный ранее [клиентский профиль безопасности VPN](#).

5. **Интерфейс** — созданный ранее [VPN-интерфейс](#).

6. **Адрес сервера** — адрес VPN-сервера (IP-адрес, FQDN), куда подключается данный VPN-клиент.

Примечание

В случае подключения по FQDN, если адрес сервера резолвится в несколько IP-адресов, то клиент подключится к одному из доступных адресов.

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Если VPN-соединение не установилось, в разделе клиентского правила в поле «Последняя ошибка» отобразится описание ошибки установления соединения.

Примеры настроек Site-to-Site VPN

О примерах настроек VPN для различных сценариев читайте в разделах::

- [Site-to-Site VPN с L2TP/IPSec\(IKEv1\)](#).
- [Site-to-Site VPN с L2TP/IPSec\(IKEv1\) с помощью интерфейса командной строки](#).
- [Site-to-Site VPN с IPSec\(IKEv2\)](#).

VPN для удаленного доступа клиентов (Remote access VPN)

Важно!

Алгоритм настройки параметров VPN, описанный в этом разделе, относится к версиям ПО ниже 7.5.0. Для версии 7.5.0 и выше — смотрите в разделе «[Настройка VPN для удаленного доступа в сеть](#)».

VPN-подключение, с помощью которого пользователи могут получить защищенный доступ к корпоративной сети компании через Интернет, называется Remote access VPN.

В этом подключении межсетевой экран UserGate (NGFW) выступает в роли VPN-сервера, а устройства пользователей — в роли VPN-клиентов. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client (версии для [Windows](#), [Linux](#) и [macOS](#)), также поддерживаются нативные клиенты большинства популярных операционных систем.

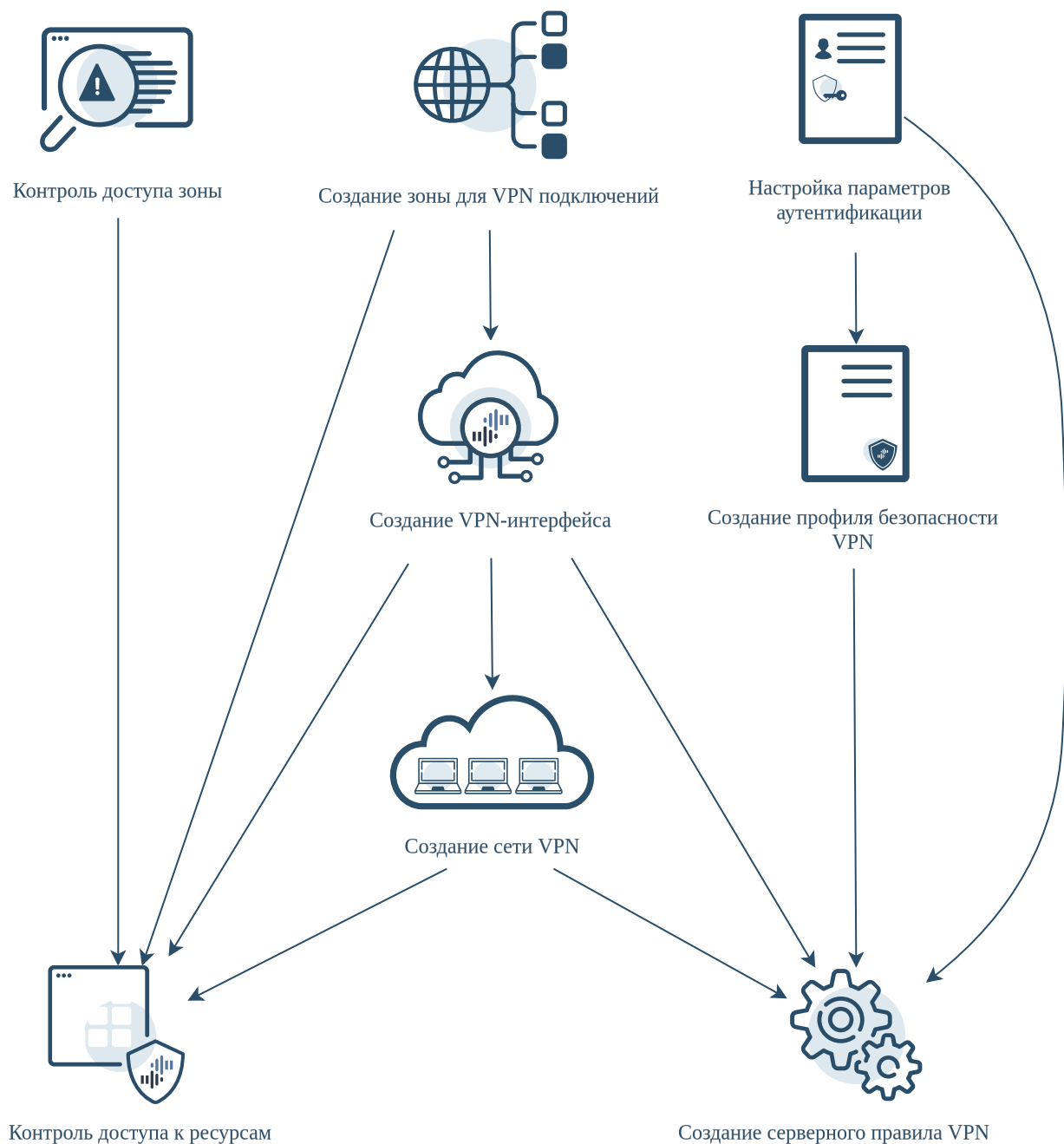
Для организации защищенного подключения используются следующие протоколы:

- L2TP/IPSec(IKEv1);
- IPSec(IKEv2).

Для создания Remote Access VPN необходимо произвести [настройки соответствующих параметров на VPN-сервере](#) (NGFW), а затем [настроить и подключить VPN-клиент](#) на оборудовании пользователя.

Настройка VPN-сервера

Алгоритм настройки VPN-сервера на UserGate NGFW включает в себя следующие основные этапы:



1. [Контроль доступа зоны.](#)
2. [Создание зоны для VPN подключений.](#)
3. [Настройка параметров аутентификации.](#)
4. [Создание профиля безопасности VPN.](#)
5. [Создание VPN-интерфейса.](#)
6. [Создание сети VPN.](#)
7. [Создание серверного правила VPN.](#)

[Контроль доступа к ресурсам.](#)

8.

Контроль доступа зоны

Необходимо разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Это можно сделать в веб-консоли администратора, перейдя в раздел **Сеть → Зоны**. Далее в настройках контроля доступа для той зоны, с которой будут подключаться VPN-клиенты, нужно разрешить сервис VPN. Как правило, это зона **Untrusted**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Создание зоны для VPN-подключений

Необходимо создать зону, в которую будут помещены подключаемые по VPN клиенты.

В веб-консоли администратора зона создается в разделе **Сеть → Зоны**. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Настройка параметров аутентификации

1. При создании защищенного соединения **IPsec** возможны следующие методы аутентификации узлов:

- Аутентификация посредством **общего ключа** (Pre-shared key).
Используется при выборе протокола **IKEv1** для организации защищенного соединения. Общий ключ задается в настройках [профиля безопасности VPN](#). Он должен совпадать на [VPN-сервере](#) и на VPN-клиентах для успешного подключения.
- Аутентификация посредством **сертификатов**,
использующих инфраструктуру открытых ключей (PKI). Используется при выборе протокола **IKEv2** для организации защищенного соединения. Необходимо заранее создать сертификаты сервера и клиентов и импортировать их в NGFW и на клиентские компьютеры. Также в NGFW необходимо создать профили клиентских сертификатов. О примерах создания и использования сертификатов для IKEv2 VPN читайте в [Приложении](#). О создании профилей клиентских сертификатов читайте в разделе [Профили клиентских сертификатов](#).

2. Для аутентификации **пользователей VPN** нужно создать соответствующий профиль аутентификации. Профили аутентификации создаются в разделе

Пользователи и устройства → Профили аутентификации. Допускается использовать тот же профиль, что используется для аутентификации пользователей с целью получения доступа к сети интернет. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP.

Примечание

Если авторизация пользователей происходит в различных поддоменах, на вкладке Домены LDAP в настройках LDAP-коннектора необходимо указывать все варианты таких поддоменов. Подробнее о настройке LDAP-коннектора читайте в разделе [Серверы аутентификации](#).

При аутентификации пользователей VPN возможно использование многофакторной аутентификации. Второй фактор может быть получен через одноразовые коды TOTP. VPN с TOTP работает для клиента UserGate Client только с IKEv2 (код вводится в отдельном окне), для других клиентов — только с IKEv1 (код вводится в пароле через двоеточие: *пароль_пользователя:totp_code*).

Примечание

При установлении L2TP/IPsec VPN-соединения с аутентификацией пользователей через Multifactor RADIUS Adapter повторное переподключение к VPN-серверу в течении 30-секундного тайм-аута с момента предыдущего успешного подключения произойдёт без обращением к RADIUS-серверу. Если переподключение будет выполняться за пределами 30-секундного тайм-аута, обращение к RADIUS-серверу произойдёт.

Подробнее о профилях аутентификации читайте в разделе руководства [Профили аутентификации](#).

Создание профиля безопасности VPN

В настройках профиля безопасности VPN определяются типы и параметры алгоритмов шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов.

Для создания профиля безопасности в веб-консоли администратора **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**:

- ▼ VPN
 - Серверные правила
 - Клиентские правила
 - Сети VPN
 - Серверные профили безопасности**
 - Клиентские профили безопасности

Нажать кнопку **Добавить** в панели инструментов раздела и заполнить необходимые поля в свойствах профиля безопасности:

Свойства серверного профиля безопасности

Общие | Фаза 1 | Фаза 2

Название: Remote access VPN profile

Описание: Example VPN security profile for Remote access VPN. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

1 Протокол: IPSEC/L2TP → IKEv2

2 Режим IKE: Основной

3 Тип идентификации: отсутствует

Значение идентификации:

4 Общий ключ:
Общий ключ (повтор): ↓

Сертификат сервера: Сертификат не выбран

Режим аутентификации: Любой

Профиль клиентского сертификата: Не выбран профиль клиентского сертификата

Подсети для VPN

+ Добавить | ✎ Редактировать | ✕ Удалить

Локальная подсеть	Удалённая подсеть

Сохранить | Отмена

Вкладка **Общие** предназначена для выбора версии протоколов VPN и задания параметров аутентификации при установлении защищенного соединения.

1. **Протокол.** Возможны следующие варианты выбора поля:

- IPsec/L2TP.

IKEv2.

- **IPsec only/IKEv1** — не используется для организации соединений Remote access VPN (используется только для организации соединений Site-to-Site VPN).

2. **Режим работы IKE** (доступно только для IKEv1) (Подробнее о режимах IKEv1 читайте в статье [VPN](#)). Возможны следующие варианты выбора поля:

- **Основной.**
- **Агрессивный.**

3. **Тип идентификации** (параметр IKE local ID). Необходим для идентификации NGFW на соседнем узле при установлении VPN-соединения с оборудованием некоторых производителей. Возможные значения выбора поля:

- **Отсутствует** — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID.
- **IPv4** — IP-адрес узла.
- **FQDN** — адрес узла в формате полностью определенного доменного имени (FQDN).
- **CIDR** — адрес узла в формате бесклассовой адресации (CIDR).
- **Значение идентификации** — значение параметра IKE local ID в формате выбранного ранее типа.

4. Тип аутентификация удаленного узла при установлении защищенного соединения.

- При выборе протоколов IPsec/L2TP используется аутентификация с **общим ключом** (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- При выборе протокола IKEv2 для организации туннеля указывается:
 - Заранее созданный **сертификат сервера**;

Режим аутентификации — возможна аутентификация с

- помощью сертификатов, использующих инфраструктуру открытых ключей (**PKI**), или с помощью методов EAP, PEAP (**AAA**).

- При выборе режима **PKI** необходимо указать сконфигурированный ранее **профиль клиентского сертификата** (подробнее о профилях клиентских сертификатов смотрите в разделе [Профили клиентских сертификатов](#)).
- В режиме аутентификации с помощью методов EAP, PEAP (**AAA**) клиент обменивается с VPN-сервером EAP-пакетами. VPN-сервер транслирует пакеты на внешний доменный RADIUS-сервер, который принимает решение об авторизации. После получения разрешения от RADIUS-сервера, VPN-сервер по полученному логину запрашивает у сервера домена информацию о пользователе, после чего принимает решение о подключении пользователя к VPN.

Далее необходимо задать криптографические параметры первой и второй фаз согласования защищенного соединения.

Во время первой фазы происходит согласование и установление IKE SA. Необходимо указать следующие параметры:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

5 время жизни ключа: 24 часов

6 Dead peer detection: Отключена 60 (в сек)

Неудачных попыток: 5

Diffie-Hellman группы

+ Добавить × Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+ Добавить ✎ Редактировать × Удалить ↕ Выше ↩ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить Отмена

5. **Время жизни ключа** — по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

6. Режим работы механизма **Dead peer detection** (DPD) — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи. DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 режима работы механизма:

- **Отключено** — Механизм отключен. DPD запросы не отсылаются.
- **Всегда включено** — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ есть, работа механизма

возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.

- **При отсутствии трафика** — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.

7. **Diffie-Hellman группы** — выбор групп Диффи-Хеллмана, которые будут использоваться для обмена ключами.

8. **Безопасность** — выбор алгоритмов аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Во второй фазе осуществляется выбор способа защиты передаваемых данных в IPsec подключении. Необходимо указать следующие параметры:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

9. Время жизни ключа: 12 часов

10. Максимальный размер данных, шифруемых одним ключом: Отключено

4500 МБ

11. Включить NAT keepalive: ☐

Время жизни NAT: 0 (в секундах)

Безопасность

+ Добавить ✎ Редактировать ✕ Удалить ↗ Выше ↘ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить Отмена

9. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

10. **Максимальный размер данных, шифруемых одним ключом** — время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии.

11. **NAT keepalive** — применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически

отправляет пакеты keeralive в сторону реер-узла для поддержания сессии NAT активной.

12. **Безопасность** — алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка переместите необходимую пару вверх/вниз или используйте кнопки **Выше/Ниже**.

Для примера в веб-консоли администратора создан профиль безопасности **Remote Access VPN profile**, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, необходимо изменить общий ключ шифрования при использовании протоколов IKEv1/IPsec.

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

VPN-интерфейс в веб-консоли администратора создается в разделе **Сеть → Интерфейсы**. Необходимо нажать кнопку **Добавить** и выбрать **Добавить VPN**, далее в настройках VPN-адаптера задать необходимые параметры:

Настройка VPN-адаптера

Общие Сеть

1 Включено: ☒

2 Название: tunnel1

Описание: Example VPN interface to be used in Remote Access VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for remote access

4 Профиль netflow: Не выбран

5 Алиас/Псевдоним:

Сохранить Отмена

1. **Включено** — включение/отключение интерфейса.
2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса.
3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В этом поле указывается зона, созданная ранее на этапе [создания зоны для VPN подключений](#).
4. **Профиль netflow**, используемый для данного интерфейса. Подробнее о профилях netflow читайте в статье [Профили netflow](#). Опциональный параметр.
5. **Алиас/Псевдоним** интерфейса. Опциональный параметр.

Настройка VPN-адаптера

Общие Сеть

6 Режим: Статический

7 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
172.30.250.1	255.255.255.0

Сохранить Отмена

6. **Режим** — тип присвоения IP-адреса. Возможные опции выбора — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Remote access VPN), то необходимо использовать статический IP-адрес.

7. **MTU** — размер MTU для выбранного интерфейса. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

8. Поле добавления **IP-адреса** VPN-интерфейса в случае, если выбран статический режим присвоения адреса.

Для примера в веб-консоли администратора создан VPN-интерфейс **tunnel1**, который может быть использован для Remote Access VPN.

Создание сети VPN

Сеть VPN определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.

Сеть VPN в веб-консоли администратора создается в разделе **VPN → Сети VPN**, Необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах VPN-сети:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

1 Название: Remote access VPN network

2 Описание:

Сохранить Отмена

1. **Название** сети VPN.
2. **Описание** сети VPN. Опциональный параметр.

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

3 Диапазон IP: 172.30.250.2-172.30.250.254

4 Маска: 255.255.255.0

5 ☒ Использовать системные DNS-серверы

Серверы DNS:

IP-адрес	Добавить	Редактировать	Удалить

Сохранить Отмена

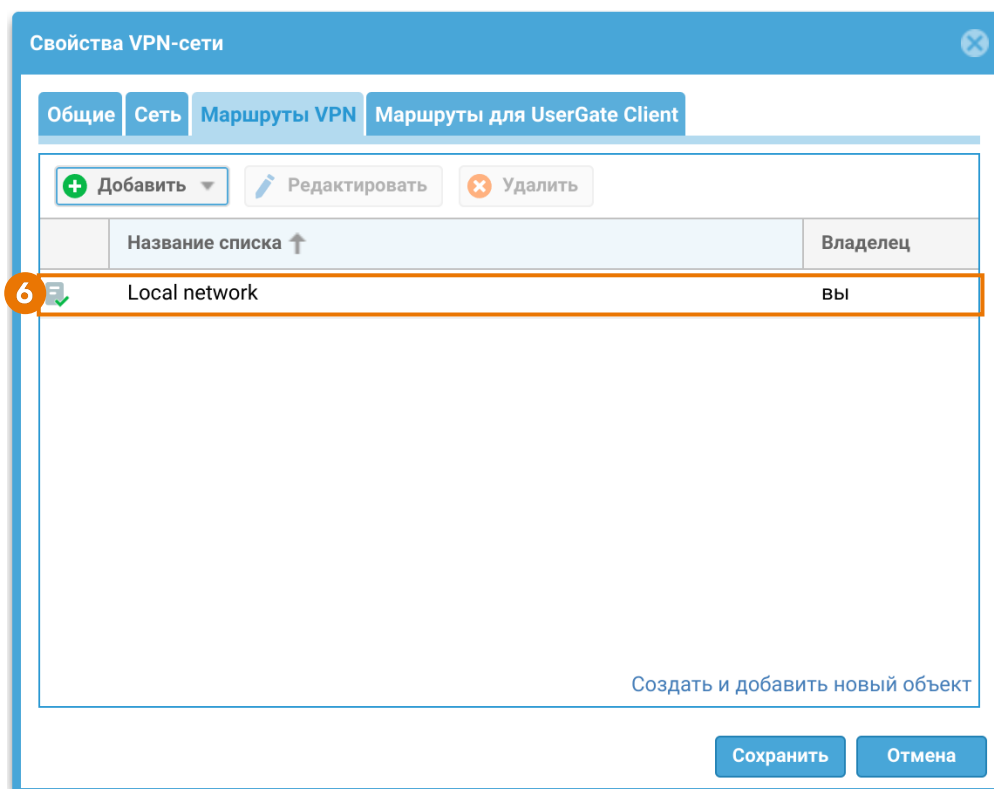
3. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен **VPN-интерфейсу** NGFW, используемому совместно с данной сетью. Не указывайте здесь адрес сети и широковещательный адрес.

4. **Маска** сети VPN.

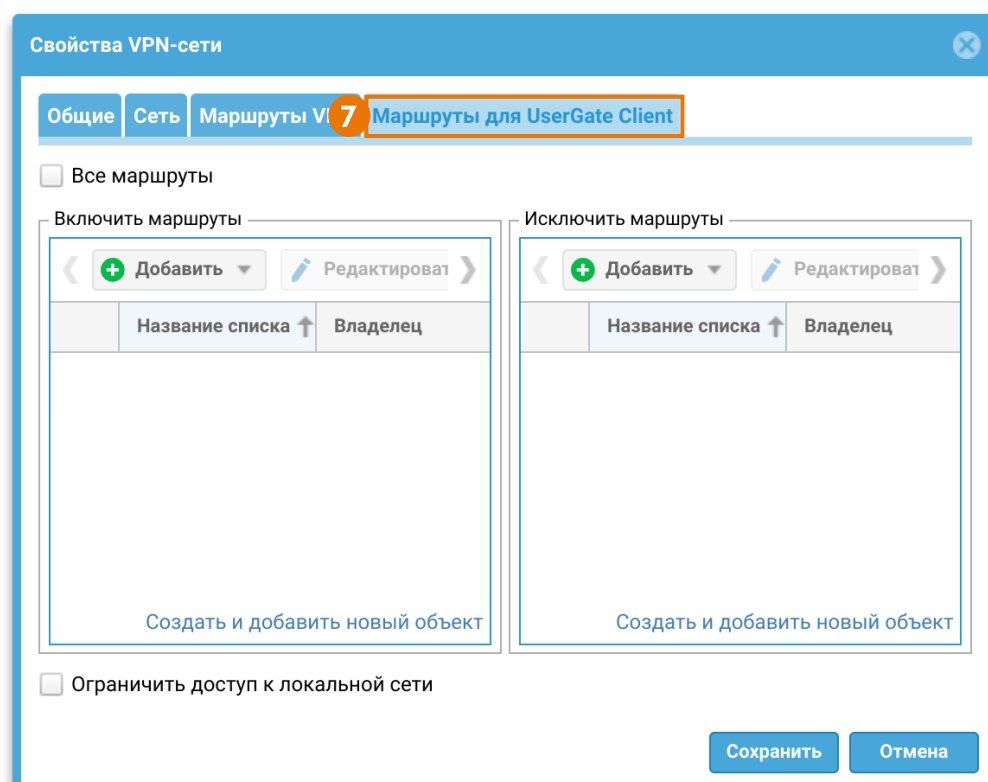
5. Указать **DNS-серверы**, которые будут переданы клиенту, или поставить флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

Важно!

Можно указать не более двух DNS-серверов.



6. **Маршруты VPN** — маршруты, передаваемые VPN-клиенту в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.



7. Вкладка **Маршруты для UserGate client** предназначена для настройки функциональности раздельного туннелирования (split tunneling) для UserGate

Client. Подробнее читайте в разделе [Настройка раздельного туннелирования для UserGate Client](#).

Для примера в веб-консоли администратора создана сеть **Remote access VPN network** с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на клиент.

Создание серверного правила VPN

Серверные правила VPN в веб-консоли администратора создаются в разделе **VPN → Серверные правила**. Далее необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах правила:

Свойства серверного правила VPN

Общие | Источник | Пользователи | Назначение

1 Включено: ☒

2 Название: Remote access VPN rule

3 Описание: Example VPN server rule which allows Remote access for VPN clients from Untrusted zone and places them to VPN for remote access zone (zone assigned to VPN interface). This rule can be changed or deleted if necessary.

4 Профиль безопасности VPN: Remote access VPN profile

5 Сеть VPN: Remote access VPN network

6 Профиль аутентификации: Example user auth profile URL инициализации TOTP

7 Интерфейс: tunnel1

8 Только для UserGate Client: ☒

Сохранить Отмена

1. **Включено** — включение/отключение правила VPN.

2. **Название** серверного правила VPN.

Теги — указание опционального тега для маркировки правила. Подробнее читайте в статье [Теги](#) руководства администратора. Опция доступна в версии ПО 7.3.0 и выше.

3. **Описание** серверного правила VPN. Опциональный параметр.

4. **Профиль безопасности VPN** — профиль безопасности, [созданный ранее](#).
5. **Сеть VPN** — сеть, созданная ранее на этапе [создания сети VPN](#).
6. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, [созданный ранее](#).
7. **Интерфейс** — созданный ранее [VPN-интерфейс](#).
8. **Только для UserGate Client** — опция (доступна в версии ПО 7.1.2 и выше) позволяет ограничить возможность подключения по данному правилу только для VPN-клиентов UserGate Client.

Свойства

Общие | **Источник** | Пользователи | Назначение

Зона источника

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☐ Trusted
- ☐ Tunnel inspection zone
- ☒ Untrusted
- ☐ VPN for remote access
- ☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

[Создать и добавить новый объект](#)

Адрес источника

[+ Добавить](#) [Редактировать](#)

Название списка ↑	Владелец
-------------------	----------

[Создать и добавить новый объект](#)

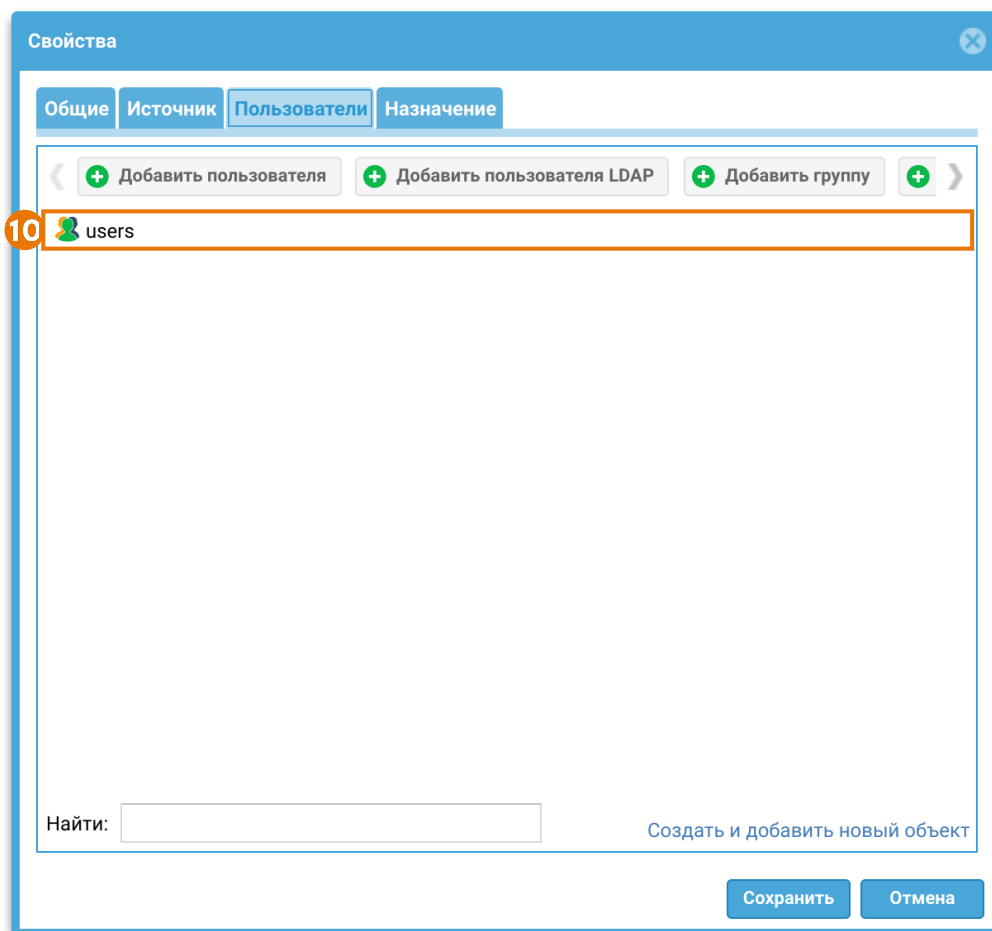
[Сохранить](#) [Отмена](#)

9. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

Важно!

Обработка трафика происходит по следующей логике:

- условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;
- условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.



10. **Пользователи** — локальные или доменные группы учетных записей пользователей или отдельные учетные записи пользователей, которым разрешено подключаться по VPN.

11 **Назначение** — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

i Важно!

Для применения различных серверных правил к разным клиентам необходимо использовать параметры Зона источника и Адрес источника. Параметр Пользователи не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

i Примечание

При изменении настроек VPN-сервера (изменение серверных правил, изменение профилей безопасности, добавление новых VPN-сетей) не происходит перезагрузка VPN-сервера, благодаря чему ранее установленные активные сессии VPN-клиентов не обрываются. Перезагрузка VPN-сервера и переподключение активных сессий VPN-клиентов может произойти в случае смены IP-адреса туннельного интерфейса VPN-сервера.

Для примера в веб-консоли администратора создана сеть **Remote access VPN network** с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на клиент.

Контроль доступа к ресурсам

Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной ранее зоны для VPN-подключений, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**. Подробнее о правилах NAT читайте в разделе NAT и маршрутизация. Для примера в веб-консоли администратора создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из зоны для VPN-подключений в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в разделе руководства Межсетевой экран.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило отключено по умолчанию.

Настройка VPN-клиента

После настройки VPN-сервера необходимо настроить VPN-клиенты. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client (версии для [Windows](#), [Linux](#) и [macOS](#)), также поддерживаются нативные клиенты большинства популярных операционных систем.

Настройка параметров клиентского ПО зависит от типа устанавливаемого соединения.

L2TP/IPsec VPN

При создании VPN с помощью L2TP/IPsec(IKEv1), протокол L2TP создает туннель, в котором передаются пакеты сетевого уровня в кадрах PPP. IPsec обеспечивает шифрование, аутентификацию и проверку целостности передаваемых данных.

Взаимная аутентификация узлов осуществляется посредством **общего ключа** (Pre-shared key). Аутентификация пользователей VPN производится с помощью логина и пароля.

В настройках клиентского ПО необходимо указать следующие параметры:

- Тип VPN (L2TP/IPsec);
- Имя или IP-адрес VPN-сервера;
- Значение общего ключа (pre-shared key);
- Метод аутентификации пользователя (PAP);
- Параметры первой и второй фаз согласования защищенного соединения;
- Параметры аутентификации пользователя (логин и пароль).

Операционные системы Windows версий 10 и выше, по умолчанию, не поддерживают L2TP-подключения к серверам, которые находятся за вышестоящими маршрутизаторами с функционалом NAT. Для возможности установки соединения необходимо внести следующие правки в реестр ОС Windows:

- в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent** создать параметр **DWORD (32 бита)** с названием **AssumeUDPEncapsulationContextOnSendRule** и значением **2**;

в разделе

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters** изменить значение параметра **AllowL2TPWeakCrypto** на 1.

Важно!

После внесения изменений в реестр их необходимо применить, например, перезагрузив компьютер.

Для получения более подробной информации обратитесь к статье Microsoft (<https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/configure-l2tp-ipsec-server-behind-nat-t-device>).

Подробнее читайте в статье [Пример настройки Remote access VPN с L2TP/IPsec\(IKEv1\)](#).

IPsec (IKEv2) VPN с аутентификацией посредством сертификатов, использующих инфраструктуру открытых ключей (PKI)

При создании VPN с помощью IPsec(IKEv2) защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии 2 (IKEv2). В процессе создания туннеля происходит взаимная аутентификация узлов с проверкой подлинности сертификатов.

Проверка сертификатов происходит следующим образом:

- По зашифрованному каналу VPN-клиент присылает свой сертификат и зашифрованные данные, подписанные закрытым ключом.
- VPN-сервер расшифровывает данные открытым ключом клиента и сравнивает со своим контрольным набором, тем самым проверяется наличие закрытого ключа у клиента.
- VPN-сервер проверяет сертификат клиента на соответствие указанной цепочки сертификатов, тем самым проверяется, что сертификат выписан от имени уполномоченного удостоверяющего центра.
- VPN-сервер может проверить сертификат на отозванность.
- VPN-сервер извлекает имя пользователя из сертификата и ищет пользователя с использованием метода, указанного в настроенном профиле аутентификации.

- Если не пройдет любой из указанных пунктов проверки, соединение не установится.
- Если все проверки пройдены, VPN-сервер со своей стороны отправляет свой сертификат и зашифрованные данные, подписанные своим закрытым ключом.
- VPN-клиент проверяет правильность подписи сервера и соответствие имени сервера из сертификата тому адресу, на который он подключился.

При настройке клиентского ПО необходимо выполнить следующие операции:

- Импортировать заранее созданный клиентский сертификат и сертификат корневого центра на рабочую станцию;
- Указать тип VPN (IKEv2);
- Указать адрес VPN-сервера;
- Указать метод аутентификации;
- Выполнить настройки параметров виртуального адаптера.

Подробнее читайте в статье [Пример настройки Remote access VPN с IPsec \(IKEv2\)](#).

IPsec (IKEv2) VPN с аутентификацией с помощью методов EAP, PEAP (AAA)

При создании VPN с помощью IPsec (IKEv2) защищенный VPN-туннель создается только протоколами группы IPsec с протоколом IKE версии 2 (IKEv2).

В режиме аутентификации с помощью методов EAP, PEAP (AAA) во время фазы обмена IKE_AUTH VPN-сервер отвечает клиенту, что требуется авторизация через EAP. Клиент обменивается с VPN-сервером несколькими EAP-пакетами. VPN-сервер транслирует пакеты на внешний доменный RADIUS-сервер, который принимает решение об авторизации. После получения разрешения от RADIUS-сервера, VPN-сервер по полученному логину запрашивает у сервера домена информацию о пользователе и принадлежности его к тем или иным группам, после чего принимает решение о подключении пользователя к VPN. Также в процессе установления соединения VPN-клиент производит проверку подлинности сертификата VPN-сервера.

При настройке клиентского ПО необходимо выполнить следующие операции:

- Импортировать сертификат корневого центра на рабочую станцию;

- Указать тип VPN (IKEv2);
- Указать адрес VPN-сервера;
- Указать метод аутентификации;
- Указать параметры аутентификации пользователя (сертификат / логин и пароль);
- Выполнить настройки параметров виртуального адаптера.

Подробнее читайте в статьях:

[Пример настройки Remote access VPN с IPsec \(IKEv2\) с аутентификацией через EAP для OS Linux.](#)

[Пример настройки Remote access VPN с IPsec \(IKEv2\) с аутентификацией EAP, PEAP для OS Windows.](#)

Настройка раздельного туннелирования для UserGate Client

Раздельное туннелирование (split tunneling) — это технология, позволяющая пользователю одновременно подключаться к одним сетевым ресурсам через защищенное VPN-соединение, а к другим — в обход него, не отключая VPN.

Функциональность раздельного туннелирования, реализованная в UserGate, позволяет модифицировать таблицу маршрутизации компьютера пользователя с ПО UserGate Client при установлении VPN-соединения в соответствии с настройками администратора VPN-сервера (NGFW). После завершения VPN-сессии локальные настройки маршрутизации на компьютере пользователя возвращаются в исходные.

При установлении VPN-соединения в таблицу маршрутов клиента добавляются два новых маршрута. Они необходимы для сохранения подключения к VPN-серверу во всех сценариях:

- Маршрут к шлюзу локальной сети. Добавляется через IP-адрес локального интерфейса в качестве шлюза.

Маршрут к VPN-серверу.

- Добавляется через IP-адрес локального интерфейса в качестве шлюза, если адрес VPN-сервера находится в адресном пространстве локальной сети.
- Добавляется через IP-адрес шлюза локальной сети в качестве шлюза в случае если адрес VPN-сервера не находится в адресном пространстве локальной сети.

Локальные маршруты в обход VPN, изначально прописанные на компьютере пользователя, удаляются на время работы VPN. После отключения VPN-соединения эти маршруты возвращаются.

В веб-консоли администратора NGFW можно настроить различные сценарии работы функциональности раздельного туннелирования. Для этого необходимо перейти в раздел **VPN → Сети VPN**. В свойствах VPN-сети для удаленного доступа выбрать вкладку **Маршруты для UserGate Client**.

Свойства VPN-сети

Общие Сеть Маршруты VPN **Маршруты для UserGate Client**

☐ Все маршруты

Включить маршруты

+ Добавить Редактировать Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

Исключить маршруты

+ Добавить Редактировать Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

☐ Ограничить доступ к локальной сети

Сохранить Отмена

Рассмотрим подробнее возможные сценарии настроек раздельного туннелирования.

а) Если поставлен флажок **Все маршруты**, в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию (default route) вида *0.0.0.0/0 → VPN-шлюз*. Имеющийся ранее маршрут по умолчанию будет удален из таблицы.

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

☒ Все маршруты

Включить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

Исключить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

☐ Ограничить доступ к локальной сети

Сохранить Отмена

б) Если в поле **Включить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида $n.n.n.n/c \rightarrow \text{VPN-шлюз}$ с гарантированно минимальной метрикой 2.

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
IP-list1	Вы
IP-list2	Вы
Создать и добавить новый объект	

Исключить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

☐ Ограничить доступ к локальной сети

Сохранить Отмена

с) Если в поле **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то в таблицу маршрутизации клиента будет добавлен маршрут по

умолчанию вида $0.0.0.0/0 \rightarrow \text{VPN-шлюз}$. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

Свойства VPN-сети

Общие

Сеть

Маршруты VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+

Добавить

Редактировать

×

Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

Исключить маршруты

+

Добавить

Редактировать

×

Удалить

Название списка ↑	Владелец
IP-list3	Вы
IP-list4	Вы
Создать и добавить новый объект	

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

d) Если в обоих полях **Включить маршруты** и **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида $n.n.n.n/c \rightarrow \text{VPN-шлюз}$ с гарантированно минимальной метрикой 2. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

Свойства VPN-сети

Общие

Сеть

Маршруты VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+

Добавить

✎

Редактировать

✖

Удалить

	Название списка ↑	Владелец
✓	IP-list1	Вы
✓	IP-list2	Вы

Создать и добавить новый объект

Исключить маршруты

+

Добавить

✎

Редактировать

✖

Удалить

	Название списка ↑	Владелец
✓	IP-list3	Вы
✓	IP-list4	Вы

Создать и добавить новый объект

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

е) Если во вкладке нет никаких настроек, то в таблицу маршрутизации клиента добавляется VPN-маршрут вида $0.0.0.0/0 \rightarrow \text{VPN-шлюз}$ с метрикой больше, чем у имеющегося маршрута по умолчанию. Имеющийся маршрут по умолчанию при этом не удаляются и маршруты для MC/NGFW/VPN-сервера не создаются.

Свойства VPN-сети

Общие

Сеть

Маршруты VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+

Добавить

✎

Редактировать

✖

Удалить

	Название списка ↑	Владелец
--	-------------------	----------

Создать и добавить новый объект

Исключить маршруты

+

Добавить

✎

Редактировать

✖

Удалить

	Название списка ↑	Владелец
--	-------------------	----------

Создать и добавить новый объект

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

f) Если поставлен флажок **Ограничить доступ к локальной сети**, то для каждой подсети локального интерфейса создается копия маршрута через *VPN-шлюз* с гарантированно минимальной метрикой 2. Такие же копии маршрутов создаются для всех адресов, которые имеют тип *local interface*.

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

Исключить маршруты

+ Добавить ✎ Редактировать ✕ Удалить

Название списка ↑	Владелец
Создать и добавить новый объект	

☒ Ограничить доступ к локальной сети

Сохранить Отмена

В зависимости от сценариев настроек метрики для VPN-маршрутов broadcast- и multicast-адресов получают следующие значения:

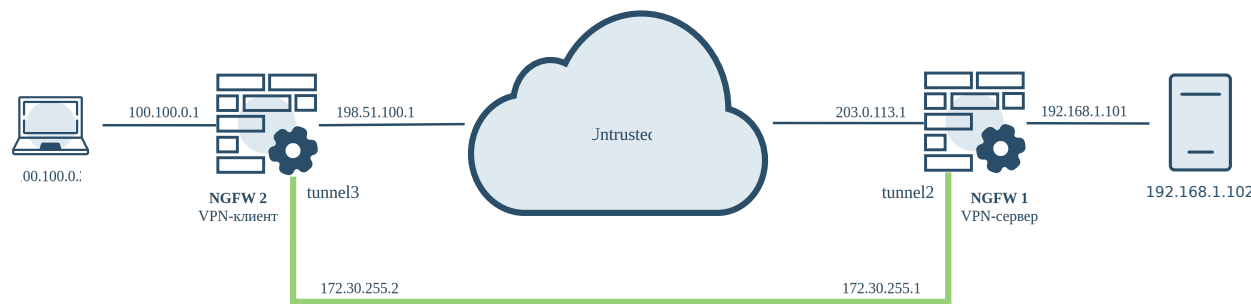
- Лучшая метрика среди соответствующих адресов — для сценариев [a\)](#) и [c\)](#);
- Гарантированно худшая метрика 10000 — для сценариев [b\)](#) и [d\)](#).

В зависимости от режима работы компьютер с установленным ПО UserGate Client осуществляет коммуникацию либо с UserGate MC, либо с NGFW. С этой целью создается отдельный маршрут для соответствующего IP-адреса в обход VPN. Данный маршрут не создается для сценария [e\)](#) и в случае, когда VPN-клиент и MC/NGFW находятся в одной сети.

ПРИМЕРЫ НАСТРОЙКИ VPN

Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1)

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:



Настройка VPN-сервера

Для настройки узла **NGFW 1** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Зоны				
+ Добавить Редактировать Копировать Удалить				
Зона	Защита от DoS включена для	Исключения ...	Защита от спуфинга	Контроль доступа
Cluster	Ничего		Отключено	Ping, Кластер, Консоль администрирования
DMZ	SYN, UDP, ICMP		Отключено	Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management	SYN, UDP, ICMP		Отключено	Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
Trusted	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-пр
Tunnel inspection zone	Ничего		Отключено	Всё отключено
Untrusted	SYN, UDP, ICMP		Отключено	Ping, SMTP(S)-прокси, POP3(S)-прокси, VPN
VPN for remote access	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств
VPN for Site-to-Site	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств

Шаг 3. Настроить параметры аутентификации.

1. Создадим локальную учетную запись, которая будет использоваться для аутентификации узла, выступающего в роли VPN-клиента при установлении

L2TP туннеля. В веб-консоли NGFW 1 в разделе **Пользователи и устройства** → **Пользователи** создадим локальную учетную запись *vpn client 1* (логин: *vpnc1nt1*) для удаленного узла VPN-клиента NGFW 2. Для удобства использования все созданные подобные учетные записи могут быть помещены в имеющуюся группу **VPN servers**, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп смотрите в статье [Пользователи и группы](#).

2. Создадим профиль аутентификации для VPN пользователей. Для примера в разделе **Пользователи и устройства** → **Профили аутентификации** создадим профиль *local*, во вкладке метода аутентификации выберем **Локальный пользователь**. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#).

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Site-to-Site VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для примера создания защищенного VPN-соединения в этой статье:

Свойства серверного профиля безопасности

Общие
Фаза 1
Фаза 2

Название:

Site-to-Site VPN profile

Описание:

Example VPN security profile for Site-to-Site VPN. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

1
IKE версия:

IKEv1

2
Режим IKE:

Основной

3
Тип идентификации:

отсутствует

Значение идентификации:

4
Общий ключ:

.....

Общий ключ (повтор):

.....

Сертификат сервера:

Сертификат не выбран

Режим аутентификации:

Любой

Профиль клиентского сертификата:

Не использовать профиль клиентского сертификата

Сохранить
Отмена

- Версия** протокола **IKE** (Internet Key Exchange). В рассматриваемом примере для создания защищенного канала будет использоваться протокол IKEv1.
- Режим** работы **IKE**. В рассматриваемом примере используется Основной режим работы IKEv1.
- Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.
- Зададим значение общего ключа (Pre-shared key) для аутентификации удаленного узла. Ключ должен совпадать на VPN-сервере и VPN-клиенте для успешного подключения.

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

+

Добавить

✕

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+

Добавить

Редактировать

✕

Удалить

Выше

Низже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

(в секундах)

Безопасность

+ Добавить

✎ Редактировать

✖ Удалить

⬆ Выше

⬆ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера.

Настройка VPN-адаптера

Общие Сеть

1 Включено: ☒

2 Название: tunnel2

Описание: Example VPN interface to be used in Site-to-Site VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for Site-to-Site

Профиль netflow: Не выбран

Алиас/Псевдоним:

Сохранить Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel2).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW 1, будут также помещены в эту зону. В этом примере указывается зона VPN for Site-to-Site.

Настройка VPN-адаптера

Общие Сеть

4 Режим: Статический

5 MTU: 1420

IP интерфейса

+ Добавить ✎ Редактировать ✕ Удалить

IP интерфейса	Маска
172.30.255.1	255.255.255.0

Сохранить Отмена

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес.

5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel2 172.30.255.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

Для примера на узле создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

1 Диапазон IP: 172.30.255.2-172.30.255.2

1 Маска: 255.255.255.0

3 ☒ Использовать системные DNS-серверы

Серверы DNS:

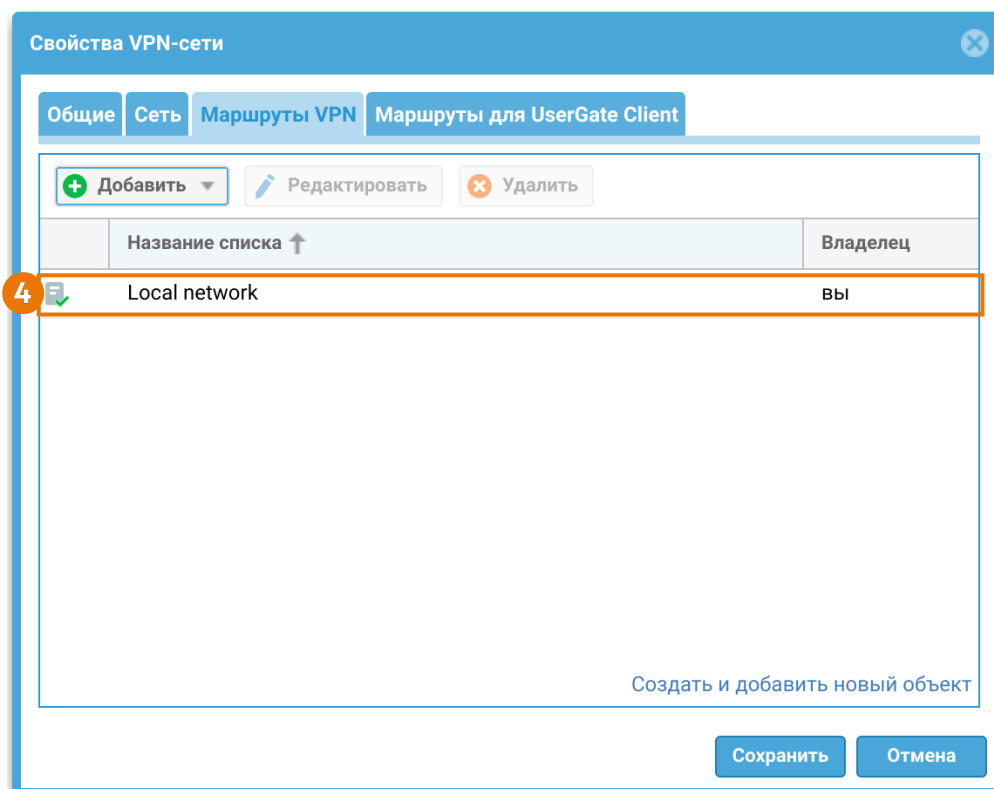
IP-адрес	Действия
	Добавить Редактировать Удалить

Сохранить Отмена

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.255.1), используемому совместно с данной сетью. Соединение будет устанавливаться с одним NGFW, выполняющим роль VPN-клиента, в таком случае диапазон IP-адресов в данном поле будет следующим:
172.30.255.2-172.30.255.2.

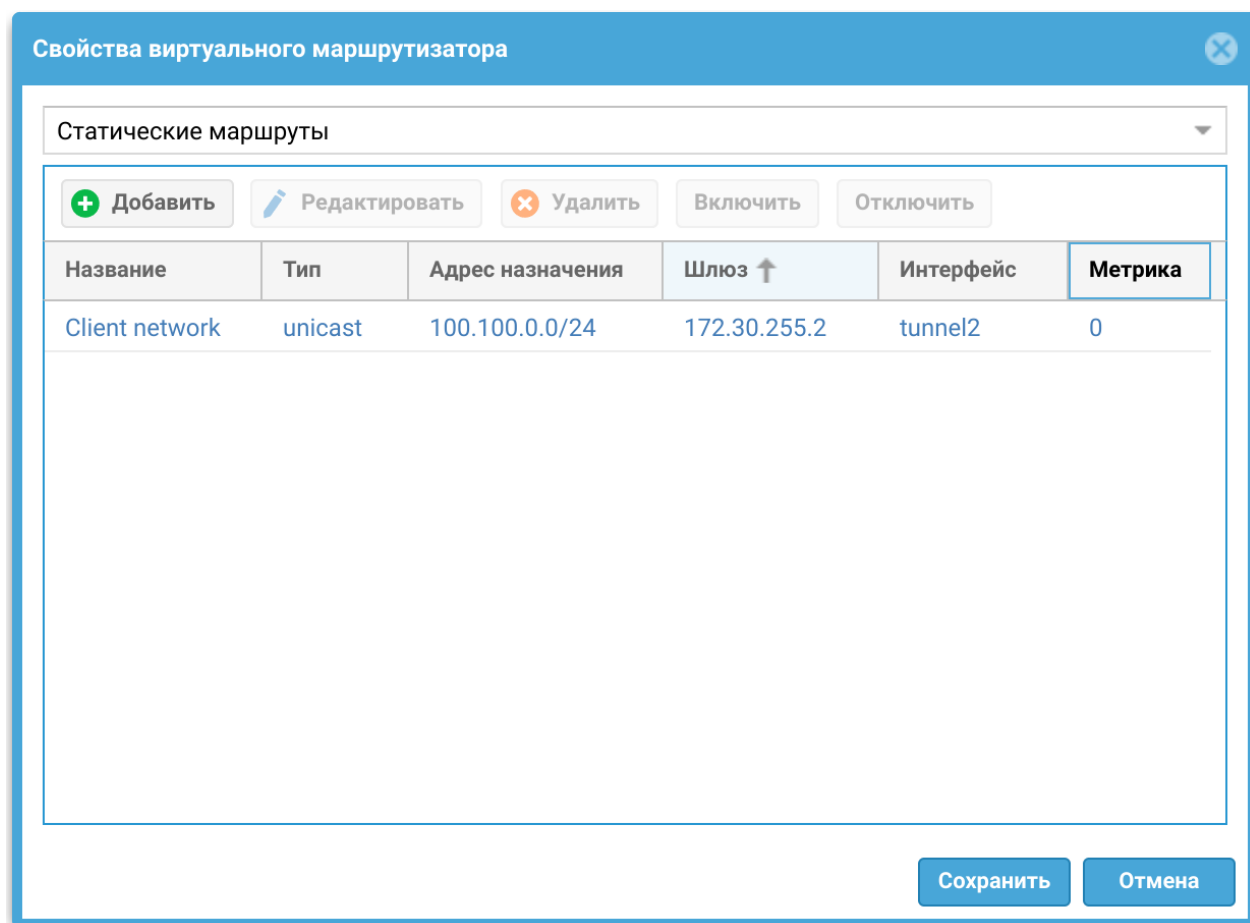
2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

Чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте:



В разделе **Журналы и отчеты** → **Мониторинг** → **Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:

Маршруты

Узел: Виртуальный маршрутизатор:

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

K>* 100.100.0.0/24 [0/0] via 172.30.255.2, tunnel2, 03:43:49

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

C>* 203.0.113.0/24 is directly connected, port2, 03:44:17
C>* 172.30.255.0/24 is directly connected, tunnel2, 03:44:17
C>* 192.168.1.0/24 is directly connected, port1, 03:44:17
C>* 192.168.56.0/24 is directly connected, port0, 03:44:17

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группы **VPN servers**. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения:

Свойства

Общие

Источник

Пользователи

Назначение

1 Включено: ☒

Название: Site-to-Site VPN rule

Описание:

Example VPN server rule which allows access for Site-to-Site VPN clients connections from Untrusted zone and places them to VPN for Site-to-Site zone (zone assigned to VPN interface). This rule can be changed or deleted if necessary.

2 Профиль безопасности VPN: Site-to-Site VPN profile

3 Сеть VPN: Site-to-Site VPN network

4 Профиль аутентификации: local

URL инициализации TOTP

5 Интерфейс: tunnel2

Сохранить

Отмена

- 1. Включено** — включить правило VPN.
- 2. Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (Site-to-Site VPN profile).
- 3. Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Site-to-Site VPN network).
- 4. Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
- 5. Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel2).

Свойства

Общие **Источник** Пользователи Назначение

Зона источника

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☐ Trusted
- ☐ Tunnel inspection zone
- 6** ☒ **Untrusted**
- ☐ VPN for remote access
- ☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Адрес источника

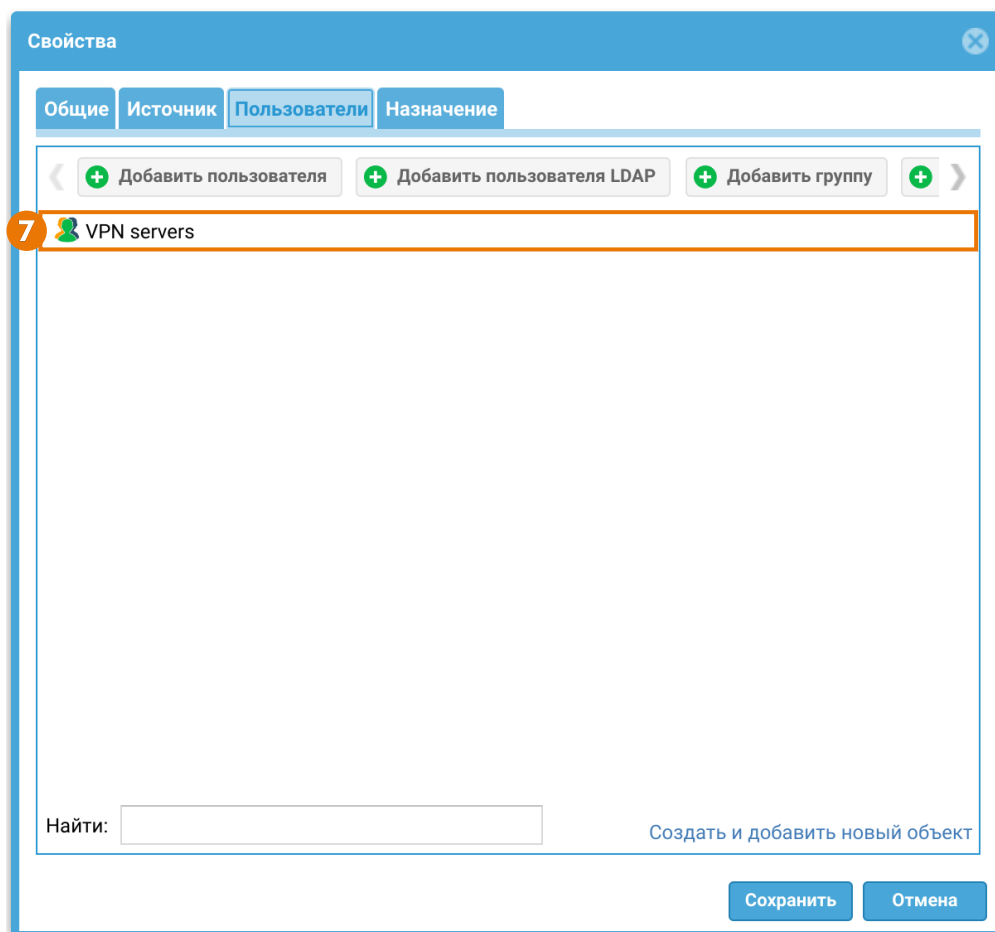
< + Добавить Редактировать >

Название списка ↑	Владелец
-------------------	----------

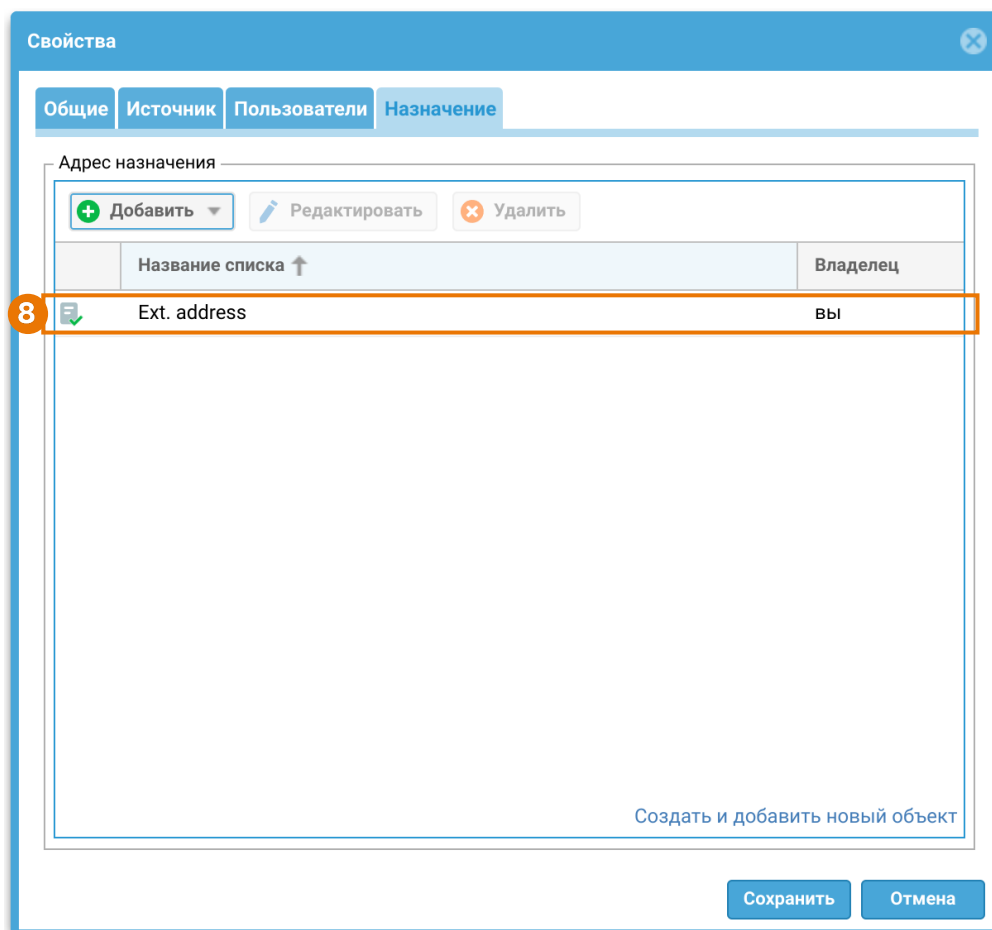
Создать и добавить новый объект

Сохранить Отмена

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. **Пользователи** — в данном примере группа **VPN servers** включает в себя созданную на [Share 3](#) учетную запись *vpn client 1*.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1.

Шаг 8. Контроль доступа к ресурсам.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной на Шаге 3 зоны в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в статье [Межсетевой экран](#).

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить.

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Межсетевой экран									
+ Добавить ✎ Редактировать ✖ Удалить ↔ Переместить 📋 Копировать 🔌 Включить 🔌 Отключить 📄 Скопировать ID правила 🔍 Открыть логи 🔄 Сбросить счётчики Все ▾ Принудительно применить									
✓									
#	Статус журн...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
1		Allow trusted to untrusted	✓ Разрешить	Trusted	Любой	Untrusted	Любой	Любой	Любой
2		VPN for Site-to-Site to Trusted and Untrusted	✓ Разрешить	VPN for Site-to-Site	Любой	Untrusted Trusted	Любой	Любой	Любой
3		Trusted and Untrusted to VPN for Site-to-Site	✓ Разрешить	Untrusted Trusted	Любой	VPN for Site-to-Site	Любой	Любой	Любой
4	[...]	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой

Настройка VPN-клиента

Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера создания защищенного VPN-соединения:

Настройка VPN-адаптера

Общие

Сеть

1 Включено: ☒

2 Название: tunnel3

Описание:

Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for Site-to-Site

Профиль netflow: Не выбран

Алиас/Псевдоним:

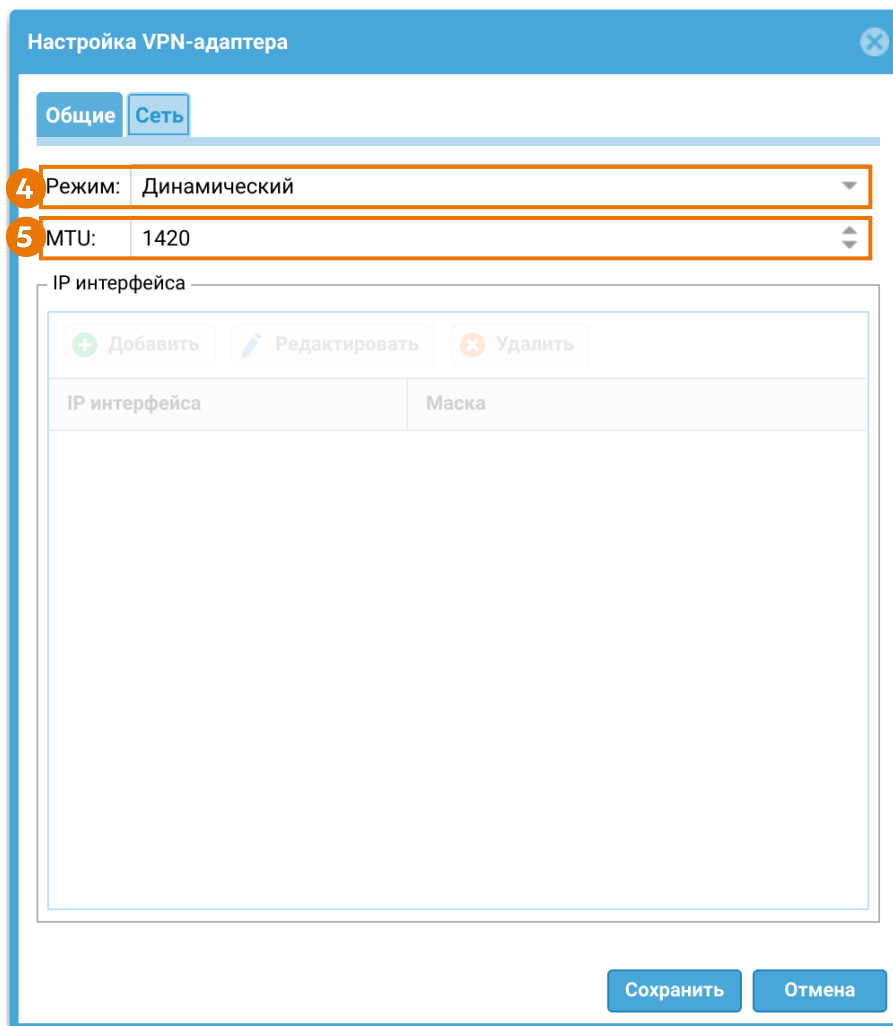
Сохранить

Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel3).

3. **Зона**, к которой будет относиться данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на [Share 1](#).



4. **Режим.** Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, созданной на [Шаге 6](#) настроек VPN-сервера.

5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

Шаг 3. Контроль доступа к ресурсам.

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site, Trusted** и **Untrusted**.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, создадим разрешающее правило межсетевого экрана, указав нужную зону источника (**Trusted** и **Untrusted**) и зону назначения **VPN for Site-to-Site**.

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для рассматриваемого примера создания защищенного VPN-соединения:

The screenshot shows a configuration window titled "Свойства клиентского профиля безопасности" (Properties of client security profile). It has three tabs: "Общие" (General), "Фаза 1" (Phase 1), and "Фаза 2" (Phase 2). The "Общие" tab is active. The settings are as follows:

- 1. Название (Name):** Client VPN profile
- Описание (Description):** Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.
- 2. Протокол (Protocol):** IPsec L2TP
- 3. Режим IKE:** Основной
- 4. Тип идентификации (Authentication type):** отсутствует
- Значение идентификации (Authentication value):** (empty field)
- Общий ключ (Pre-shared key):** (masked with dots)
- Общий ключ (повтор) (Pre-shared key (repeat)):** (masked with dots)
- Сертификат клиента (Client certificate):** Сертификат не выбран
- Подсети для VPN (VPN subnets):**
 - Локальная подсеть (Local subnet): (empty field)
 - Удалённая подсеть (Remote subnet): (empty field)
- 5. Аутентификация (Authentication):**
 - Логин (Login): vpncint1
 - Пароль (Password): (masked with dots)

At the bottom right, there are two buttons: "Сохранить" (Save) and "Отмена" (Cancel).

1. **Протокол.** В рассматриваемом примере для создания защищенного канала будет использоваться **IPsec L2TP**.

2. **Режим работы IKE.** В рассматриваемом примере используется **Основной** режим работы IKEv1.

3. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

4. Зададим значение общего ключа (Pre-shared key) для аутентификации удаленного узла. Ключ должен совпадать с ключом, заданным на VPN-сервере на [Шаге 4](#).

5. **Аутентификация** — логин и пароль учетной записи, созданной на [Шаге 3](#) при настройке VPN-сервера для аутентификации узла, выступающего в роли VPN-клиента при установлении L2TP туннеля (vpncInt1).

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Выше

Низже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

(в секундах)

Безопасность

Добавить

Редактировать

Удалить

Выше

Низже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создать клиентское правило VPN.

Для примера на узле создано клиентское правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения:

Свойства

Общие

1 Включено: ☒

Название: Client VPN rule

Описание:

Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.

2 Профиль безопасности VPN: Client VPN profile

3 Интерфейс: tunnel3

4 Адрес сервера: ug.testd.local

Сохранить

Отмена

1. **Включено** — включить правило.

2. **Профиль безопасности VPN** — созданный на [Share 4](#) клиентский профиль безопасности VPN.

3. **Интерфейс** — созданный на [Share 2](#) VPN-интерфейс.

4. **Адрес сервера**. В рассматриваемом примере это доменный адрес NGFW 1, выполняющего роль VPN-сервера (ug.testd.local).

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узле NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля:

Клиентские правила

+

Добавить

Редактировать

✕

Удалить

Включить

Отключить

↺↻

✓

Название	Адрес сервера	Интерфейс	Профиль безопасности V...	Последняя ошибка VPN	Состояние
Client VPN rule	192.168.1.101	tunnel3	Client VPN profile		●

На узлах NGFW 1 и NGFW 2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

На NGFW 1:

VPN

ug

Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	GeO IP	Шифрование
vpn client1	Сервер	Site-to-Site VPN rule (L2TP/IPSec)	20 февраля 2024 г., 16:42 (19м 5с)	172.30.255.2	198.51.100.1		aes

На NGFW 2:

VPN

ug2

Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	GeO IP	Шифрование
vpncnt1	Клиент	—	20 февраля 2024 г., 16:42 (2м...	172.30.255.2	203.0.113.1		aes256

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW 2 добавится маршрут в сеть удаленного офиса 192.168.1.0/24 через туннельный интерфейс tunnel3:

Маршруты

Узел: Виртуальный маршрутизатор:

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,

O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,

> - selected route, * - FIB route, q - queued, r - rejected, b - backup

t - trapped, o - offload failure

VRF default:

K>* 192.168.1.0/24 [0/0] via 172.30.255.1, tunnel3, src 172.30.255.2, 00:08:47

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,

O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,

> - selected route, * - FIB route, q - queued, r - rejected, b - backup

t - trapped, o - offload failure

VRF default:

C>* 198.51.100.0/24 is directly connected, port2, 03:18:01

C>* 100.100.0.0/24 is directly connected, port1, 03:18:01

C>* 172.30.255.0/24 is directly connected, tunnel3, 00:08:52

C>* 192.168.56.0/24 is directly connected, port0, 03:18:01

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW 1:

Ping

Настройка ping

Ping host TTL Интерфейс

Счётчик ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

PING 172.30.255.2 (172.30.255.2) from 172.30.255.1 : 56(84) bytes of data.

64 bytes from 172.30.255.2: icmp_req=1 ttl=64 time=1.03 ms

64 bytes from 172.30.255.2: icmp_req=2 ttl=64 time=3.33 ms

64 bytes from 172.30.255.2: icmp_req=3 ttl=64 time=2.01 ms

64 bytes from 172.30.255.2: icmp_req=4 ttl=64 time=2.07 ms

64 bytes from 172.30.255.2: icmp_req=5 ttl=64 time=3.76 ms

64 bytes from 172.30.255.2: icmp_req=6 ttl=64 time=2.19 ms

--- 172.30.255.2 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5006ms

rtt min/avg/max/mdev = 1.036/2.402/3.760/0.903 ms

Со стороны NGFW 2:

Ping

Настройка ping

Ping host TTL Интерфейс

Счётчик ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

```
PING 172.30.255.1 (172.30.255.1) from 172.30.255.2 : 56(84) bytes of data.
64 bytes from 172.30.255.1: icmp_req=1 ttl=64 time=0.984 ms
64 bytes from 172.30.255.1: icmp_req=2 ttl=64 time=1.07 ms
64 bytes from 172.30.255.1: icmp_req=3 ttl=64 time=0.497 ms
64 bytes from 172.30.255.1: icmp_req=4 ttl=64 time=2.92 ms
64 bytes from 172.30.255.1: icmp_req=5 ttl=64 time=1.00 ms
64 bytes from 172.30.255.1: icmp_req=6 ttl=64 time=4.41 ms

--- 172.30.255.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 0.497/1.817/4.416/1.391 ms
```

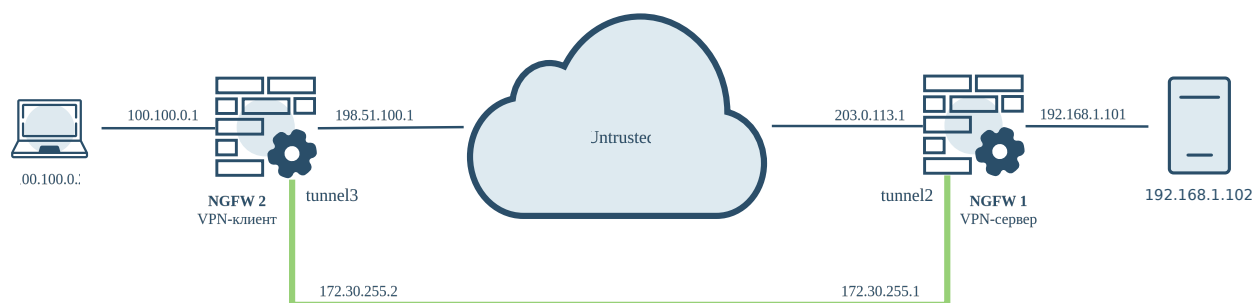
Хосты в сетях обоих офисов доступны друг для друга:

```
~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:60:bc:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
~$ ping 100.100.0.2
PING 100.100.0.2 (100.100.0.2) 56(84) bytes of data.
64 bytes from 100.100.0.2: icmp_seq=1 ttl=62 time=3.89 ms
64 bytes from 100.100.0.2: icmp_seq=2 ttl=62 time=4.39 ms
64 bytes from 100.100.0.2: icmp_seq=3 ttl=62 time=4.21 ms
64 bytes from 100.100.0.2: icmp_seq=4 ttl=62 time=1.72 ms
64 bytes from 100.100.0.2: icmp_seq=5 ttl=62 time=2.74 ms
^C
--- 100.100.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4020ms
rtt min/avg/max/mdev = 1.721/3.388/4.390/1.012 ms
```

```
~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:04:97:9a brd ff:ff:ff:ff:ff:ff
    inet 100.100.0.2/24 brd 100.100.0.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
~$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=62 time=5.97 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=62 time=4.27 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=62 time=8.62 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=62 time=7.34 ms
64 bytes from 192.168.1.102: icmp_seq=5 ttl=62 time=2.01 ms
64 bytes from 192.168.1.102: icmp_seq=6 ttl=62 time=1.97 ms
^C
--- 192.168.1.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.969/5.030/8.621/2.522 ms
```

Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1) с помощью интерфейса CLI

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:



Настройка VPN-сервера

Для настройки узла NGFW 1 в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Контроль доступа зоны.

Разрешим сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Для редактирования параметров зоны используется следующая команда:

```
Admin@ug# set network zone <parameters>
```

Подробнее о командах и параметрах для создания/редактирования зон в CLI смотрите в статье [Зоны](#).

Пример редактирования зоны **Untrusted** с целью разрешить сервис VPN в этой зоне:

```
Admin@ug# set network zone Untrusted enabled-services [ VPN ]
```

Шаг 2. Создание зоны для VPN подключений.

Для создания зон используется следующая команда:

```
Admin@ug# create network zone <parameters>
```

Подробнее о командах и параметрах для создания/редактирования зон в CLI смотрите в статье [Зоны](#).

На узле уже создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@ug# show network zone
+ <Enter>                               Finish input
+ (                                       Start complex filter
+ Cluster
+ DMZ
+ Management
+ Trusted
+ "Tunnel inspection zone"
+ Untrusted
+ "VPN for remote access"
+ "VPN for Site-to-Site"

Admin@ug# show network zone "VPN for Site-to-Site"

name                               : VPN for Site-to-Site
antispoof-enable                   : off
antispoof-negate                   : off
dos-protection-syn                 :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 3000
    drop-threshold                 : 6000
dos-protection-udp                 :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 3000
    drop-threshold                 : 6000
dos-protection-icmp                :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 100
```

```

drop-threshold      : 200
services-access      :
  service            : Any ICMP
  allowed-addresses  : Any
  enabled            : on

  service            : reponse_pages
  allowed-addresses  : Any
  enabled            : on

  service            : DNS
  allowed-addresses  : Any
  enabled            : on

  service            : HTTP Proxy
  allowed-addresses  : Any
  enabled            : on

  service            : Endpoint connect
  allowed-addresses  : Any
  enabled            : on

sessions-limit-enabled : off
sessions-limit-threshold : 0

```

Шаг 3. Настройка параметров аутентификации.

1. Создадим локальную учетную запись для аутентификации сервера, выступающего в роли VPN-клиента.

Для этого используется следующая команда:

```
Admin@ug# create users user <parameters>
```

Подробнее о командах и параметрах для создания локальных пользователей в CLI смотрите в статье [Настройки пользователей](#).

Пример создания учетной записи vpn client 1 с логином **vpncInt1**, входящего в группу **VPN servers**:


```
Admin@ug# create users user name "vpn client 1" login vpnc1nt1 groups
[ "VPN servers" ] enabled on
```

2. Создадим профиль аутентификации для VPN пользователей.

Для этого используется следующая команда:

```
Admin@ug# create users auth-profile <parameter>
```

Подробнее о порядке создания профилей аутентификации для пользователей в CLI смотрите в статье [Настройка профилей аутентификации](#).

Пример создания профиля аутентификации local с аутентификацией по базе данных локально заведенных пользователей:

```
Admin@ug# create users auth-profile name local auth-methods local-user-
auth on
```

Шаг 4. Создание профиля безопасности VPN-сервера.

Для создания профиля безопасности VPN-сервера используется следующая команда:

```
Admin@ug# create vpn server-security-profiles <parameters>
```

Подробнее о порядке создания профилей безопасности VPN в CLI смотрите в статье [Настройка профилей безопасности VPN](#).

Изначально для примера на узле уже создан профиль безопасности **Site-to-Site VPN profile**, задающий необходимые настройки:

```
Admin@ug# show vpn server-security-profiles

Site-to-Site VPN profile
  name           : Site-to-Site VPN profile
  description    : Example VPN security profile for Site-to-
Site VPN. Preshared key is "examplepresharedkey" - it must be changed!
This profile can be changed or deleted if necessary.
```

```

ike-version          : 1
ike-mode             : main
local-id-type        : none
certificate           : no certificate
authentication-mode   : any
dh-groups             : Group 2 Prime 1024 bit; Group 14 Prime
2048 bit
dpd-state            : off
dpd-interval          : 60
dpd-max-failures      : 5
phase1-security      :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

phase1-key-lifetime   : 1 d
phase2-key-lifetime   : 12 h
key-lifetime-enabled  : off
key-lifetime          : 4 GB
phase2-security       :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

nat-keepalive         : 0
Admin@ug# set vpn server-security-profiles "Site-to-Site VPN profile"
ike-version 1 psk 123456

```

Шаг 5. Создание VPN-интерфейса.

Для создания VPN-интерфейса используется следующая команда:

```
Admin@ug# create network interface vpn <parameters>
```

Подробнее о порядке создания VPN-интерфейса в CLI смотрите в статье [Интерфейсы](#).

Для примера на узле уже создан VPN-интерфейс **tunnel2**, который может быть использован для настройки Site-to-Site VPN:

```
Admin@ug# show network interface vpn tunnel2

type           : vpn
node_name      : cluster
name           : tunnel2
description     : Example VPN interface to be used in Site-to-Site
                  VPN server rule. This is an example VPN interface which
                  can be changed or deleted if necessary.
enabled        : on
netflow-profile : Undefined
iface-mode     : manual
mtu            : 1420
speed          : 0
zone           : VPN for Site-to-Site
running        : off
master         : off

Admin@ug# set network interface vpn tunnel2 ip-addresses
[ 172.30.255.1/24 ]

Admin@ug# show network interface vpn tunnel2

type           : vpn
node_name      : cluster
name           : tunnel2
description     : Example VPN interface to be used in Site-to-Site
                  VPN server rule. This is an example VPN interface which
                  can be changed or deleted if necessary.
enabled        : on
netflow-profile : Undefined
iface-mode     : static
mtu            : 1420
speed          : 0
zone           : VPN for Site-to-Site
running        : off
```

```

master          : off
ip-addresses    : 172.30.255.1/24

```

Шаг 6. Создание сети VPN.

Для создания сети VPN используется следующая команда:

```
Admin@ug# create vpn networks <parameters>
```

Подробнее о порядке создания сети VPN в CLI смотрите в статье [Настройка сетей VPN](#).

Для примера на узле уже создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Скорректируем в ней диапазон IP-адресов для установления VPN с NGFW 2:

```

Admin@ug# show vpn networks

Site-to-Site VPN network
  name          : Site-to-Site VPN network
  description    : Example VPN network for Site-to-Site VPN.
  It can be changed or deleted if necessary.
  mask          : 255.255.255.0
  use-system-dns : on
  ip-range      : 172.30.255.2-172.30.255.254
  all-routes    : off
  restrict-lan-access : off
Admin@ug# set vpn networks "Site-to-Site VPN network" ip-range
172.30.255.2-172.30.255.2
Admin@ug# show vpn networks

Site-to-Site VPN network
  name          : Site-to-Site VPN network
  description    : Example VPN network for Site-to-Site VPN.
  It can be changed or deleted if necessary.
  mask          : 255.255.255.0
  use-system-dns : on
  ip-range      : 172.30.255.2-172.30.255.2

```

```
all-routes      : off
restrict-lan-access : off
```

В качестве маршрута, передаваемого VPN-клиенту, добавим в настройки этой сети заранее созданный список Local network, включающий в себя подсеть 192.168.1.0/24:

```
Admin@ug# set vpn networks "Site-to-Site VPN network routes-ip-list
[ "Local network" ]
Admin@ug# show vpn networks

Site-to-Site VPN network
  name           : Site-to-Site VPN network
  description     : Example VPN network for Site-to-Site VPN.
  It can be changed or deleted if necessary.
  mask           : 255.255.255.0
  use-system-dns  : on
  routes-ip-list  : Local network
  ip-range       : 172.30.255.2-172.30.255.2
  all-routes      : off
  restrict-lan-access : off
```

Шаг 7. Создание серверного правила VPN.

Правила для VPN-сервера создаются с помощью синтаксиса UPL командой:

```
Admin@ug# create vpn server-rules <position> upl-rule <commands>
```

Подробнее о порядке настройки серверных правил VPN в CLI смотрите в статье [Настройка серверных правил](#).

Для примера на узле создано серверное правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группы **VPN servers**:

```
Admin@ug# show vpn server-rules

% ----- 1 -----
OK \
```

```

user = "CN=VPN servers,DC=LOCAL" \
src.zone = Untrusted \
profile("Site-to-Site VPN profile") \
auth_profile(local) \
vpn_network("Site-to-Site VPN network") \
interface(tunnel2) \
desc("Example VPN server rule which allows access for Site-to-Site
VPN clients connections from Untrusted zone and places them to VPN for
Site-to-Site zone (zone assigned to VPN interface). This rule can be
changed or deleted if necessary.") \
enabled(false) \
name("Site-to-Site VPN rule")

```

В качестве адреса назначения добавим в правило заранее созданный список Ext. address, в который входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1, и включим это правило:

```

Admin@ug# set vpn server-rules 1 upl-rule OK \
...dst.ip = lib.network("Ext. address") \
...enabled(true)
Admin@ug# show vpn server-rules

% ----- 1 -----
OK \
  user = "CN=VPN servers,DC=LOCAL" \
  src.zone = Untrusted \
  dst.ip = lib.network("Ext. address") \
  profile("Site-to-Site VPN profile") \
  auth_profile(local) \
  vpn_network("Site-to-Site VPN network") \
  interface(tunnel2) \
  desc("Example VPN server rule which allows access for Site-to-Site
VPN clients connections from Untrusted zone and places them to VPN for
Site-to-Site zone (zone assigned to VPN interface). This rule can be
changed or deleted if necessary.") \
  enabled(true) \
  name("Site-to-Site VPN rule")

```

Шаг 8. Контроль доступа к ресурсам.

Правила межсетевого экрана создаются с помощью синтаксиса UPL командой:

```
Admin@ug# create network-policy firewall <position> upl-rule <commands>
```

Подробнее о порядке настройки правил межсетевого экрана в CLI смотрите в статье [Настройка правил межсетевого экрана](#).

Изначально для примера на узле уже создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить:

```
Admin@ug# show network-policy firewall

% ----- 1 -----
PASS \
  src.zone = Trusted \
  dst.zone = Untrusted \
  desc("Firewall rule which allows traffic from Trusted zone to
Untrusted zone. This is an example rule which can be changed or deleted
if necessary.") \
  rule_log(session) \
  enabled(false) \
  name("Allow trusted to untrusted")
% ----- 2 -----
PASS \
  src.zone = "VPN for Site-to-Site" \
  dst.zone = (Untrusted, Trusted) \
  desc("Example firewall rule which allows traffic from VPN for Site-
to-Site zone to Trusted and Untrusted zones. This is an example rule
which can be changed or deleted if necessary.") \
  rule_log(session) \
  enabled(false) \
  name("VPN for Site-to-Site to Trusted and Untrusted")
Admin@ug# set network-policy firewall 2 upl-rule PASS \
...enabled(true)
Admin@ug# show network-policy firewall 2

% ----- 2 -----
PASS \
```

```
src.zone = "VPN for Site-to-Site" \
dst.zone = (Untrusted, Trusted) \
desc("Example firewall rule which allows traffic from VPN for Site-
to-Site zone to Trusted and Untrusted zones. This is an example rule
which can be changed or deleted if necessary.") \
rule_log(session) \
enabled(true) \
name("VPN for Site-to-Site to Trusted and Untrusted")
```

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Пример создания правила межсетевого экрана для разрешения трафика из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**:

```
Admin@ug# create network-policy firewall 3 upl-rule PASS \
...src.zone = "VPN for Site-to-Site" \
...dst.zone = (Trusted, Untrusted) \
...rule_log(session) \
...name("VPN for Site-to-Site to Trusted and Untrusted") \
...enabled(true)
```

Настройка VPN-клиента

Для настройки NGFW 2 в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создание зоны, в которую будут помещен интерфейс, используемый для подключения по VPN.

На узле уже создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@ug2# show network zone "VPN for Site-to-Site"

name                : VPN for Site-to-Site
antispoof-enable     : off
antispoof-negate     : off
dos-protection-syn   :
```



```

    enabled          : on
    aggregate        : off
    alert-threshold   : 3000
    drop-threshold    : 6000
dos-protection-udp   :
    enabled          : on
    aggregate        : off
    alert-threshold   : 3000
    drop-threshold    : 6000
dos-protection-icmp  :
    enabled          : on
    aggregate        : off
    alert-threshold   : 100
    drop-threshold    : 200
services-access      :
    service          : Any ICMP
    allowed-addresses : Any
    enabled           : on

    service          : reponse_pages
    allowed-addresses : Any
    enabled           : on

    service          : DNS
    allowed-addresses : Any
    enabled           : on

    service          : HTTP Proxy
    allowed-addresses : Any
    enabled           : on

    service          : Endpoint connect
    allowed-addresses : Any
    enabled           : on

sessions-limit-enabled : off
sessions-limit-threshold : 0

```

Шаг 2. Создать VPN-интерфейс.

Для примера на узле уже создан VPN-интерфейс **tunnel3**, который может быть использован для настройки Site-to-Site VPN.

```
Admin@ug2# show network interface vpn tunnel3

type           : vpn
node_name      : cluster
name           : tunnel3
description    : Example VPN interface to be used in Site-to-Site
VPN client rule. This is an example VPN interface which
                  can be changed or deleted if necessary.
enabled        : off
netflow-profile : Undefined
iface-mode     : dynamic
mtu            : 1420
speed          : 0
zone           : VPN for Site-to-Site
running        : off
master         : off
Admin@ug2# set network interface vpn tunnel3 enabled on
Admin@ug2# show network interface vpn tunnel3

type           : vpn
node_name      : cluster
name           : tunnel3
description    : Example VPN interface to be used in Site-to-Site
VPN client rule. This is an example VPN
                  interface which can be changed or deleted if
necessary.
enabled        : on
netflow-profile : Undefined
iface-mode     : dynamic
mtu            : 1420
speed          : 0
zone           : VPN for Site-to-Site
running        : off
master         : off
```

Шаг 3. Контроль доступа к ресурсам.

Настройки в CLI аналогичны настройкам на NGFW 1 (См. [Шаг 8](#) настройки NGFW 1 в cli).

Шаг 4. Создать профиль безопасности VPN-клиента.

Для создания профиля безопасности VPN-клиента используется следующая команда:

```
Admin@ug2# create vpn client-security-profiles <parameters>
```

Подробнее о порядке создания профилей безопасности VPN в CLI смотрите в статье [Настройка профилей безопасности VPN](#).

Для примера на узле уже создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Добавим в профиль общий ключ, аналогичный заданному в настройках VPN-сервера на [Шаге 4](#), и логин/пароль созданной на [Шаге 3](#) учетной записи для аутентификации VPN-клиента при установлении L2TP туннеля:

```
Admin@ug2# show vpn client-security-profiles
```

Client VPN profile

```

name                : Client VPN profile
description          : Example VPN security profile for client
VPN rule. Preshared key is
                        "examplepresharedkey" - it must be
changed! This profile can be changed or deleted if
                        necessary.
protocol             : ipsec2
ike-mode              : main
local-id-type         : none
certificate           : no certificate
dh-groups             : Group 2 Prime 1024 bit; Group 14 Prime
2048 bit
dpd-state             : off
dpd-interval          : 60
dpd-max-failures      : 5
phase1-security       :
  authentication      : SHA1
  encryption           : AES256
```

```

        authentication      : SHA256
        encryption          : AES256

phase1-key-lifetime        : 1 d
phase2-key-lifetime        : 12 h
key-lifetimesize-enabled   : off
key-lifetimesize           : 4 GB
phase2-security            :
    authentication         : SHA1
    encryption             : AES256

        authentication      : SHA256
        encryption          : AES256

nat-keepalive              : 0
Admin@ug2# set vpn client-security-profiles "Client VPN profile"
protocol ipsec2 psk 123456 authentication-login vpnc1nt1
authentication-password 123123

```

Шаг 5. Создать клиентское правило VPN.

Правила для VPN-клиента создаются с помощью синтаксиса UPL командой:

```
Admin@ug2# create vpn client-rules <position> upl-rule <commands>
```

Подробнее о порядке настройки клиентских правил VPN в CLI смотрите в статье [Настройка клиентских правил](#).

Для примера на узле уже создано серверное правило **Client VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Необходимо добавить в это правило IP-адрес VPN-сервера, куда подключается данный VPN-клиент. В рассматриваемом примере это IP-адрес интерфейса в зоне **Untrusted** на NGFW 1 — 203.0.113.1.

```

Admin@ug2# set vpn client-rules 1 upl-rule OK \
...server_address("203.0.113.1") \
...enabled(true)
Admin@ug2# show vpn client-rules

```

```
% ----- 1 -----
OK \
  server_address("203.0.113.1") \
  last_error(Disabled) \
  status(disconnected) \
  connection_time(0) \
  profile("Client VPN profile") \
  interface(tunnel3) \
  desc("Example VPN client rule which connect UserGate server as
client to another UserGate server acting as VPN server. This rule can
be changed or deleted if necessary.") \
  enabled(true) \
  name("Client VPN rule")
```

После завершения настройки VPN-сервера и VPN-клиента и активации правил VPN клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

Проверка доступности соседнего узла и маршрута в сеть удаленного офиса.

Со стороны NGFW 1:

```
Admin@ug> show network route

Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b -
backup
       t - trapped, o - offload failure
C>* 203.0.113.0/24 is directly connected, port2, 04:20:11
K>* 100.100.0.0/24 [0/0] via 172.30.255.2, tunnel2, 04:19:43
C>* 172.30.255.0/24 is directly connected, tunnel2, 04:20:11
C>* 192.168.1.0/24 is directly connected, port1, 04:20:11
C>* 192.168.56.0/24 is directly connected, port0, 04:20:11
```

```
Admin@ug> ping host 172.30.255.2
```

```
PING 172.30.255.2 (172.30.255.2) 56(84) bytes of data.
64 bytes from 172.30.255.2: icmp_req=1 ttl=64 time=3.34 ms
64 bytes from 172.30.255.2: icmp_req=2 ttl=64 time=2.49 ms
64 bytes from 172.30.255.2: icmp_req=3 ttl=64 time=1.04 ms
^C
--- 172.30.255.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.041/2.292/3.347/0.953 ms
```

Со стороны NGFW 2:

```
Admin@ug2> show network route
```

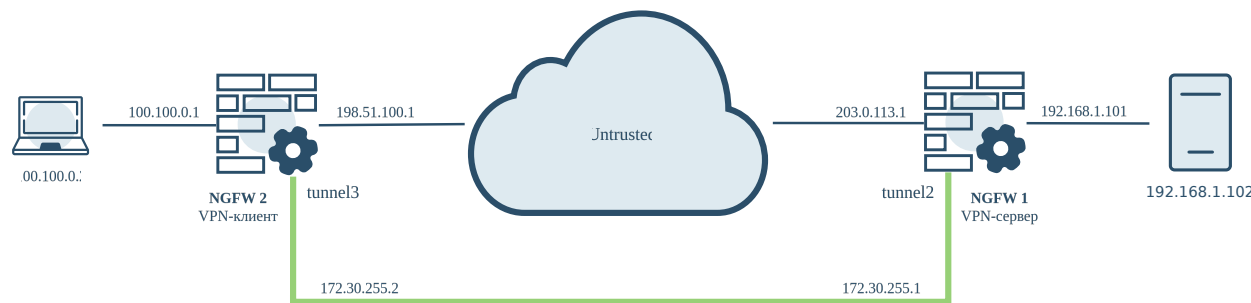
```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b -
backup
       t - trapped, o - offload failure
C>* 198.51.100.0/24 is directly connected, port2, 04:18:41
C>* 100.100.0.0/24 is directly connected, port1, 04:18:41
C>* 172.30.255.0/24 is directly connected, tunnel3, 00:08:00
C>* 192.168.56.0/24 is directly connected, port0, 04:18:41
```

```
Admin@ug2> ping host 172.30.255.1
```

```
PING 172.30.255.1 (172.30.255.1) 56(84) bytes of data.
64 bytes from 172.30.255.1: icmp_req=1 ttl=64 time=2.92 ms
64 bytes from 172.30.255.1: icmp_req=2 ttl=64 time=2.04 ms
64 bytes from 172.30.255.1: icmp_req=3 ttl=64 time=1.13 ms
^C
--- 172.30.255.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 1.138/2.032/2.920/0.729 ms
```

Пример настройки Site-to-Site VPN с IPSec(IKEv2)

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:



Настройка VPN-сервера

Для настройки узла **NGFW 1** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Зоны				
Добавить Редактировать Копировать Удалить				
Зона	Защита от DoS включена для	Исключения ...	Защита от спуфинга	Контроль доступа
Cluster	Ничего		Отключено	Ping, Кластер, Консоль администрирования
DMZ	SYN, UDP, ICMP		Отключено	Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management	SYN, UDP, ICMP		Отключено	Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
Trusted	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-пркс
Tunnel inspection zone	Ничего		Отключено	Все отключено
Untrusted	SYN, UDP, ICMP		Отключено	Ping, SMTP(S)-прокси, POP3(S)-прокси, VPN
VPN for remote access	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств
VPN for Site-to-Site	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств

Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

Сертификаты				
✎ Редактировать Показать Копировать + Создать ▾ 📁 Импорт 📄 Экспорт ▾ ✖ Удалить ↺				
Название	Назначение сертификата	Используется	Издатель	Субъект
👤 root	Отсутствует		DOC	DOC
🔑 server	Digital signature		DOC	ug.testd.local

Создадим профиль клиентских сертификатов в веб-консоли администратора NGFW 1, исполняющего роль VPN-сервера. Для этого необходимо перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя:

Профиль клиентского сертификата

Название:

Profile1

Описание:

Получать имя пользователя из:

Common-name

Subject altname email

Common-name

Principal name

Сертификаты УЦ

Добавить

Название	Издатель	Истекает
root	DOC	2026-12-05T10:45:40Z

Наверх

Выше

Ниже

Вниз

Проверка отозванных сертификатов:

Не проверять

Таймаут проверки:

1

(в секундах)

Сохранить

Отмена

2. Создадим профиль аутентификации для VPN пользователей. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль аутентификации в домене testd.local через LDAP-коннектор:

Свойства профиля аутентификации

Общие

Методы аутентификации

+

Добавить

×

Удалить

↑

Выше

↓

Нижe

Название

Сервер LDAP/Active Directory: ldapcon

Сохранить

Отмена

Свойства коннектора LDAP

Настройки

Домены LDAP

Kerberos keytab

Пути поиска

Включено:

☒

Название:

ldapcon

Описание:

SSL:

☒ Использовать для соединений SSL

Доменное имя LDAP или IP-адрес:

203.0.113.10

Bind DN («логин»):

uid=ug,cn=users,cn=accounts,dc=testd,dc=local

Пароль:

.....

Проверить соединение

Сохранить

Отмена

Шаг 4. Создать профиль безопасности VPN.

В данном примере воспользуемся уже созданным по умолчанию на узле профилем безопасности **Site-to-Site VPN profile**, задающим необходимые настройки. Рассмотрим ключевые настройки этого профиля для примера создания защищенного VPN-соединения в этой статье:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Название:

Site-to-Site VPN profile

Описание:

Example VPN security profile for Site-to-Site VPN. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

1 IKE версия:

IKEv2

Режим IKE:

Основной

2 Тип идентификации:

отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

3 Сертификат сервера:

server

4 Режим аутентификации:

PKI

5 Профиль клиентского сертификата:

Profile1

Сохранить

Отмена

1. **Версия** протокола **IKE** (Internet Key Exchange). В данном примере для создания защищенного канала будет использоваться протокол IKEv2.

2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

3. Указать **сертификат сервера**, импортированный ранее на [Share 3](#).

4. В качестве **режима аутентификации** выберем PKI.

5. Выберем профиль клиентского сертификата, созданный ранее на [Share 3](#).

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

+ Добавить

✕ Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+ Добавить

✎ Редактировать

✕ Удалить

⬆ Выше

⬇ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие
Фаза 1
Фаза 2

Время жизни ключа:
12
часов

Максимальный размер данных, шифруемых одним ключом:
Отключено

4500
МБ

Включить NAT keepalive:

Время жизни NAT:
0
(в секундах)

Безопасность

+ Добавить
✎ Редактировать
✕ Удалить
⬆ Выше
⬆ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить
Отмена

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

The screenshot shows a window titled "Настройка VPN-адаптера" (VPN Adapter Configuration). It has two tabs: "Общие" (General) and "Сеть" (Network). The "Общие" tab is active. The form contains the following fields:

- 1 Включено:** A checkbox that is checked.
- 2 Название:** A text field containing "tunnel2".
- Описание:** A text area containing the text: "Example VPN interface to be used in Site-to-Site VPN server rule. This is an example VPN interface which can be changed or deleted if necessary."
- 3 Зона:** A dropdown menu showing "VPN for Site-to-Site".
- Профиль netflow:** A dropdown menu showing "Не выбран" (Not selected).
- Алиас/Псевдоним:** An empty text field.

At the bottom right, there are two buttons: "Сохранить" (Save) and "Отмена" (Cancel).

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel2).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW 1, будут также помещены в эту зону. В данном примере указывается зона VPN for Site-to-Site.

Настройка VPN-адаптера

Общие Сеть

4 Режим: Статический

5 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
6 172.30.255.1	255.255.255.0

Сохранить Отмена

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.255.1, который задается в поле 6.

5. **MTU** — размер MTU в данном примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel2 172.30.255.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Site-to-Site VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

1 Диапазон IP: 172.30.255.2-172.30.255.2

1 Маска: 255.255.255.0

3 ☒ Использовать системные DNS-серверы

Серверы DNS:

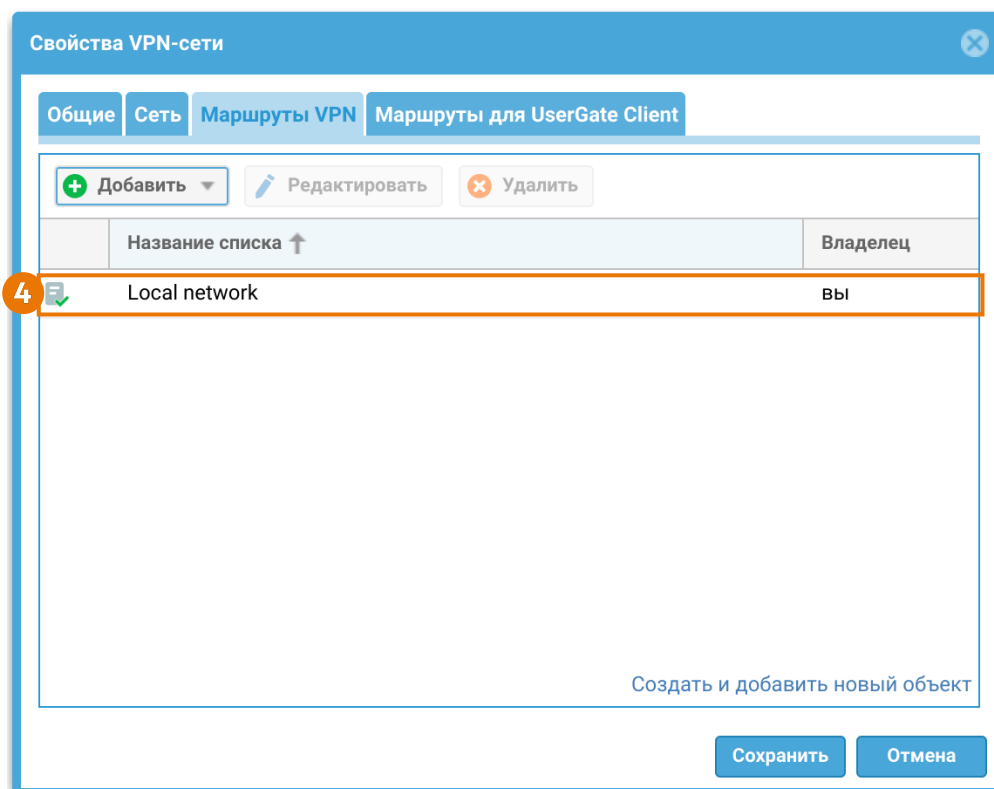
IP-адрес	Действия
	Добавить Редактировать Удалить

Сохранить Отмена

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.255.1), используемому совместно с данной сетью.

2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

Чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте:

Свойства виртуального маршрутизатора

Статические маршруты

Добавить

Редактировать

Удалить

Включить

Отключить

Название	Тип	Адрес назначения	Шлюз ↑	Интерфейс	Метрика
Client network	unicast	100.100.0.0/24	172.30.255.2	tunnel2	0

Сохранить

Отмена

В разделе **Журналы и отчеты → Мониторинг → Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:

Маршруты

Узел: ug

Виртуальный маршрутизатор: Все

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct, > - selected route, * - FIB route, q - queued, r - rejected, b - backup t - trapped, o - offload failure

VRF default:

K>* 100.100.0.0/24 [0/0] via 172.30.255.2, tunnel2, 03:43:49

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct, > - selected route, * - FIB route, q - queued, r - rejected, b - backup t - trapped, o - offload failure

VRF default:

C>* 203.0.113.0/24 is directly connected, port2, 03:44:17

C>* 172.30.255.0/24 is directly connected, tunnel2, 03:44:17

C>* 192.168.1.0/24 is directly connected, port1, 03:44:17

C>* 192.168.56.0/24 is directly connected, port0, 03:44:17

Шаг 7. Создать серверное правило VPN.

В данном примере воспользуемся уже созданным по умолчанию на узле серверным правилом **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для примера создания защищенного VPN-соединения в этой статье:

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Share 4](#) (Site-to-Site VPN profile).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Share 6](#) (Site-to-Site VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Share 3](#)).
5. **Интерфейс** — созданный ранее на [Share 5](#) интерфейс VPN (tunnel2).

Свойства

Общие

Источник

Пользователи

Назначение

Зона источника

☐ Cluster
☐ DMZ
☐ Management
☐ Trusted
☐ Tunnel inspection zone
☒ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Адрес источника

+ Добавить

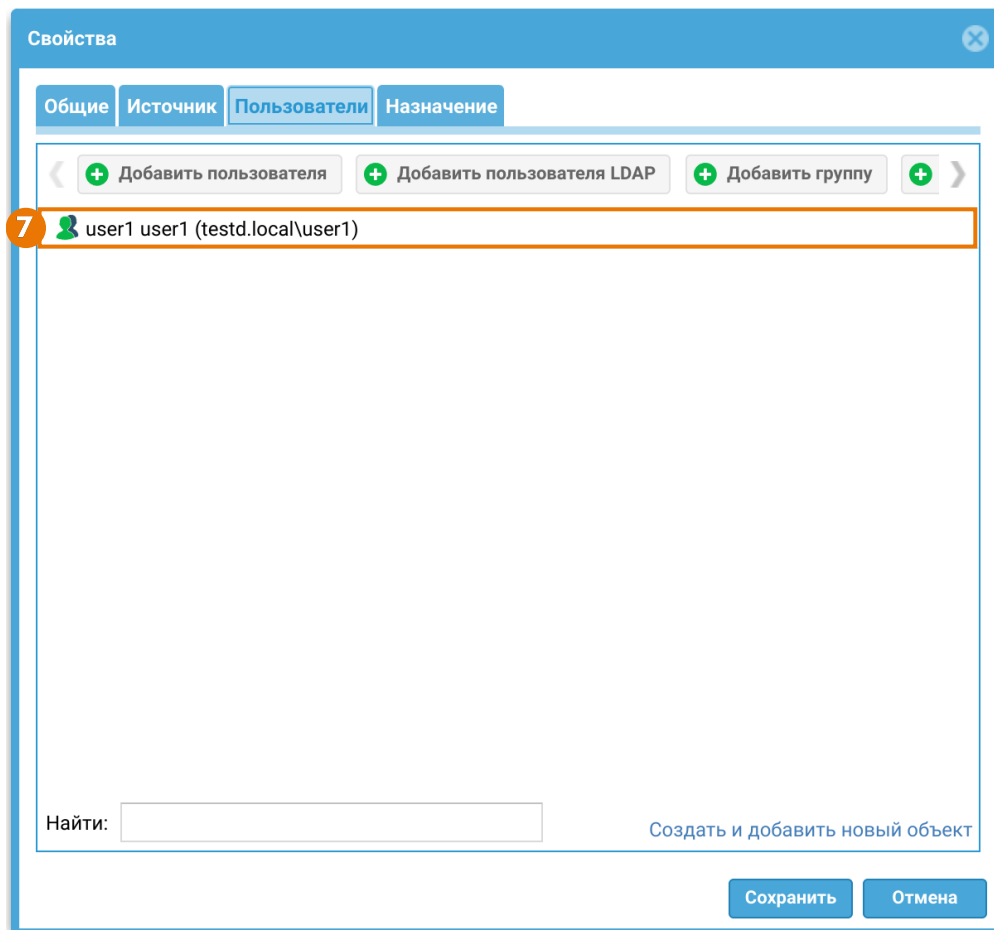
Редактировать

Название списка ↑	Владелец
Создать и добавить новый объект	

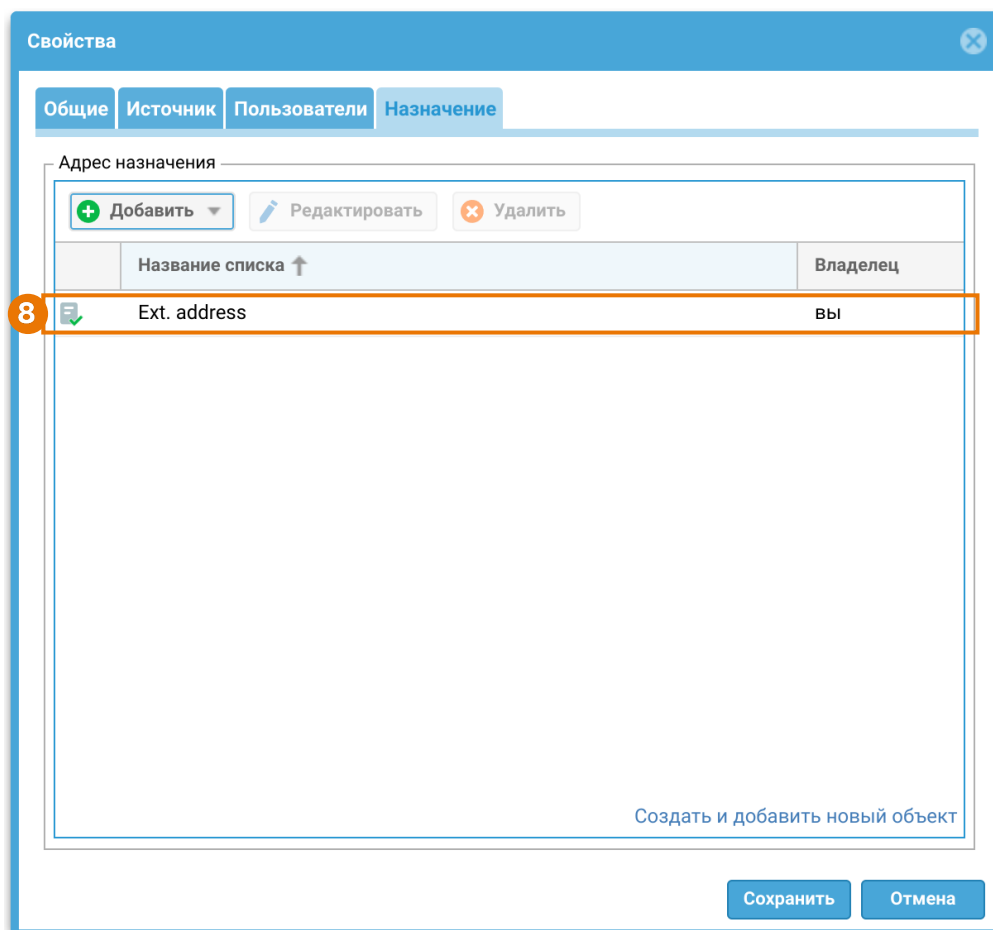
Сохранить

Отмена

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. Пользователи — в данном примере указывается имя пользователя домена user1 (testd.local\user1), на которого был выписан сертификат, с которым аутентифицируется VPN-клиент NGFW 2 при установлении защищенного соединения.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной на [Шаге 2](#) зоны в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в статье [Межсетевой экран](#).

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить.

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Межсетевой экран									
+ Добавить ✎ Редактировать ✖ Удалить ↔ Переместить 📋 Копировать 🔌 Включить 🔌 Отключить 📄 Скопировать ID правила 🔍 Открыть логи 🗑 Сбросить счётчики Все ▾ Принудительно применить									
✓									
#	Статус журн...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
1		Allow trusted to untrusted	✓ Разрешить	Trusted	Любой	Untrusted	Любой	Любой	Любой
2		VPN for Site-to-Site to Trusted and Untrusted	✓ Разрешить	VPN for Site-to-Site	Любой	Untrusted Trusted	Любой	Любой	Любой
3		Trusted and Untrusted to VPN for Site-to-Site	✓ Разрешить	Untrusted Trusted	Любой	VPN for Site-to-Site	Любой	Любой	Любой
4	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой

Настройка VPN-клиента

Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

Настройка VPN-адаптера

Общие Сеть

1 Включено: ☒

2 Название: tunnel3

Описание: Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for Site-to-Site

Профиль netflow: Не выбран

Алиас/Псевдоним:

Сохранить Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel3).

3. **Зона**, к которой будет относиться данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на [Share 1](#).

Настройка VPN-адаптера

Общие Сеть

4 Режим: Динамический

5 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска

Сохранить Отмена

4. **Режим.** Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, созданной на [Шаге 6](#) настроек VPN-сервера.

5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

Шаг 3. Настроить параметры аутентификации.

Импортируем созданный ранее сертификат VPN-клиента. Примеры создания самоподписанных сертификатов приведены в [Приложении](#).

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-клиента и приватного ключа.

Сертификаты				
Редактировать	Показать	Копировать	Создать	Импорт
			Экспорт	Удалить
Название	Назначение сертификата	Используется	Издатель	Субъект
client	Digital signature		DOC	user1@TESTD.LOCAL

Шаг 4. Контроль доступа к ресурсам.

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site**, **Trusted** и **Untrusted**.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, создадим разрешающее правило межсетевого экрана, указав нужную зону источника (**Trusted** и **Untrusted**) и зону назначения **VPN for Site-to-Site**.

Межсетевой экран									
+ Добавить ✎ Редактировать ✖ Удалить ↔ Переместить 📋 Копировать 🔌 Включить 🔌 Отключить 📄 Скопировать ID правила 🔍 Открыть логи 🔄 Сбросить счётчики Все ▾ Принудительно применить									
✓									
#	Статус журн...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
1		Allow trusted to untrusted	✓ Разрешить	Trusted	Любой	Untrusted	Любой	Любой	Любой
2		VPN for Site-to-Site to Trusted and Untrusted	✓ Разрешить	VPN for Site-to-Site	Любой	Untrusted Trusted	Любой	Любой	Любой
3		Trusted and Untrusted to VPN for Site-to-Site	✓ Разрешить	Untrusted Trusted	Любой	VPN for Site-to-Site	Любой	Любой	Любой
4	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой

Шаг 5. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для рассматриваемого примера создания защищенного VPN-соединения.

Свойства клиентского профиля безопасности

Общие

Фаза 1

Фаза 2

Название:

Client VPN profile

Описание:

Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

1

Протокол:

IKEv2 с сертификатом

Режим IKE:

Основной

2

Тип идентификации:

отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

3

Сертификат клиента:

client

Подсети для VPN

Локальная подсеть:

Удалённая подсеть:

Аутентификация

Логин:

Пароль:

Сохранить

Отмена

1. **Протокол.** В рассматриваемом примере для создания защищенного канала будет использоваться **IKEv2 с сертификатом**.

2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

3. Выберем сертификат клиента, импортированный ранее на [Share 3](#).

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

+

Добавить

✕ Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+

Добавить

✎

Редактировать

✕

Удалить

⬆

Выше

⬇

Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

(в секундах)

Безопасность

+ Добавить

✎ Редактировать

✖ Удалить

⬆ Выше

⬇ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 6. Создать клиентское правило VPN.

Для примера на узле создано клиентское правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения.

Свойства

Общие

1 Включено: ☒

Название: Client VPN rule

Описание:

Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.

2 Профиль безопасности VPN: Client VPN profile

3 Интерфейс: tunnel3

4 Адрес сервера: ug.testd.local

Сохранить

Отмена

1. **Включено** — включить правило.

2. **Профиль безопасности VPN** — созданный на [Шаре 5](#) клиентский профиль безопасности VPN.

3. **Интерфейс** — созданный на [Шаре 2](#) VPN-интерфейс.

4. **Адрес сервера.** В рассматриваемом примере это доменное имя NGFW 1 (ug.testd.local), выполняющего роль VPN-сервера.

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узлах NGFW 1 и NGFW 2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

На NGFW 1:

VPN							
ug							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user1 user1 (testd.local\user1)	Сервер	Site-to-Site VPN rule	19 февраля 2024 г., 18:05 (24м 3...)	172.30.255.2	10.10.0.2		aes

На NGFW 2:

VPN							
ug2							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user1@TESTD.LOCAL	Клиент	—	19 февраля 2024 г., 18:05 (13м 19с)	172.30.255.2	ug.testd.local		aes256

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW 2 добавится маршрут в сеть удаленного офиса 192.168.1.0/24 через туннельный интерфейс tunnel3:

Маршруты
Узел: ug2 Виртуальный маршрутизатор: Все
VRF default Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct, > - selected route, * - FIB route, q - queued, r - rejected, b - backup t - trapped, o - offload failure VRF default: K>* 192.168.1.0/24 [0/0] via 172.30.255.2, tunnel3, 00:18:51 VRF default Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct, > - selected route, * - FIB route, q - queued, r - rejected, b - backup t - trapped, o - offload failure VRF default: C>* 198.51.100.0/24 is directly connected, port2, 00:29:37 C>* 100.100.0.0/24 is directly connected, port1, 00:29:37 C>* 172.30.255.0/24 is directly connected, tunnel3, 00:18:51 C>* 192.168.56.0/24 is directly connected, port0, 00:29:37

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW 1:

Ping

Настройка ping

Ping host TTL Интерфейс

Счётчик ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

```

PING 172.30.255.2 (172.30.255.2) from 172.30.255.1 : 56(84) bytes of data.
64 bytes from 172.30.255.2: icmp_req=1 ttl=64 time=3.00 ms
64 bytes from 172.30.255.2: icmp_req=2 ttl=64 time=2.47 ms
64 bytes from 172.30.255.2: icmp_req=3 ttl=64 time=0.611 ms
64 bytes from 172.30.255.2: icmp_req=4 ttl=64 time=1.64 ms
64 bytes from 172.30.255.2: icmp_req=5 ttl=64 time=3.77 ms
64 bytes from 172.30.255.2: icmp_req=6 ttl=64 time=2.07 ms

--- 172.30.255.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.611/2.262/3.770/1.002 ms

```

Со стороны NGFW 2:

Ping

Настройка ping

Ping host TTL Интерфейс

Счётчик ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

```

PING 172.30.255.1 (172.30.255.1) from 172.30.255.2 : 56(84) bytes of data.
64 bytes from 172.30.255.1: icmp_req=1 ttl=64 time=2.79 ms
64 bytes from 172.30.255.1: icmp_req=2 ttl=64 time=1.08 ms
64 bytes from 172.30.255.1: icmp_req=3 ttl=64 time=3.11 ms
64 bytes from 172.30.255.1: icmp_req=4 ttl=64 time=0.799 ms
64 bytes from 172.30.255.1: icmp_req=5 ttl=64 time=1.00 ms
64 bytes from 172.30.255.1: icmp_req=6 ttl=64 time=3.78 ms

--- 172.30.255.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 0.799/2.096/3.789/1.175 ms

```

Хосты в сетях обоих офисов доступны друг для друга:

```

:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:60:bc:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
:~$ ping 100.100.0.2
PING 100.100.0.2 (100.100.0.2) 56(84) bytes of data.
64 bytes from 100.100.0.2: icmp_seq=1 ttl=62 time=3.89 ms
64 bytes from 100.100.0.2: icmp_seq=2 ttl=62 time=4.39 ms
64 bytes from 100.100.0.2: icmp_seq=3 ttl=62 time=4.21 ms
64 bytes from 100.100.0.2: icmp_seq=4 ttl=62 time=1.72 ms
64 bytes from 100.100.0.2: icmp_seq=5 ttl=62 time=2.74 ms
^C
--- 100.100.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4020ms
rtt min/avg/max/mdev = 1.721/3.388/4.390/1.012 ms

```

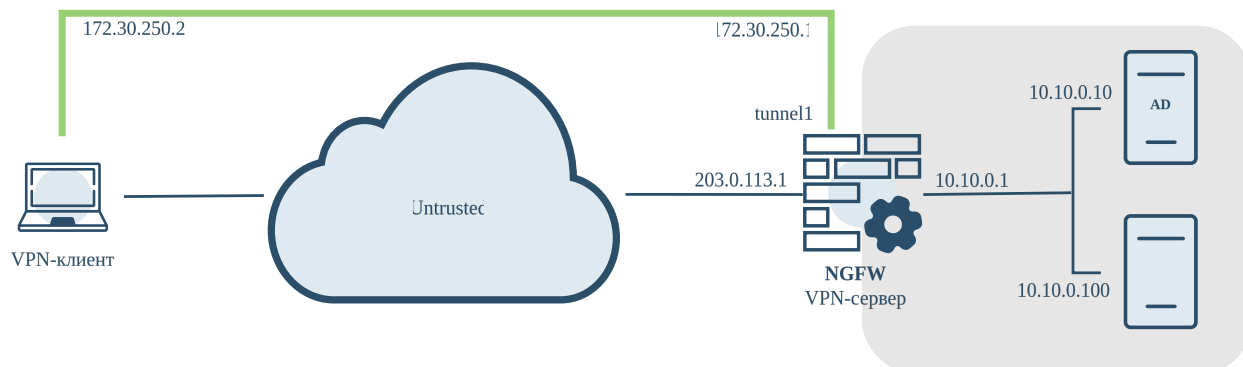
```

~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:04:97:9a brd ff:ff:ff:ff:ff:ff
    inet 100.100.0.2/24 brd 100.100.0.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
~$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=62 time=5.97 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=62 time=4.27 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=62 time=8.62 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=62 time=7.34 ms
64 bytes from 192.168.1.102: icmp_seq=5 ttl=62 time=2.01 ms
64 bytes from 192.168.1.102: icmp_seq=6 ttl=62 time=1.97 ms
^C
--- 192.168.1.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.969/5.030/8.621/2.522 ms

```

Пример настройки Remote access VPN с L2TP/IPSec(IKEv1)

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:



В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя — в роли VPN-клиента. При создании VPN с помощью L2TP/IPsec(IKEv1), протокол L2TP создает туннель, в котором передаются пакеты сетевого уровня в кадрах PPP. IPsec обеспечивает шифрование, аутентификацию и проверку целостности передаваемых данных.

Сначала необходимо настроить VPN-сервер, затем произвести настройки VPN-клиента на компьютере пользователя и инициировать подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки **NGFW** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервисы **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы **VPN** и **Подключение конечных устройств** в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 3. Настроить параметры аутентификации.

Для примера в разделе **Пользователи и устройства → Профили аутентификации** создадим профиль **ldap_con** для аутентификации пользователей VPN через имеющийся сервер AD. На вкладке **Методы аутентификации** выберем ранее настроенный в системе сервер аутентификации LDAP/Active Directory. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#).

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Remote access VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для данного примера:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

Название: Remote access VPN profile

Описание:

1 IKE версия: IKEv1

2 Режим IKE: Основной

3 Тип идентификации: отсутствует

Значение идентификации:

4 Общий ключ:

Общий ключ (повтор):

Сертификат сервера: server

Режим аутентификации: PKI

Профиль клиентского сертификата: Profile1

Сохранить Отмена

1. **Версия** протокола **IKE** (Internet Key Exchange). В рассматриваемом примере для создания защищенного канала будет использоваться протокол IKEv1.

2. **Режим** работы **IKE**. В рассматриваемом примере используется Основной режим работы IKEv1.

3. **Тип идентификации** (параметр IKE local ID). Опциональный параметр. В рассматриваемом примере указывать не требуется.

4. **Общий ключ** (Pre-shared key) для аутентификации удаленных компьютеров пользователей. Ключ должен совпадать на VPN-сервере и VPN-клиенте для успешного подключения.

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения.

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

(сек)

Неудачных попыток:

5

Diffie-Hellman группы

+ Добавить

✗ Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+ Добавить

✎ Редактировать

✗ Удалить

⬆ Выше

⬇ Ниже

Аутентификация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES
SHA1	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

секунд

Безопасность

Добавить

Редактировать

Удалить

Выше

Низже

Аутентификация	Шифрование
SHA1	AES192
SHA1	3DES
MD5	AES128
MD5	3DES
SHA1	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера:

Настройка VPN-адаптера

Общие

Сеть

1 Включено: ☒

2 Название: tunnel1

Описание:

Example VPN interface to be used in Remote Access VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for remote access

Профиль netflow: Не выбран

Алиас/Псевдоним:

Сохранить

Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel1).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В этом примере указывается зона **VPN for remote access**, созданная на [шаге 2](#).

Настройка VPN-адаптера

Общие Сеть

4 Режим: Статический

5 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
172.30.250.1	255.255.255.0

Сохранить Отмена

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес.

5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

Для примера на узле создана сеть **Remote access VPN network** с настройками по умолчанию. Рассмотрим ключевые настройки этой сети для данного примера:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

1 Диапазон IP: 172.30.250.2-172.30.250.254

2 Маска: 255.255.255.0

3 ☒ Использовать системные DNS-серверы

Серверы DNS:

Добавить Редактировать Удалить

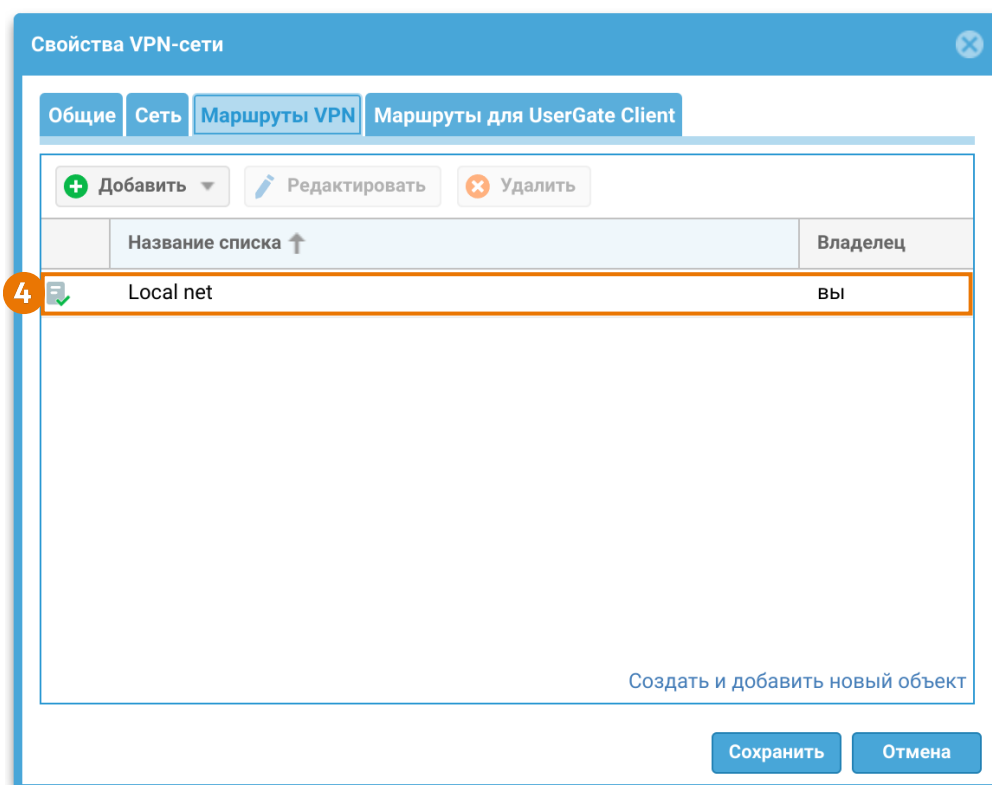
IP-адрес

Сохранить Отмена

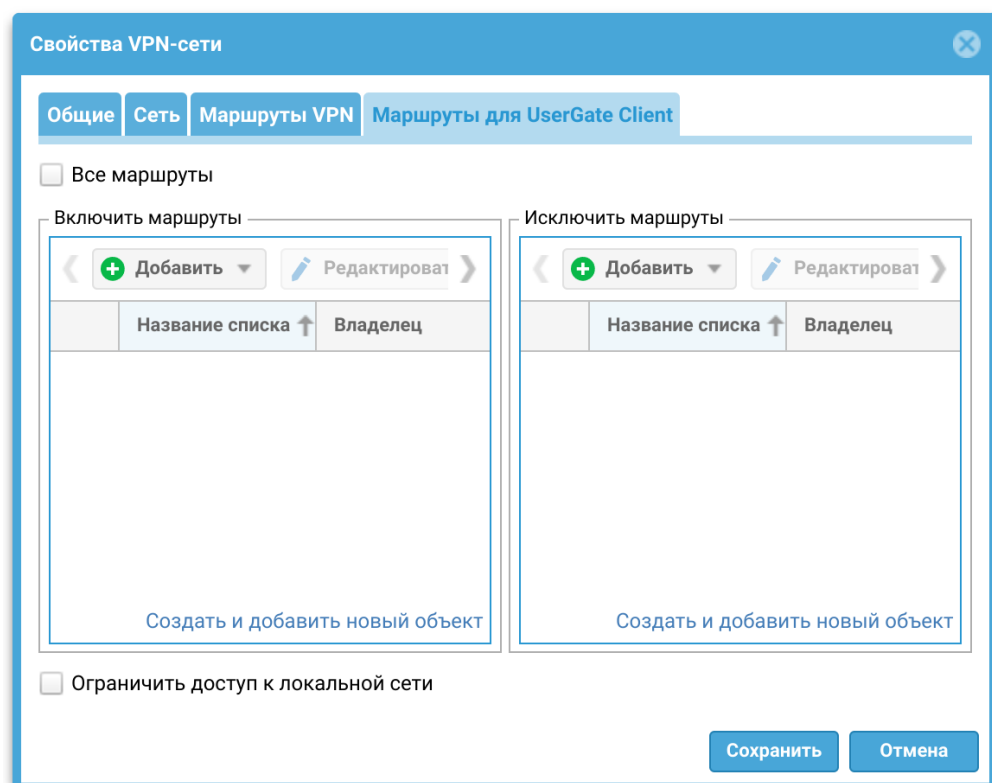
1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW (172.30.250.1), используемому совместно с данной сетью.

2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



4. На вкладке **Маршруты VPN** настраиваются маршруты, передаваемые клиенту при установлении соединения. В данном примере добавлен список *Local net*, включающий в себя подсеть офиса 192.168.1.0/24.



На вкладке **Маршруты для UserGate client** настраивается функциональность раздельного туннелирования (split tunneling) для UserGate Client. Подробнее читайте в разделе [Настройка раздельного туннелирования для UserGate Client](#).

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

Свойства

Общие | Источник | Пользователи | Назначение

1 Включено: ☒

Название: Remote access VPN rule

Описание:

2 Профиль безопасности VPN: Remote access VPN profile

3 Сеть VPN: Remote access VPN network

4 Профиль аутентификации: ldap_profile URL инициализации TOTP

5 Интерфейс: tunnel1

Вставить: Вниз списка правил

Сохранить Отмена

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (Remote access VPN profile).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).

Свойства

Общие **Источник** Пользователи Назначение

Зона источника

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☐ Trusted
- ☐ Tunnel inspection zone
- 6** ☒ **Untrusted**
- ☐ VPN for remote access
- ☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Адрес источника

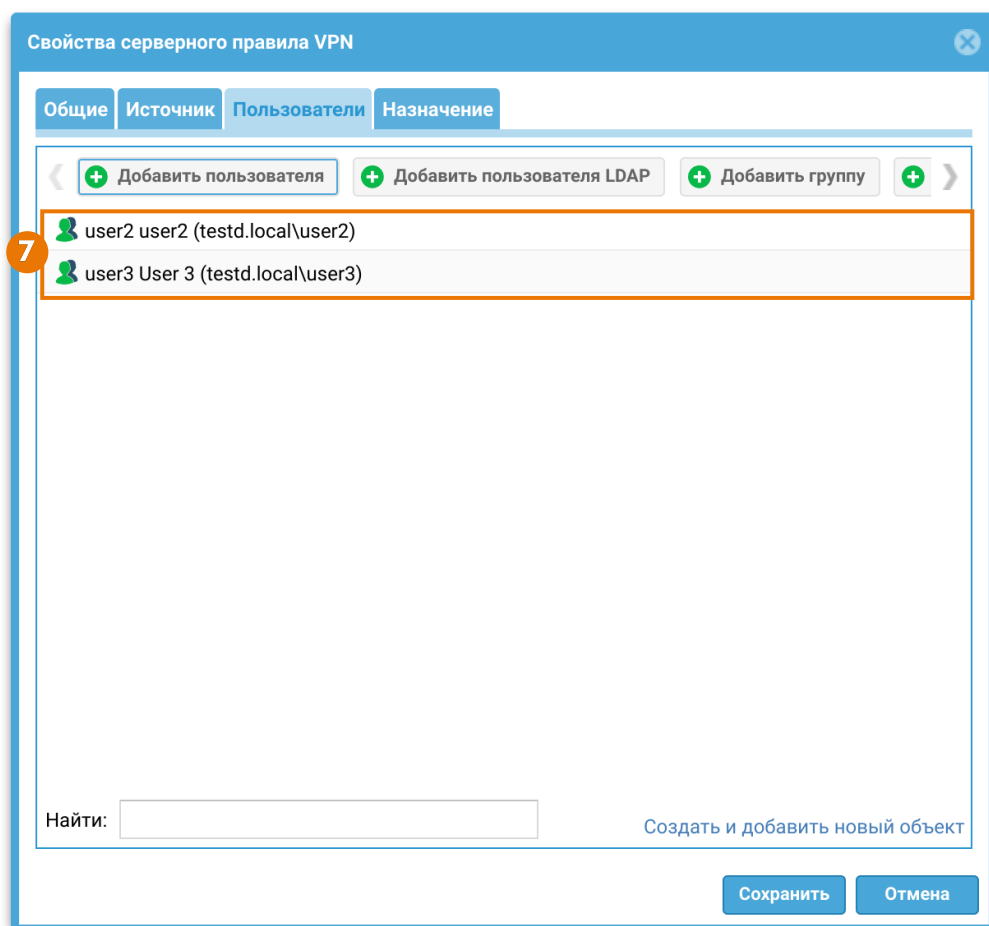
< + Добавить Редактировать >

Название списка ↑	Владелец
-------------------	----------

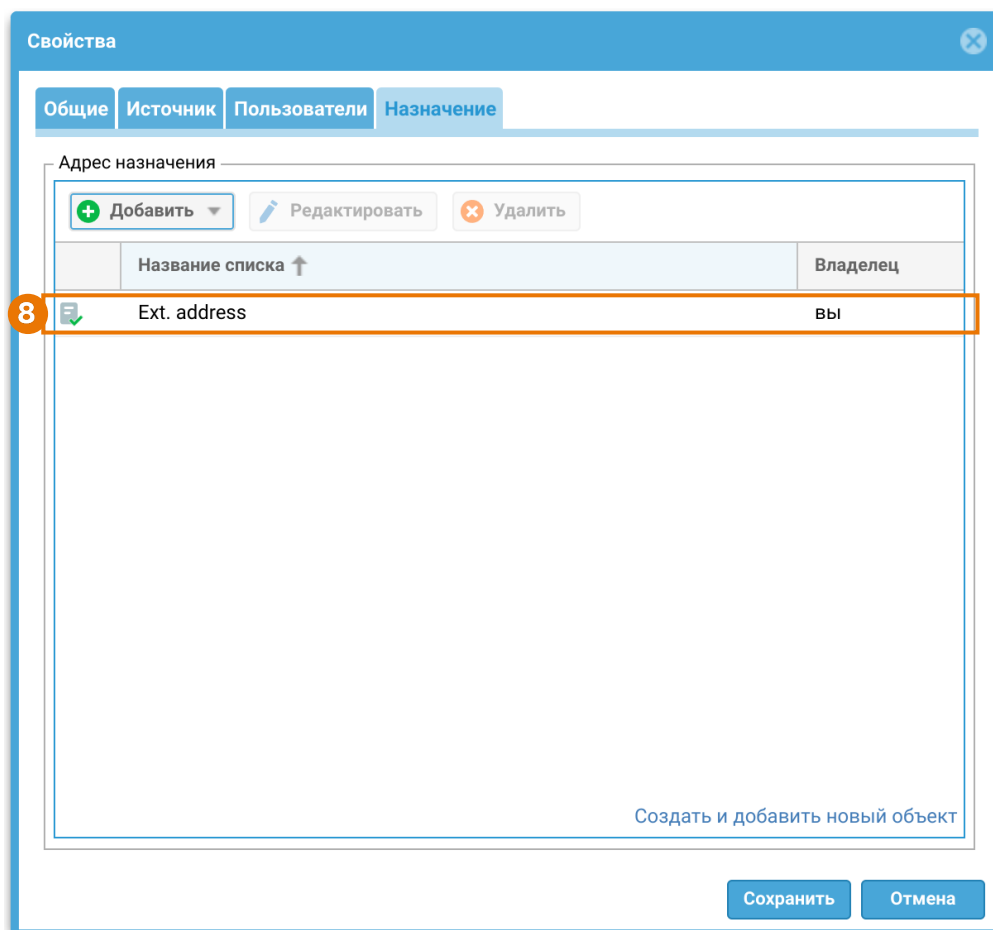
Создать и добавить новый объект

Сохранить Отмена

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. Пользователи — доменные пользователи, которым разрешено пользоваться сервисом VPN.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1.

Шаг 8. Контроль доступа к ресурсам.

1. Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь

трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

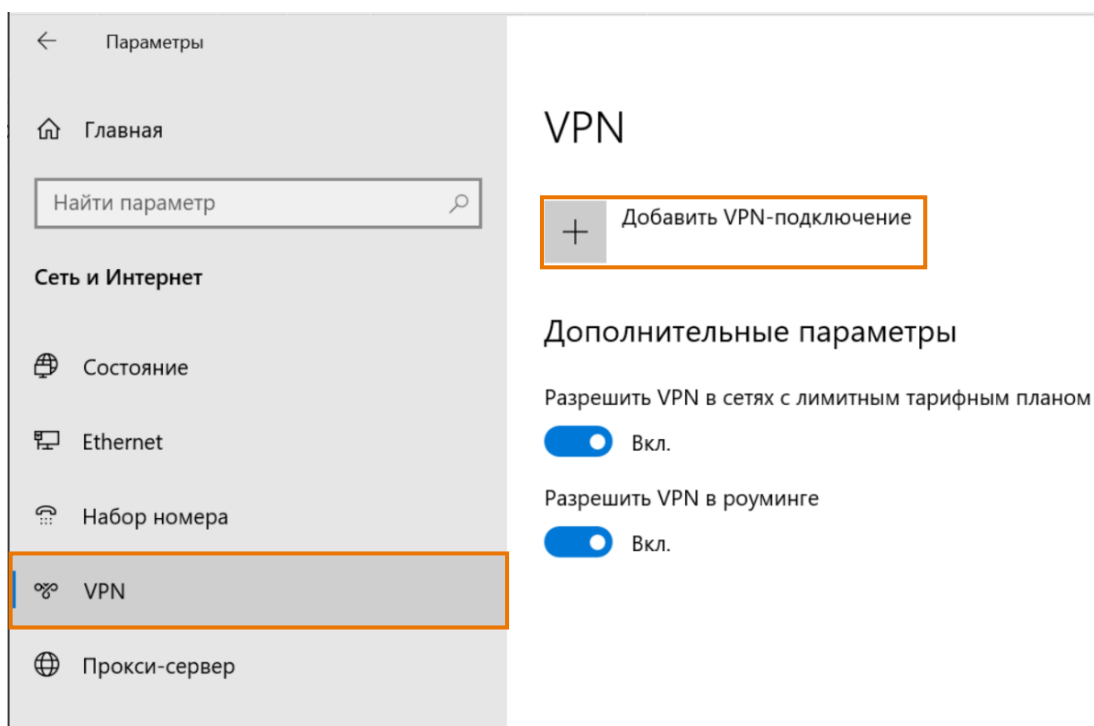
Настройка VPN-клиента

В данном примере рассмотрим настройку "нативных" клиентов для операционных систем Windows и Linux для удаленного VPN-подключения.

Встроенный VPN-клиент OS Windows

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Кликнуть правой кнопкой мыши по значку сетевого подключения в трее и выбрать пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выбрать пункт **VPN**, а затем нажать на пункт **Добавить VPN-подключение**:



3. В окне **Добавить VPN-подключение** настроить параметры подключения:

- В поле **Поставщик услуг VPN** выбрать **Windows (встроенные)**;
- В поле **Имя подключения** указать имя для этого подключения;
- В поле **Имя или адрес сервера** указать IP-адрес внешнего интерфейса NGFW, к которому будут подключаться клиенты(203.0.113.1);
- В поле **Тип VPN** выбрать **L2TP/IPsec с общим ключом**;

- В поле **Общий ключ** указать тот же ключ, что был указан на [шаге 4](#)
- настройки VPN-сервера;
 - В поле **Тип данных для входа** выбрать **Имя пользователя и пароль**;
 - В поле Имя пользователя указать имя доменного пользователя, в данном примере: user2@testd.local;
 - В поле Пароль указать пароль пользователя.

Добавить VPN-подключение

Поставщик услуг VPN

Windows (встроенные) ▾

Имя подключения

L2TP

Имя или адрес сервера

203.0.113.1

Тип VPN

L2TP/IPsec с общим ключом ▾

Общий ключ

••••••••

Тип данных для входа

Имя пользователя и пароль ▾

Имя пользователя (необязательно)

user2@testd.local

Пароль (необязательно)

••••••••

☒ Запомнить мои данные для входа

Сохранить

4. Нажать кнопку Сохранить, чтобы сохранить настройки VPN-соединения.

5. В панели управления перейти в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выбрать пункт **Настройки параметров адаптера**:

Дополнительные сетевые параметры



Настройка параметров адаптера

Просмотр сетевых адаптеров и изменение параметров подключения.



Центр управления сетями и общим доступом

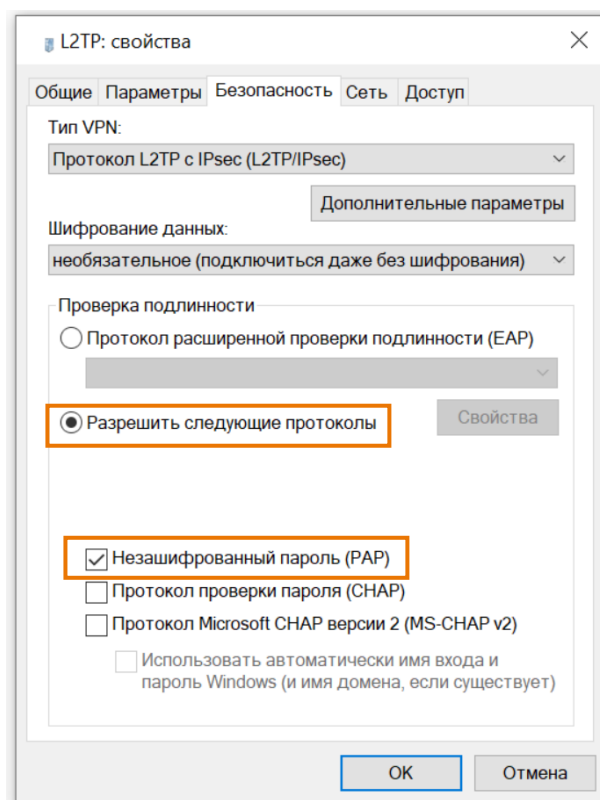
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.

[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

[Сброс сети](#)

6. Выбрать только что созданное сетевое подключение **L2TP** и через меню правой кнопки мыши перейти в свойства этого подключения. В открывшемся окне перейти во вкладку **Безопасность**:



Выбрать пункт **Разрешить следующие протоколы** и далее выбрать **PAP**.

7. Сохранить настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **L2TP** и нажмите кнопку **Подключиться**.

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@thihichinnde							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	GeO IP	Шифрование
user2 user2 (testd.local\user2)	Сервер	Remote access VPN rule	14 мая 2024 г., 13:48 (40с)	172.30.250.2	203.0.113.11		aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий							
Сегодня (14 Май 2024 г.) Важность: Все Компоненты и события: Все Ещё Сброс Поиск Расширенный Фильтры							
Узел	Время	Компонент	Тип события	Пользователь	IP источника	Модуль	Детали события
utmcore@thihichinnde	13:48:11	VPN	Подключение пользователя к VPN прошло успешно	user2 user2 (testd.local\user2)	203.0.113.11	VPN сервер	Логин: user2@testd.local

На стороне удаленного Windows-компьютера добавится rpp-адаптер L2TP, появятся маршруты в сеть виртуального адаптера и сеть удаленного офиса. Хост (10.10.0.100) в сети офиса доступен:

```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::88cd:862:5a32:beaf%11
    IPv4 Address. . . . . : 203.0.113.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 203.0.113.1

PPP adapter L2TP_VPN:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.30.250.2
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 0.0.0.0

C:\Users\ >route print -4
=====
Interface List
12...02 50 f2 dc 11 00 .....UserGate Client VPN Adapter
11...08 00 27 b3 b3 bb .....Intel(R) PRO/1000 MT Desktop Adapter
28.....L2TP_VPN
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          203.0.113.1     203.0.113.11     4506
0.0.0.0                    0.0.0.0          On-link         172.30.250.2     26
10.10.0.0                  255.255.255.0    On-link         172.30.250.2     26
10.10.0.255                255.255.255.255  On-link         172.30.250.2     281
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        4556
127.0.0.1                  255.255.255.255  On-link         127.0.0.1        4556
127.255.255.255            255.255.255.255  On-link         127.0.0.1        4556
172.30.250.2               255.255.255.255  On-link         172.30.250.2     281
203.0.113.0                255.255.255.0    On-link         203.0.113.11     4506
203.0.113.1                255.255.255.255  On-link         203.0.113.11     4251
203.0.113.11               255.255.255.255  On-link         203.0.113.11     4506
203.0.113.255              255.255.255.255  On-link         203.0.113.11     4506
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        4556
224.0.0.0                  240.0.0.0        On-link         203.0.113.11     4506
224.0.0.0                  240.0.0.0        On-link         172.30.250.2     26
255.255.255.255            255.255.255.255  On-link         127.0.0.1        4556
255.255.255.255            255.255.255.255  On-link         203.0.113.11     4506
255.255.255.255            255.255.255.255  On-link         172.30.250.2     281
=====
Persistent Routes:
Network Address            Netmask    Gateway Address  Metric
0.0.0.0                    0.0.0.0    203.0.113.1     Default
=====

C:\Users\ >ping 10.10.0.100

Pinging 10.10.0.100 with 32 bytes of data:
Reply from 10.10.0.100: bytes=32 time=1ms TTL=63
Reply from 10.10.0.100: bytes=32 time=2ms TTL=63
Reply from 10.10.0.100: bytes=32 time=4ms TTL=63
Reply from 10.10.0.100: bytes=32 time=4ms TTL=63

Ping statistics for 10.10.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

```

L2TP VPN-клиент для OS Linux

Рассмотрим настройку L2TP VPN-клиента для Linux на примере OS Ubuntu.

Для начала необходимо установить L2TP-плагин для приложения Network Manager:

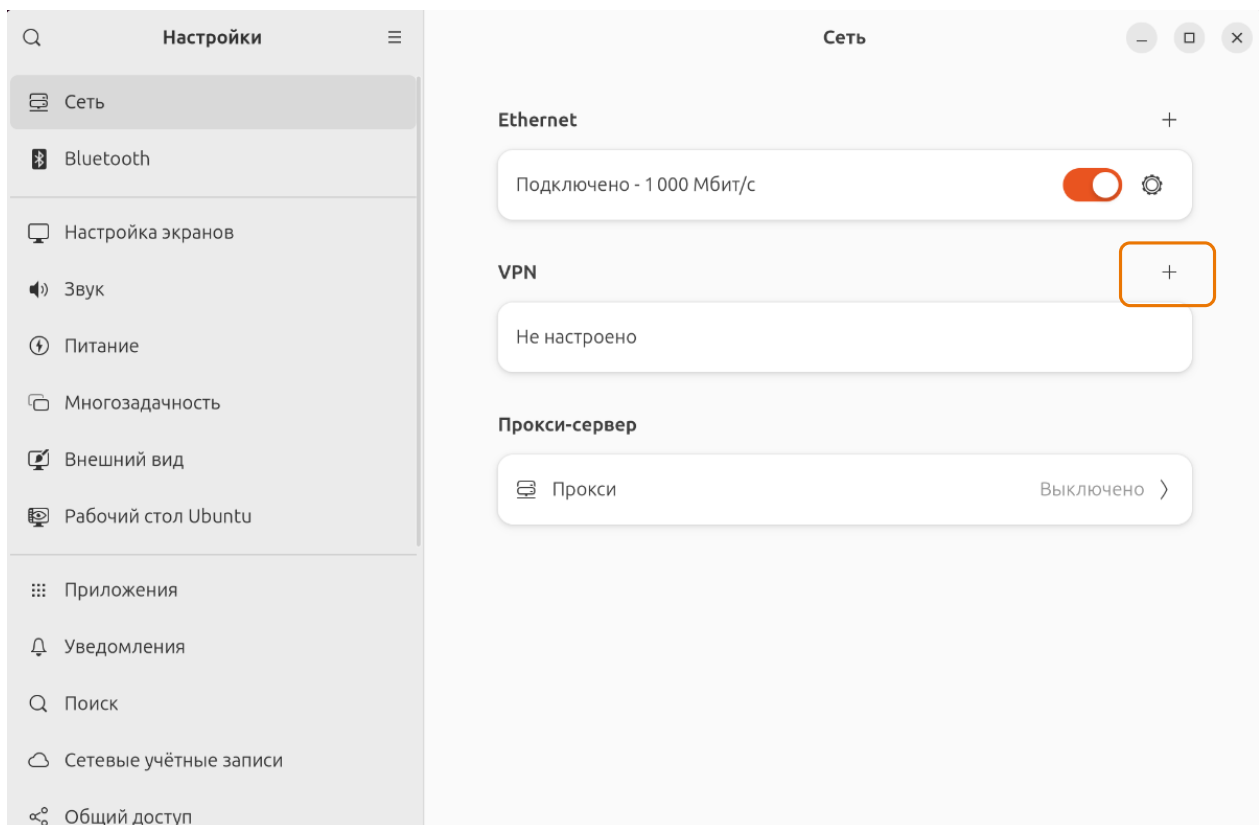
```

sudo apt update
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome

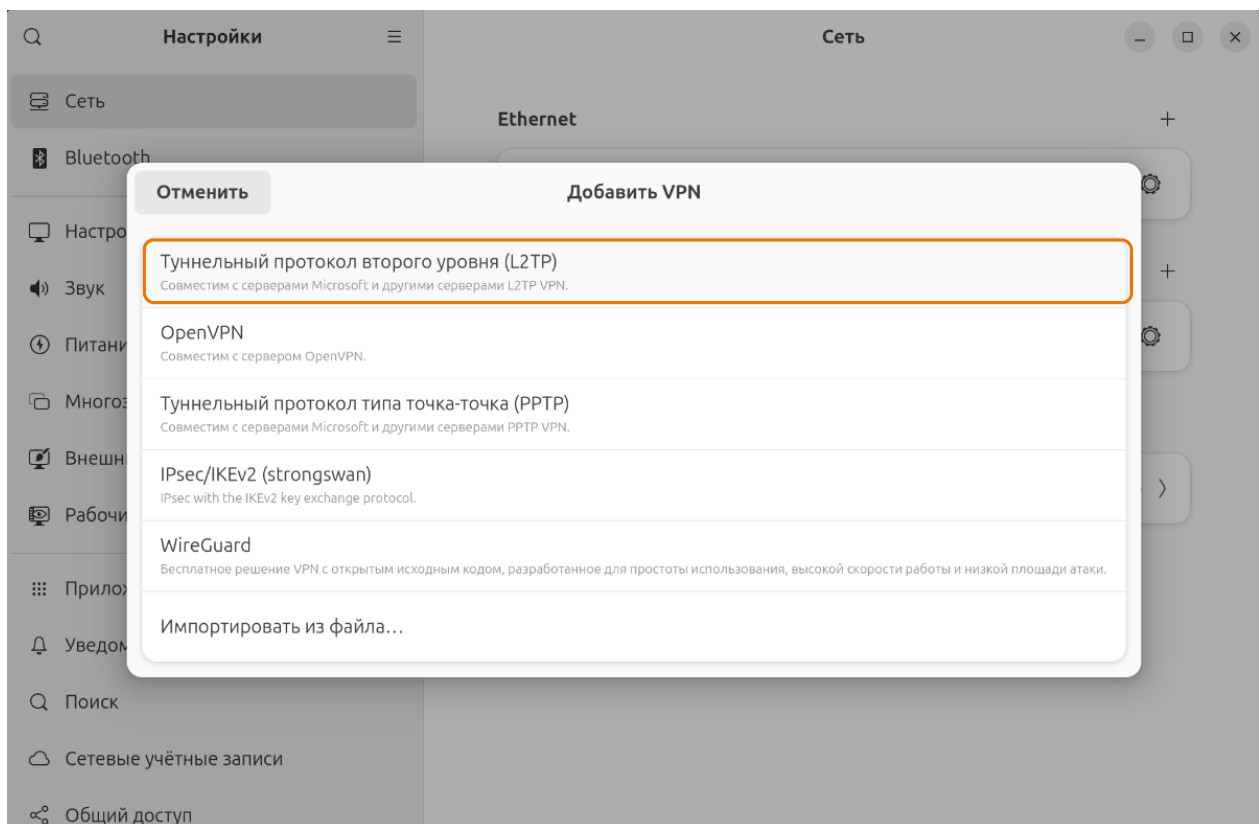
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

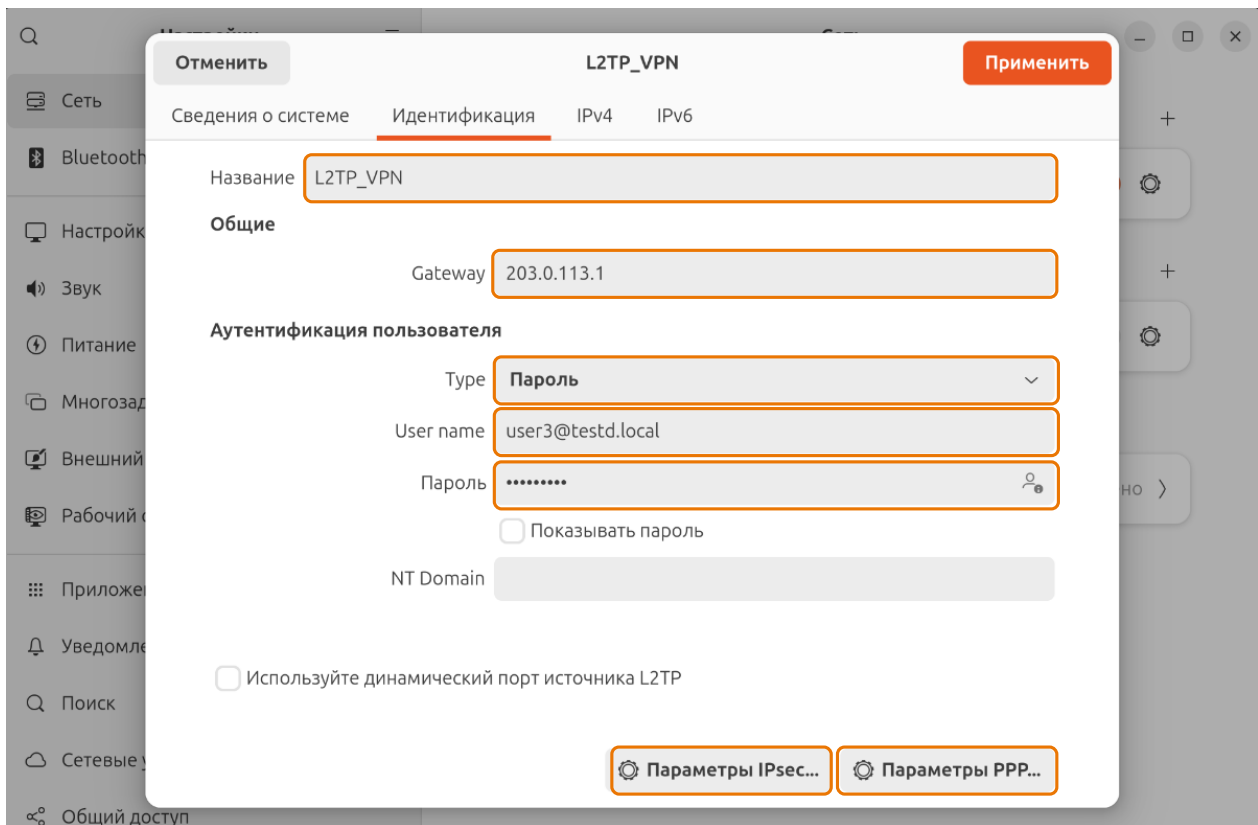
1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



2. Выбрать из списка опцию **Туннельный протокол второго уровня (L2TP)**:



3. В настройках L2TP VPN перейти на вкладку **Идентификация**. Указать название соединения, адрес VPN-сервера, параметры аутентификации пользователя:



4. Перейти к настройкам протокола IPsec, нажав внизу окна настроек VPN кнопку **Параметры IPsec**. В открывшемся окне настроек поставить флажок для активации настроек IPsec туннеля к L2TP хосту, указать общий ключ и параметры первой и второй фаз согласования защищенного соединения:

Отменить

IPsec Properties

Применить

☒ Enable IPsec tunnel to L2TP host

Machine Authentication

Type

Общий ключ

Pre-shared key

.....

☐ Show password

Advanced

☐ Remote ID:

☒ Phase1 Algorithms: aes256-sha1-modp1024!

☒ Phase2 Algorithms: aes256-sha1!

☐ Phase1 Lifetime: 3:00 — + (HH:MM)

☐ Phase2 Lifetime: 1:00 — + (HH:MM)

☐ Enforce UDP encapsulation

☐ Use IP compression

☐ Use IKEv2 key exchange

☐ Disable PFS

Нажать **Применить** для сохранения настроек IPsec.

5. Перейти к настройкам протокола PPP, нажав внизу окна настроек VPN кнопку **Параметры PPP**. В открывшемся окне настроек поставить флажок, разрешая в качестве метода аутентификации PAP. Остальные методы отключить:

Cancel **PPP Properties** Apply

Аутентификация
Разрешить следующие методы аутентификации:

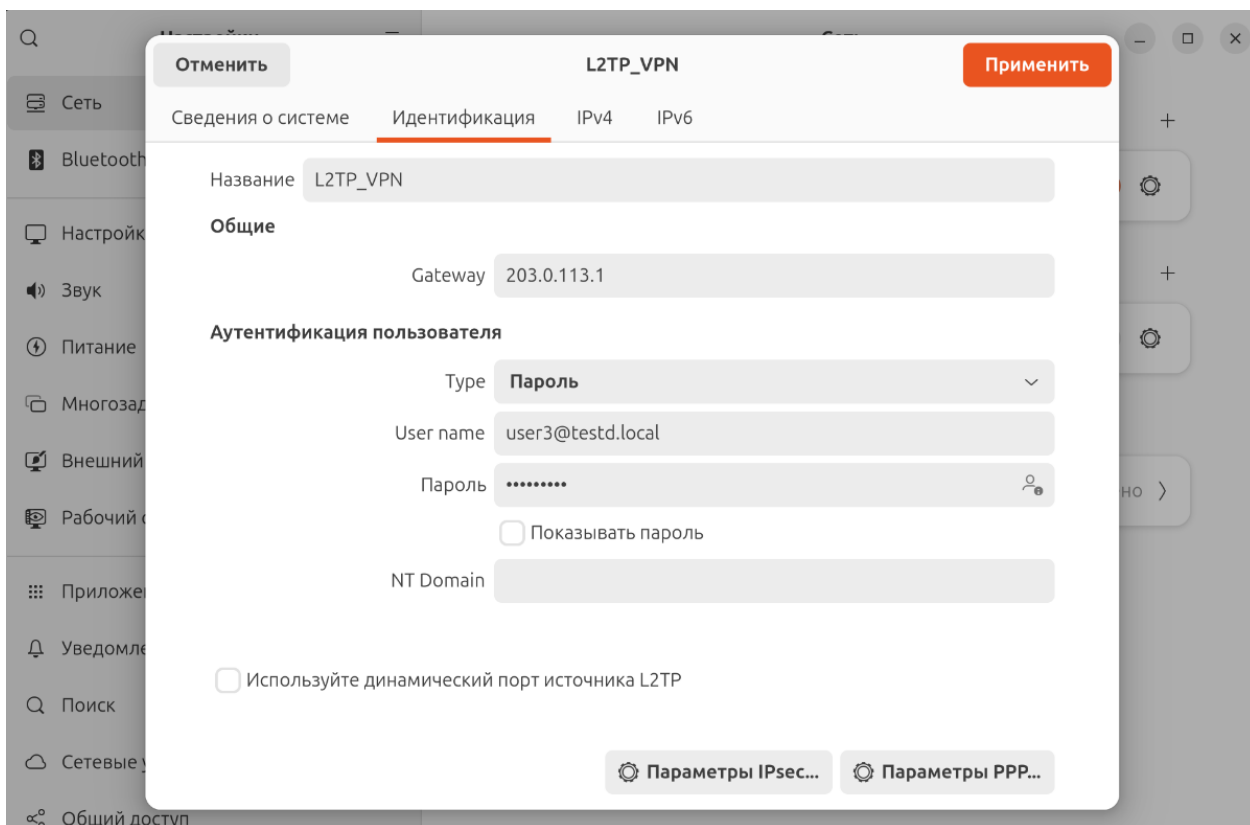
☒ PAP
☐ CHAP
☐ MSCHAP
☐ MSCHAPv2
☐ EAP

Шифрование и сжатие
☐ Использовать шифрование MPPE
Security **Любой доступный (по умолчанию)** ▾
☐ Включить шифрование с сохранением состояния
☐ Разрешить сжатие данных BSD
☐ Разрешить сжатие данных Deflate
☐ Использовать сжатие заголовков TCP
☐ Использовать согласование сжатия поля протокола
☐ Использовать сжатие полей «адрес»/«управление»

Прочие
☐ Посылать эхо-пакеты PPP
☐ Multilink PPP MRRU: 1600 — +
MTU 1420 — +
MRU 1400 — +

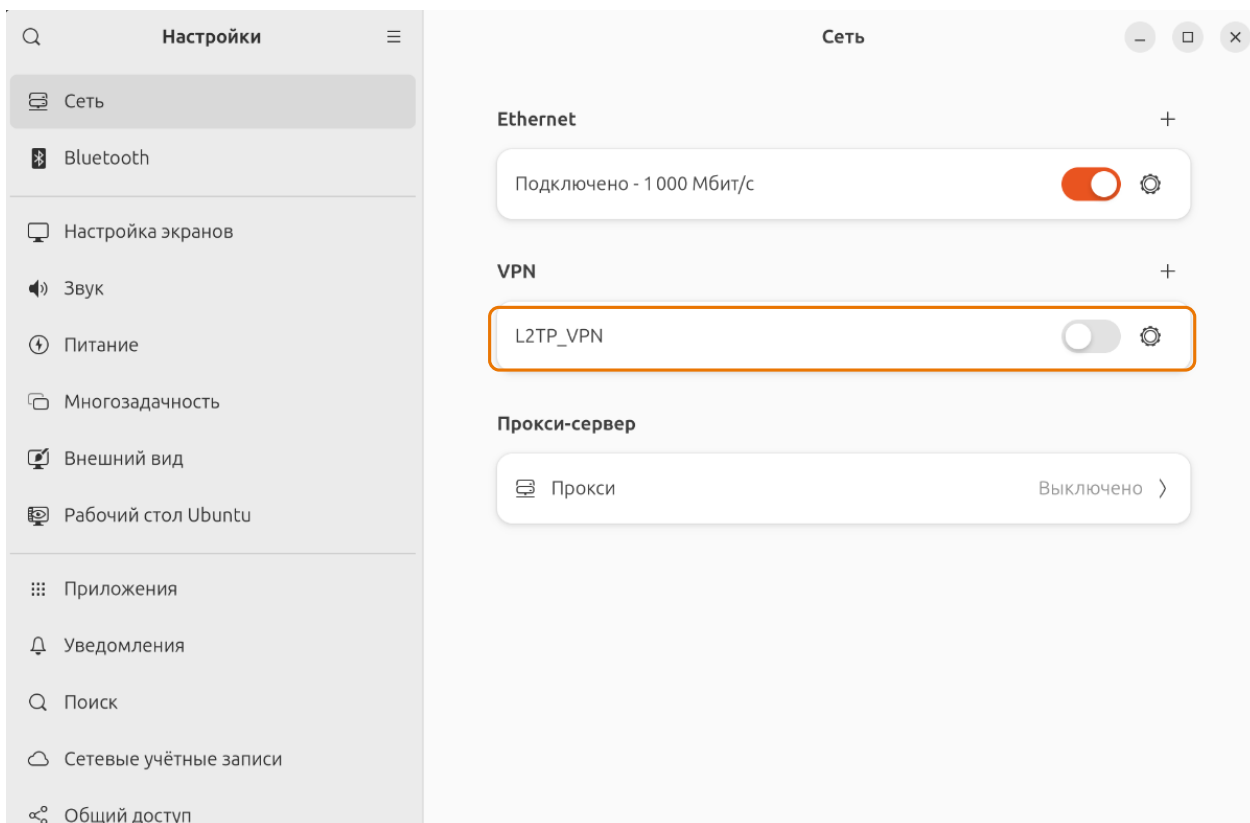
Нажать **Apply** для сохранения настроек PPP.

6. В окне настроек VPN нажать Применить для сохранения настроек соединения:



Настройка VPN-клиента завершена.

Для установления VPN-соединения нажмите кнопку включения созданного соединения VPN:



Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@thihichinnde							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user3 User 3 (testd.local/user3)	Сервер	Remote access VPN rule	14 мая 2024 г., 13:16 (51с)	172.30.250.2	203.0.113.10		aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий							
Сегодня (14 Май 2024 г.) Важность: Все Компоненты и события: Все Ещё Сброс Q Расширенный							
Узел	Время	Компонент	Тип события	Пользователь	IP источника	Модуль	Детали события
utmcore@thihichinnde	13:16:21	VPN	Подключение пользователя к VPN прошло успешно	user3 User 3 (testd.local/user3)	203.0.113.10	VPN сервер	Логин: user3@testd.local

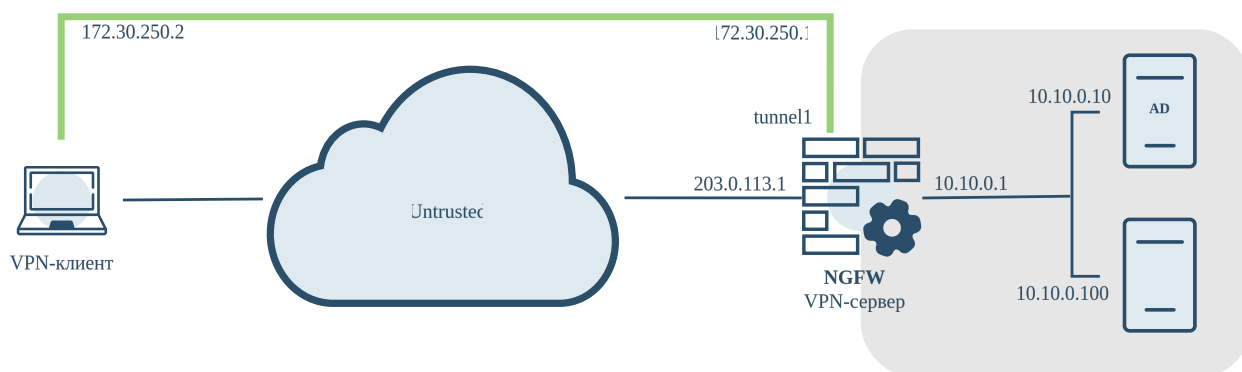
На стороне удаленного Linux-компьютера добавится ppp-адаптер, появятся маршрут в сеть виртуального адаптера. Хост (10.10.0.100) в сети офиса доступен:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:d5:0b:f6 brd ff:ff:ff:ff:ff:ff
inet 203.0.113.10/24 brd 203.0.113.255 scope global noprefixroute enp0s3
    valid_lft forever preferred_lft forever
9: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1400 qdisc pfifo_fast state UNKNOWN group default qlen 3
link/ppp
inet 172.30.250.2 peer 172.30.250.1/32 scope global ppp0
    valid_lft forever preferred_lft forever

$
$
$ ip rou
default dev ppp0 proto static scope link metric 50
default via 203.0.113.1 dev enp0s3 proto static metric 20100
172.30.250.1 dev ppp0 proto kernel scope link src 172.30.250.2
172.30.250.1 dev ppp0 proto kernel scope link src 172.30.250.2 metric 50
203.0.113.0/24 dev enp0s3 proto kernel scope link src 203.0.113.10 metric 100
$ ping 10.10.0.100
PING 10.10.0.100 (10.10.0.100) 56(84) bytes of data.
64 bytes from 10.10.0.100: icmp_seq=1 ttl=63 time=2.96 ms
64 bytes from 10.10.0.100: icmp_seq=2 ttl=63 time=4.17 ms
64 bytes from 10.10.0.100: icmp_seq=3 ttl=63 time=1.31 ms
64 bytes from 10.10.0.100: icmp_seq=4 ttl=63 time=2.78 ms
^C
--- 10.10.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4904ms
rtt min/avg/max/mdev = 1.305/2.804/4.169/1.016 ms
```

Пример настройки Remote access VPN с IPsec(IKEv2)

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:



В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя — в роли VPN-клиента.

Сначала необходимо настроить VPN-сервер, затем произвести настройки VPN-клиента на компьютере пользователя и инициировать подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки узла **NGFW** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы VPN и Подключение конечных устройств в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

Сертификаты				
Редактировать Показать Копировать Создать Импорт Экспорт Удалить				
Название	Назначение сертификата	Используется	Издатель	Субъект
root	Отсутствует		DOC	DOC
server	Digital signature		DOC	ug.testd.local

Создадим профиль клиентских сертификатов в веб-консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого необходимо перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя:

Профиль клиентского сертификата

Название:

Profile1

Описание:

Получать имя пользователя из:

Common-name

Subject altname email

Common-name

Principal name

Сертификаты УЦ

Добавить

Название	Издатель	Истекает
root	DOC	2026-12-05T10:45:40Z

Наверх

Выше

Низже

Вниз

Проверка отозванных сертификатов:

Не проверять

Таймаут проверки:

1

(в секундах)

Сохранить

Отмена

2. Создадим профиль аутентификации для VPN пользователей. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль аутентификации в домене testd.local через LDAP-коннектор:

Свойства профиля аутентификации

Общие

Методы аутентификации

+

Добавить

×

Удалить

↑

Выше

↓

Нижне

Название

Сервер LDAP/Active Directory: ldapcon

Сохранить

Отмена

Свойства коннектора LDAP

Настройки

Домены LDAP

Kerberos keytab

Пути поиска

Включено:

☒

Название:

ldapcon

Описание:

SSL:

☒ Использовать для соединений SSL

Доменное имя LDAP или IP-адрес:

10.10.0.10

Bind DN («логин»):

uid=ug,cn=users,cn=accounts,dc=testd,dc=local

Пароль:

.....

Проверить соединение

Сохранить

Отмена

Шаг 4.Создать профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создадим профиль безопасности, указав в настройках следующие ключевые параметры:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

Название: RA 1

Описание:

1. Протокол: IKEv2

Режим IKE: Основной

2. Тип идентификации: отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

3. Сертификат сервера: Server

4. Режим аутентификации: PKI

5. Профиль клиентского сертификата: Profile 1

Подсети для VPN

+ Добавить ✎ Редактировать ✕ Удалить

Локальная подсеть	Удалённая подсеть

Сохранить Отмена

1. **Протокол**. В данном примере для создания защищенного канала будет использоваться протокол IKEv2.
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере можно не указывать тип идентификации.
3. Указать **сертификат сервера**, импортированный ранее на [Share 3](#).
4. В качестве **режима аутентификации** выберем PKI.
5. Выберем профиль клиентского сертификата, созданный ранее на [Share 3](#).

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

+

Добавить

×

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+

Добавить

Редактировать

×

Удалить

Выше

Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

(в секундах)

Безопасность

+ Добавить

✎ Редактировать

✖ Удалить

⬆ Выше

⬆ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

Настройка VPN-адаптера

Общие

Сеть

1 Включено: ☒

2 Название: tunnel1

Описание:

Example VPN interface to be used in Remote Access VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for remote access

Профиль netflow: Не выбран

Алиас/Псевдоним:

Сохранить

Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel1).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В данном примере указывается зона VPN for Remote access.

Настройка VPN-адаптера

Общие Сеть

4 Режим: Статический

5 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
172.30.250.1	255.255.255.0

6

Сохранить Отмена

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.250.1, который задается в поле 6.

5. **MTU** — размер MTU в данном примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Remote access VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

3 Диапазон IP: 172.30.250.2-172.30.250.254

4 Маска: 255.255.255.0

5 ☒ Использовать системные DNS-серверы

Серверы DNS:

IP-адрес

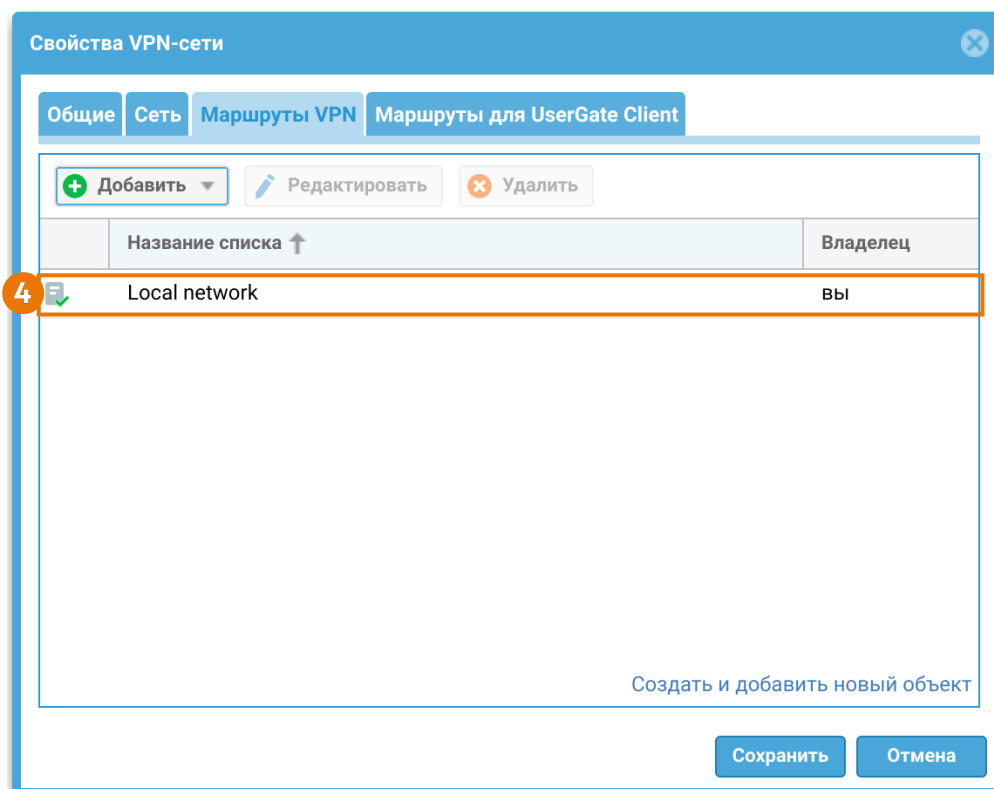
Добавить Редактировать Удалить

Сохранить Отмена

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.250.1), используемому совместно с данной сетью.

2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть офиса 10.10.0.0/24.

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

Свойства серверного правила VPN

Общие

Источник

Пользователи

Назначение

1 Включено: ☒

Название: RA VPN rule 1

Описание:

2 Профиль безопасности VPN: RA 1

3 Сеть VPN: Remote access VPN network

4 Профиль аутентификации: ldap_profile

URL инициализации TOTP

5 Интерфейс: tunnel1

Только для UserGate Client: ☐

Сохранить

Отмена

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (RA 1).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).

Свойства

Общие

Источник

Пользователи

Назначение

Зона источника

☐ Cluster
☐ DMZ
☐ Management
☐ Trusted
☐ Tunnel inspection zone
☒ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Адрес источника

+ Добавить

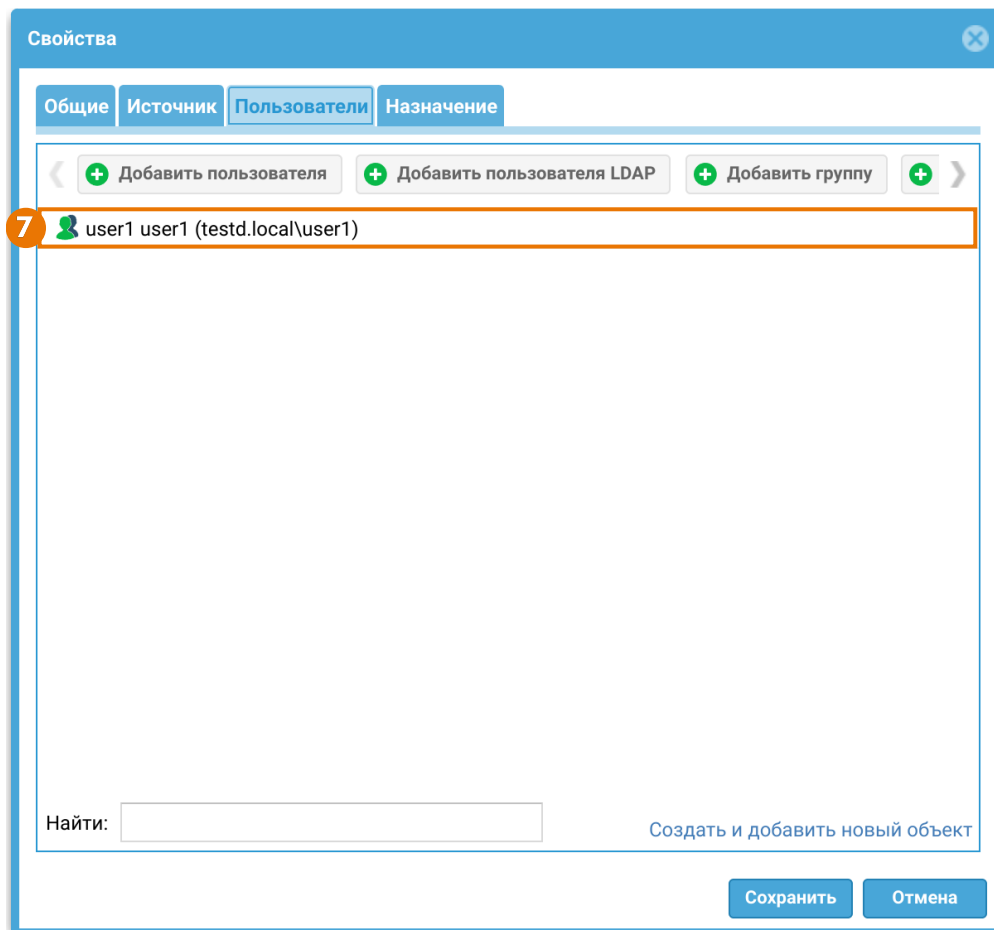
Редактировать

Название списка ↑	Владелец
Создать и добавить новый объект	

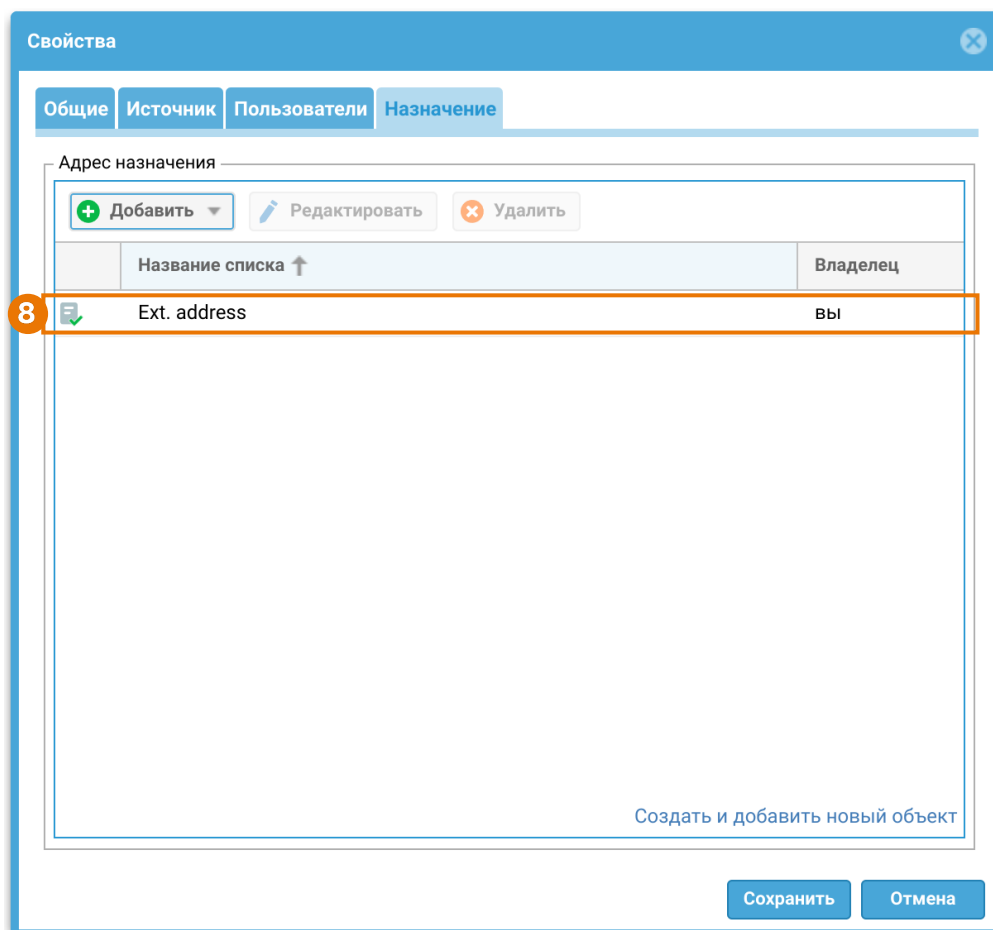
Сохранить

Отмена

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. Пользователи — доменные пользователи, которым разрешено пользоваться сервисом VPN.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

1. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**. По умолчанию оно не активно. Необходимо его включить.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь

трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

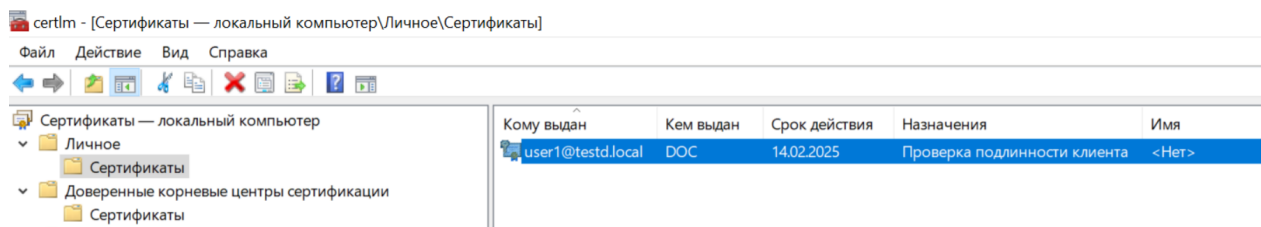
Настройка VPN-клиента

В данном примере рассмотрим настройку "нативных" клиентов для операционных систем Windows и Linux для удаленного VPN-подключения.

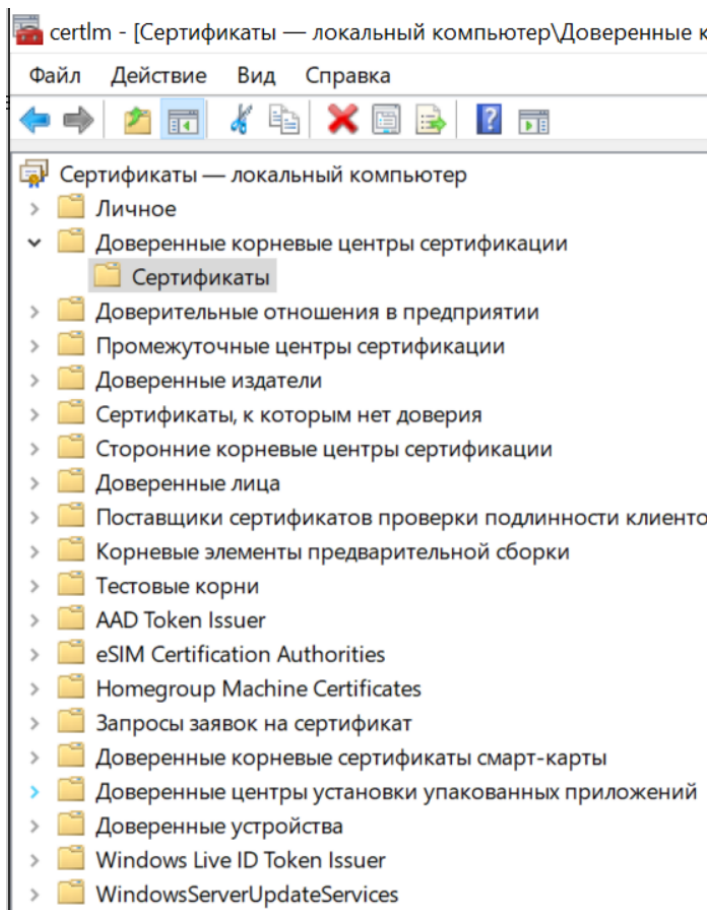
Встроенный VPN-клиент OS Windows

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Импортировать ранее созданный пользовательский сертификат в хранилище сертификатов компьютера в личную папку:

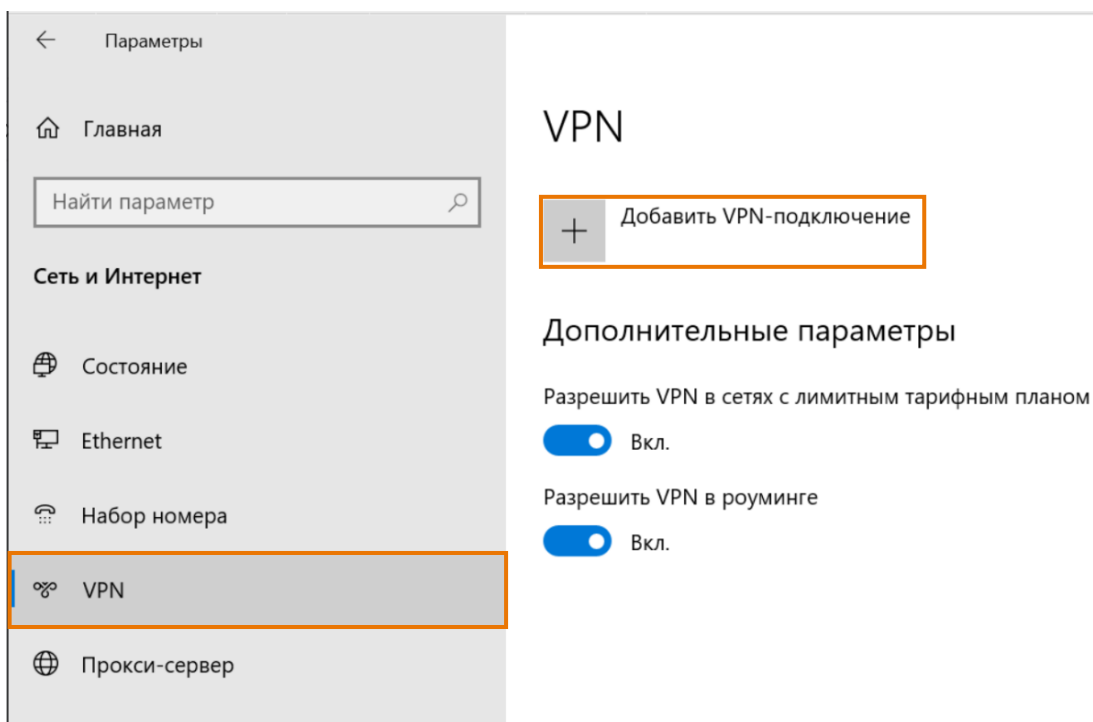


Сертификат корневого центра импортировать в раздел **Доверенные корневые центры сертификации**:



2. Кликнуть правой кнопкой мыши по значку сетевого подключения в трее и выбрать пункт **Открыть "Параметры сети и Интернет"**.

3. В появившемся окне **Параметры** выбрать пункт **VPN**, а затем нажать на пункт **Добавить VPN-подключение**:



4. В окне Добавить VPN-подключение настроить параметры подключения:

- В поле **Поставщик услуг VPN** выбрать **Windows (встроенные)**;
- В поле **Имя подключения** указать имя для этого подключения (IKEv2 VPN);
- В поле **Имя или адрес сервера** указать доменное имя NGFW (ug.testd.local);
- В поле **Тип VPN** выбрать **IKEv2**;
- В поле **Тип данных для входа** выбрать **Сертификат**;

Добавить VPN-подключение

Поставщик услуг VPN

Windows (встроенные) ▾

Имя подключения

IKEv2 VPN

Имя или адрес сервера

ug.testd.local

Тип VPN

IKEv2 ▾

Тип данных для входа

Сертификат ▾

Имя пользователя (необязательно)

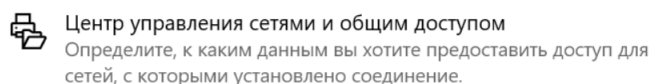
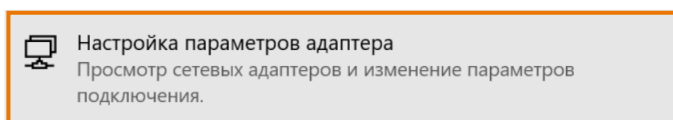
Пароль (необязательно)

☒ Запомнить мои данные для входа

Сохранить

5. Нажать кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.
6. В панели управления перейти в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выбрать пункт **Настройки параметров адаптера**:

Дополнительные сетевые параметры

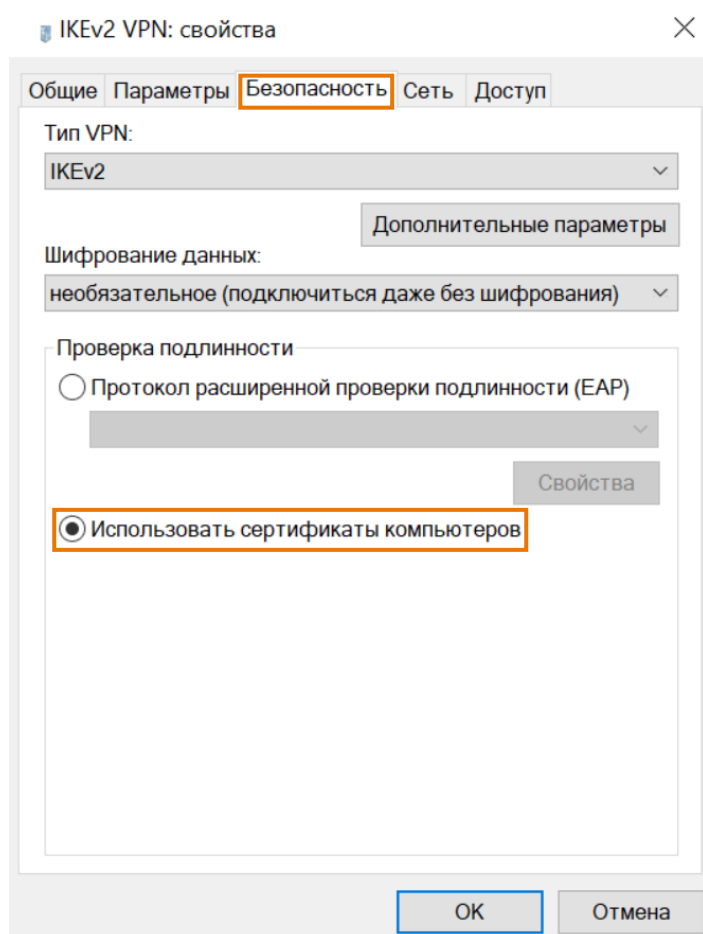


[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

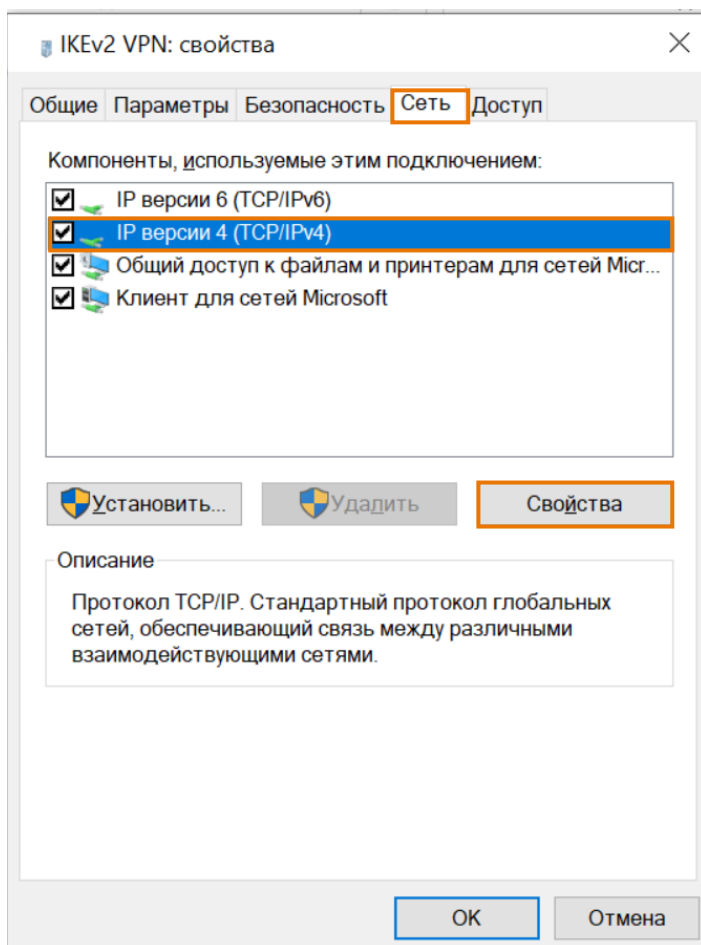
[Сброс сети](#)

7. Выбрать только что созданное сетевое подключение **IKEv2 VPN** и через меню правой кнопки мыши перейти в свойства этого подключения. В открывшемся окне перейти во вкладку **Безопасность**:

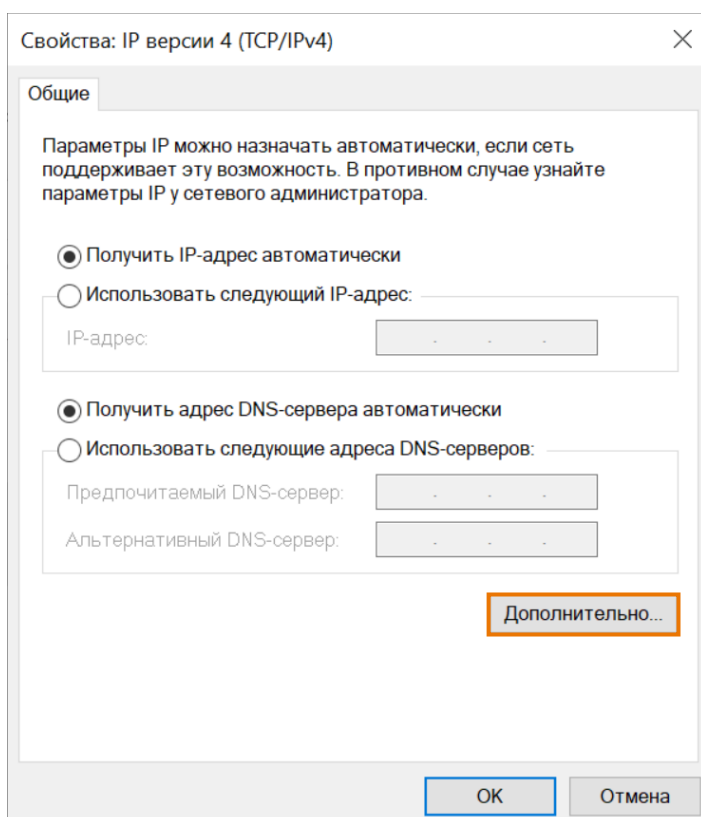


Выбрать пункт **Использовать сертификаты компьютеров**.

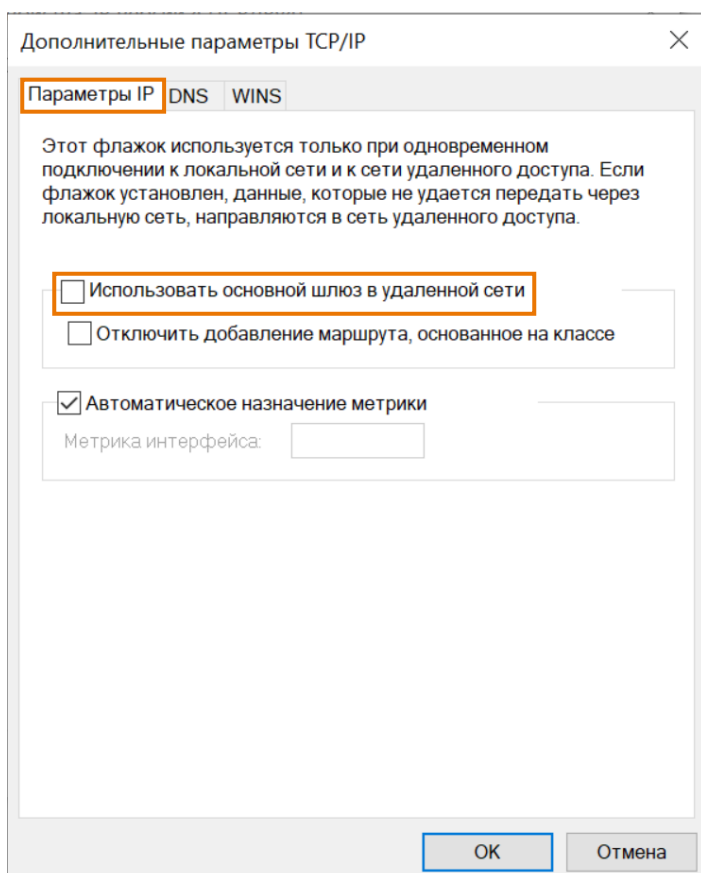
Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** открыть свойства **IP версии 4 (TCP/IPv4)**:



Нажать **Дополнительно** в настройках общих параметров IP:



Убрать флажок в поле **Использовать основной шлюз в удаленной сети**:



8. Сохранить настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **IKEv2 VPN** и нажмите кнопку **Подключиться**.

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@sthattreshat							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	GeO IP	Шифрование
user1 user1 (testd.local\user1)	Сервер	RA VPN rule 1	22 августа 2024 г., 16:13 (2м 27с)	172.30.250.2	203.0.113.11		aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий							
date >= 2024-08-22T00:00:00 AND date <= 2024-08-22T23:59:59 AND component = 'vpn'							
Узел	Время ↓	Компонент	Тип события	Пользователь	IP источника	Модуль	Детали события
utmcore@sthattreshat	16:13:20	VPN	Подключение пользователя к VPN прошло успешно	user1 user1 (testd.local\user1)	203.0.113.11	VPN сервер	Логин: user1@testd.local

На стороне удаленного Windows-компьютера добавится rppr-адаптер IKEv2 VPN, хост (10.10.0.100) в сети офиса доступен:


```

C:\Users\> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 203.0.113.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 203.0.113.1

PPP adapter IKEv2 VPN:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 172.30.250.2
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :

C:\Users\> ping 10.10.0.100

Pinging 10.10.0.100 with 32 bytes of data:
Reply from 10.10.0.100: bytes=32 time=1ms TTL=63
Reply from 10.10.0.100: bytes=32 time=2ms TTL=63
Reply from 10.10.0.100: bytes=32 time=2ms TTL=63
Reply from 10.10.0.100: bytes=32 time=3ms TTL=63

Ping statistics for 10.10.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

```

IKEv2 VPN-клиент (strongswan) для OS Linux

Рассмотрим настройку IKEv2 VPN-клиента для Linux на примере OS Ubuntu.

Для начала необходимо установить дополнительные пакеты для работы с IKEv2 VPN:

```

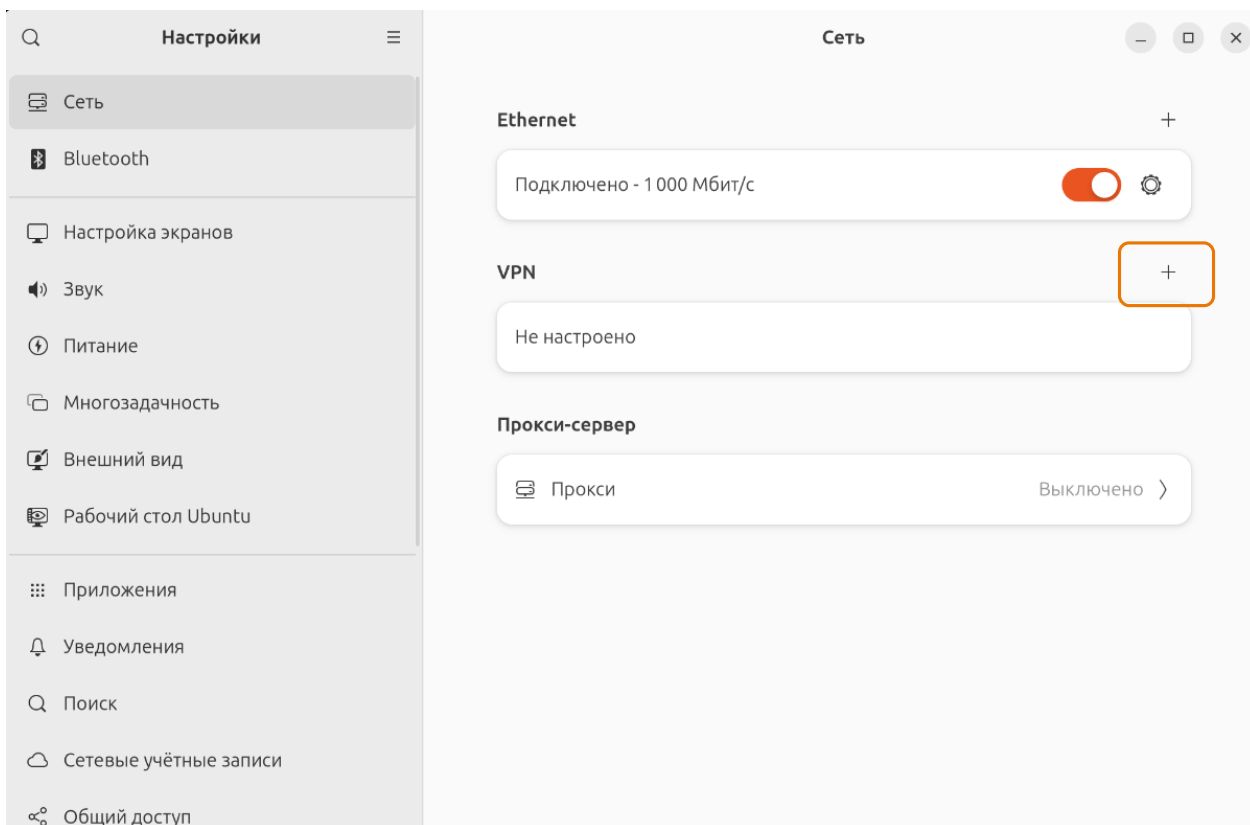
sudo apt update && sudo apt upgrade

sudo apt install network-manager-strongswan libcharon-extra-plugins

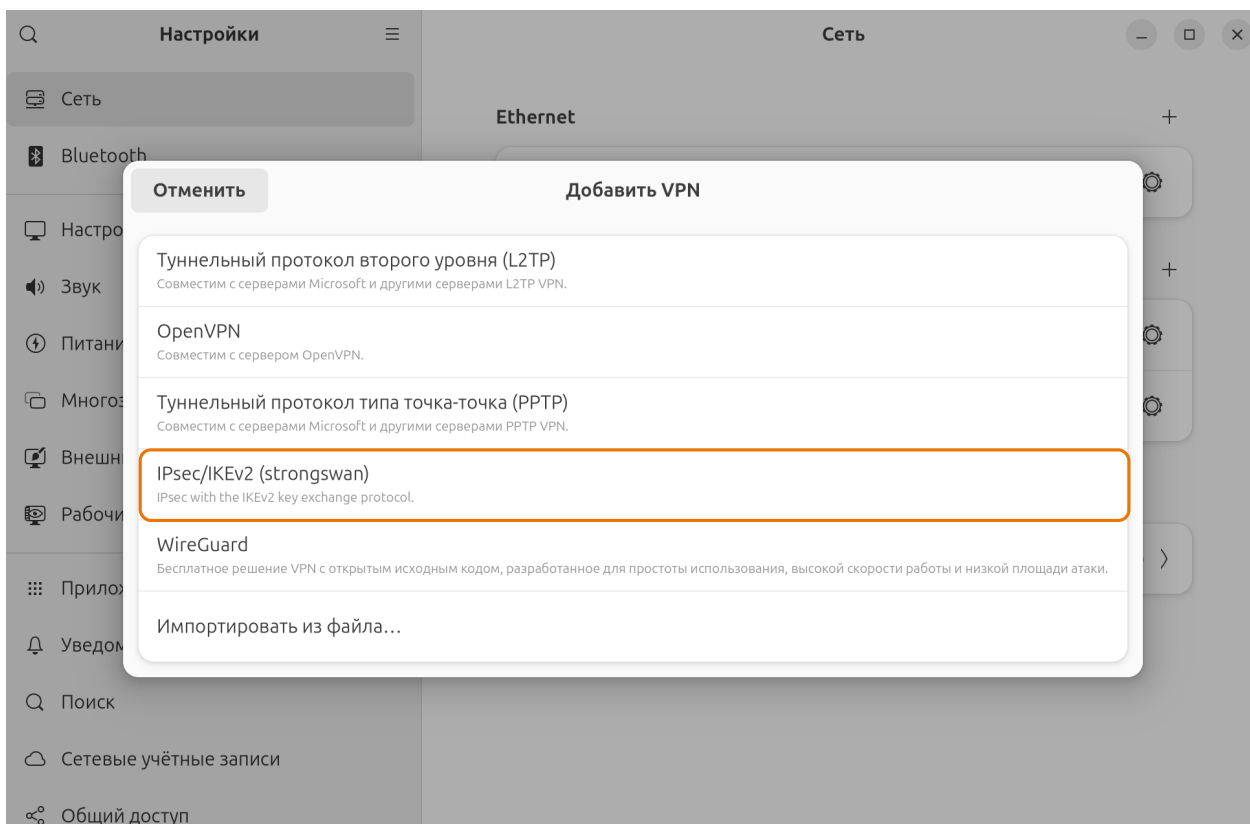
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



2. Выбрать из списка опцию **IPsec/IKEv2 (strongswan)**:



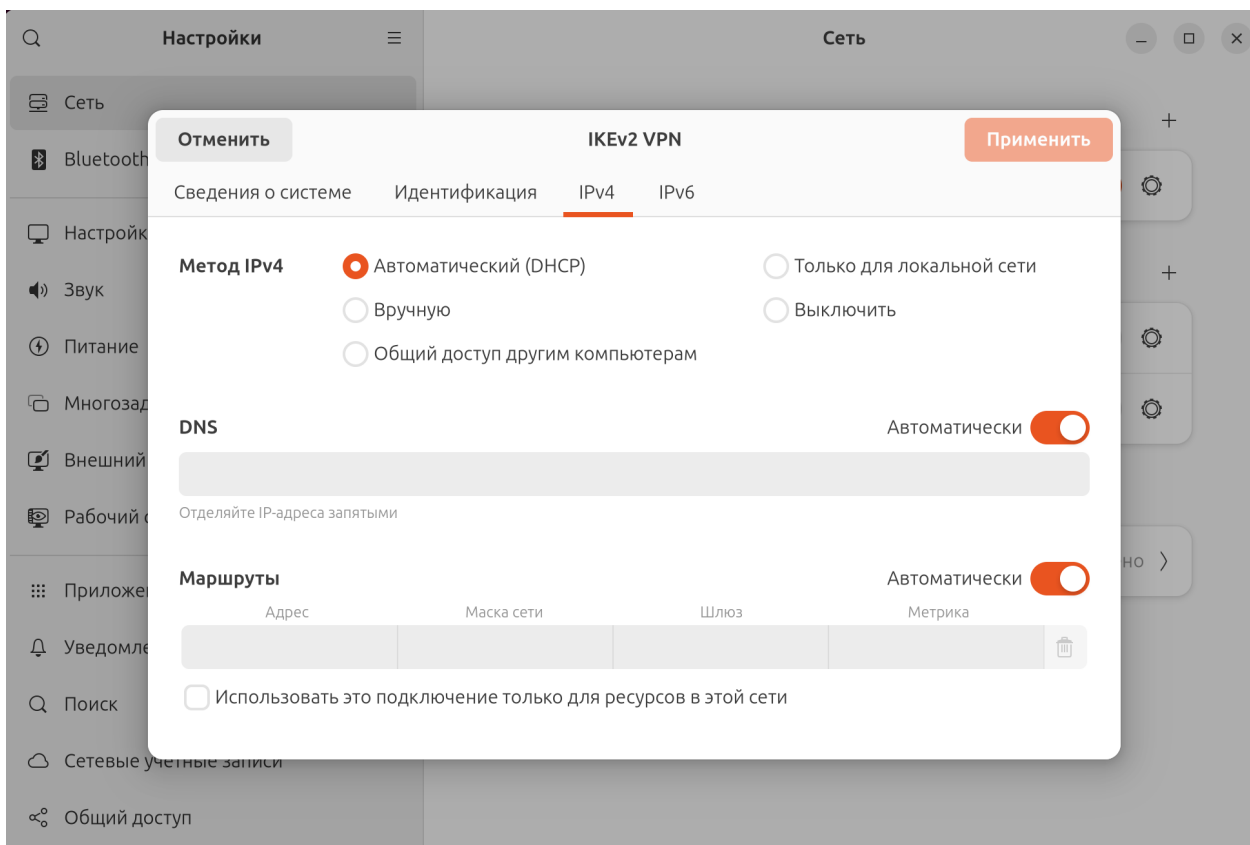
3. В настройках VPN перейти на вкладку **Идентификация**. Указать название соединения, метод аутентификации (Certificate), способ аутентификации

(Certificate/private key), указать заранее созданные файлы клиентского сертификата и ключа, параметры соединения:

The screenshot shows the 'IKEv2 VPN' configuration window. The 'Идентификация' (Identification) tab is selected. The configuration is as follows:

- Name:** IKEv2 VPN
- Server:**
 - Address: ug.testd.local
 - Certificate: (None)
 - Identity: (Defaults to address or certificate subject)
- Client:**
 - Authentication: Certificate
 - Certificate: Certificate/private key
 - Certificate file: client-cert.crt
 - Private key: client-key.pem
 - Identity: (Defaults to username, certificate subject or IP address)
 - Username: (empty)
 - Password: (Use icon to change password storage policy)
 - ☐ Show password
- Options:**
 - ☒ Request an inner IP address
 - ☒ Enforce UDP encapsulation
 - ☐ Use IP compression
- Server port:** (Defaults to UDP 500/4500)

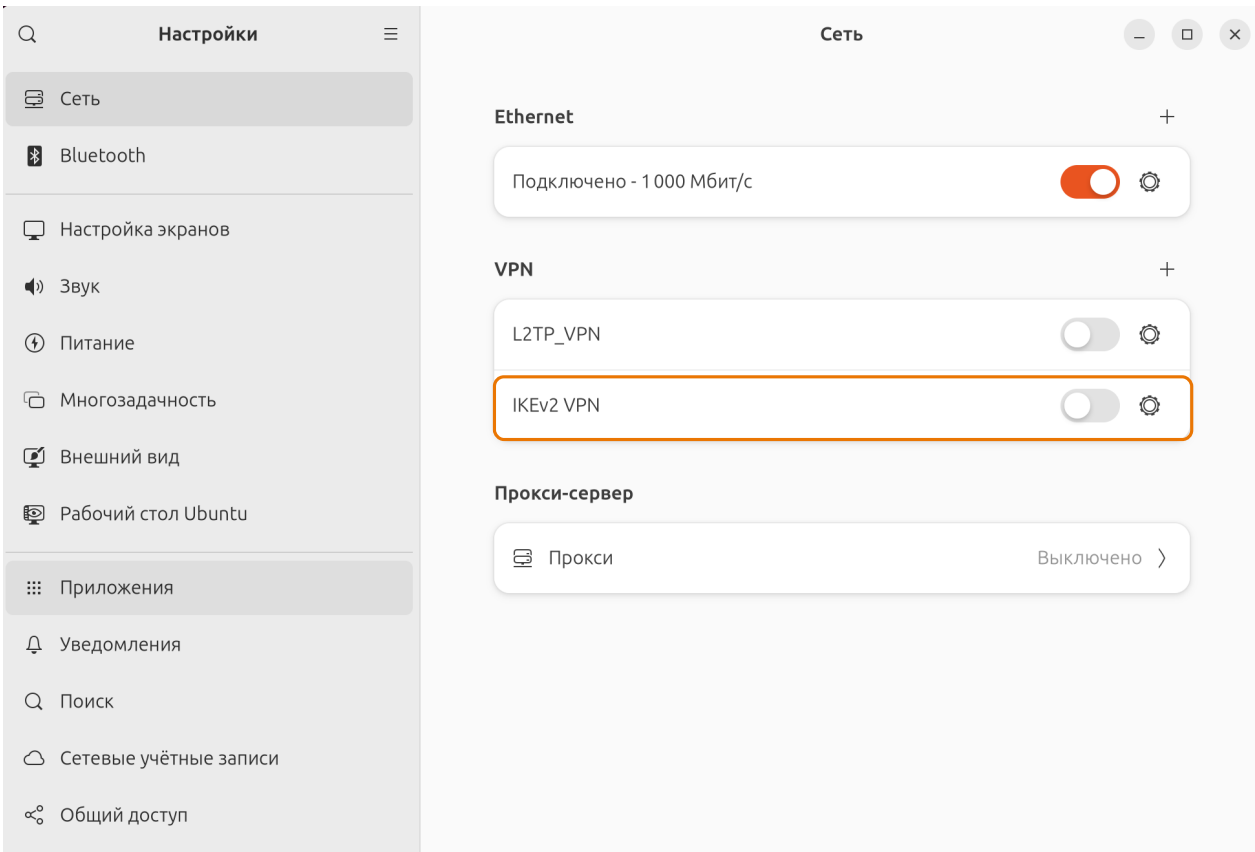
4. На вкладке IPv4 оставить указанный по умолчанию метод получения адресов по DHCP:



5. В системе должен присутствовать корневой сертификат. При необходимости нужно поместить его в системный раздел `/etc/ssl/certs/`.

Настройка VPN-клиента завершена.

Для установления VPN-соединения нажать кнопку включения созданного соединения VPN:



Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@sthattreshat							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный ...	IP адрес	GeO IP	Шифрование
user1 user1 (testd.local/user1)	Сервер	RA VPN rule 1	26 августа 2024 г., 14:34 (3...	172.30.250.2	203.0.113.11	?	aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий							
date >= 2024-08-26T00:00:00 AND date <= 2024-08-26T23:59:59 AND component = 'vpn'							
Узел	Время ↓	Компонент	Тип события	Пользователь	IP источника	Модуль	Детали события
utmcore@sthattreshat	14:34:45	VPN	Подключение пользователя к VPN прошло успешно	user1 user1 (testd.local/user1)	203.0.113.11	VPN сервер	Логин: user1@testd.local

На стороне удаленного Linux-компьютера добавится виртуальный адаптер, хост (10.10.0.100) в сети офиса доступен:

```

:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet 172.30.250.2/32 scope global lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d9:0a:07 brd ff:ff:ff:ff:ff:ff
    inet 203.0.113.12/24 brd 203.0.113.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
14: nm-xfrm-1955498@NONE: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 172.30.250.2/32 scope global noprefixroute nm-xfrm-1955498
        valid_lft forever preferred_lft forever
    inet6 fe80::6141:968b:2ce5:5035/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
:/$ ping 10.10.0.100
PING 10.10.0.100 (10.10.0.100) 56(84) bytes of data.
64 bytes from 10.10.0.100: icmp_seq=1 ttl=63 time=3.23 ms
64 bytes from 10.10.0.100: icmp_seq=2 ttl=63 time=3.22 ms
64 bytes from 10.10.0.100: icmp_seq=3 ttl=63 time=1.57 ms
64 bytes from 10.10.0.100: icmp_seq=4 ttl=63 time=1.93 ms
^C
--- 10.10.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 1.574/2.486/3.227/0.745 ms

```

Приложение

Для частного случая, когда в среде OS Windows необходимо в явном виде выбирать один из нескольких имеющихся в хранилище пользователя (Current User) сертификатов, подходит следующее решение:

На VPN-сервере

UserGate NGFW начиная с релиза ПО 7.2.0 поддерживает метод аутентификации EAP TLS. Необходимо в настройках профиля безопасности VPN (см. [Шар 4](#) в настройках VPN-сервера) указать в поле режима аутентификации: **AAA**.

На VPN-клиенте

На [шаре 7](#) настройки встроенного VPN-клиента OS Windows сделать следующую конфигурацию:

- В настройках параметров адаптера через меню правой кнопки мыши перейти в свойства созданного подключения (в данном примере это подключение с названием **IKv2 VPN**). В открывшемся окне перейти во вкладку **Безопасность**:

В разделе **Проверка подлинности** выбрать **Протокол расширенной проверки подлинности (EAP)** → **Microsoft смарт-карта или иной сертификат**.

- В свойствах выбранного метода проверки подлинности выбрать опцию **Использовать сертификат на этом компьютере** и поставить флажок **Использовать для подключения другое имя пользователя**:

На контроллере домена

Настроить NPS для новой политики:

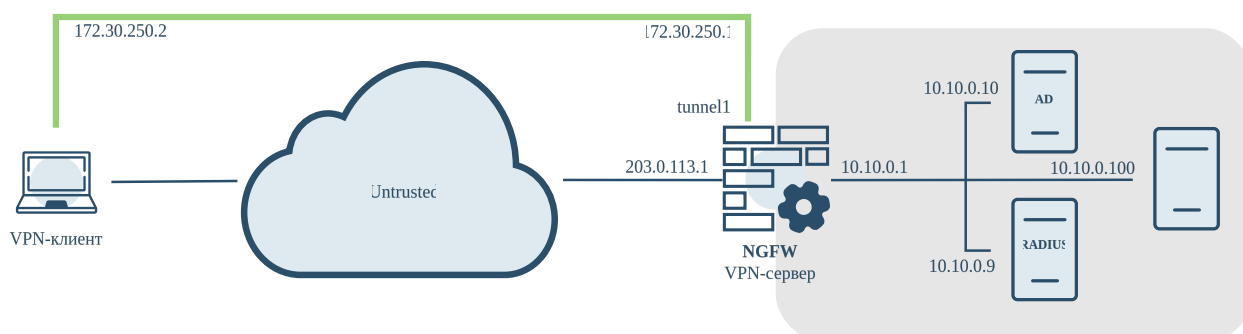
Остальные шаги настройки [VPN-сервера](#) и [встроенного VPN-клиента OS Windows](#) аналогичны рассмотренным ранее в этой статье.

При установлении VPN-соединения со стороны клиента кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите сконфигурированное VPN-соединение (в данном примере соединение с названием **IKEv2 VPN**) и нажмите кнопку **Подключиться**:

Появится опция выбора сертификата из хранилища пользователя:

Пример настройки Remote access VPN с IPsec(IKEv2) с аутентификацией через EAP для OS Linux

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:



В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя с OS Linux — в роли VPN-клиента.

Сначала необходимо [настроить VPN-сервер](#), затем произвести [настройку VPN-клиента](#) на компьютере пользователя и инициировать подключение к VPN-серверу.

Пример настройки RADIUS-сервера, используемого в рассматриваемом методе аутентификации, приведен в [Приложении](#).

Настройка VPN-сервера

Для настройки узла **NGFW** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы VPN и Подключение конечных устройств в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

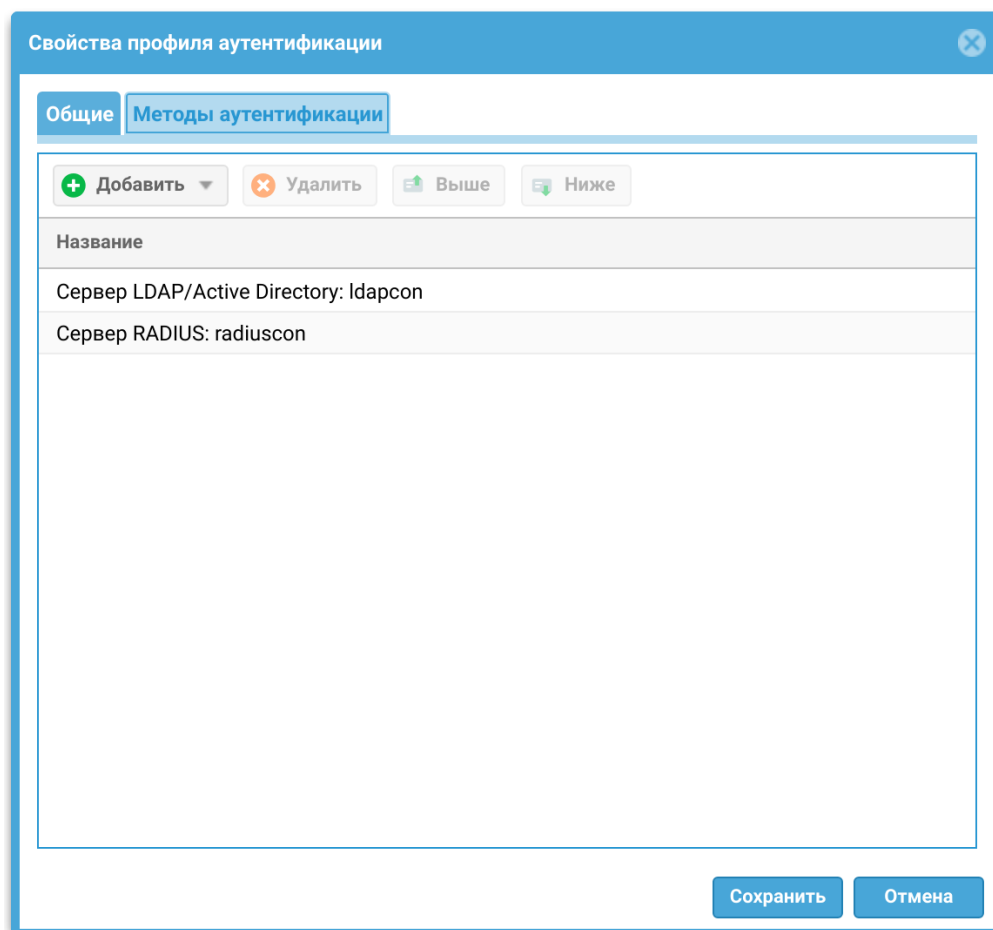
Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

Сертификаты				
✎ Редактировать 👁 Показать 📋 Копировать ➕ Создать ▾ 📁 Импорт 📄 Экспорт ▾ ✖ Удалить 🔄				
Название	Назначение сертификата	Используется	Издатель	Субъект
👤 root	Отсутствует		DOC	DOC
🔑 server	Digital signature		DOC	ug.testd.local

2. Создадим профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль, содержащий в качестве методов аутентификации LDAP-коннектор (ldapcon) и RADIUS-сервер (radiuscon):



Настройка LDAP-коннектора:

Свойства коннектора LDAP

Настройки

Домены LDAP

Kerberos keytab

Пути поиска

Включено:

☒

Название:

ldapcon

Описание:

SSL:

☒ Использовать для соединений SSL

Доменное имя LDAP или IP-адрес:

10.10.0.10

Bind DN («логин»):

uid=ug,cn=users,cn=accounts,dc=testd,dc=local

Пароль:

.....

Проверить соединение

Сохранить

Отмена

Настройка RADIUS-сервера:

Свойства RADIUS-сервера

Включено: ☒

Имя сервера:

Описание:

Секрет:

Адреса

+ Добавить

✎ Редактировать

✖ Удалить

Хост	Порт
10.10.0.9	1812

Сохранить

Отмена

Шаг 4.Создать профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создадим профиль безопасности, указав в настройках следующие ключевые параметры:

Свойства серверного профиля безопасности

Общие Фаза 1 Фаза 2

Название: RA 2

Описание:

1 Протокол: IKEv2

Режим IKE: Основной

2 Тип идентификации: отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

3 Сертификат сервера: Server

4 Режим аутентификации: AAA

Профиль клиентского сертификата: Не выбран профиль клиентского сертификата

Подсети для VPN

+ Добавить ✎ Редактировать ✕ Удалить

Локальная подсеть	Удалённая подсеть

Сохранить Отмена

1. **Протокол.** В данном примере для создания защищенного канала будет использоваться протокол IKEv2.
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере можно не указывать тип идентификации.
3. Указать **сертификат сервера**, импортированный ранее на [Share 3](#).
4. В качестве **режима аутентификации** выберем AAA.

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле по умолчанию:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Dead peer detection:

Отключена

60

(в сек)

Неудачных попыток:

5

Diffie-Hellman группы

+ Добавить

✕ Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+ Добавить

✎ Редактировать

✕ Удалить

⬆ Выше

⬇ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

556

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

12

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

4500

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

(в секундах)

Безопасность

+ Добавить

✎ Редактировать

✖ Удалить

⬆ Выше

⬇ Ниже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

Настройка VPN-адаптера

Общие

Сеть

1 Включено: ☒

2 Название: tunnel1

Описание:

Example VPN interface to be used in Remote Access VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

3 Зона: VPN for remote access

Профиль netflow: Не выбран

Алиас/Псевдоним:

Сохранить

Отмена

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel1).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В данном примере указывается зона VPN for Remote access.

Настройка VPN-адаптера

Общие Сеть

4 Режим: Статический

5 MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
6 172.30.250.1	255.255.255.0

Сохранить Отмена

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.250.1, который задается в поле 6.

5. **MTU** — размер MTU в данном примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Remote access VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

3 Диапазон IP: 172.30.250.2-172.30.250.254

4 Маска: 255.255.255.0

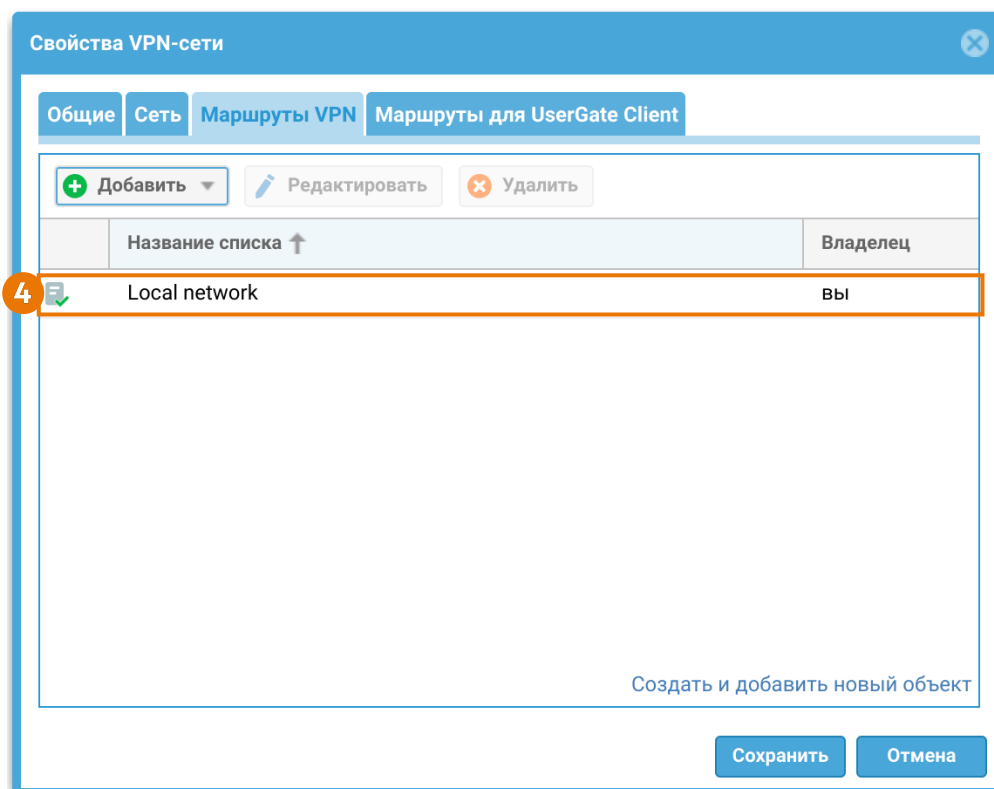
5 ☒ Использовать системные DNS-серверы

Серверы DNS:

IP-адрес	Действия
	Добавить Редактировать Удалить

Сохранить Отмена

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.250.1), используемому совместно с данной сетью.
2. **Маска** сети VPN.
3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть офиса 10.10.0.0/24.

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

Свойства серверного правила VPN

Общие | Источник | Пользователи | Назначение

Включено: ☒

1 Название: RA VPN rule 2

Описание:

2 Профиль безопасности VPN: RA 2

3 Сеть VPN: Remote access VPN network

4 Профиль аутентификации: profile2 URL инициализации TOTP

5 Интерфейс: tunnel1

Только для UserGate Client: ☐

Сохранить Отмена

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (RA 2).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).

Свойства

Общие

Источник

Пользователи

Назначение

Зона источника

☐ Cluster
☐ DMZ
☐ Management
☐ Trusted
☐ Tunnel inspection zone
☒ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается «любая зона»

Создать и добавить новый объект

Адрес источника

+ Добавить

✎ Редактировать

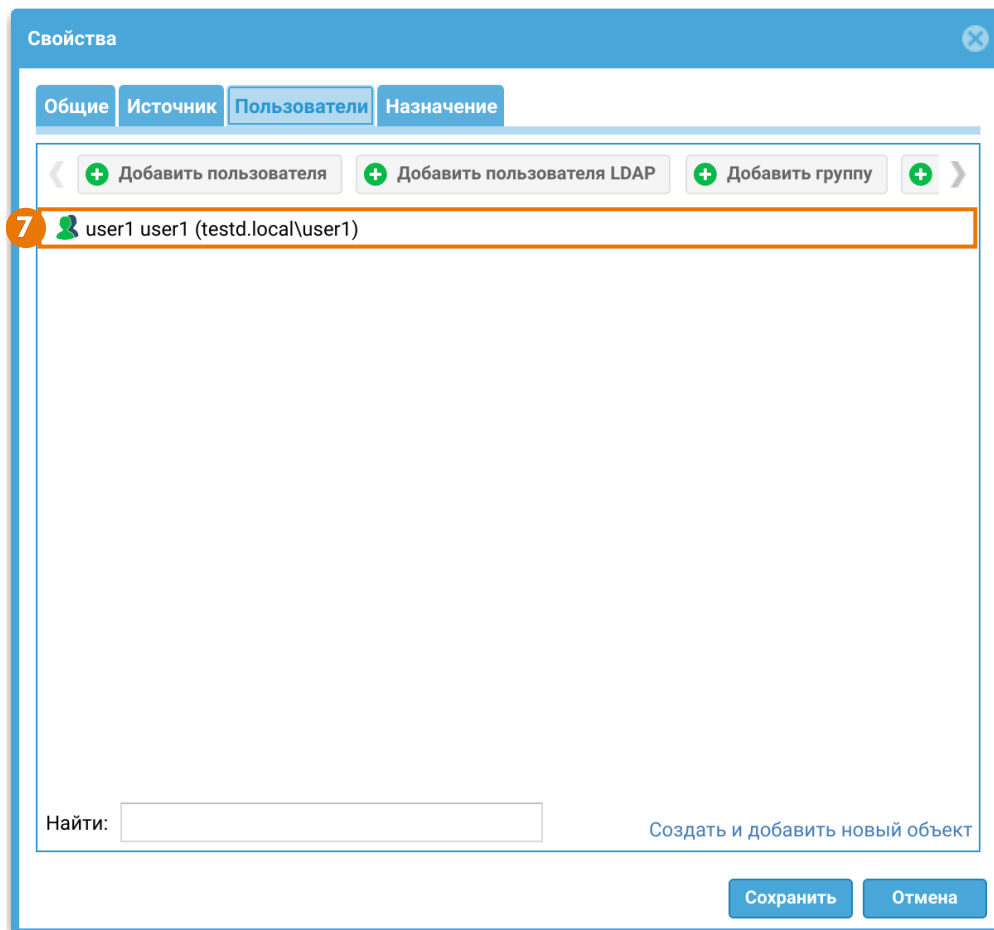
Название списка ↑	Владелец
Создать и добавить новый объект	

Сохранить

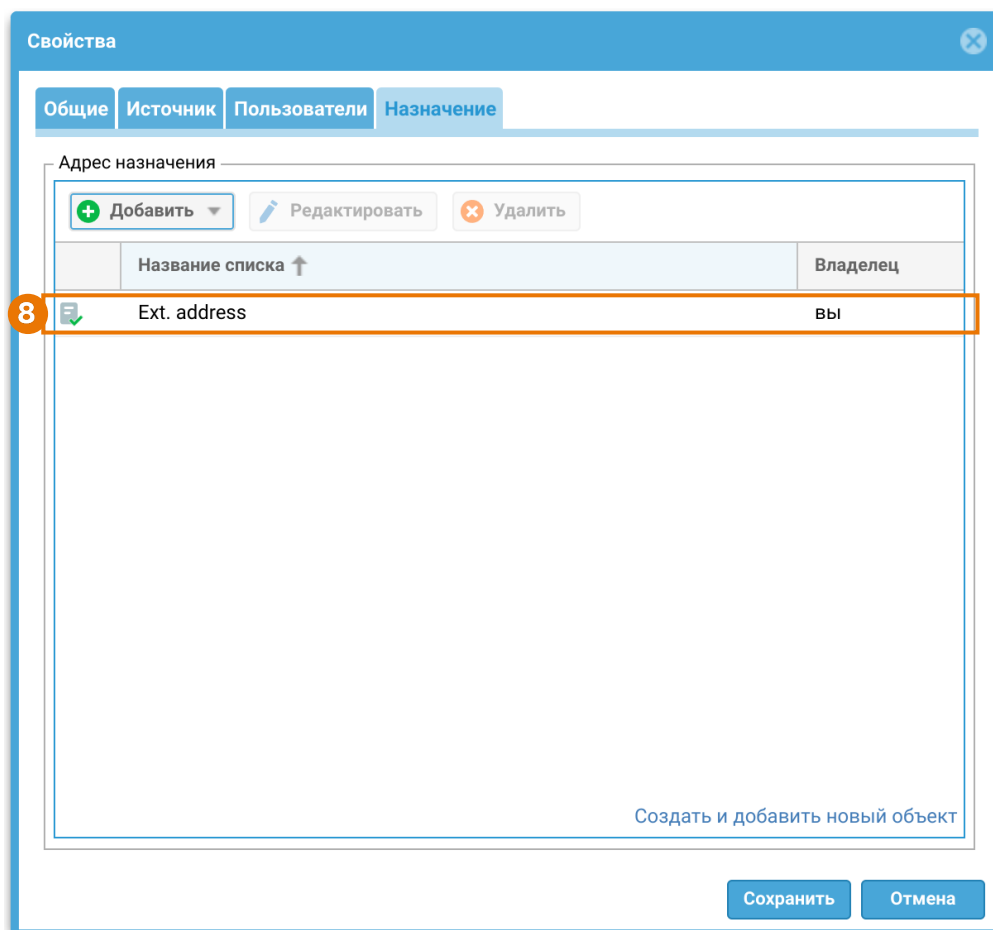
Отмена

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.

563



7. Пользователи — доменные пользователи, которым разрешено пользоваться сервисом VPN.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

1. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**. По умолчанию оно не активно. Необходимо его включить.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь

трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

В данном примере рассмотрим настройку VPN-клиента strongswan на операционной системе Ubuntu.

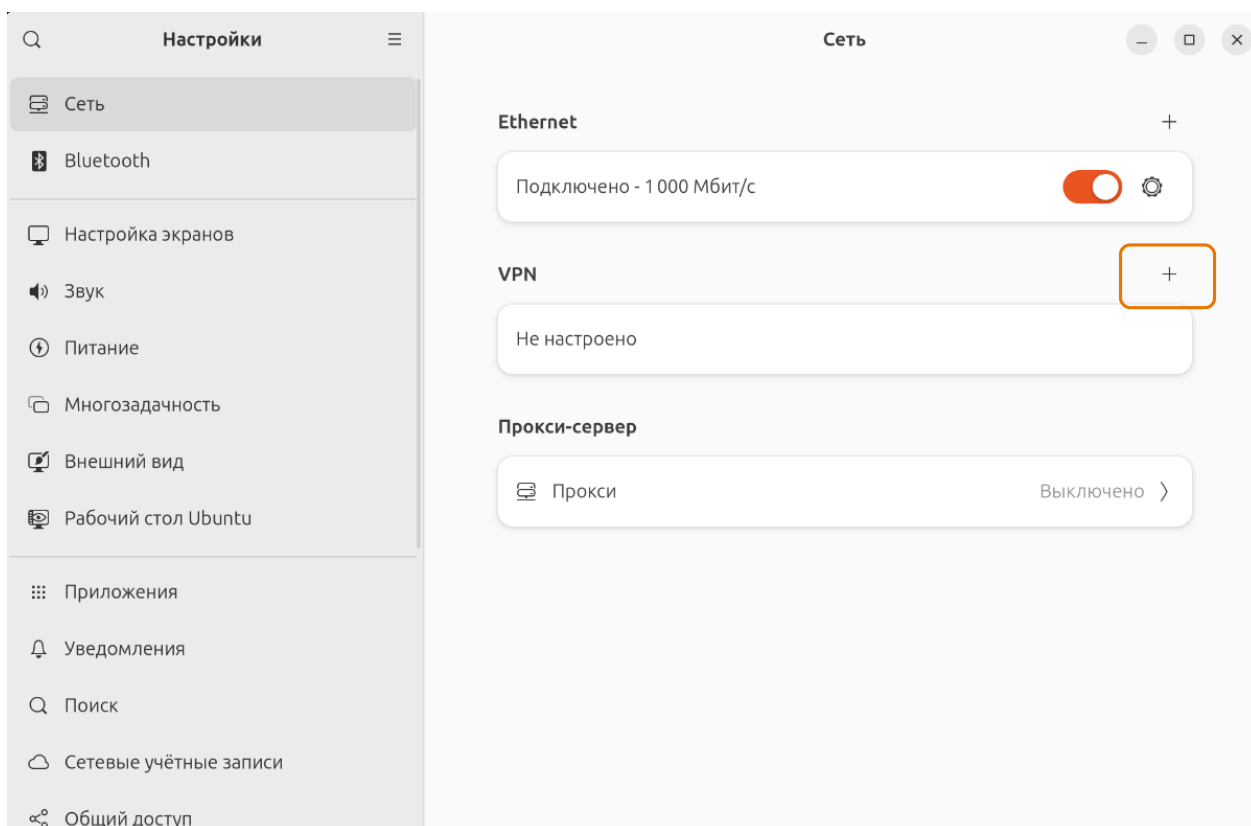
Для начала необходимо установить дополнительные пакеты для работы с IKEv2 VPN:

```
sudo apt update && sudo apt upgrade
```

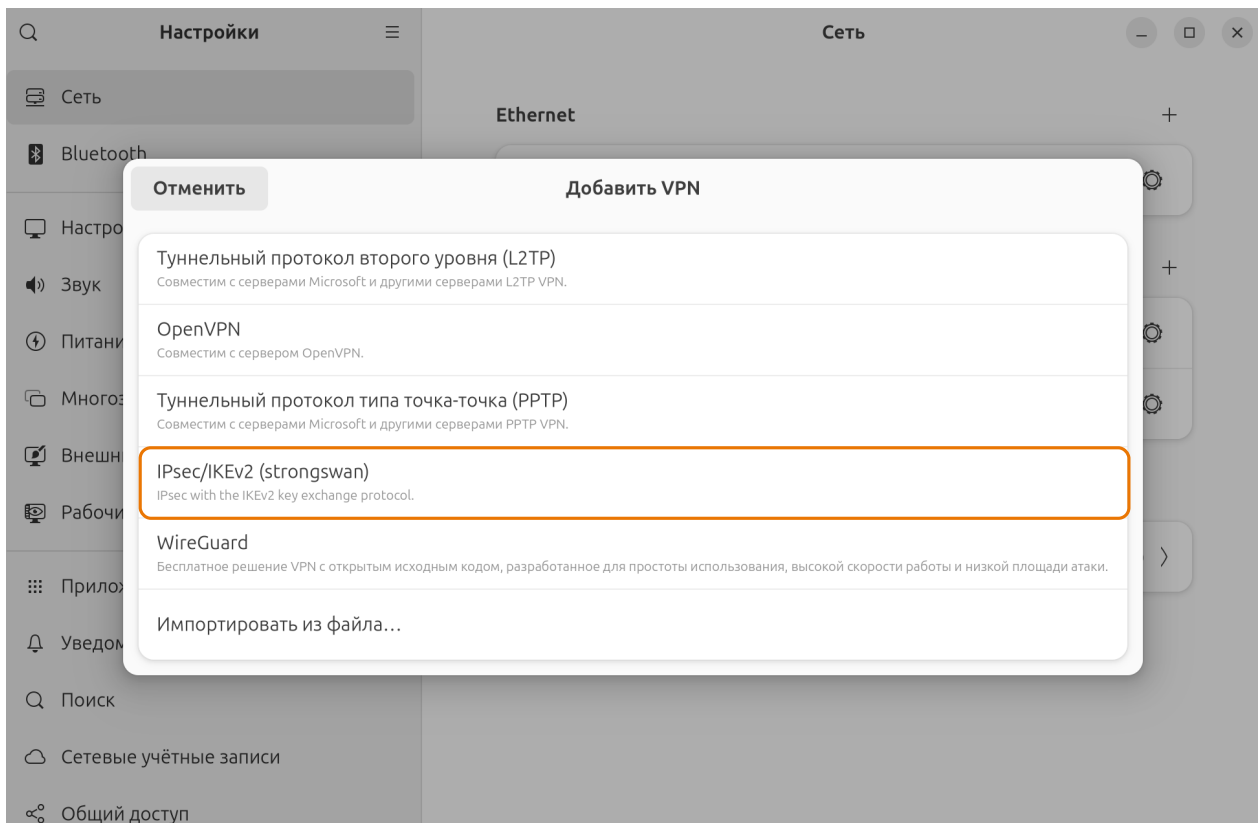
```
sudo apt install network-manager-strongswan libcharon-extra-plugins
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

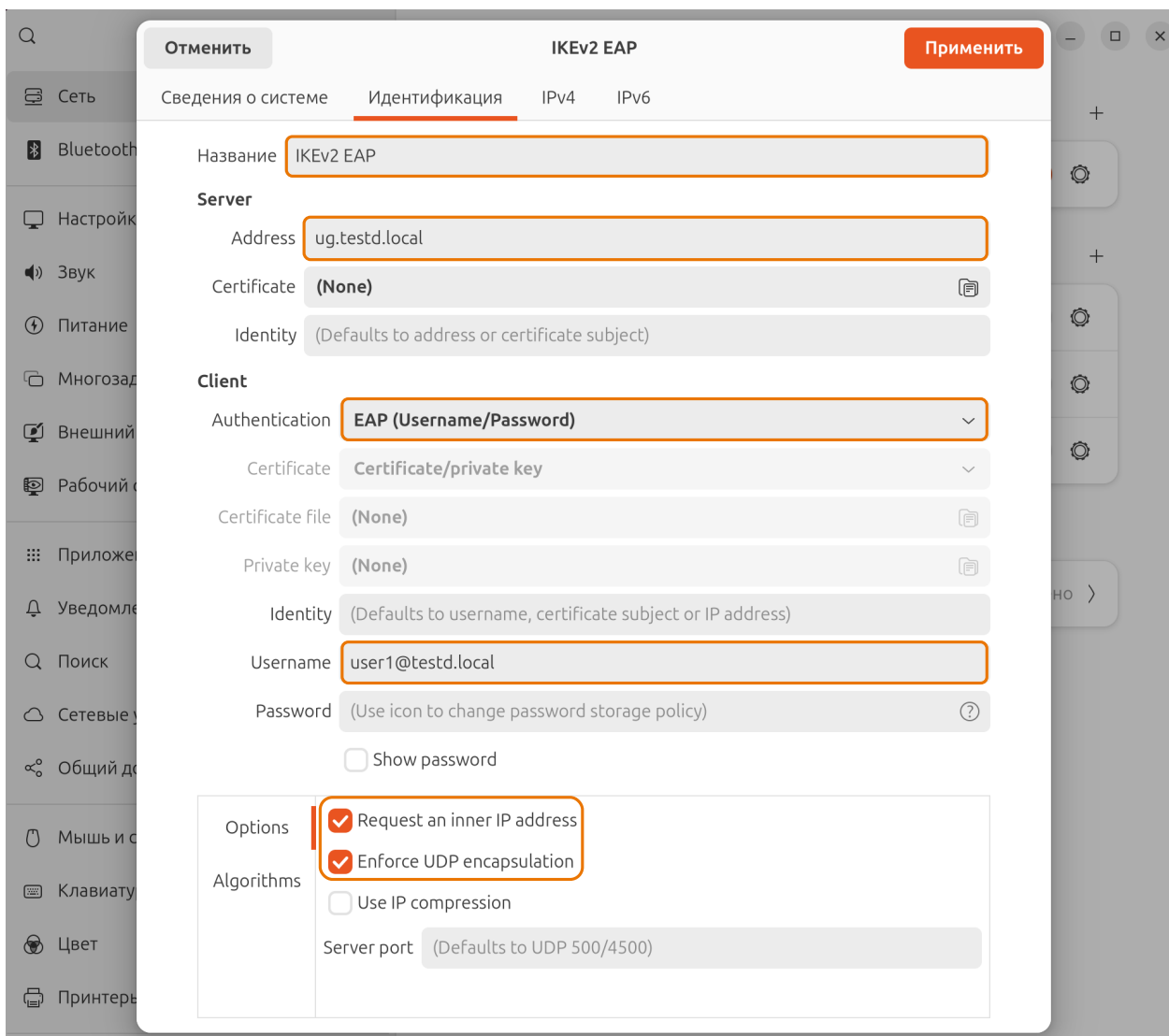
1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



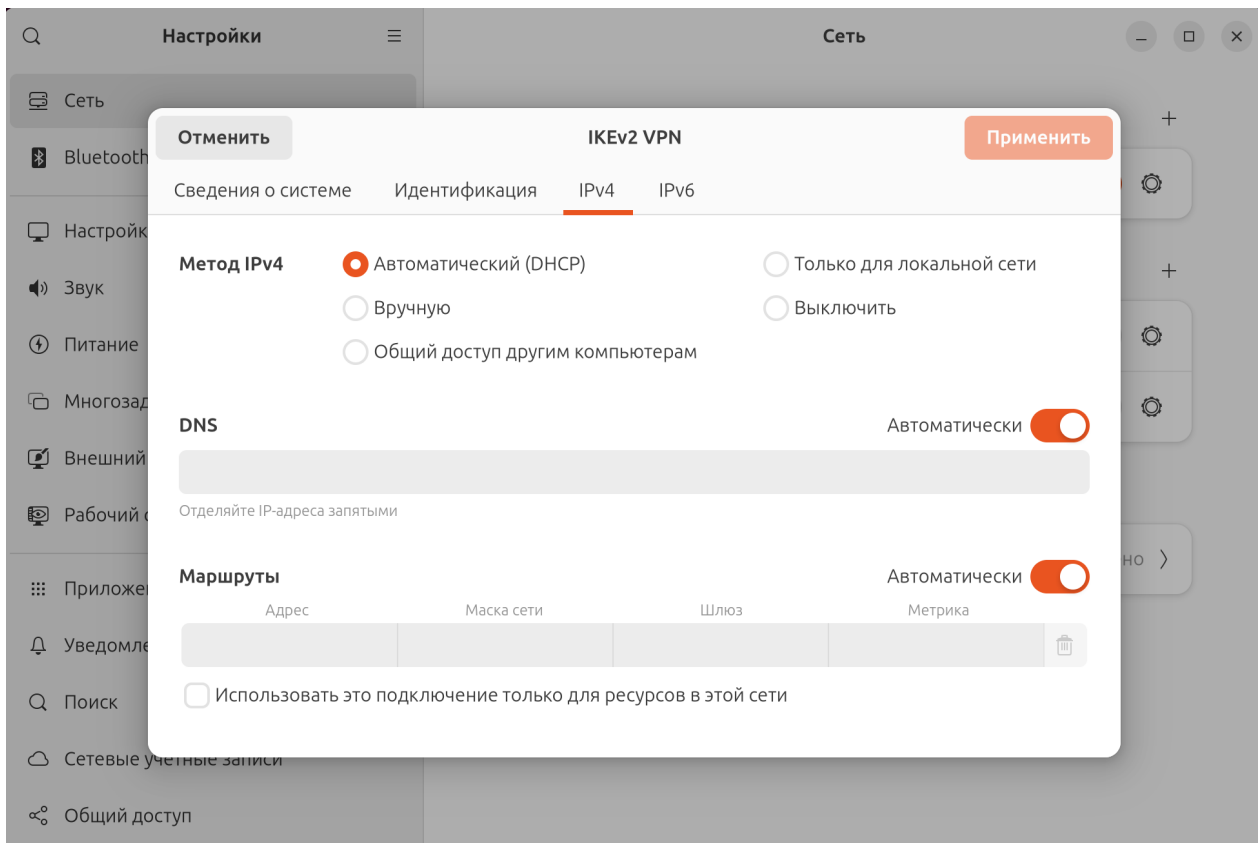
2. Выбрать из списка опцию **IPsec/IKEv2 (strongswan)**:



3. В настройках VPN перейти на вкладку **Идентификация**. Указать название соединения, имя сервера, метод аутентификации, указать имя пользователя, параметры соединения:



4. На вкладке IPv4 оставить указанный по умолчанию метод получения адресов по DHCP:



5. В системе должен присутствовать корневой сертификат. При необходимости нужно поместить его в системный раздел `/etc/ssl/certs/`.

6. Так.как в данном примере используется аутентификация с методом EAP MSCHAPv2 необходимо проверить настройки в файле `/etc/strongswan.conf` (должны быть отключены `eap-peap`, `eap-md5`, `eap-gtc`):

```
# strongswan.conf - strongSwan configuration file
#
# Refer to the strongswan.conf(5) manpage for details
#
# Configuration changes should be made in the included files

charon {
    load_modular = yes
    plugins {
        include strongswan.d/charon/*.conf
    }
}

charon-nm {
```

```

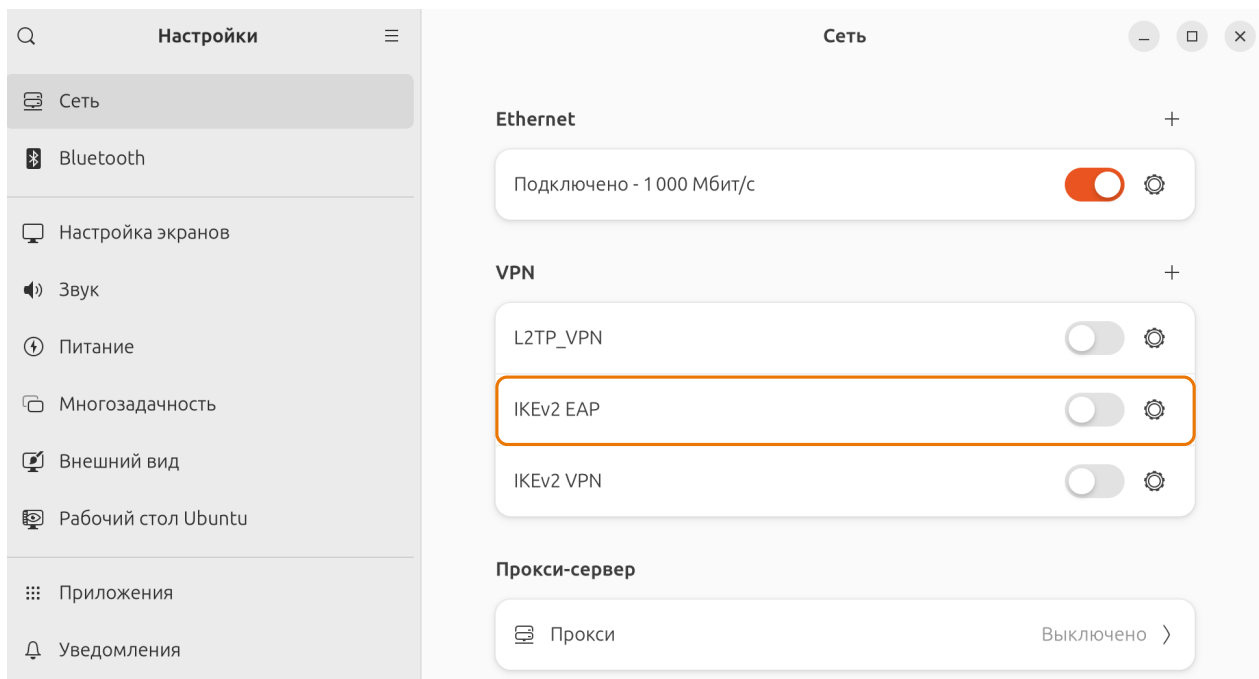
plugins {
    eap-peap {
        load = no
    }
    eap-md5 {
        load = no
    }
    eap-gtc {
        load = no
    }
}

include strongswan.d/*.conf

```

Настройка VPN-клиента завершена.

Для установления VPN-соединения нажать кнопку включения созданного соединения VPN:



Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@sthattreshat							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user1 user1 (testd.local\user1)	Сервер	RA VPN rule 2	28 августа 2024 г., 14:41 (5...	172.30.250.2	203.0.113.11		aes

В Журнале событий на вкладке Журналы и отчеты отобразится соответствующая запись:

Журнал событий							
date >= 2024-08-28T00:00:00 AND date <= 2024-08-28T23:59:59 AND component = 'vpn'							
Узел	Время ↓	Компонент	Тип события	Пользователь	IP источника	Модуль	Детали события
utmcore@sth...	14:41:20	VPN	Подключение пользователя к VPN прошло успешно	user1 user1 (testd.local\user1)	203.0.113.11	VPN сервер	Логин: user1@testd.local

На стороне удаленного Linux-компьютера добавится виртуальный адаптер, хост (10.10.0.100) в сети офиса доступен:

```
:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet 172.30.250.2/32 scope global lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d9:0a:07 brd ff:ff:ff:ff:ff:ff
    inet 203.0.113.12/24 brd 203.0.113.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
14: nm-xfrm-1955498@NONE: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 172.30.250.2/32 scope global noprefixroute nm-xfrm-1955498
        valid_lft forever preferred_lft forever
    inet6 fe80::6141:968b:2ce5:5035/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
:/# ping 10.10.0.100
PING 10.10.0.100 (10.10.0.100) 56(84) bytes of data.
64 bytes from 10.10.0.100: icmp_seq=1 ttl=63 time=3.23 ms
64 bytes from 10.10.0.100: icmp_seq=2 ttl=63 time=3.22 ms
64 bytes from 10.10.0.100: icmp_seq=3 ttl=63 time=1.57 ms
64 bytes from 10.10.0.100: icmp_seq=4 ttl=63 time=1.93 ms
^C
--- 10.10.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 1.574/2.486/3.227/0.745 ms
```

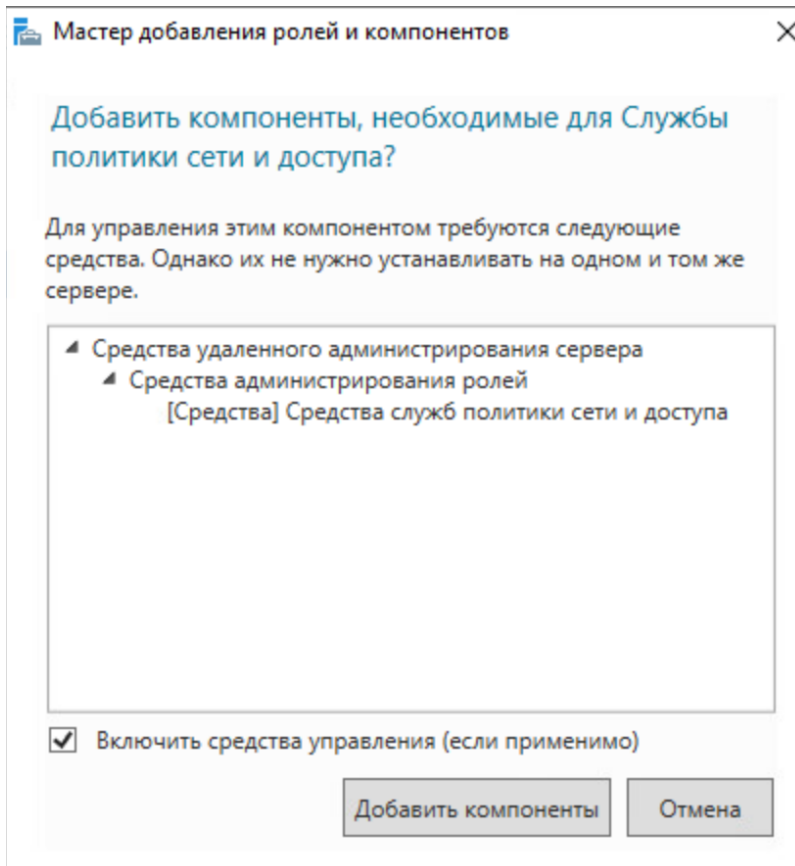
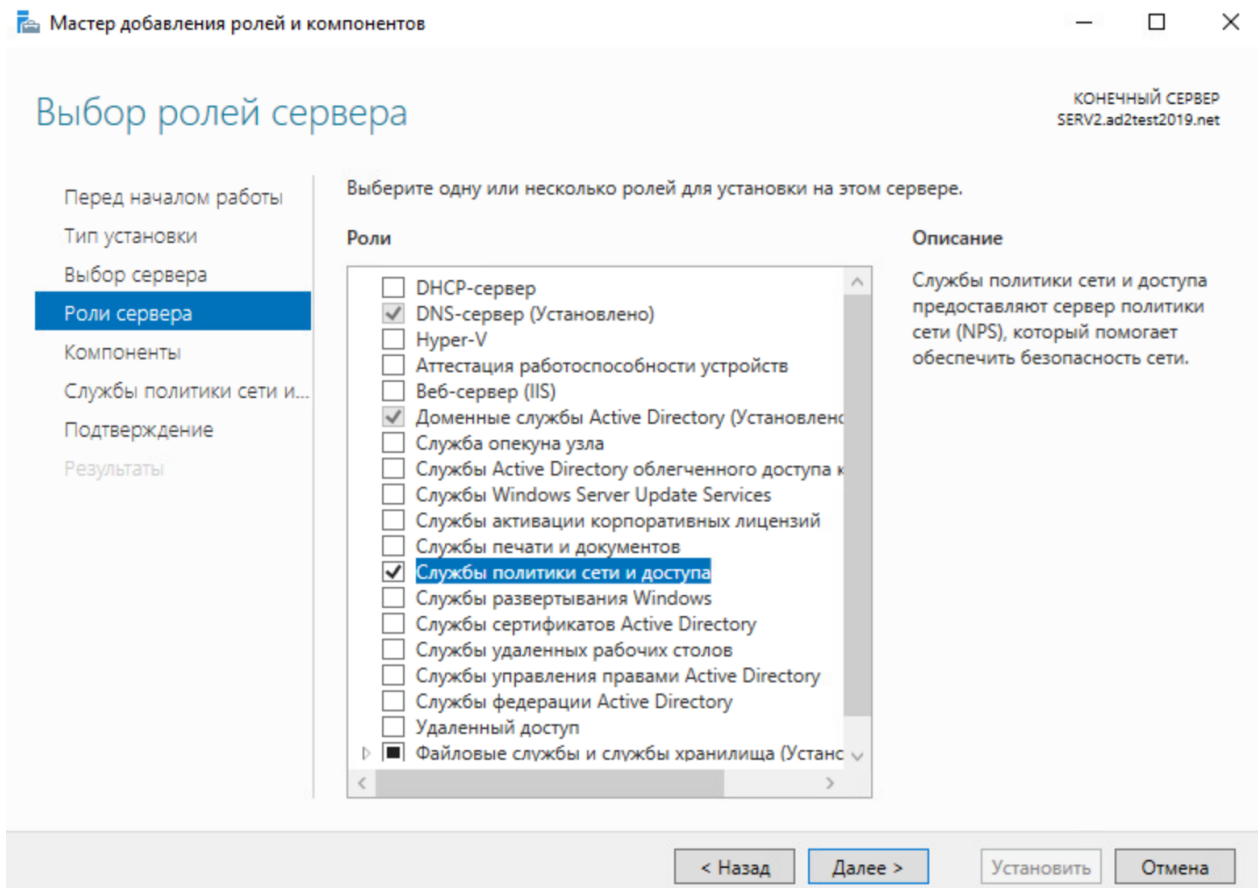
Приложение

Настройка RADIUS-сервера

Рассматривается настройка RADIUS-сервера на примере Windows Server 2019 с настроенной Active Directory.

- 1. Установить службы политики сети и доступа (Network Policy and Access Services).

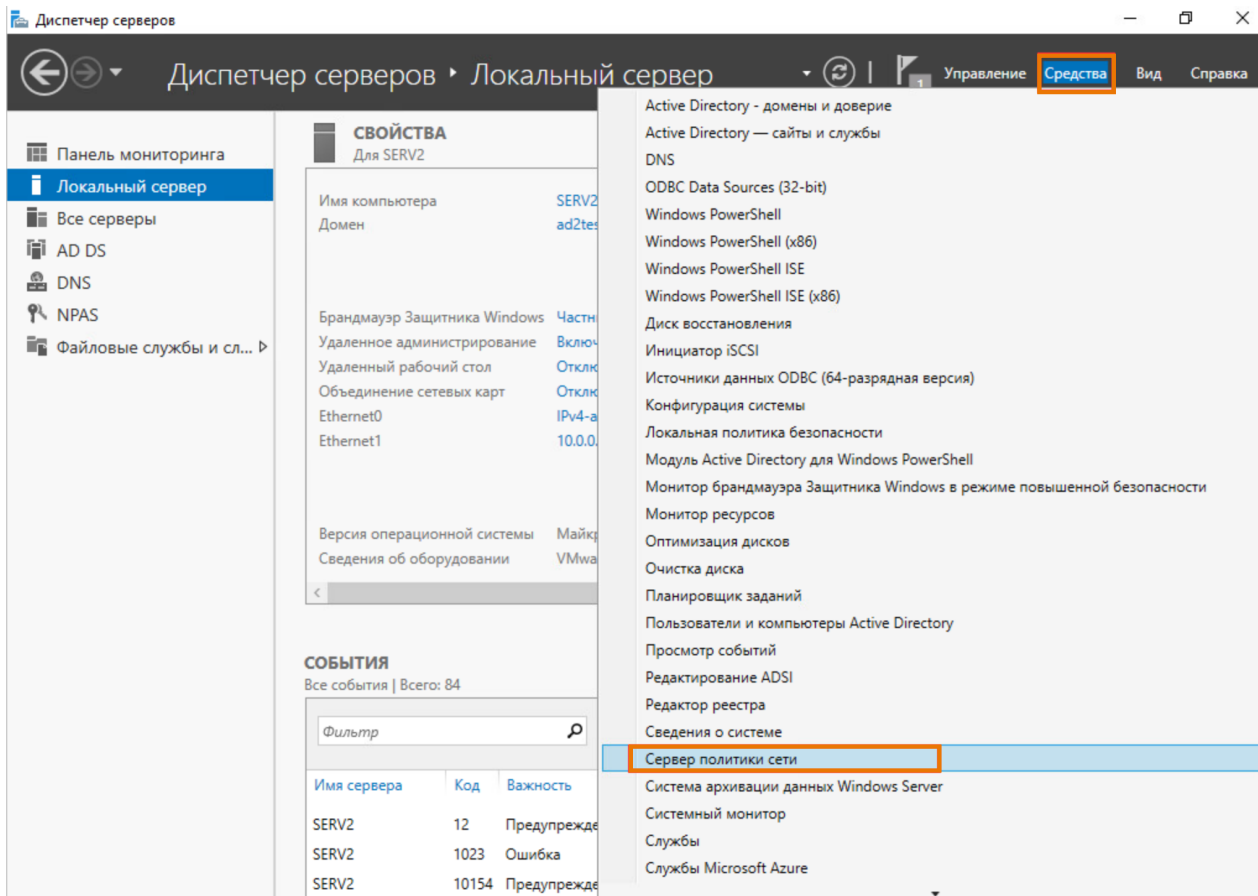
В диспетчере серверов добавить роли и компоненты. В окне мастера добавления ролей и компонентов на шаге **Роли сервера** найти в списке и выбрать **Службы политики сети и доступа**:



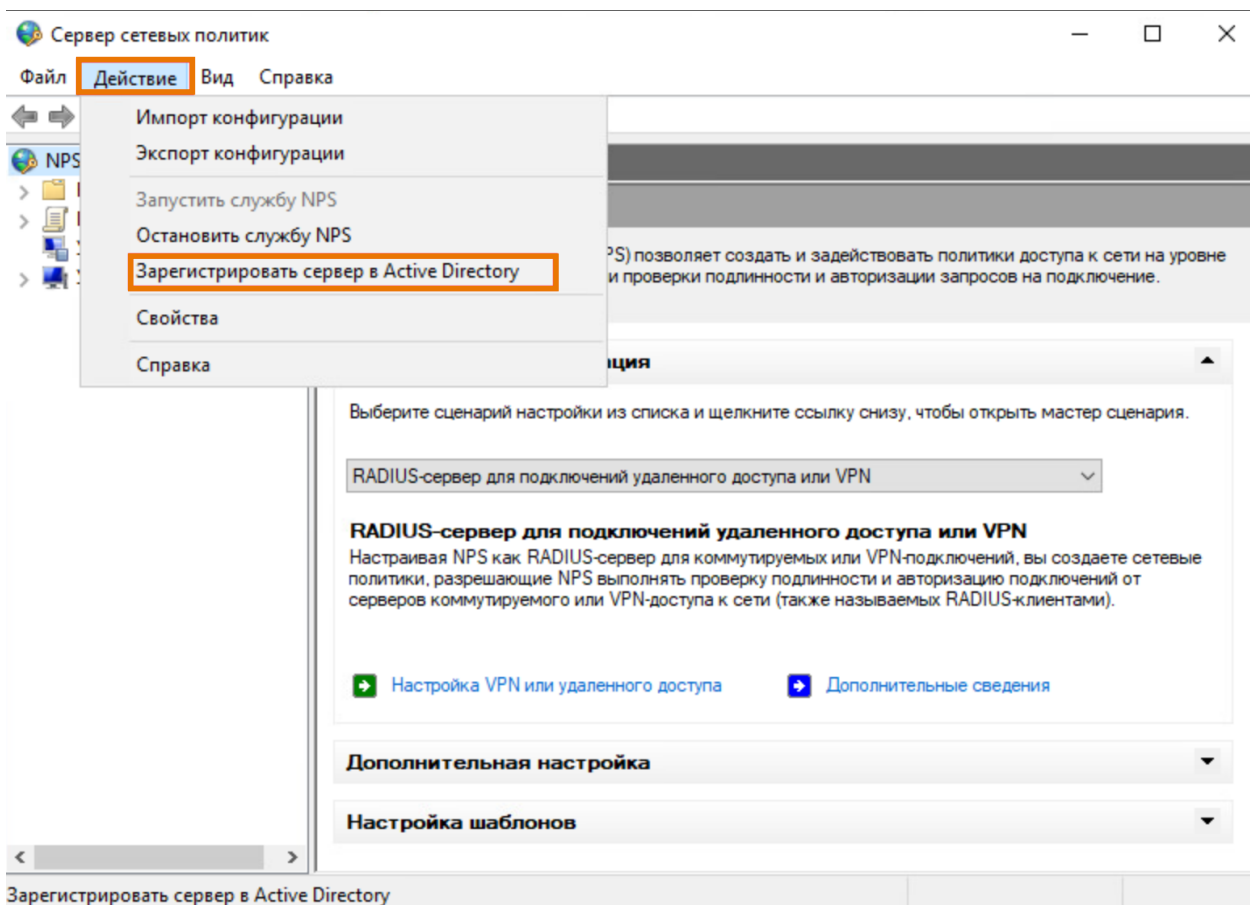
Далее следовать инструкции мастера для установки компонентов.

2. Зарегистрировать сервер в AD.

В окне диспетчера серверов выбрать **Средства** → **Сервер политики сети**:

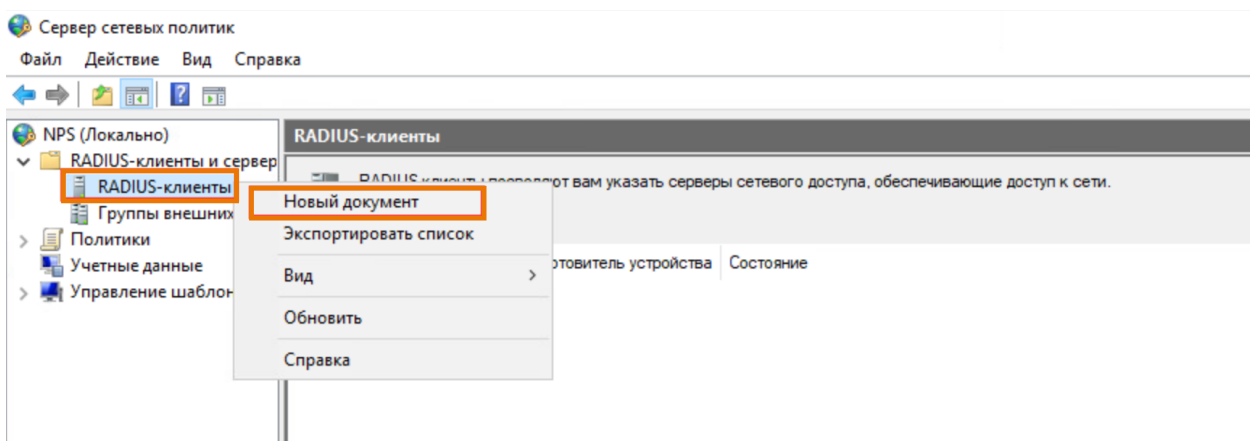


Далее нажать **Действие** → **Зарегистрировать сервер в Active Directory**:



3. Добавить RADIUS-клиента.

Устройства, с которыми RADIUS-сервер будет взаимодействовать (в данном случае это NGFW), необходимо добавить в список RADIUS-клиентов:



Далее заполнить следующие поля (остальные настройки оставить по умолчанию):

- **Понятное имя;**
- **Адрес** устройства (клиента), с которого будут приходить запросы на RADIUS-сервер;

Общий секрет для авторизации устройства на RADIUS-сервер.

Новый RADIUS-клиент

Параметры Дополнительно

☒ Включить этот RADIUS-клиент

☐ Выберите существующий шаблон:

Имя и адрес:

Понятное имя:
UserGate NGFW

Адрес (IP или DNS):
10.10.0.1

Проверить...

Общий секрет

Выберите существующий шаблон общих секретов:
Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

☒ Вручную ☐ Создать

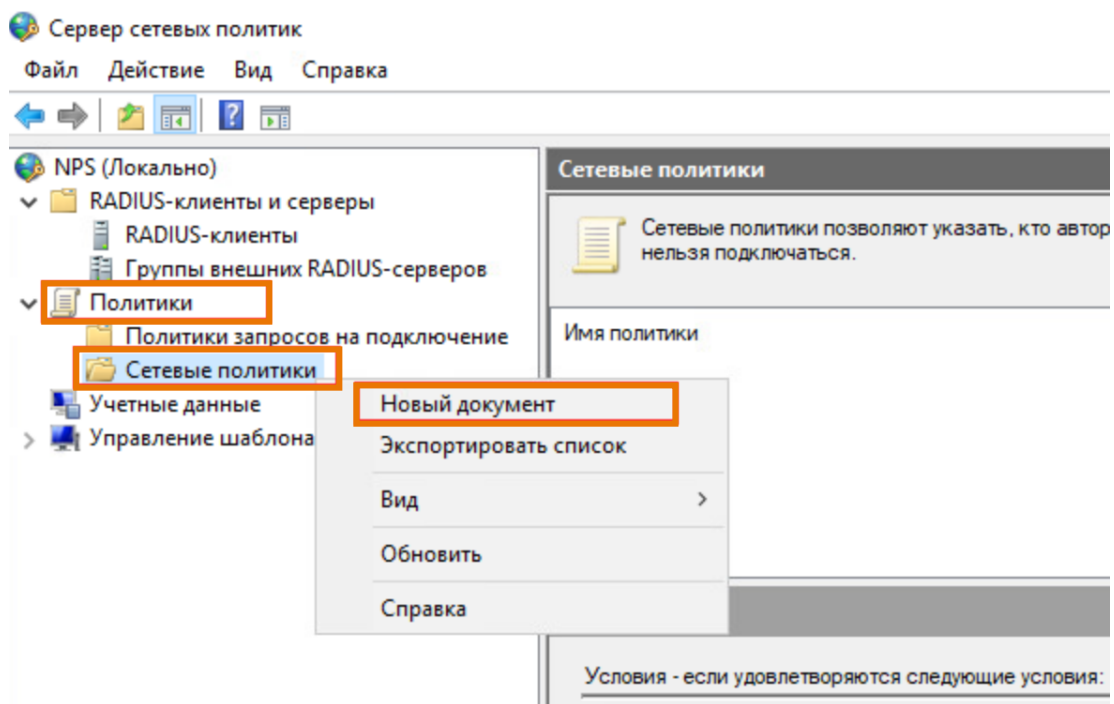
Общий секрет:

Подтверждение общего секрета:

OK Отмена

4. Настроить Сетевую политику.

Добавить политику:



Настроить политику. Указать название политики и условия её применения:

**Укажите имя политики сети и тип подключения**

Вы можете указать имя политики сети и тип подключений, к которому применяется политика.

Имя политики:**Способ сетевого подключения**

Выберите тип сервера доступа к сети, отправляющего запрос на подключение серверу сетевых политик. Можно выбрать тип сетевого сервера или параметр "Зависящие от поставщика" (ни то, ни другое не является обязательным). Если в качестве сервера сетевых политик используется коммутатор 802.1X или беспроводная точка доступа, выберите "Не указано".

☒ Тип сервера доступа к сети:☐ Зависящие от поставщика:

В качестве условия добавить заранее созданную группу пользователей, которой разрешен удаленный доступ:

Указать разрешение доступа — **Доступ разрешен:**

Новая политика сети X



Укажите разрешение доступа

Укажите, предоставлять или запрещать сетевой доступ, если запрос на подключение соответствует данной политике.

☒ **Доступ разрешен**
Предоставить доступ, если при попытке подключения клиента имеется соответствие условиям политики.

☐ **Доступ запрещен**
Запретить доступ, если при попытке подключения клиента имеется соответствие условиям политики.

☐ **Доступ определяется свойствами удаленного доступа пользователя (переопределяющими политику NPS)**
Предоставить или запретить доступ в соответствии со свойствами удаленного доступа пользователя, если при попытке подключения клиента имеется соответствие условиям политики.

Назад
Далее
Готово
Отмена

Далее выбрать следующие методы проверки подлинности:

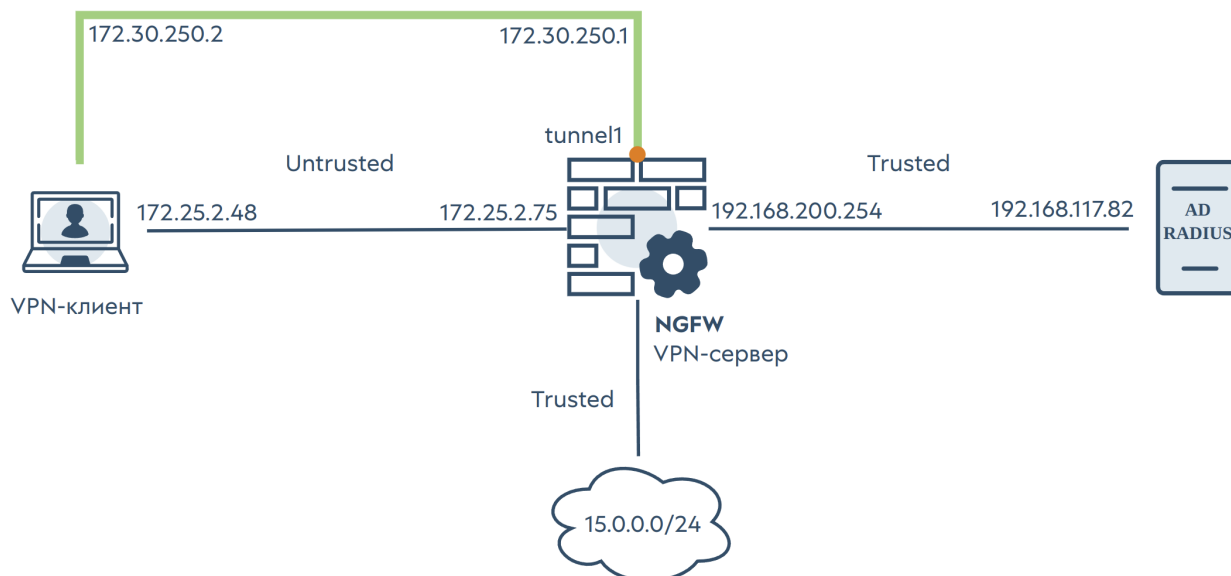
- **Типы EAP — Microsoft: защищённый пароль (EAP-MSCHAP v2);**
- Разрешить пункт **Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2);**
- Метод PAP (**Проверка открытым тестом (PAP, SPAP)**) рекомендуется разрешить для параллельной работы IKEv1 AAA. Если планируется использовать только IKEv2 AAA, то достаточно включения только EAP-MSCHAP v2.

Рекомендуемые настройки вкладки **Параметры**:

Настройка завершена:

Пример настройки Remote access VPN с IPsec(IKEv2) с аутентификацией через EAP, PEAP для OS Windows

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:



UserGate NGFW выступает в роли VPN-сервера, а компьютер пользователя с ОС Windows — в роли VPN-клиента.

Будут рассмотрены следующие сценарии аутентификации:

- EAP с аутентификацией по MSCHAPv2 с логином и паролем;
- EAP-TLS с аутентификацией по сертификату пользователя;
- PEAP с аутентификацией по сертификату пользователя;
- PEAP с аутентификацией по MSCHAPv2 с логином и паролем.

Сначала необходимо [настроить VPN-сервер](#), затем произвести [настройку VPN-клиента](#) на компьютере пользователя и инициировать подключение к VPN-серверу.

Пример настройки RADIUS-сервера, используемого в рассматриваемых сценариях, приведён в [Приложении](#).

Настройка VPN-сервера

Для настройки узла NGFW в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Откройте сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируйте параметры контроля доступа для зоны Untrusted. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон — в разделе документации [Настройка зон](#).

Шаг 2. Создайте зону для VPN подключений.

В этом примере используется созданная по умолчанию зона VPN for Remote access. Подробнее о создании и настройках зон — в разделе документации [Настройка зон](#).

Шаг 3. Настройте параметры аутентификации.

Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируйте созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажмите **Импортировать**. В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируйте корневой сертификат без указания приватного ключа:

Сертификаты				
Редактировать Показать Копировать Создать Импорт Экспорт Удалить				
Название	Назначение сертификата	Используется	Издатель	Субъект
ca2016	Digital signature, Certificate signing, CRL signing	undefined	adtest1	adtest1
vpntest.ad16.net no ch...	Digital signature, Non-repudiation	undefined	adtest1	vpntest.ad16.net

Создайте профиль аутентификации для пользователей VPN. Подробнее о профилях аутентификации — в разделе руководства [Профили аутентификации](#). Для этого примера был создан профиль, содержащий в качестве методов аутентификации RADIUS-сервер (rad16) и LDAP-коннектор (adtest1):

Свойства профиля аутентификации

Общие

Методы аутентификации

+

Добавить

×

Удалить

↑

Выше

↓

Нижне

Название
Сервер RADIUS: rad16
Сервер LDAP/Active Directory: adtest1

Сохранить

Отмена

Настройка LDAP-коннектора:

Свойства коннектора LDAP

Настройки

Домены LDAP

Kerberos keytab

Пути поиска

☒ Включено

☐ Использовать для соединений SSL

Название:

adtest1

Описание:

Доменное имя LDAP или IP-адрес:

192.168.117.82

Привязать DN («логин»):

ADTEST1\Test1

Пароль:

Время жизни кэша:

28800

секунд

Проверить соединение

Сохранить

Отмена

Настройка RADIUS-сервера:

Свойства RADIUS-сервера коннектора

Включено: ☒

Имя сервера:

Описание:

Секрет:

Адреса

+

Добавить

Редактировать

×

Удалить

Хост	Порт
192.168.117.82	1812

Сохранить

Отмена

Шаг 4.Создайте профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создайте профиль безопасности со следующими настройками:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Название:

eap-tls-16

Описание:

Протокол:

IKEv2

Режим IKE:

Основной

Тип идентификации:

отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

Сертификат сервера:

vpntest.ad16.net no chain

Режим аутентификации:

AAA

Профиль клиентского сертификата:

for vpntest.ad16.net

Подсети для VPN

Добавить

Редактировать

Удалить

Локальная подсеть

Удалённая подсеть

Сохранить

Отмена

- в качестве протокола для создания защищённого канала укажите IKEv2;
- тип идентификации в рассматриваемом примере можно не указывать;
- укажите сертификат сервера, импортированный ранее на [шаге 3](#);
- в качестве режима аутентификации выберите AAA.

Далее необходимо задать параметры первой и второй фаз согласования защищённого соединения:

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Dead peer detection:

Отключена

60

(сек)

Неудачных попыток:

5

Diffie-Hellman группы

+

Добавить

✕Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

+

Добавить

✎

Редактировать

✕

Удалить

⬆

Выше

⬇

Низже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256
SHA1	AES128

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

Включить NAT keepalive:

☐

Время жизни NAT:

0

секунд

Безопасность

Добавить

Редактировать

Удалить

Выше

Низже

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256
SHA1	AES128
SHA1	3DES

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую

Сохранить

Отмена

Шаг 5. Создайте VPN-интерфейс.

В этом примере используется созданный по умолчанию VPN-интерфейс tunnel1. Ключевые параметры этого интерфейса для примера создания защищённого VPN-соединения:

Настройка VPN-адаптера

Общие

Сеть

Включено:

☒

Название:

tunnel1

Описание:

Example VPN interface to be used in Remote Access VPN server rule. This is an example VPN interface which can be changed or deleted if necessary.

Зона:

VPN for remote access

Профиль netflow:

Не выбран

Алиас/Псевдоним:

Сохранить

Отмена

- поставьте флажок включения интерфейса;
- название интерфейса уже задано — tunnel1;
- указана зона VPN for remote access, к которой будет относиться данный интерфейс; все клиенты, подключившиеся по VPN к NGFW, будут помещены в эту зону;

Настройка VPN-адаптера

Общие Сеть

Режим: Статический

MTU: 1420

IP интерфейса

+ Добавить Редактировать Удалить

IP интерфейса	Маска
172.30.250.1	255.255.255.0

Сохранить Отмена

- при использовании интерфейса для приёма VPN-подключений необходимо использовать статический IP-адрес;
- размер MTU в этом примере оставим по умолчанию;
- статический IP-адрес туннельного интерфейса tunnel1: 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создайте сеть VPN.

В данном примере используется созданная по умолчанию сеть Remote access VPN network. Ключевые настройки этой сети для примера создания защищённого VPN-соединения:

Свойства VPN-сети

Общие Сеть Маршруты VPN Маршруты для UserGate Client

Диапазон IP: 172.30.250.2-172.30.250.254

Маска: 255.255.255.0

☒ Использовать системные DNS-серверы

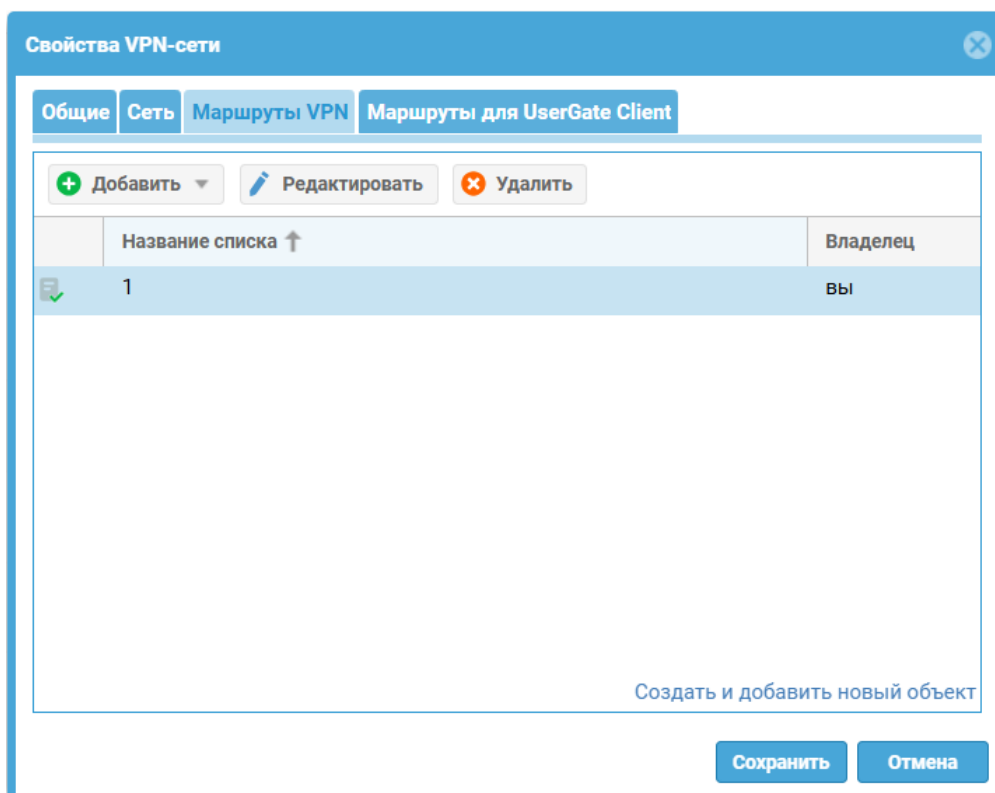
Серверы DNS:

+ Добавить ✎ Редактировать ✕ Удалить

IP-адрес

Сохранить Отмена

- диапазон IP-адресов, которые будут использованы клиентами; необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW (172.30.250.1), используемому совместно с данной сетью;
- маска сети VPN.
- оставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.



В этом примере на вкладке **Маршруты VPN** добавлен список "1", включающий в себя адрес сети (15.0.0.0/24).

Шаг 7. Создайте серверное правило VPN.

Воспользуемся созданным по умолчанию серверным правилом Remote access VPN rule. Ключевые настройки правила для данного примера:

- в качестве профиля безопасности VPN укажите серверный профиль безопасности, созданный ранее на [шаге 4](#);
- в качестве сети VPN укажите сеть, созданная ранее на [шаге 6](#);
- в качестве профиля аутентификации указан профиль, созданный ранее (см. [шаг 3](#));
- указан интерфейс VPN, созданный ранее на [шаге 5](#).

Шаг 8. Контроль доступа к ресурсам.

Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создаётся в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило NAT from VPN for remote access to Trusted and Untrusted, разрешающее подмену IP-адресов из зоны VPN for remote access в зоны Trusted и Untrusted. По умолчанию оно не активно. Необходимо его включить.

При необходимости предоставления доступа пользователям VPN в определённые сегменты сети в разделе **Политики сети → Межсетевой**

экран необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

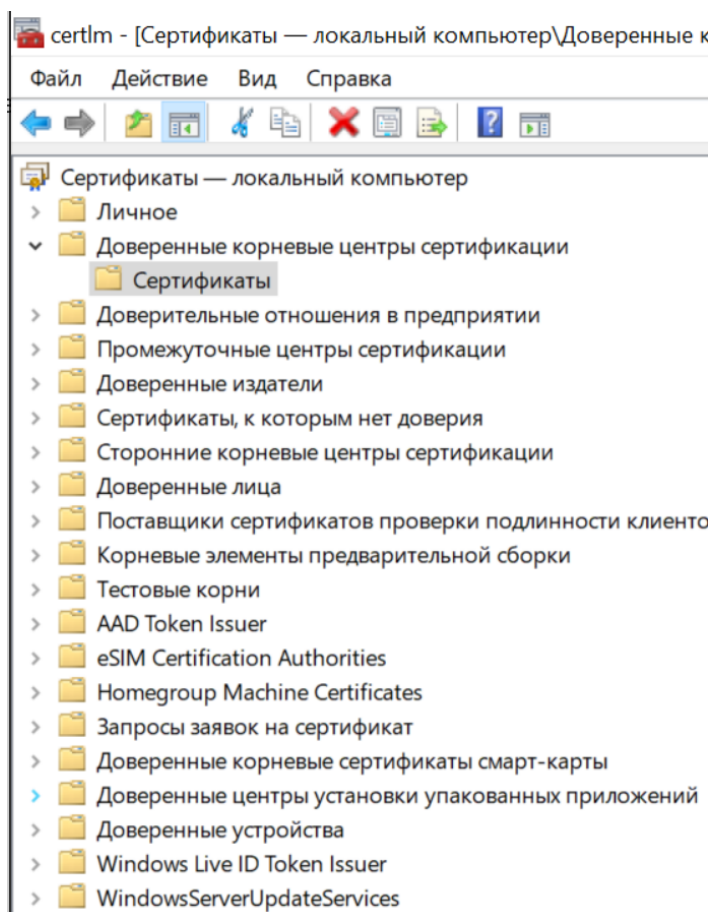
Для примера в консоли администратора создано правило межсетевого экрана VPN for Remote Access to Trusted and Untrusted, разрешающее весь трафик из зоны VPN for Remote Access в зоны Trusted и Untrusted. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

Общие настройки

В этом разделе рассматриваются настройки нативного клиента операционной системы Windows для удалённого VPN-подключения.

Для всех сценариев настроек VPN-клиента в этой статье необходимо импортировать сертификат корневого центра в раздел **Доверенные корневые центры сертификации** компьютера пользователя:

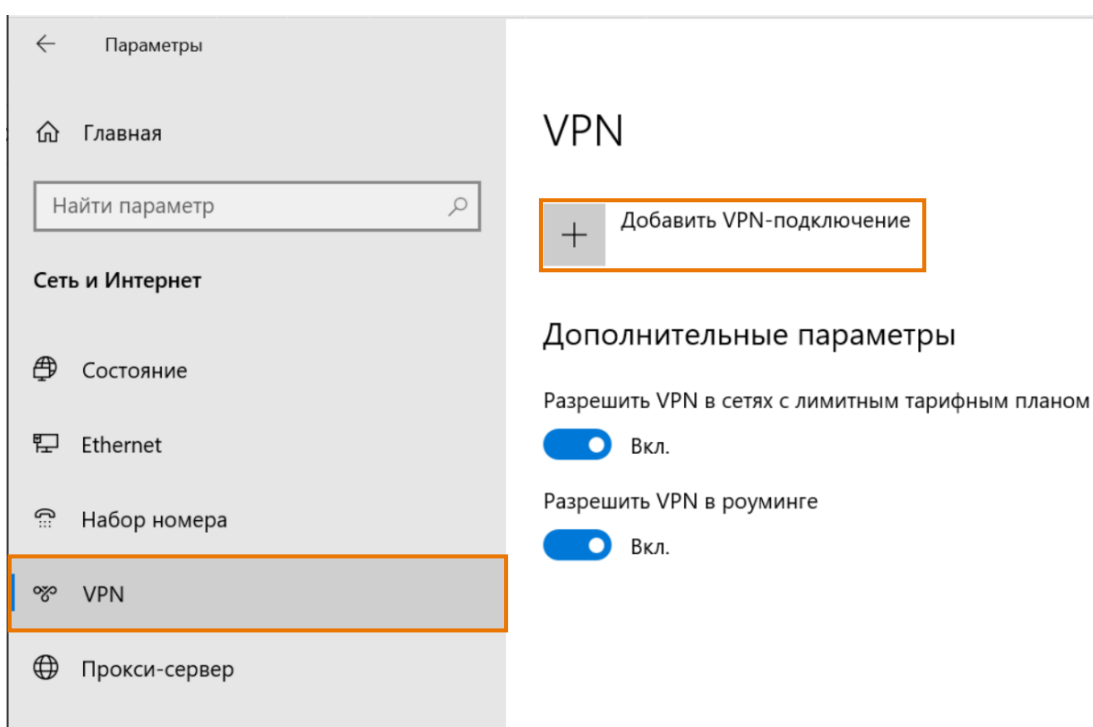


Сценарий настройки VPN-клиента с аутентификацией посредством метода EAP с MSCHAPv2 с логином и паролем

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



3. В окне **Добавить VPN-подключение** настройте параметры подключения:

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (EAP LOGIN);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;
- В поле **Тип данных для входа** выберите **Имя пользователя и пароль**.

Добавить VPN-подключение

Поставщик услуг VPN

Windows (встроенные) ▾

Имя подключения

EAP LOGIN

Имя или адрес сервера

vpntest.ad16.net

Тип VPN

IKEv2 ▾

Тип данных для входа

Имя пользователя и пароль ▾

Имя пользователя (необязательно)

Пароль (необязательно)

☒ Запомнить мои данные для входа

Сохранить

4. Нажмите **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 2. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт **Настройки параметров адаптера**:

Дополнительные сетевые параметры



Настройка параметров адаптера

Просмотр сетевых адаптеров и изменение параметров подключения.



Центр управления сетями и общим доступом

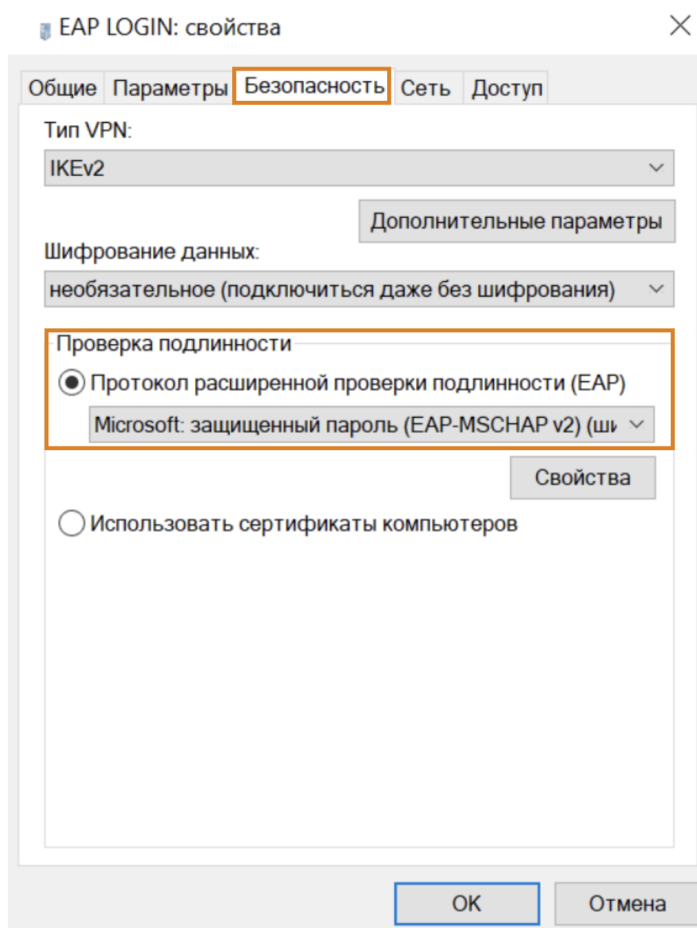
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.

[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

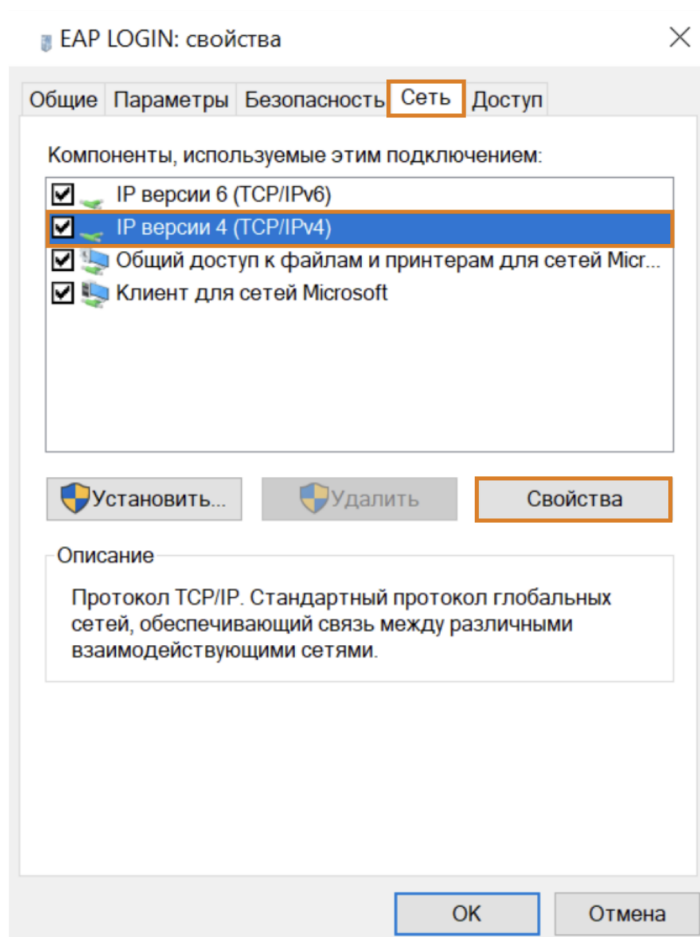
[Сброс сети](#)

2. Выберите только что созданное сетевое подключение **EAP LOGIN** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:

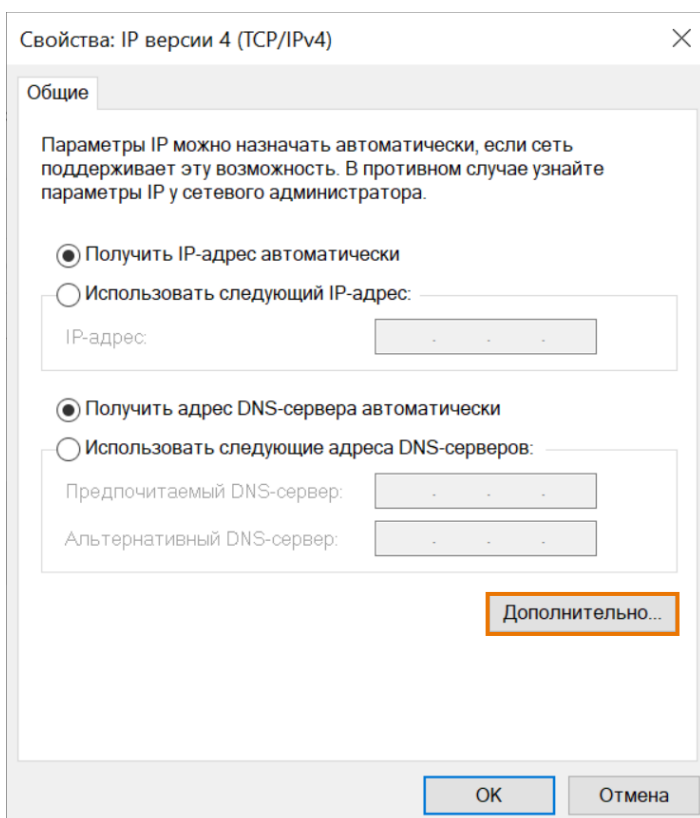


В поле **Проверка подлинности** выберите пункт **Microsoft: защищённый пароль (EAP-MSCHAP v2) (шифрование включено)**.

3. Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** откройте свойства **IP версии 4 (TCP/IPv4)**:



Нажмите **Дополнительно** в настройках общих параметров IP:



Уберите флажок в поле **Использовать основной шлюз в удалённой сети**:

Дополнительные параметры TCP/IP

Параметры IP DNS WINS

Этот флажок используется только при одновременном подключении к локальной сети и к сети удаленного доступа. Если флажок установлен, данные, которые не удается передать через локальную сеть, направляются в сеть удаленного доступа.

☐ Использовать основной шлюз в удаленной сети

☐ Отключить добавление маршрута, основанное на классе

☒ Автоматическое назначение метрики

Метрика интерфейса:

OK Отмена

4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **EAP LOGIN** и нажмите **Подключиться**.

Проверка подключения

После установления VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN						
utmcore@plaratanyan						
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Шифрование
user (adtest1.net\user)	Сервер	eap-tls 2016	25 февраля 2...	172.30.250.2	172.25.2.48	aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий

date >= 2025-02-25T00:00:00 AND date <= 2025-02-25T23:59:59 AND component = 'vpn'

	Узел	Время	И	Компоне...	Тип события	Пользователь	IP источника	Модуль	Детали события
!	utmcorg...	13:15:24	VPN		Подключение пользователя к VPN прошло успешно	user (adtest1.net\user)	172.25.2.48	VPN сервер	Логин: user, Серверное правило VPN: eap-tls 2016

На стороне удалённого Windows-компьютера добавится rppr-адаптер EAP LOGIN:

```
Адаптер Ethernet Ethernet1:

DNS-суффикс подключения . . . . . : esafeline.com
Локальный IPv6-адрес канала . . . : fe80::19b2:703e:82a8:4fb6%10
IPv4-адрес . . . . . : 172.25.2.48
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 172.25.0.1

Адаптер PPP EAP LOGIN:

DNS-суффикс подключения . . . . . :
IPv4-адрес . . . . . : 172.30.250.2
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . :
```

Появился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Шаге 6](#):

```
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс  Метрика
0.0.0.0            0.0.0.0        172.25.0.1       172.25.2.48  25
15.0.0.0           255.255.255.0   On-link          172.30.250.2  26
15.0.0.255         255.255.255.255 On-link          172.30.250.2  281
127.0.0.0          255.0.0.0       On-link          127.0.0.1    331
127.0.0.1          255.255.255.255 On-link          127.0.0.1    331
127.255.255.255    255.255.255.255 On-link          127.0.0.1    331
172.25.0.0         255.255.0.0     On-link          172.25.2.48  281
172.25.2.48        255.255.255.255 On-link          172.25.2.48  281
172.25.2.75        255.255.255.255 On-link          172.25.2.48  26
172.25.255.255     255.255.255.255 On-link          172.25.2.48  281
172.30.0.0         255.255.0.0     On-link          172.30.250.2  26
172.30.250.2       255.255.255.255 On-link          172.30.250.2  281
172.30.255.255     255.255.255.255 On-link          172.30.250.2  281
224.0.0.0          240.0.0.0       On-link          127.0.0.1    331
224.0.0.0          240.0.0.0       On-link          172.25.2.48  281
224.0.0.0          240.0.0.0       On-link          172.30.250.2  281
255.255.255.255    255.255.255.255 On-link          127.0.0.1    331
255.255.255.255    255.255.255.255 On-link          172.25.2.48  281
255.255.255.255    255.255.255.255 On-link          172.30.250.2  281
=====
Постоянные маршруты:
Сетевой адрес      Маска  Адрес шлюза      Метрика
0.0.0.0            0.0.0.0  192.168.200.154 По умолчанию
=====
```

IP-адрес в удалённой сети доступен:

```

Обмен пакетами с 15.0.0.200 по с 32 байтами данных:
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=5мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=1мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=5мс TTL=64

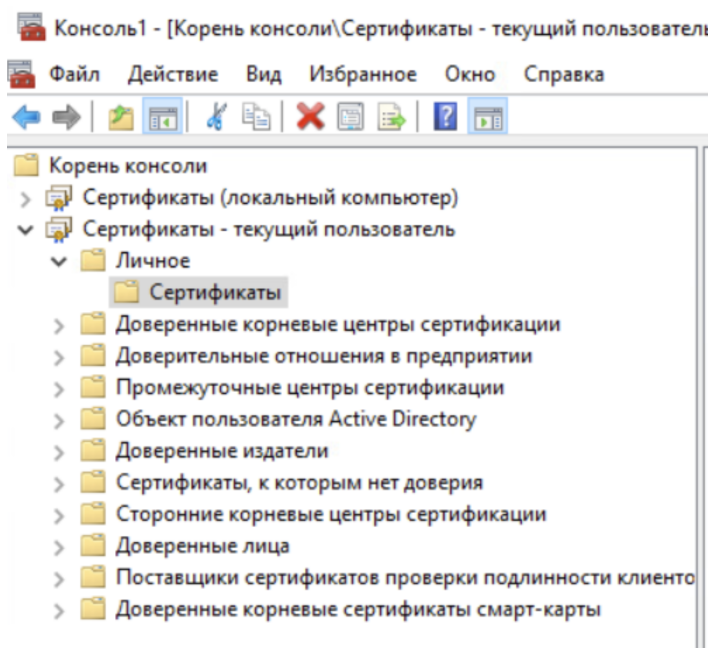
Статистика Ping для 15.0.0.200:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 5 мсек, Среднее = 3 мсек

```

Сценарий настройки VPN-клиента с аутентификацией посредством метода EAP-TLS

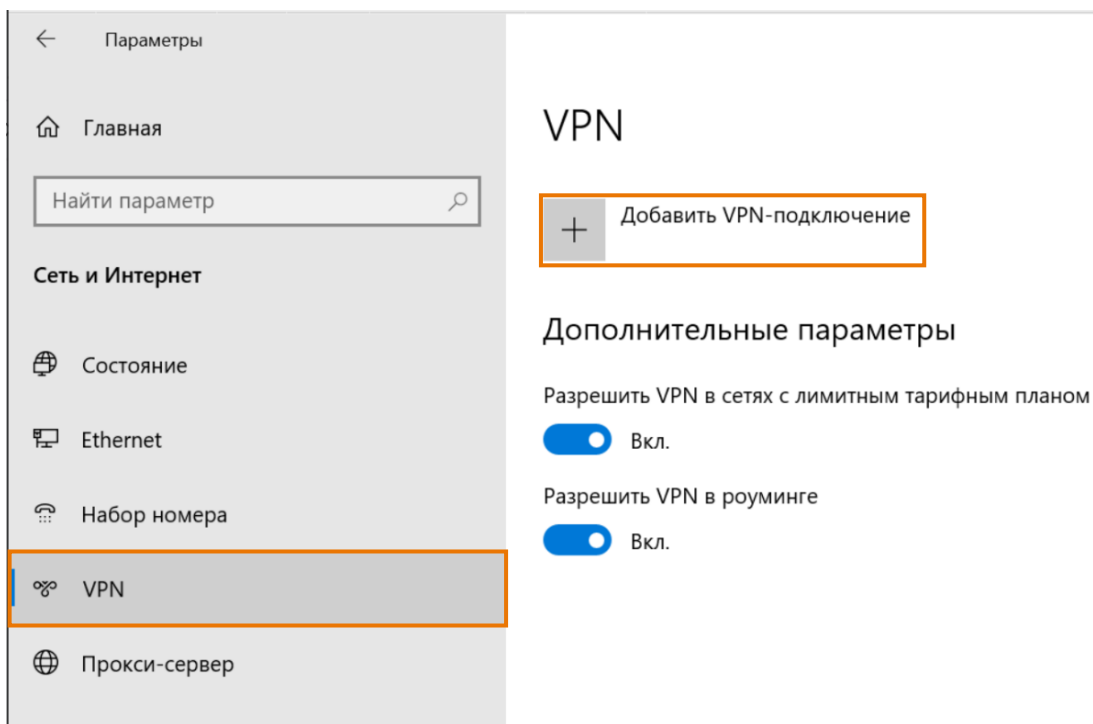
Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Импортируйте ранее созданный пользовательский сертификат в хранилище сертификатов пользователя в личную папку:



Шаг 2. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



3. В окне **Добавить VPN-подключение** настройте параметры подключения:

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (EAP-TLS);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;
- В поле **Тип данных для входа** выберите **Сертификат**.

Добавить VPN-подключение

Поставщик услуг VPN
Windows (встроенные) ▾

Имя подключения
EAP-TLS

Имя или адрес сервера
vpntest.ad16.net

Тип VPN
IKEv2 ▾

Тип данных для входа
Сертификат ▾

Имя пользователя (необязательно)

Пароль (необязательно)

☒ Запомнить мои данные для входа

Сохранить

4. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 3. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт **Настройки параметров адаптера**:

Дополнительные сетевые параметры



Настройка параметров адаптера

Просмотр сетевых адаптеров и изменение параметров подключения.



Центр управления сетями и общим доступом

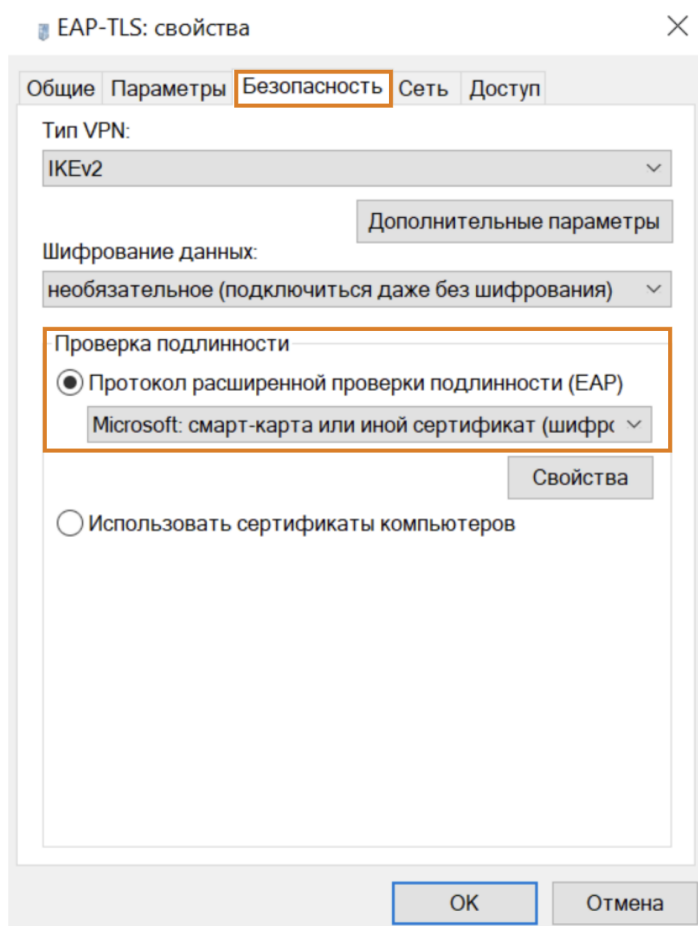
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.

[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

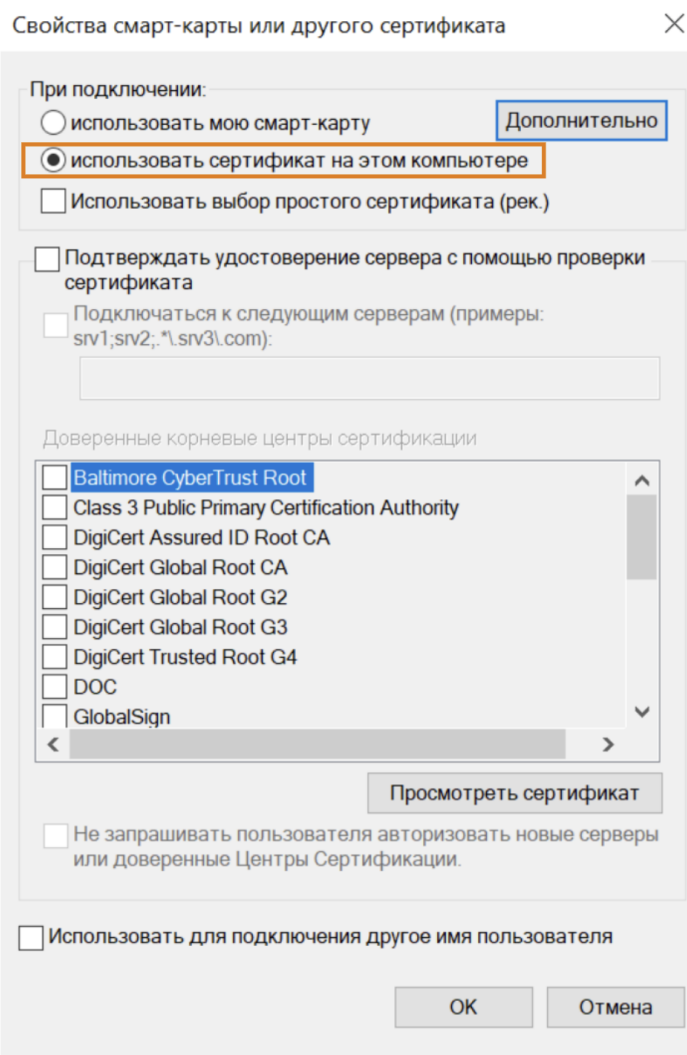
[Сброс сети](#)

2. Выберите только что созданное сетевое подключение **EAP-TLS** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите во вкладку **Безопасность**:

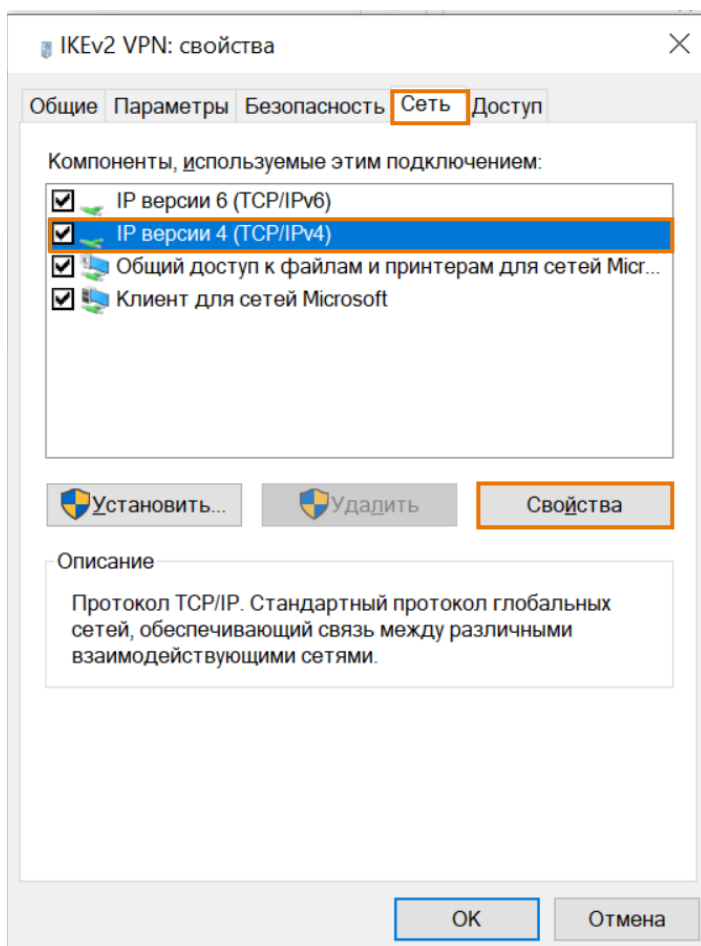


В поле **Проверка подлинности** должен быть выбран пункт **Microsoft: смарт-карта или иной сертификат (шифрование включено)**.

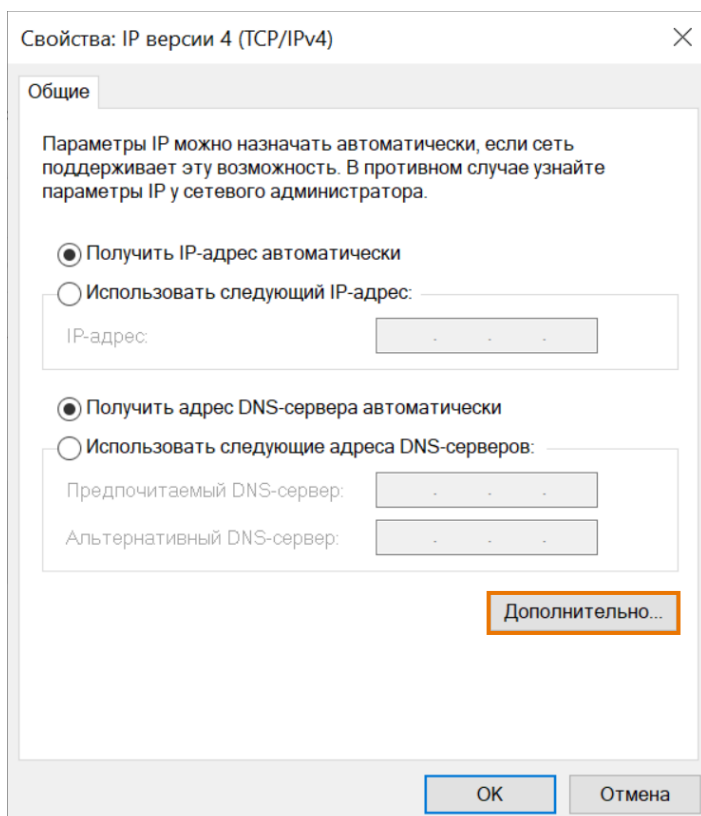
В свойствах проверки подлинности в разделе **При подключении** должен быть выбран пункт **Использовать сертификат на этом компьютере**:



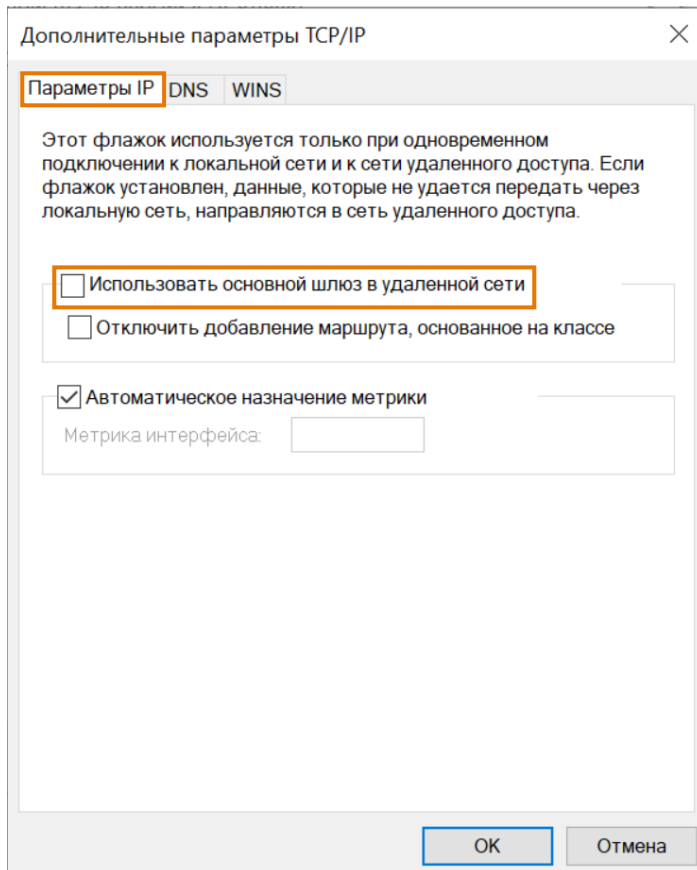
3. Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** откройте свойства **IP версии 4 (TCP/IPv4)**:



Нажмите **Дополнительно** в настройках общих параметров IP:



Уберите флажок в поле **Использовать основной шлюз в удалённой сети**:



4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **EAP-TLS** и нажмите **Подключиться**.

При наличии нескольких сертификатов пользователя перед установлением соединения будет предложен выбор нужного сертификата.

Проверка подключения

После установления VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@plaratanyan							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user (adtest1.net\user)	Сервер	eap-tls 2016	21 февраля 2...	172.30.250.2	172.25.2.48	?	aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий						
date >= 2025-02-21T00:00:00 AND date <= 2025-02-21T23:59:59 AND component = 'vpn'						
Узел	Время	Ком...	Тип события	Пользователь	IP источника	Детали события
utmsco...	13:06:45	VPN	Подключение пользователя к VPN прошло успешно	user (adtest1.net\user)	172.25.2.48	Логин: user@adtest1.net, Северное правило VPN: eap-tls 2016

На стороне удалённого Windows-компьютера добавится rppr-адаптер EAP-TLS:

```
Адаптер Ethernet Ethernet1:
DNS-суффикс подключения . . . . . : esafeline.com
Локальный IPv6-адрес канала . . . : fe80::19b2:703e:82a8:4fb6%10
IPv4-адрес. . . . . : 172.25.2.48
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 172.25.0.1

Адаптер PPP EAP-TLS:
DNS-суффикс подключения . . . . . :
IPv4-адрес. . . . . : 172.30.250.2
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . :
```

Добавился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [шаге 6](#):

```
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        172.25.0.1      172.25.2.48    25
15.0.0.0           255.255.255.0   On-link         172.30.250.2   26
15.0.0.255         255.255.255.255 On-link         172.30.250.2   281
127.0.0.0          255.0.0.0      On-link         127.0.0.1      331
127.0.0.1          255.255.255.255 On-link         127.0.0.1      331
127.255.255.255    255.255.255.255 On-link         127.0.0.1      331
172.25.0.0         255.255.0.0    On-link         172.25.2.48    281
172.25.2.48        255.255.255.255 On-link         172.25.2.48    281
172.25.2.75        255.255.255.255 On-link         172.25.2.48    26
172.25.255.255     255.255.255.255 On-link         172.25.2.48    281
172.30.0.0         255.255.0.0    On-link         172.30.250.2   26
172.30.250.2       255.255.255.255 On-link         172.30.250.2   281
172.30.255.255     255.255.255.255 On-link         172.30.250.2   281
224.0.0.0          240.0.0.0      On-link         127.0.0.1      331
224.0.0.0          240.0.0.0      On-link         172.25.2.48    281
224.0.0.0          240.0.0.0      On-link         172.30.250.2   281
255.255.255.255    255.255.255.255 On-link         127.0.0.1      331
255.255.255.255    255.255.255.255 On-link         172.25.2.48    281
255.255.255.255    255.255.255.255 On-link         172.30.250.2   281
=====
Постоянные маршруты:
Сетевой адрес      Маска      Адрес шлюза      Метрика
0.0.0.0            0.0.0.0    192.168.200.154 По умолчанию
=====
```

IP-адрес в удалённой сети доступен:

```

C:\Users\user1>ping 15.0.0.200

Обмен пакетами с 15.0.0.200 по 32 байтами данных:
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=5мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=3мс TTL=64

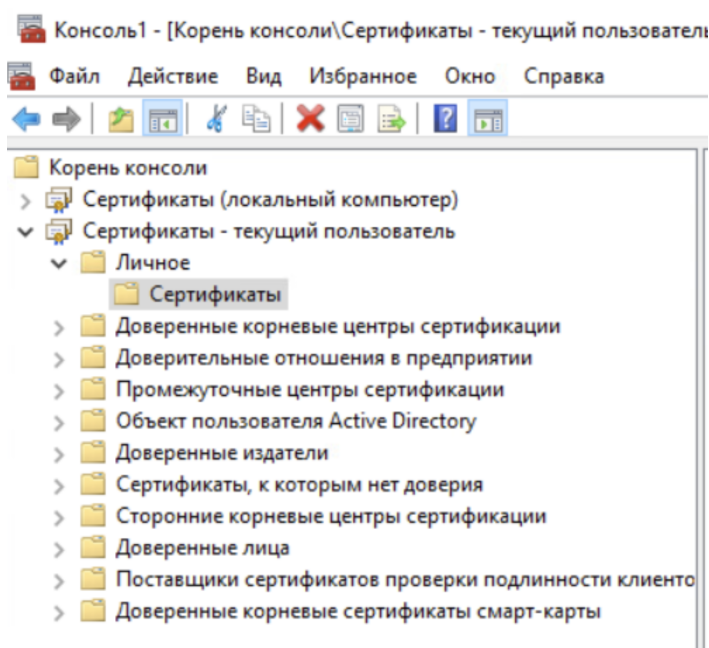
Статистика Ping для 15.0.0.200:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 5 мсек, Среднее = 3 мсек

```

Сценарий настройки VPN-клиента с аутентификацией посредством метода PEAP с сертификатом

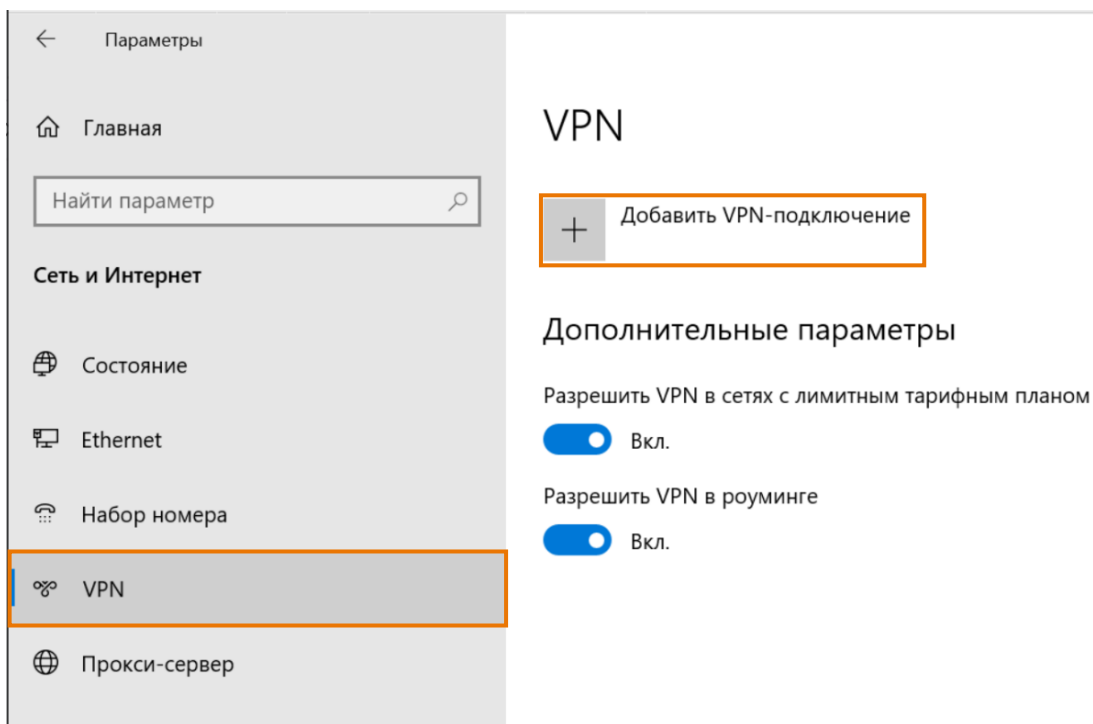
Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Импортируйте ранее созданный пользовательский сертификат в хранилище сертификатов пользователя в личную папку:



Шаг 2. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



3. В окне **Добавить VPN-подключение** настройте параметры подключения:

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (PEAP CERT);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;

Добавить VPN-подключение

Поставщик услуг VPN

Windows (встроенные) ▾

Имя подключения

PEAP CERT

Имя или адрес сервера

vpntest.ad16.net

Тип VPN

IKEv2 ▾

Тип данных для входа

Имя пользователя и пароль ▾

Имя пользователя (необязательно)

Пароль (необязательно)

☒ Запомнить мои данные для входа

Сохранить

4. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 3. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт: **Настройки параметров адаптера**:

Дополнительные сетевые параметры



Настройка параметров адаптера

Просмотр сетевых адаптеров и изменение параметров подключения.



Центр управления сетями и общим доступом

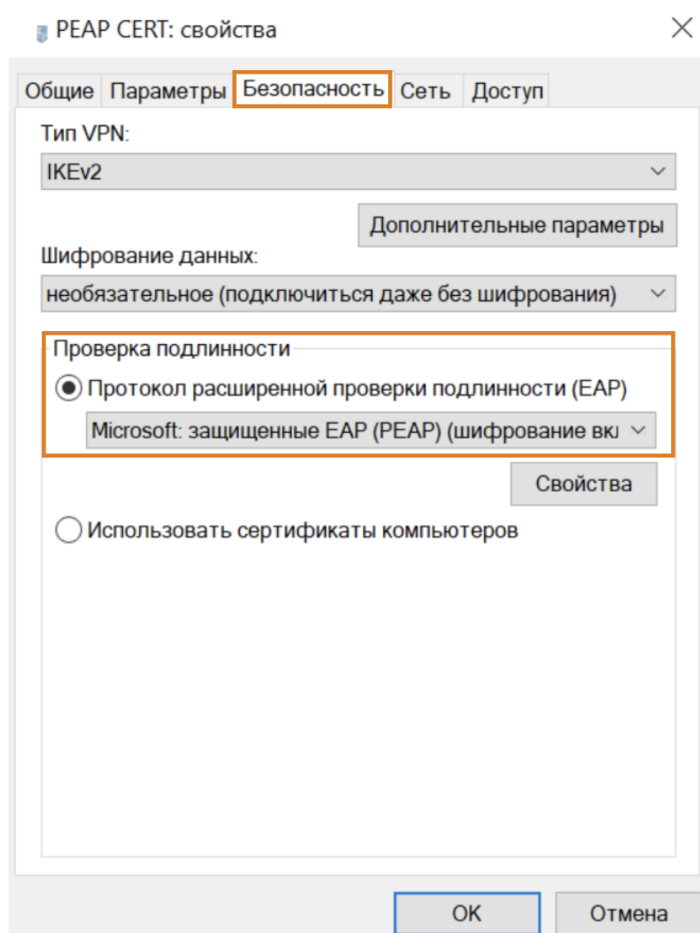
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.

[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

[Сброс сети](#)

2. Выберите только что созданное сетевое подключение **PEAP CERT** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:



В поле **Проверка подлинности** выберите пункт: **Microsoft: защищенные EAP (PEAP) (шифрование включено)**.

В свойствах проверки подлинности в поле выбора метода проверки необходимо выбрать: **Смарт-карта или иной сертификат**.

Флажки **Подтверждать удостоверение сервера с помощью проверки сертификата** и **Включить быстрое переподключение** могут быть установлены опционально:

Свойства защищенного EAP

При подключении:

☒ Подтверждать удостоверение сервера с помощью проверки сертификата

☐ Подключаться к следующим серверам (примеры: srv1;srv2;*.srv3\com):

Доверенные корневые центры сертификации:

- ☐ Baltimore CyberTrust Root
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert Global Root G2
- ☐ DigiCert Global Root G3
- ☐ DigiCert Trusted Root G4

Уведомления перед подключением:

Уведомить пользователя, если не указано имя сервера или коря

Выберите метод проверки подлинности:

смарт-карта или иной сертификат

Настроить...

☒ Включить быстрое переподключение

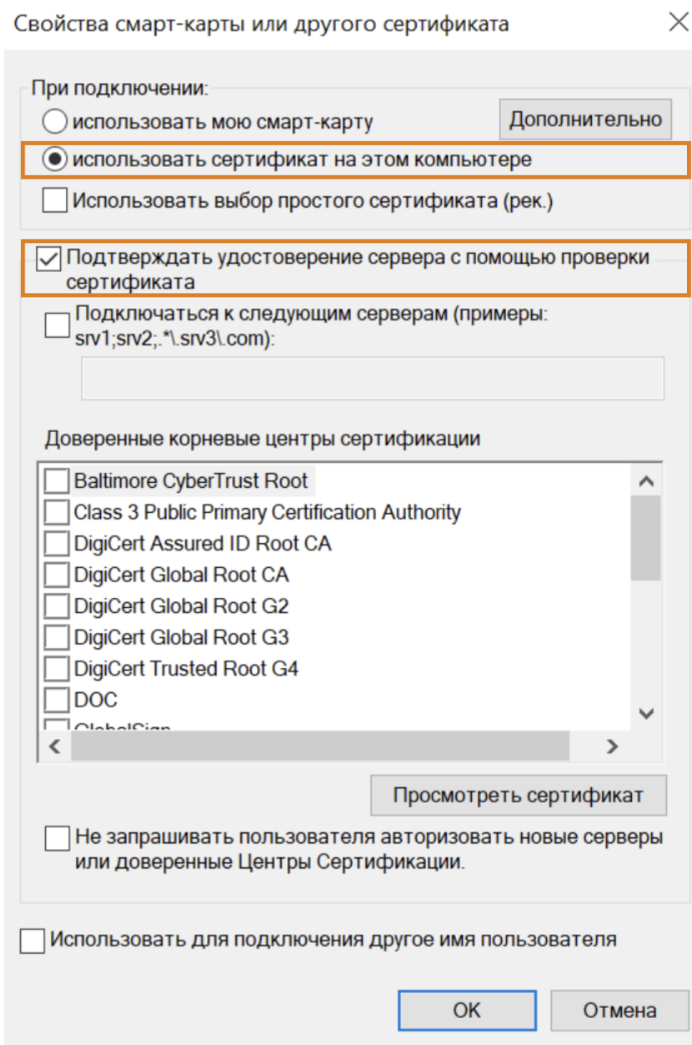
☐ Отключаться, если сервер не поддерживает привязку с шифрованием через механизм TLV

☐ Включить удостоверение конфиденциальности

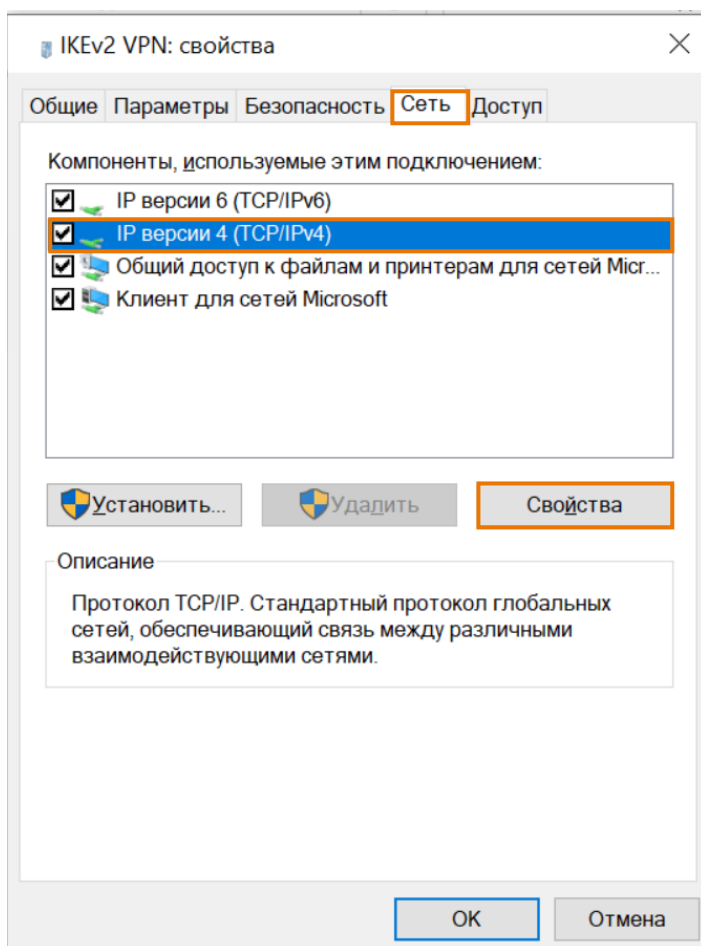
OK Отмена

В настройках метода проверки подлинности должен быть активен пункт: **Использовать сертификат на этом компьютере.**

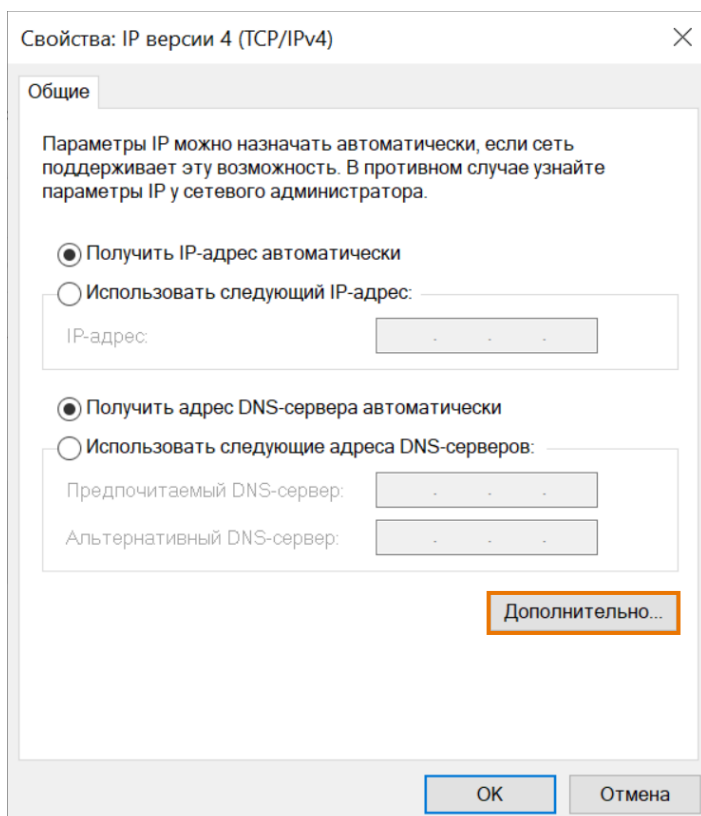
Опционально может быть активировано поле **Подтверждать удостоверение сервера с помощью проверки сертификата**:



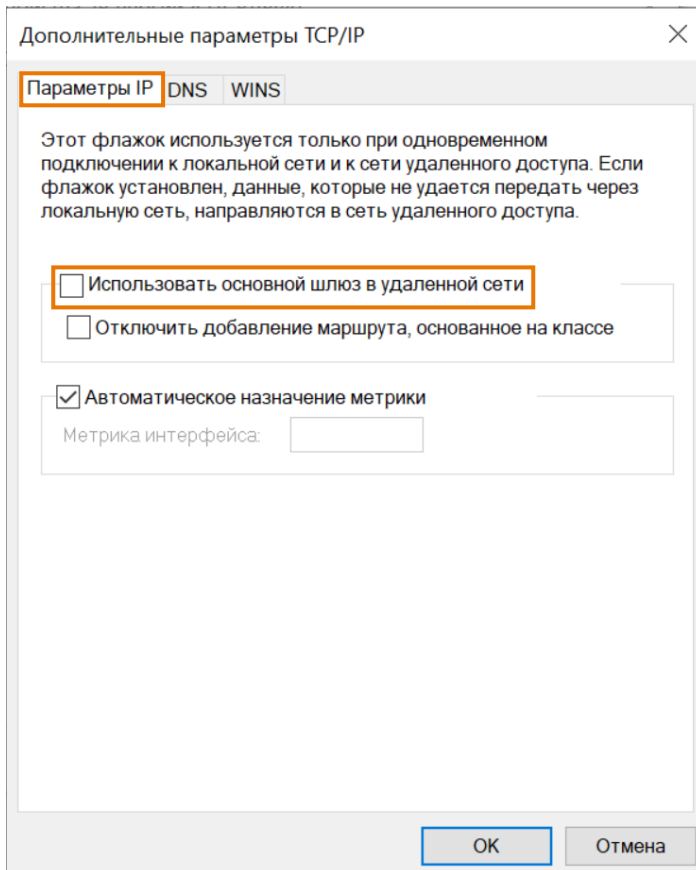
3. Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** откройте свойства **IP версии 4 (TCP/IPv4)**:



Нажмите **Дополнительно** в настройках общих параметров IP:



Уберите флажок в поле **Использовать основной шлюз в удалённой сети**:

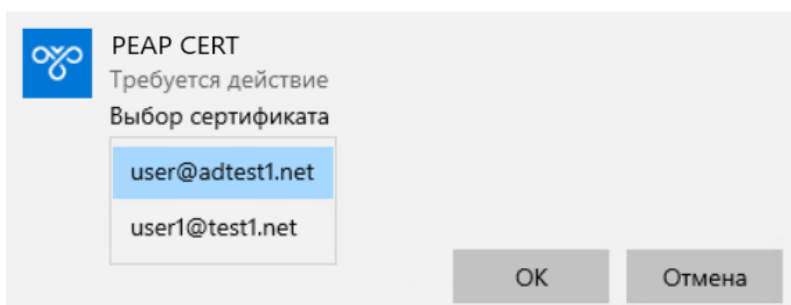


4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **PEAP CERT** и нажмите **Подключиться**.

При наличии нескольких сертификатов пользователя перед установлением соединения будет предложен выбор нужного сертификата:



Проверка подключения

После установления VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@plaratanyan							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user (adtest1.net\user)	Сервер	eap-tls 2016	21 февраля 2...	172.30.250.2	172.25.2.48	?	aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий							
date >= 2025-02-21T00:00:00 AND date <= 2025-02-21T23:59:59 AND component = 'vpn'							
Узел	Время	Ком...	Тип события	Пользователь	IP источника	Детали события	
utmco...	13:22:33	VPN	Подключение пользователя к VPN прошло успешно	user (adtest1.net\user)	172.25.2.48	Логин: user@adtest1.net, Серверное правило VPN: eap-tls 2016	

На стороне удалённого Windows-компьютера добавится rppr-адаптер PEAP CERT:

```
Адаптер Ethernet Ethernet1:

DNS-суффикс подключения . . . . . : esafeline.com
Локальный IPv6-адрес канала . . . : fe80::19b2:703e:82a8:4fb6%10
IPv4-адрес. . . . . : 172.25.2.48
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 172.25.0.1

Адаптер PPP PEAP CERT:

DNS-суффикс подключения . . . . . :
IPv4-адрес. . . . . : 172.30.250.2
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . :
```

Появился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Share 6](#):

IPv4 таблица маршрута

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	172.25.0.1	172.25.2.48	25
15.0.0.0	255.255.255.0	On-link	172.30.250.2	26
15.0.0.255	255.255.255.255	On-link	172.30.250.2	281
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
172.25.0.0	255.255.0.0	On-link	172.25.2.48	281
172.25.2.48	255.255.255.255	On-link	172.25.2.48	281
172.25.2.75	255.255.255.255	On-link	172.25.2.48	26
172.25.255.255	255.255.255.255	On-link	172.25.2.48	281
172.30.0.0	255.255.0.0	On-link	172.30.250.2	26
172.30.250.2	255.255.255.255	On-link	172.30.250.2	281
172.30.255.255	255.255.255.255	On-link	172.30.250.2	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	172.25.2.48	281
224.0.0.0	240.0.0.0	On-link	172.30.250.2	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	172.25.2.48	281
255.255.255.255	255.255.255.255	On-link	172.30.250.2	281

Постоянные маршруты:

Сетевой адрес	Маска	Адрес шлюза	Метрика
0.0.0.0	0.0.0.0	192.168.200.154	По умолчанию

IP-адрес в удалённой сети доступен:

```
C:\Users\user1>ping 15.0.0.200

Обмен пакетами с 15.0.0.200 по с 32 байтами данных:
Ответ от 15.0.0.200: число байт=32 время=4мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=1мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64

Статистика Ping для 15.0.0.200:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 4 мсек, Среднее = 2 мсек
```

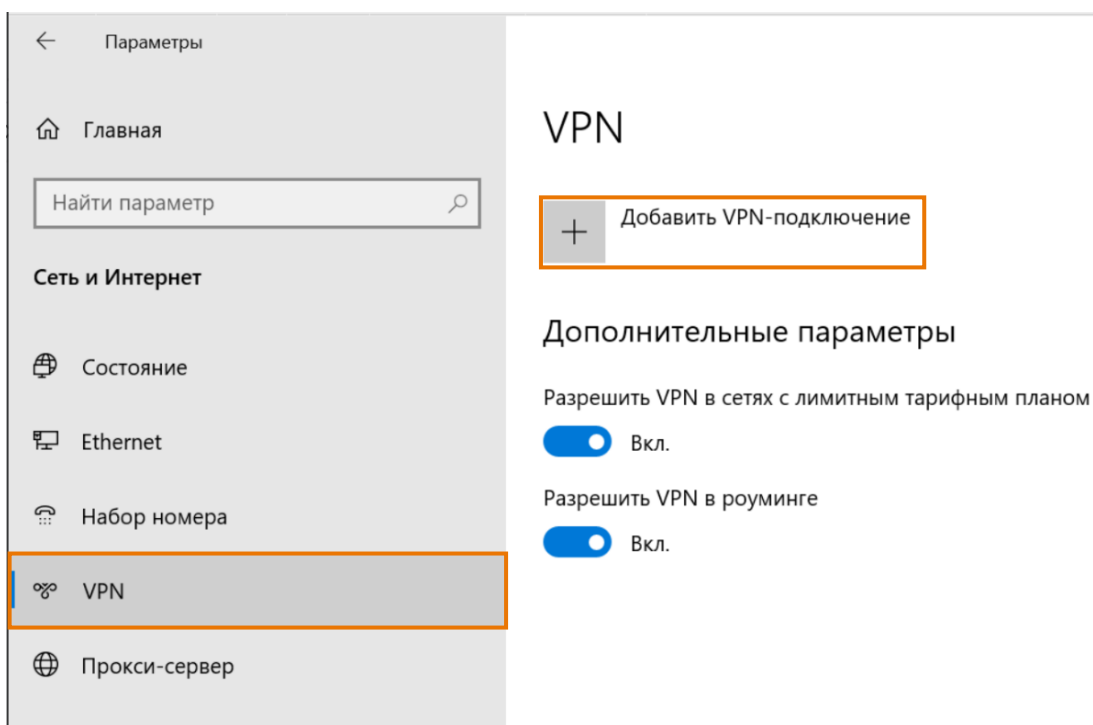
Сценарий настройки VPN-клиента с аутентификации посредством PEAP с методом MSCHAPv2 с логином и паролем

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.

3. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



4. В окне **Добавить VPN-подключение** настройте параметры подключения:

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (PEAP LOGIN);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;

Добавить VPN-подключение

Поставщик услуг VPN

Windows (встроенные) ▾

Имя подключения

PEAP LOGIN

Имя или адрес сервера

vpntest.ad16.net

Тип VPN

IKEv2 ▾

Тип данных для входа

Имя пользователя и пароль ▾

Имя пользователя (необязательно)

Пароль (необязательно)

☒ Запомнить мои данные для входа

Сохранить

5. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 2. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт: **Настройки параметров адаптера**:

Дополнительные сетевые параметры



Настройка параметров адаптера

Просмотр сетевых адаптеров и изменение параметров подключения.



Центр управления сетями и общим доступом

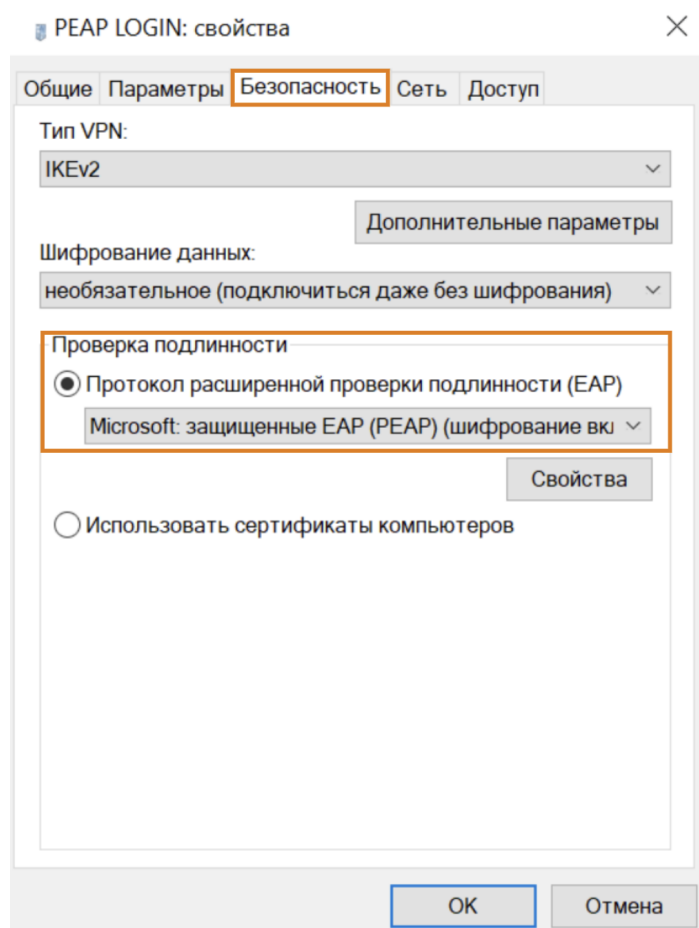
Определите, к каким данным вы хотите предоставить доступ для сетей, с которыми установлено соединение.

[Просмотр свойств оборудования и подключения](#)

[Брандмауэр Windows](#)

[Сброс сети](#)

2. Выберите только что созданное сетевое подключение **PEAP LOGIN** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:

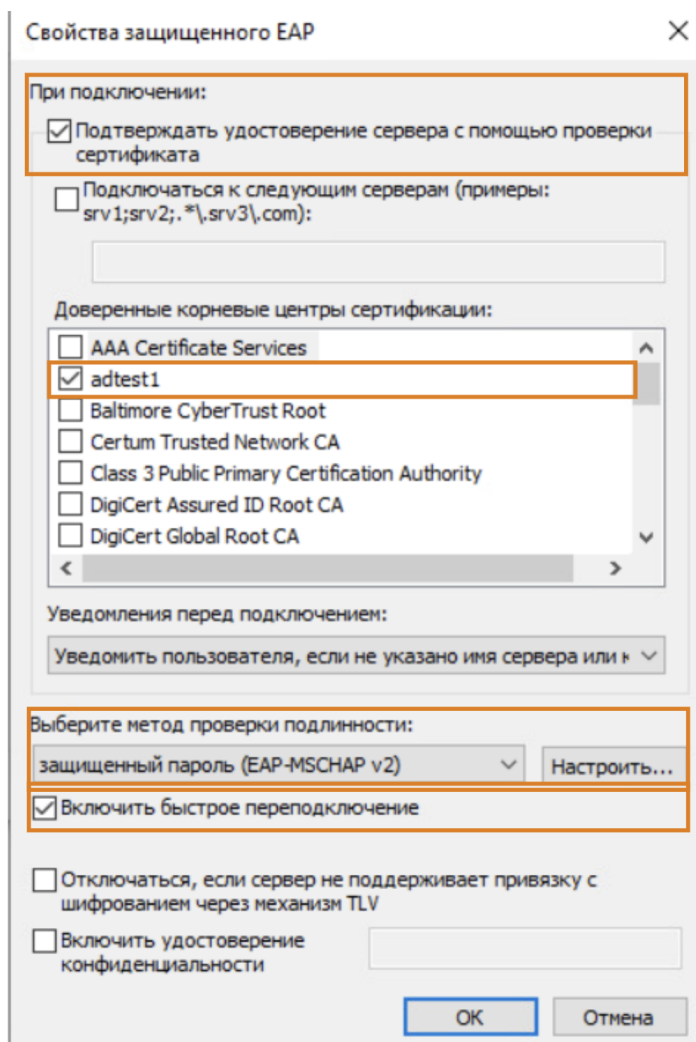


В поле **Проверка подлинности** выберите пункт: **Microsoft: защищенные EAP (PEAP) (шифрование включено)**.

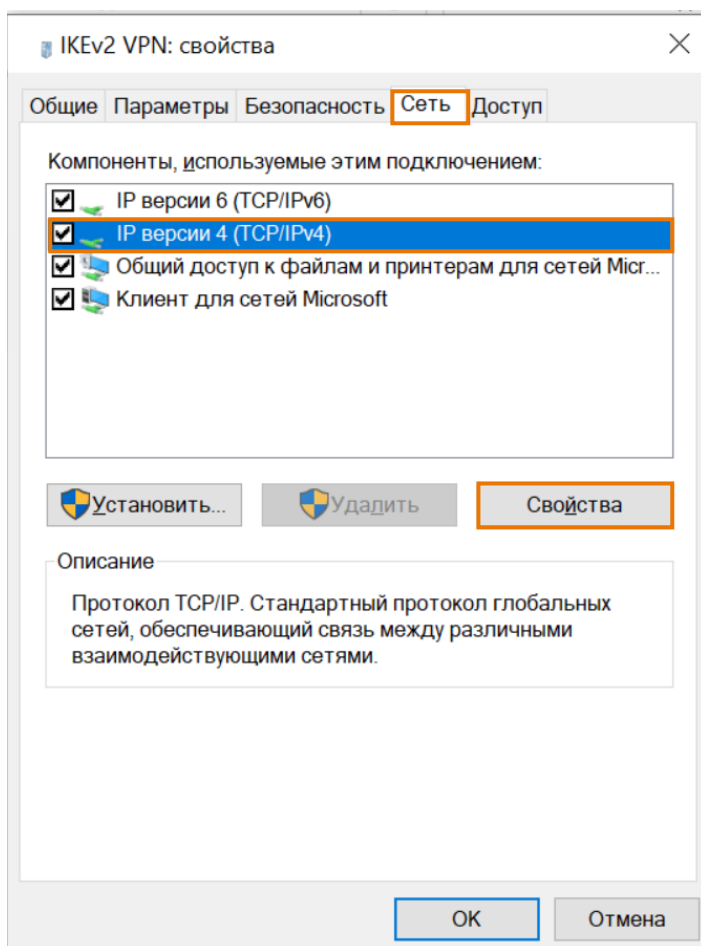
В свойствах проверки подлинности в поле выбора метода проверки необходимо выбрать: **Защищенный пароль (EAP-MSCHAP v2)**. В разделе

Доверенные корневые центры сертификации необходимо указать сертификат корневого центра.

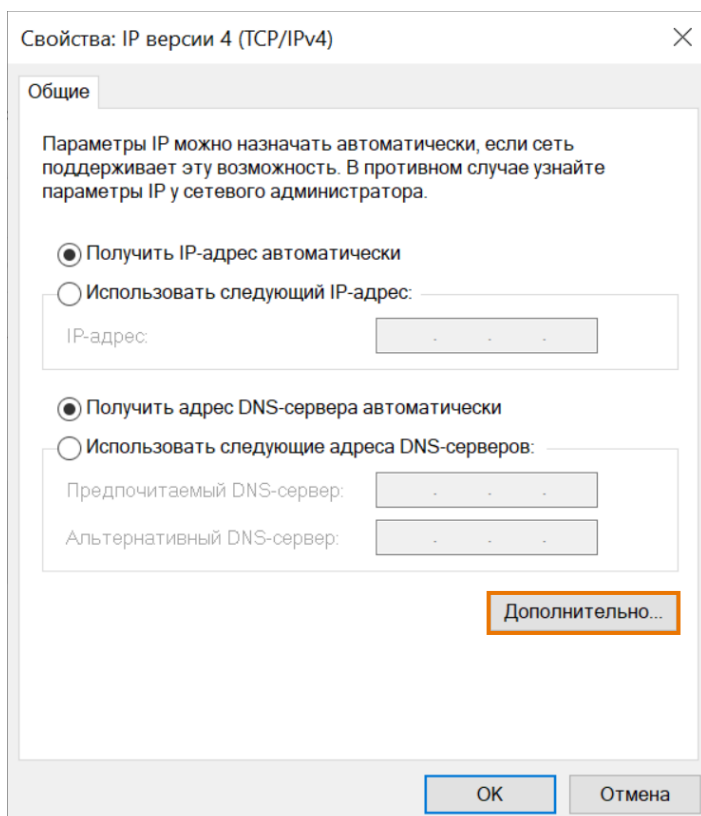
Флажки **Подтверждать удостоверение сервера с помощью проверки сертификата** и **Включить быстрое переподключение** могут быть установлены опционально:



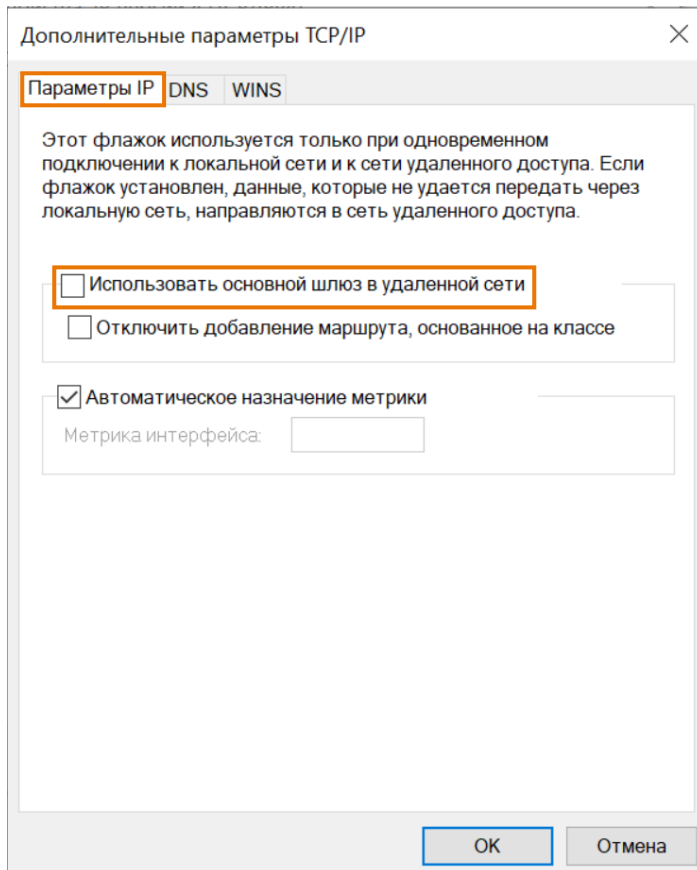
3. Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** откройте свойства **IP версии 4 (TCP/IPv4)**:



Нажмите **Дополнительно** в настройках общих параметров IP:



Уберите флажок в поле **Использовать основной шлюз в удалённой сети**:



4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **PEAP LOGIN** и нажмите **Подключиться**.

Проверка подключения

После установления VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

VPN							
utmcore@plaratanyan							
Пользователь ↑	Роль этого устройства	Серверное правило VPN	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
user (adtest1.net\user)	Сервер	eap-tls 2016	21 февраля 2...	172.30.250.2	172.25.2.48	?	aes

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

Журнал событий						
date >= 2025-02-21T00:00:00 AND date <= 2025-02-21T23:59:59 AND component = 'vpn'						
Узел	Время	Ком...	Тип события	Пользователь	IP источника	Детали события
utmcso...	13:38:33	VPN	Подключение пользователя к VPN прошло успешно	user (adtest1.net\user)	172.25.2.48	Логин: user, Серверное правило VPN: eap-tls 2016

На стороне удалённого Windows-компьютера добавится rppr-адаптер PEAP LOGIN:

```
Адаптер Ethernet Ethernet1:

DNS-суффикс подключения . . . . . : esafeline.com
Локальный IPv6-адрес канала . . . : fe80::19b2:703e:82a8:4fb6%10
IPv4-адрес. . . . . : 172.25.2.48
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 172.25.0.1

Адаптер PPP PEAP LOGIN:

DNS-суффикс подключения . . . . . :
IPv4-адрес. . . . . : 172.30.250.2
Маска подсети . . . . . : 255.255.255.255
Основной шлюз. . . . . :
```

Появится маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Шаге 6](#):

```
IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
0.0.0.0            0.0.0.0        172.25.0.1       172.25.2.48    25
15.0.0.0          255.255.255.0   On-link         172.30.250.2    26
15.0.0.255        255.255.255.255 On-link         172.30.250.2   281
127.0.0.0         255.0.0.0       On-link         127.0.0.1     331
127.0.0.1         255.255.255.255 On-link         127.0.0.1     331
127.255.255.255   255.255.255.255 On-link         127.0.0.1     331
172.25.0.0        255.255.0.0     On-link         172.25.2.48   281
172.25.2.48       255.255.255.255 On-link         172.25.2.48   281
172.25.2.75       255.255.255.255 On-link         172.25.2.48    26
172.25.255.255    255.255.255.255 On-link         172.25.2.48   281
172.30.0.0        255.255.0.0     On-link         172.30.250.2    26
172.30.250.2      255.255.255.255 On-link         172.30.250.2   281
172.30.255.255    255.255.255.255 On-link         172.30.250.2   281
224.0.0.0         240.0.0.0       On-link         127.0.0.1     331
224.0.0.0         240.0.0.0       On-link         172.25.2.48   281
224.0.0.0         240.0.0.0       On-link         172.30.250.2   281
255.255.255.255   255.255.255.255 On-link         127.0.0.1     331
255.255.255.255   255.255.255.255 On-link         172.25.2.48   281
255.255.255.255   255.255.255.255 On-link         172.30.250.2   281
=====
Постоянные маршруты:
Сетевой адрес      Маска      Адрес шлюза      Метрика
0.0.0.0            0.0.0.0     192.168.200.154  По умолчанию
=====
```

IP-адрес в удалённой сети доступен:


```

C:\Users\user1>ping 15.0.0.200

Обмен пакетами с 15.0.0.200 по 32 байтами данных:
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=5мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64
Ответ от 15.0.0.200: число байт=32 время=2мс TTL=64

Статистика Ping для 15.0.0.200:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 5 мсек, Среднее = 2 мсек

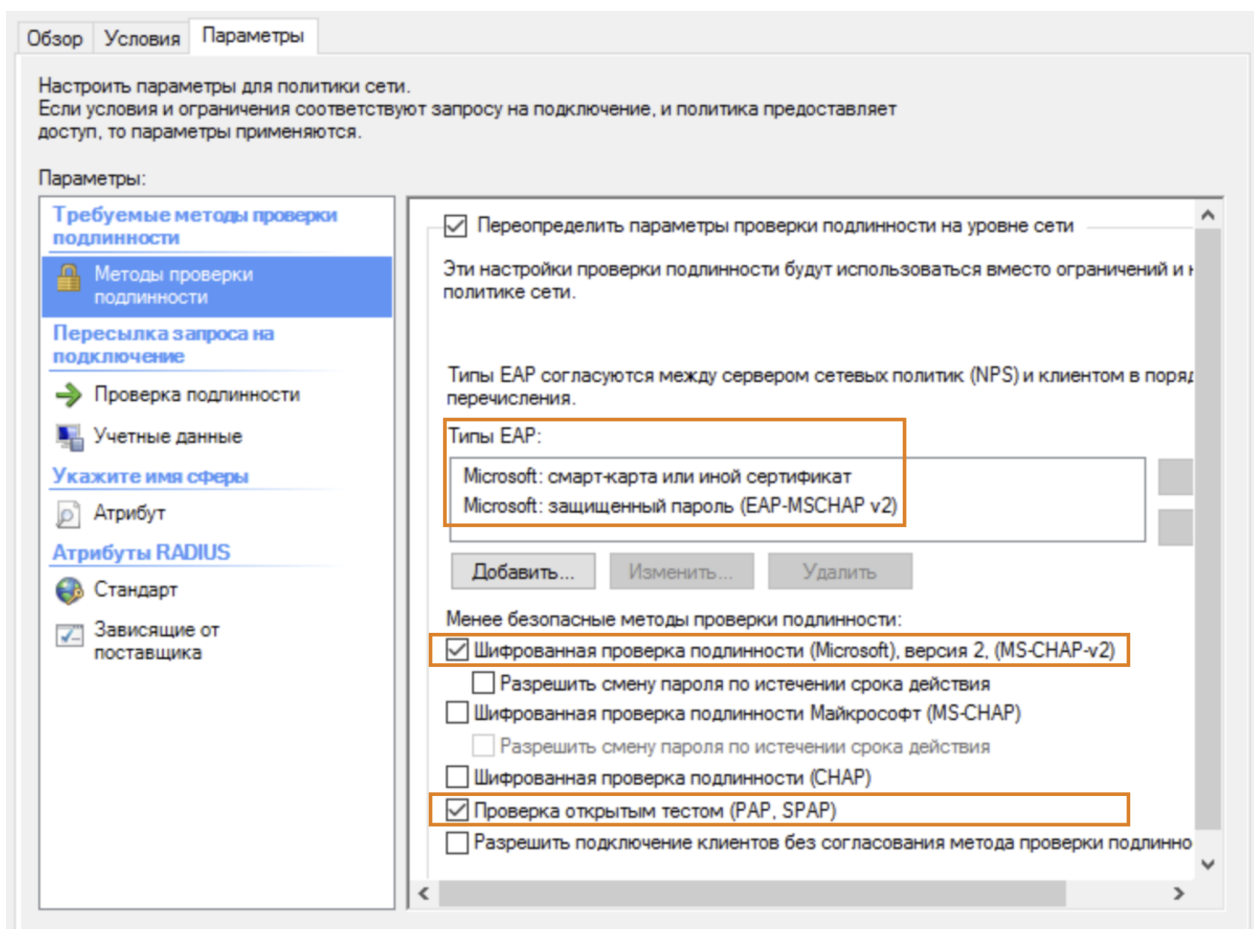
```

Приложение

Рассматривается настройка RADIUS-сервера на примере Windows Server 2019 с настроенной Active Directory.

Настройки политики запросов на подключение

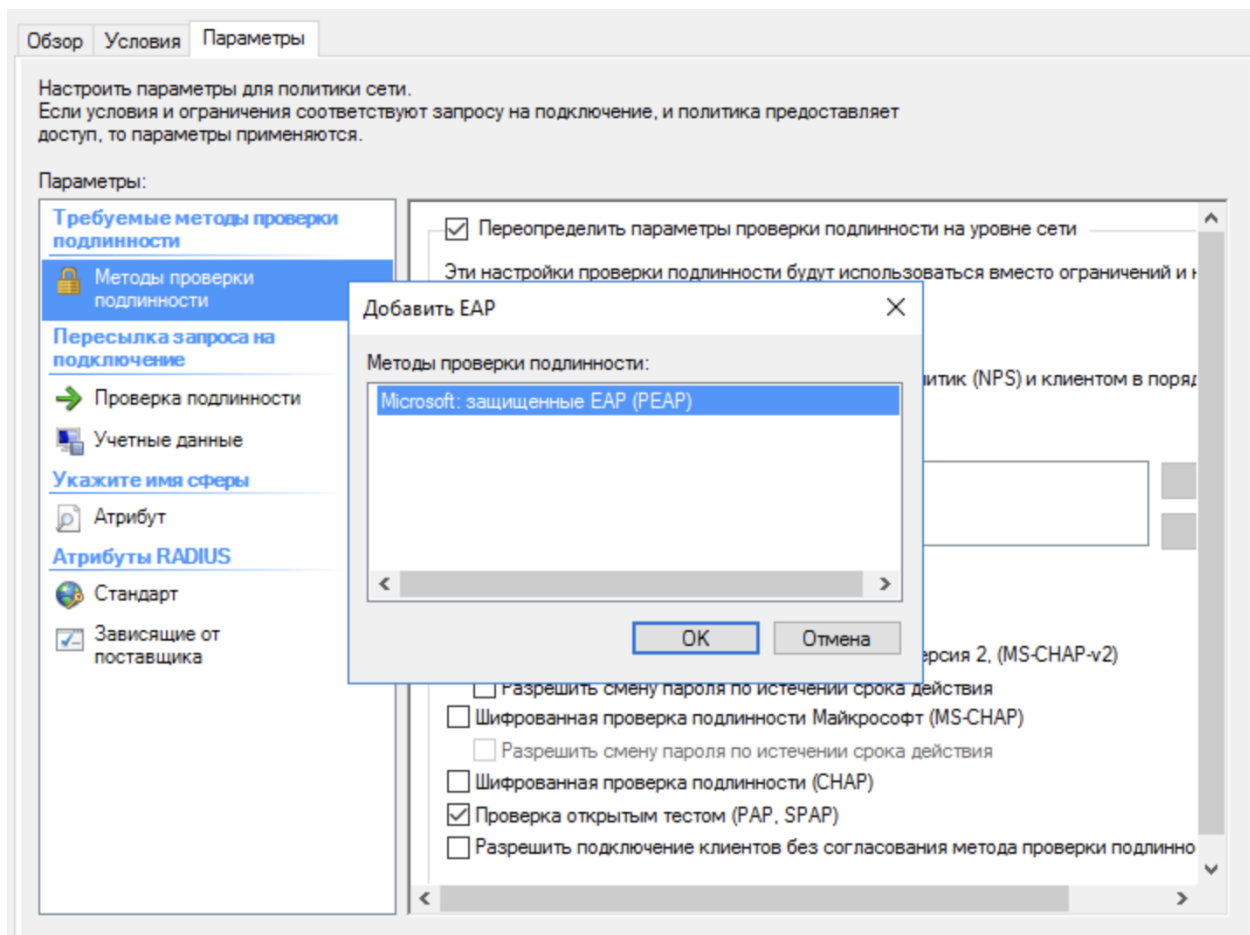
Для работы со сценариями аутентификации с помощью EAP-TLS и EAP MSCHAP v2 необходимы соответствующие типы EAP в настройках методов проверки подлинности сервера:

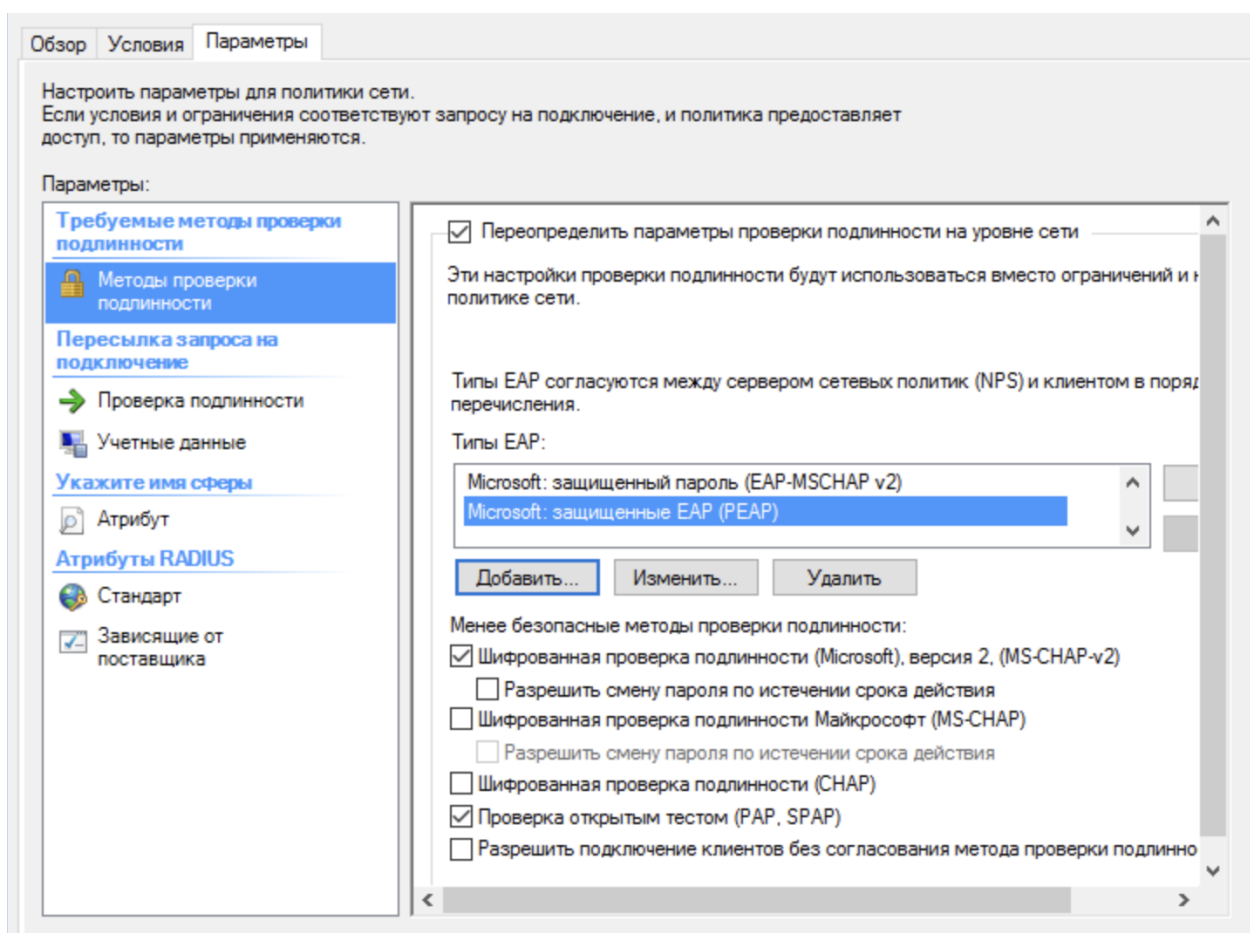


Необходимо разрешить пункт **Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2)**;

Метод PAP (**Проверка открытым тестом (PAP, SPAP)**) рекомендуется разрешить для параллельной работы IKEv1 AAA. Если планируется использовать только IKEv2 AAA, то достаточно включения только EAP-MSCHAP v2.

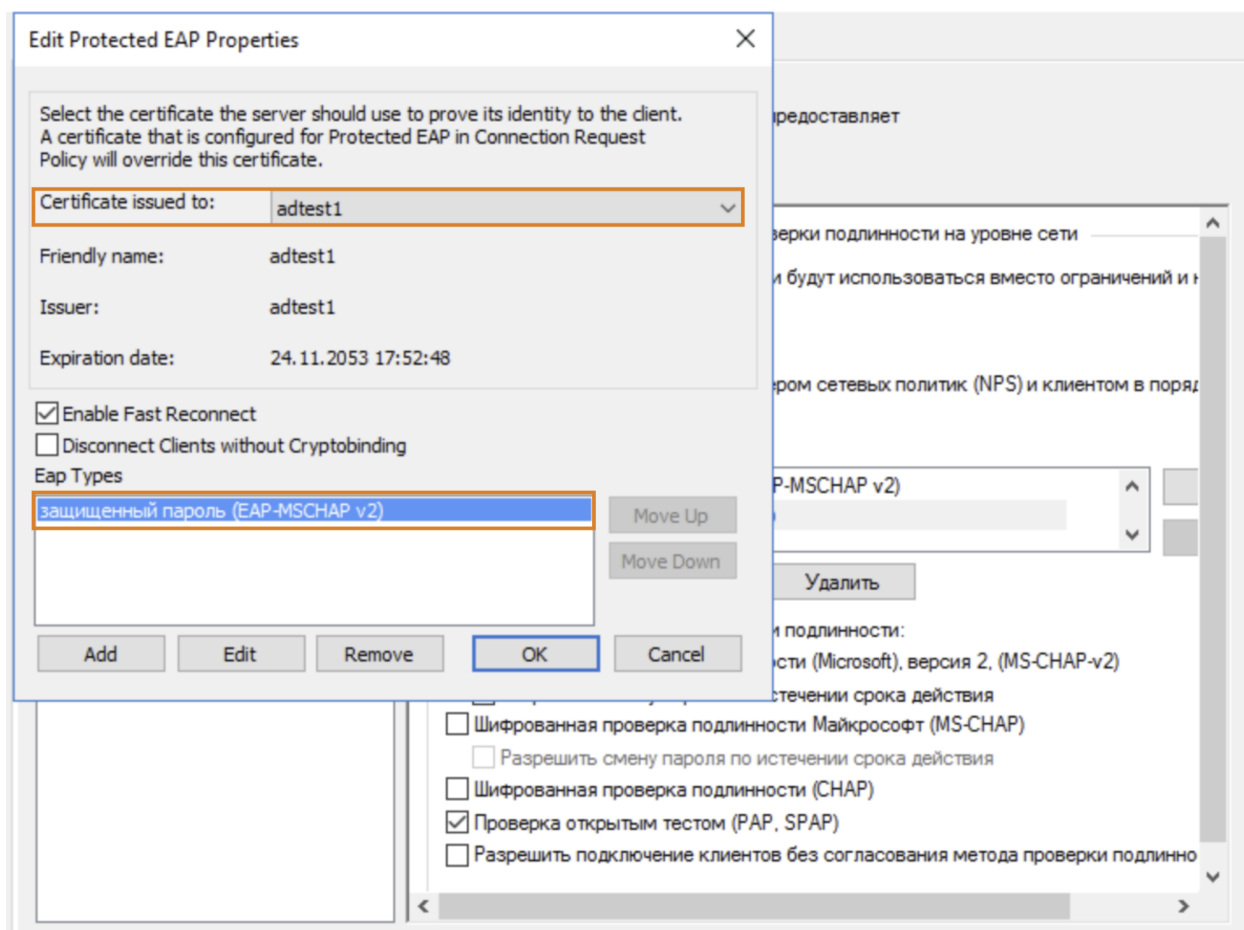
Для работы со сценариями аутентификации с помощью PEAP необходимо добавить соответствующий тип EAP в настройках методов проверки подлинности сервера:



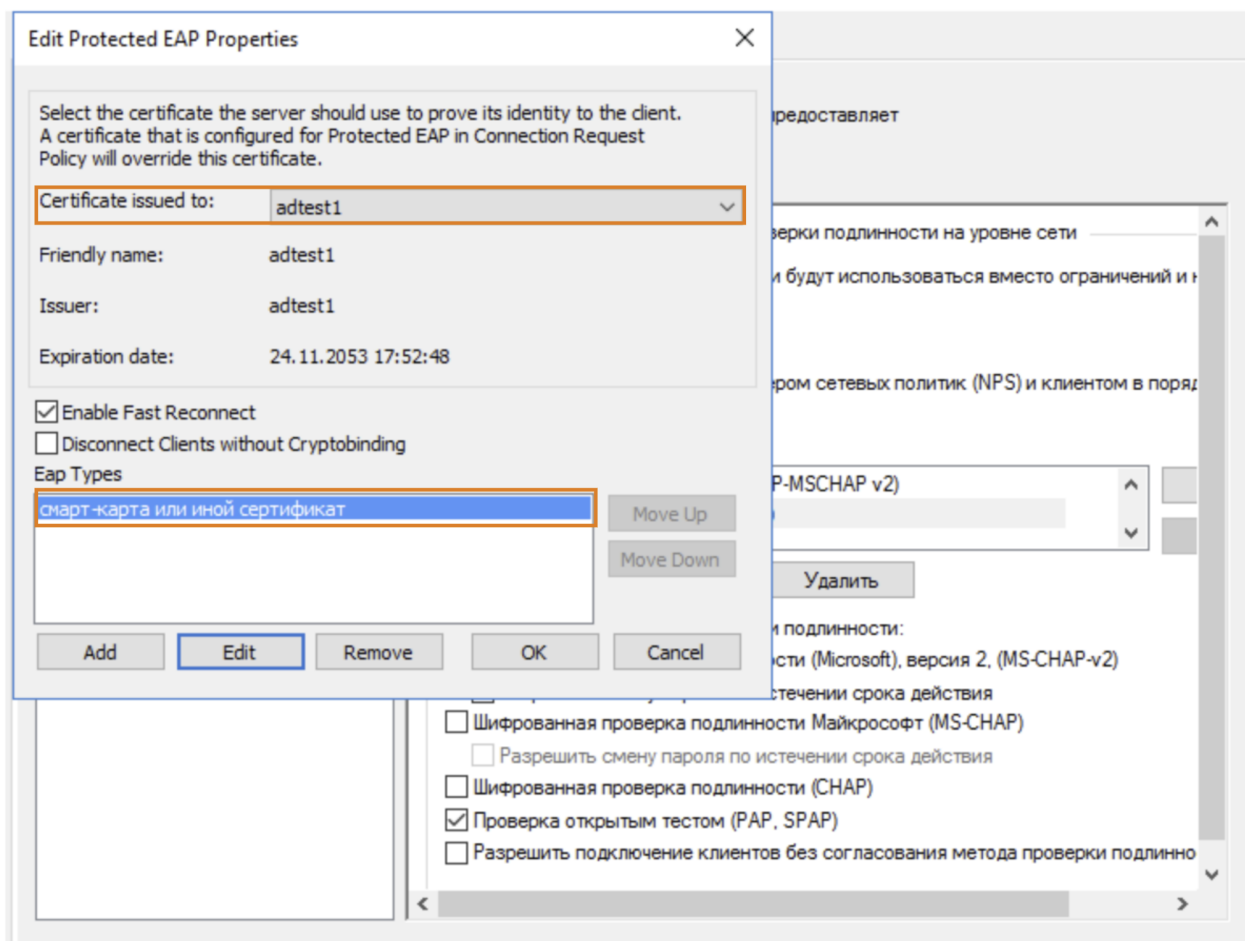


В настройках добавленного метода укажите сертификат корневого центра и необходимый тип EAP.

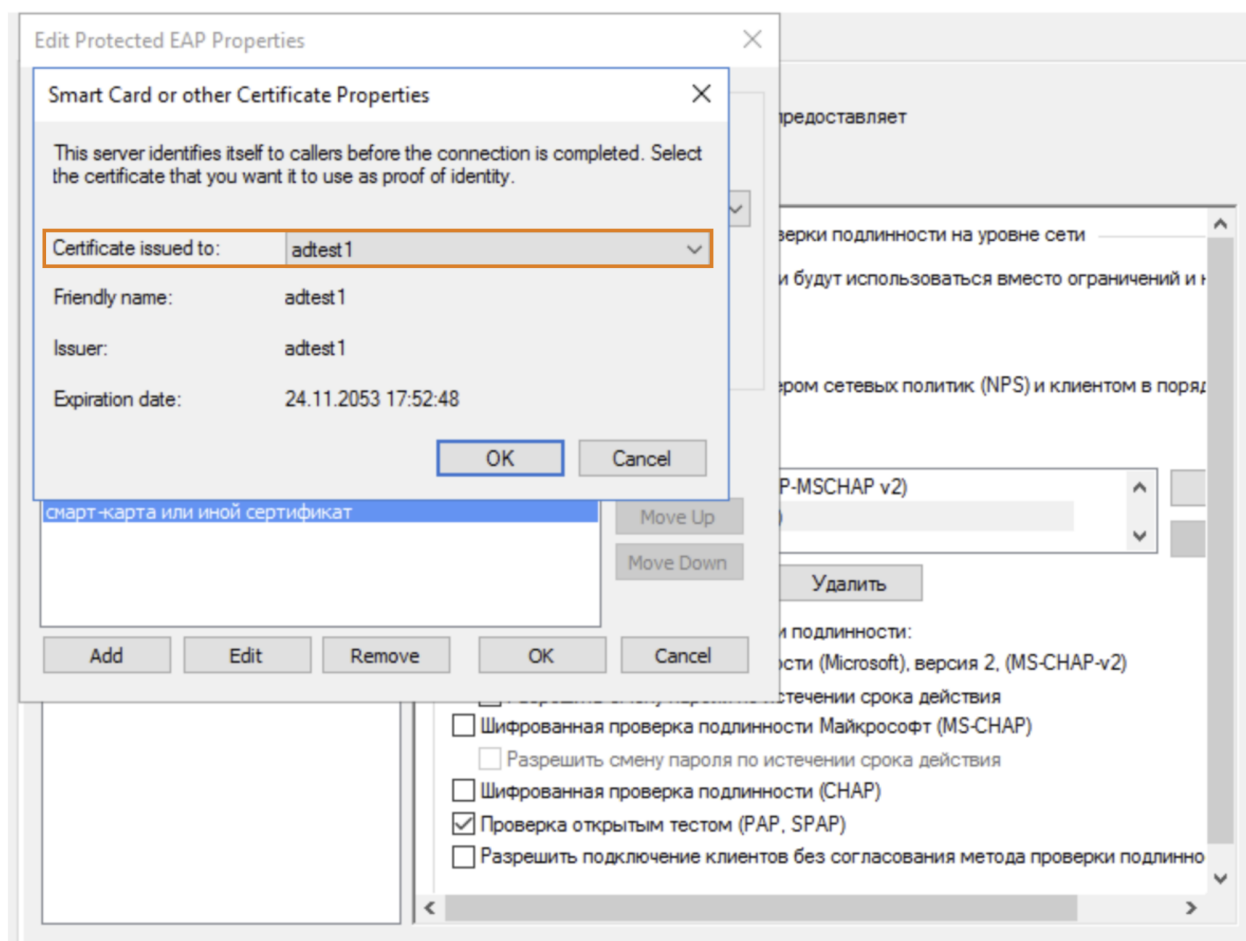
Для сценария PEAP с аутентификацией по MSCHAPv2 с логином и паролем:



Для сценария PEAP с аутентификацией по сертификату:



Для сертификата далее нажмите **Edit** и добавьте сертификат корневого центра:



НАСТРОЙКА VPN (ВЕРСИЯ 7.5.0 И ВЫШЕ)

Общие принципы

С помощью функции VPN-сервера на UserGate NGFW вы можете создавать VPN-подключения следующих типов:

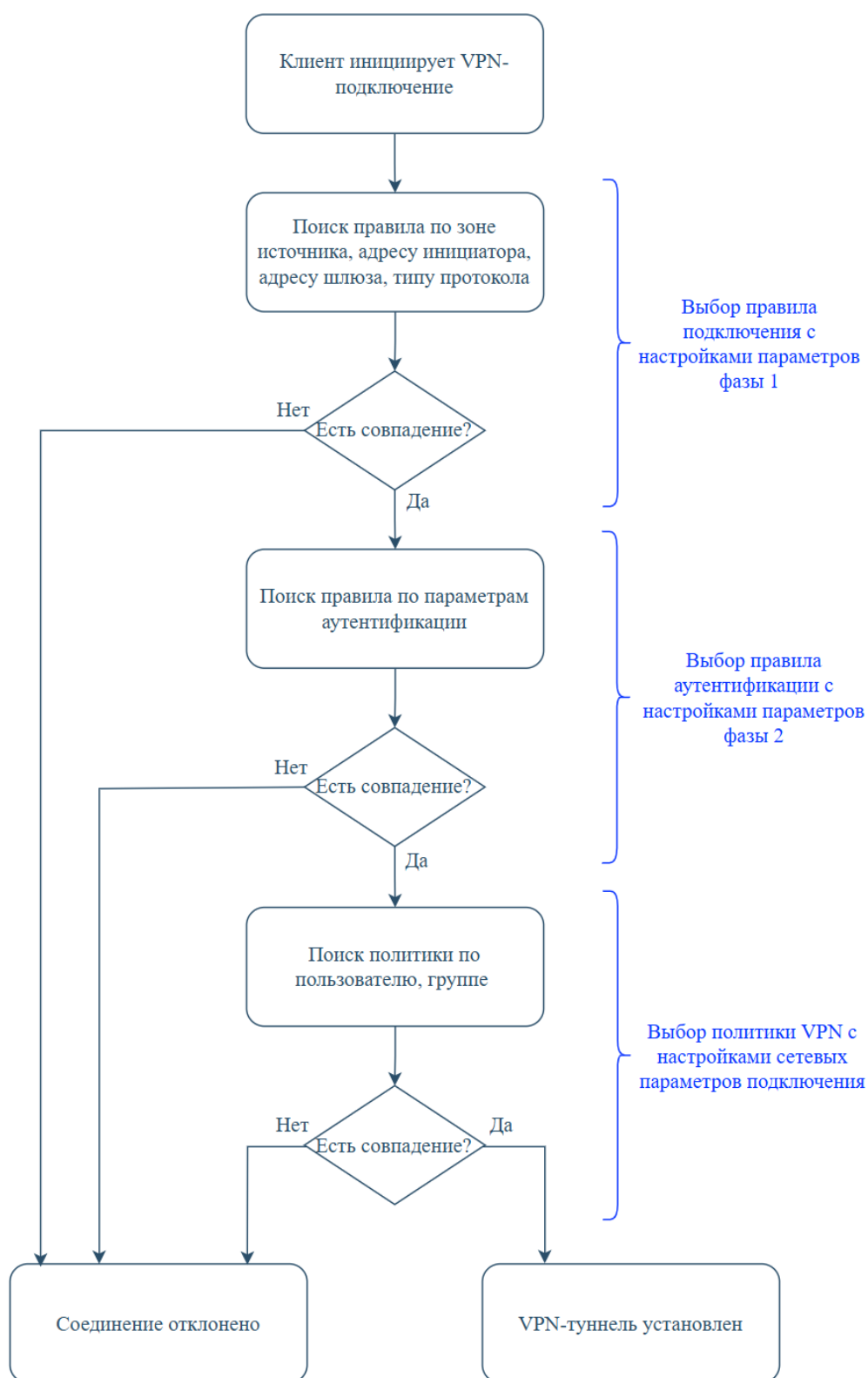
- Защищенное соединение офисов (site-to-site VPN). Подключение типа сервер-сервер позволяет объединить офисы компании в единую логическую сеть. UserGate NGFW может выступать как в роли узла-инициатора соединения (initiator), так и в роли узла-ответчика (responder).
- Удаленный доступ клиентов в сеть офиса (remote access VPN). В этом сценарии UserGate NGFW выступает в роли VPN-сервера, а устройства пользователей с установленным VPN-клиентом — в роли конечных устройств. В качестве VPN-клиента на устройствах пользователей может использоваться ПО UserGate Client (клиенты для [Windows](#), [Linux](#) и [macOS](#)),

также поддерживаются встроенные VPN-клиенты большинства известных операционных систем, таких как Windows, Linux, Mac OS X, iOS, Android.

Серверные правила VPN в UserGate NGFW версии 7.5.0 и выше реализованы в виде модульной структуры, состоящей из трех отдельно настраиваемых объектов:

- правил подключения;
- правил аутентификации;
- политик VPN.

С помощью такого подхода обеспечивается гибкость в комбинировании параметров на каждом этапе — от инициации сессии до применения индивидуальных настроек доступа в сеть для отдельных пользователей или групп пользователей. Одному методу подключения может соответствовать несколько способов аутентификации; каждому способу аутентификации может соответствовать один или несколько вариантов сетевых параметров подключения.



Подробнее о настройке VPN-подключений типа site-to-site — в разделе [«Настройка VPN для защищенного соединения офисов»](#), о настройке VPN-подключений типа remote access — в разделе [«Настройка VPN для удаленного доступа в сеть»](#).

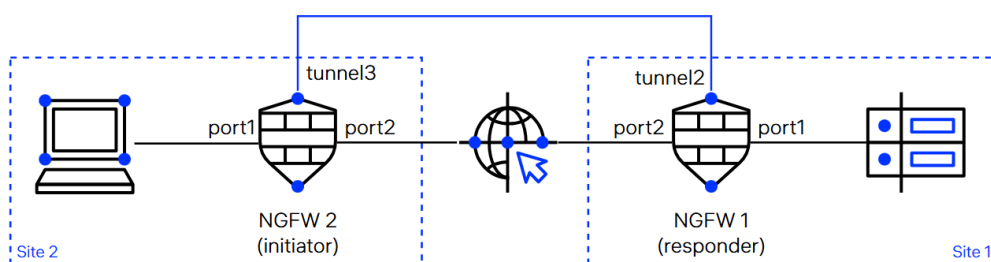
Настройка VPN для защищенного соединения офисов

Примечание

В этом разделе описан алгоритм настройки параметров VPN-соединений для версии 7.5.0 и выше.

VPN-подключение, с помощью которого создается защищенное соединение локальных сетей удаленных офисов, называется site-to-site VPN.

При подключении один VPN-сервер выступает в роли инициатора соединения (initiator), а другой — в роли ответчика (responder). После успешного создания туннеля распределение ролей VPN-серверов не оказывает влияния на характеристики соединения — передача данных через туннель осуществляется двунаправленно и симметрично.



Вы можете создать VPN-подключение между устройствами UserGate NGFW, либо между UserGate NGFW и VPN-шлюзами сторонних производителей. UserGate NGFW может выступать как в роли инициатора соединения, так и в роли ответчика.

При создании VPN-туннелей в сценарии site-to-site могут использоваться протоколы:

- L2TP/IPsec (IKEv1) — только между устройствами UserGate;
- IPsec (IKEv1);
- IPsec (IKEv2).

Для создания VPN-подключения необходимо выполнить настройки соответствующих параметров на обоих граничных узлах защищенного соединения: узле-инициаторе и узле-ответчике.

Настройка UserGate NGFW в качестве узла-ответчика

Для работы UserGate NGFW в качестве VPN-сервера (ответчика) в сценарии site-to-site VPN необходимо настроить:

- [сетевые параметры](#);
- [параметры аутентификации](#);
- [правила подключения](#);
- [правила аутентификации](#);
- [политики VPN](#);
- [доступ к сетевым ресурсам](#).

Настройка сетевых параметров

На узле UserGate NGFW, исполняющем роль VPN-сервера (ответчика), необходимо выполнить ряд дополнительных настроек сетевых параметров:

- разрешить доступ к узлу для установления VPN-соединения;
- создать зону для контроля подключаемых узлов;
- создать VPN-интерфейс для организации туннеля.

Предоставление доступа для VPN-соединений

В настройках зоны, из которой будут подключаться узлы-инициаторы (например, Untrusted), активируйте доступ к сервису VPN. Для этого в веб-консоли UserGate NGFW перейдите в раздел **Настройки → Сеть → Зоны**, затем в параметрах контроля доступа зоны поставьте флажок для сервиса VPN. Подробнее о создании и настройках параметров зон — в разделе «[Настройка зон](#)».

Создание зоны для VPN-подключений

Создайте зону, к которой будут принадлежать подключаемые по VPN узлы. Эту зону в дальнейшем можно будет использовать в правилах политик безопасности.

В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны**. Подробнее о создании и настройках зон — в разделе «[Настройка зон](#)».

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения узлов-инициаторов VPN-подключения. Такой тип интерфейса является кластерным — он будет автоматически создаваться на всех узлах UserGate NGFW, входящих в кластер конфигурации. Если настроен кластер отказоустойчивости, узлы-инициаторы будут автоматически переключаться на резервный узел VPN-сервера в случае обнаружения проблем с активным узлом.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы**. Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**. Подробнее о создании VPN-интерфейса — в разделе «[Настройка интерфейсов](#)».

Настройка параметров аутентификации

Порядок взаимной аутентификации узлов, участвующих в организации site-to-site VPN, описывается [правилами аутентификации](#).

Чтобы настроить правила аутентификации, сначала необходимо создать набор средств аутентификации (например, общие ключи, сертификаты или профили клиентских сертификатов), которые затем будут использоваться в правилах в зависимости от выбранного метода аутентификации.

При настройке защищенного IPsec-соединения могут понадобиться следующие средства аутентификации узлов:

- Общий ключ (pre-shared key, PSK). Используется для аутентификации в протоколах IKEv1 и IKEv2. Ключ задается в параметрах [правил подключения](#) (для IKEv1) или [правил аутентификации](#) (для IKEv2) на VPN-сервере (ответчике), а также в настройках [параметров подключения](#) на узле-инициаторе. Для успешного установления соединения значения ключа на обеих сторонах должны совпадать.
- Сертификаты VPN-серверов. Применяются для аутентификации с использованием инфраструктуры открытых ключей (PKI) в протоколе IKEv2. Такие сертификаты необходимо заранее создать и импортировать в UserGate NGFW.

О примерах создания и использования сертификатов для IKEv2 VPN — в разделе «[Приложение](#)». О правилах импорта сертификатов в UserGate NGFW — в разделе «[Управление сертификатами](#)».

- Профили клиентских сертификатов. Позволяют идентифицировать узел-инициатор по определенному атрибуту его сертификата, а также проверить цепочку доверия и подлинность сертификата с учетом списков отозванных сертификатов. При создании профиля используются сертификаты корневых и промежуточных удостоверяющих центров, выдавших сертификаты узлов-инициаторов. Подробнее о профилях клиентских сертификатов — в разделе «[Профили клиентских сертификатов](#)».

Чтобы VPN-сервер мог проверить IP-адрес узла-инициатора при установлении соединения по IPsec IKEv2, в сертификате инициатора в поле iPAddress расширения SAN (Subject Alternative Name) должен быть указан тот IP-адрес, с которого поступит запрос на подключение. При этом в профиле клиентского сертификата на VPN-сервере в параметре **Получать имя пользователя из** необходимо выбрать значение **Subject altname IPv4**.

Если между узлом-инициатором и VPN-сервером используется NAT, IP-адрес из сертификата не совпадет с фактическим адресом источника пакетов, из-за чего соединение не будет установлено. Для такого сценария можно в поле **Получать имя пользователя из** в профиле клиентского сертификата выбрать любое другое значение, кроме **Subject altname IPv4**, VPN-сервер в таком случае не будет выполнять проверку IP-адреса инициатора соединения.

Для настройки VPN-туннеля с использованием протокола L2TP на стороне VPN-сервера (ответчика) необходимо создать учетную запись для аутентификации узла-инициатора, а также настроить профиль аутентификации, определяющий применяемый метод проверки подлинности.

В веб-консоли UserGate NGFW профили аутентификации создаются в разделе **Настройки → Пользователи и устройства → Профили аутентификации**. Подробнее о профилях аутентификации — в разделе «[Профили аутентификации](#)».

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом (узлом-инициатором) и завершается ответом VPN-сервера (узла-ответчика) — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах

задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Для создания правила подключения в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила подключения** и нажмите **Добавить**.

2. Выберите протокол подключения **IKE**.

3. На вкладке **Общие** в свойствах протокола IKE:

- Укажите название и описание правила;
- Выберите версию протокола IKE:
 - **IKEv1PSK**. Для этого протокола выберите режим работы IKEv1 (основной или агрессивный) и укажите значение общего ключа (pre-shared key). Ключ должен совпадать [на узле-инициаторе](#) и на узле-ответчике.
 - **IKEv2**.

4. На вкладке **Источник** укажите зоны и адреса, с которых разрешено принимать подключения к VPN:

- Укажите зону инициатора подключения;
- Укажите адрес инициатора подключения:
 - выберите или создайте список IP-адресов;
 - выберите или создайте список доменов;
 - выберите GeoIP.

Примечание

Обработка трафика происходит по следующей логике:

- условия объединяются по логическому ИЛИ, если указаны несколько списков IP-адресов или доменов;
- условия объединяются по логическому И, если указаны GeoIP и списки IP-адресов или доменов.

5. На вкладке **Назначение** выберите или создайте список IP-адресов или доменных имен интерфейса, на который будут приходить запросы на VPN-подключение. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

6. На вкладке **Фаза 1** укажите параметры настройки фазы 1 для установления защищенного канала IKE SA:

- Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
- Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения **R - U - THERE** для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
 - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
 - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается.
 - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданный канал. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.
- Выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.
- Выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.

О создании правил подключения с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа узла-инициатора на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

Для создания правила аутентификации в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила аутентификации** и нажмите **Добавить**.
2. Выберите сценарий **site-to-site** и затем протокол установления защищенного соединения:
 - **IPsec only/IKEv1;**
 - **IKEv2;**
 - **IPsec/L2TP.**
3. На вкладке **Общие** в свойствах выбранного протокола:
 - Для протокола IPsec only/IKEv1:
 - Укажите название и описание правила;
 - Выберите одно или несколько созданных ранее [правил подключения](#).
 - Для протокола IKEv2:
 - Укажите название и описание правила;
 - Выберите режим аутентификации (PKI или PSK):
 - Для аутентификации с помощью сертификатов (PKI) укажите созданные ранее [сертификат сервера и профиль клиентского сертификата](#);
 - Для аутентификации с помощью общего ключа (PSK) укажите общий ключ и созданный ранее [сертификат сервера](#).

- Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (initiator) и ответчика (responder). В качестве идентификатора можно указать IP-адрес узла или FQDN.
 - Выберите одно или несколько созданных ранее [правил подключения](#).
- Для протокола IPsec/L2TP:
 - Укажите название и описание правила;
 - Выберите созданный ранее [профиль аутентификации](#) для пользователей VPN.
 - Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (initiator) и ответчика (responder). В качестве идентификатора можно указать IP-адрес узла или FQDN.
 - Выберите одно или несколько созданных ранее [правил подключения](#).

4. На вкладке **Фаза 2** укажите параметры настройки фазы 2 для установления защищенного канала IPsec SA:

- Укажите время жизни ключа. По истечении этого времени узлы должны сменить ключ шифрования.
- Укажите максимальный размер данных, шифруемых одним ключом.

Примечание

Если заданы оба параметра (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела параметр запустит пересоздание ключей сессии.

- При необходимости включите параметр NAT keepalive. NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер,

находящийся за шлюзом NAT, периодически отправляет пакеты keeralive в сторону противоположного узла соединения для поддержания сессии NAT активной.

- Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
- Для протоколов IPsec only/IKEv1 и IKEv2 в блоке **Peer networks** укажите адреса локальных и удаленных подсетей. Адреса подсетей используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Если поставить флажок **Не проверять сети инициатора**, VPN-сервер не будет проверять подсети инициатора соединения в селекторе трафика при организации защищенного канала передачи данных. Функция удобна для подключения множества клиентов (инициаторов) по одному правилу.

Для протокола IKEv2 можно разрешить работу протоколов динамической маршрутизации через туннель.

О создании правил аутентификации с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации узла-инициатора и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Для создания политики VPN в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Политики VPN** и нажмите **Добавить**.
2. Выберите сценарий **site-to-site** и затем протокол установления VPN-туннеля:
 - IPsec;

IPsec/L2TP.

•

3. Для протокола IPsec:

- На вкладке **Общие** в свойствах протокола:
 - Укажите название и описание правила.
 - Выберите VPN-адаптер, который будет использоваться для установления подключения.
 - Выберите одно или несколько созданных ранее правил аутентификации.

4. Для протокола IPsec/L2TP:

- На вкладке **Общие** в свойствах протокола:
 - Укажите название и описание правила.
 - Выберите одно или несколько созданных ранее правил аутентификации.
- На вкладке **Пользователи** выберите учетные записи или группы, созданные для серверов, которым разрешено подключаться по VPN.
- На вкладке **Подсети для VPN**:
 - Укажите VPN-интерфейс, который будет использоваться для подключения.
 - Укажите диапазон IP-адресов, которые будут использованы узлами-инициаторами подключения. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с этой сетью. Не указывайте адреса сети и широковещательный адрес.
 - Укажите маску сети VPN.
 - Укажите DNS-серверы, которые будут переданы узлу-инициатору подключения, или поставьте флажок **Использовать системные DNS**, в этом случае узел-инициатор будет использовать системные DNS-серверы.

- На вкладке **Маршруты VPN** укажите маршруты, передаваемые узлу-инициатору в виде бесклассовой адресации (CIDR) или заранее созданный список IP-адресов.

О создании политик VPN с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка доступа к ресурсам

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в веб-консоли UserGate NGFW в разделе **Настройки → Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из [зоны для VPN-подключений](#) в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана — в разделе «[Межсетевой экран](#)».

Для примера в веб-консоли создано правило межсетевого экрана VPN for site-to-site to Trusted and Untrusted, разрешающее весь трафик из зоны VPN for site-to-site в зоны Trusted и Untrusted. Правило отключено по умолчанию

Чтобы трафик передавался обратно клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например созданную ранее [зону для VPN-подключений](#).

Настройка UserGate NGFW в качестве узла-инициатора подключения

Для работы UserGate NGFW в качестве инициатора VPN-соединения в сценарии site-to-site VPN необходимо настроить:

- [сетевые параметры](#);
- [параметры аутентификации](#);
- [параметры подключения клиента](#);
- [клиентские правила](#).

Настройка сетевых параметров

На узле UserGate NGFW, исполняющем роль инициатора VPN-соединения, необходимо выполнить ряд дополнительных настроек сетевых параметров:

- создать зону для контроля VPN-подключений;

создать VPN-интерфейс для организации туннеля.

Создание зоны для VPN-подключений

Создайте зону, которой будут принадлежать интерфейсы, используемые для подключения по VPN. В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны**. Подробнее о создании и настройках зон — в статье [«Настройка зон»](#).

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения по VPN.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы**. Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**, далее в настройках VPN-адаптера задайте необходимые параметры. Подробнее о создании VPN-интерфейса — в разделе [«Настройка интерфейсов»](#).

Контроль доступа к сетевым ресурсам

Чтобы трафик передавался на VPN-сервер из нужной зоны узла-источника через VPN-туннель, создайте правило межсетевого экрана, разрешающее трафик между зоной для VPN-подключений и зонами назначения. Подробнее о создании и настройке правил межсетевого экрана — в разделе [«Межсетевой экран»](#).

Настройка параметров аутентификации

При настройке защищенного IPsec-соединения с использованием протокола IKEv2 можно применять аутентификацию на основе сертификатов (PKI). Для этого необходимо заранее создать сертификат и импортировать его на узел, выступающий в роли VPN-клиента (инициатора соединения), через веб-интерфейс в разделе **Настройки → Консоль администратора → Сертификаты..**

Примечание

Если VPN-сервер выполняет проверку IP-адреса узла-инициатора соединения по сертификату, сертификат узла-инициатора должен содержать значение IP-адреса, с которого придет запрос на подключение к VPN-серверу, в поле iPAddress расширения SAN (Subject Alternative Name).

О примерах создания и использования сертификатов для IKEv2 VPN — в разделе [«Приложение»](#).

Настройка параметров подключения

При настройке VPN-подключения указываются используемые протоколы для установления соединения, выбираются методы аутентификации, а также определяются параметры обеих фаз формирования защищенного канала.

Для настройки параметров подключения узла-инициатора в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN site-to-site клиент → Подключение клиента** и нажмите **Добавить**.

2. Выберите протокол установления защищенного соединения:

- **IPsec only/IKEv1;**
- **IKEv2;**
- **IPsec/L2TP.**

3. На вкладке **Общие** в свойствах выбранного протокола:

- Для протокола IPsec only/IKEv1:
 - Укажите название и описание подключения;
 - Выберите режим работы IKE (основной или агрессивный);
 - Укажите общий ключ (pre-shared key). Ключ должен совпадать на узле-инициаторе и [на узле-ответчике](#).
 - Укажите параметр идентификации узла-инициатора. В качестве идентификатора можно указать IP-адрес узла или FQDN.

Если флажок не поставлен, механизм согласования сетевых параметров для проверки IP-адреса туннельного интерфейса на VPN-сервере не применяется. Значение IP-адреса определяется настройками туннельного интерфейса на узле-инициаторе.

- Для протокола IKEv2:
 - Укажите название и описание подключения;

- Укажите параметры взаимной идентификации граничных узлов соединения: инициатора (**Initiator**) и ответчика (**Responder**). В качестве идентификатора можно указать IP-адрес узла или FQDN.
- Укажите параметры аутентификации (логин и пароль) узла-инициатора на узле-ответчике. Параметры аутентификации должны соответствовать параметрам [учетной записи](#), созданной при настройке узла-ответчика.

4. На вкладке **Фаза 1** укажите параметры настройки фазы 1 для установления защищенного канала IKE SA:

- Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
- Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения **R - U - THERE** для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
 - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
 - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.
 - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.

- Выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.
- Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы, используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.

5. На вкладке **Фаза 2** укажите параметры настройки фазы 2 для установления защищенного канала IPsec SA:

- Укажите время жизни ключа. По истечении этого времени узлы должны сменить ключ шифрования.
- Укажите максимальный размер данных, шифруемых одним ключом.

Примечание

Если заданы оба значения (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела параметр запустит пересоздание ключей сессии.

- Выберите алгоритмы аутентификации и шифрования в блоке **Безопасность**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
- Для протоколов IPsec only/IKEv1 и IKEv2 в блоке **Peer networks** укажите адреса локальных и удаленных подсетей. Адреса подсетей используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения.

Для протокола IKEv2 можно разрешить работу протоколов динамической маршрутизации через туннель.

О настройках параметров подключения узла-инициатора с помощью команд интерфейса командной строки — в разделе «[Настройка клиентских правил](#)».

Настройка клиентских правил

Клиентское правило в сценарии site-to-site VPN используется для инициирования подключения к VPN-серверу (узлу-ответчику).

Для настройки клиентского правила в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN site-to-site клиент → Клиентские правила** и нажмите **Добавить**.
2. Укажите название и описание клиентского правила.
3. Выберите одно из созданных ранее [подключений клиента](#).
4. Выберите ранее созданный [VPN-интерфейс](#).
5. Укажите адрес VPN-сервера (ответчика) в формате IP-адреса или FQDN.

О настройках клиентских правил с помощью команд интерфейса командной строки — в разделе «[Настройка клиентских правил](#)».

После завершения настройки параметров VPN-сервиса узел-инициатор получает возможность установить соединение с VPN-сервером (ответчиком). При корректной конфигурации параметров будет сформирован VPN-туннель. Для разрыва соединения необходимо отключить клиентское VPN-правило.

Если VPN-соединение не установилось, в разделе клиентского правила в поле **Последняя ошибка** отобразится описание ошибки установления соединения.

События работы VPN-сервера (изменения параметров правил, установление соединений, ошибки установления соединений) записываются в системном журнале событий (Event log). Подробнее — в разделе «[Журналирование событий VPN-сервера](#)».

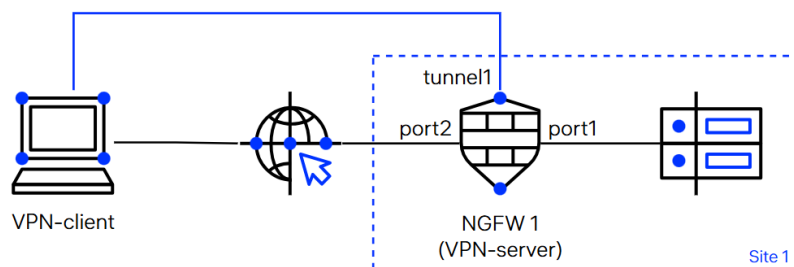
Настройка VPN для удаленного доступа в сеть



Примечание

В этом разделе описан алгоритм настройки параметров VPN-соединений для версии 7.5.0 и выше.

VPN-подключение, с помощью которого пользователи могут получить защищенный доступ к сети компании через интернет, называется remote access VPN.



В этом типе подключения UserGate NGFW выступает в роли VPN-сервера, а устройства пользователей — в роли конечных устройств. В качестве клиентского ПО на устройствах пользователей может использоваться [UserGate Client](#), также поддерживаются встроенные клиенты большинства известных операционных систем, таких как Windows, Linux, macOS, iOS, Android.

Для организации защищенного соединения могут использоваться протоколы:

- IPsec (IKEv2);
- DTLS — только при работе с UserGate Client;
- L2TP/IPsec (IKEv1) — только для работы со встроенными VPN-клиентами операционных систем.

Для создания VPN-подключения необходимо произвести настройку соответствующих параметров [на VPN-сервере](#), а затем настроить и подключить VPN-клиент [на конечном устройстве](#).

Настройка VPN-сервера на UserGate NGFW

Для работы UserGate NGFW в качестве VPN-сервера в сценарии remote access VPN необходимо настроить:

- [сетевые параметры](#);
- [параметры аутентификации](#);
- [правила подключения](#);
- [правила аутентификации](#);
- [политики VPN](#);
- [доступ к сетевым ресурсам](#).

Настройка сетевых параметров

На узле UserGate NGFW необходимо выполнить ряд дополнительных настроек сетевых параметров:

- разрешить доступ к узлу для установления VPN-соединения;
- создать зону для контроля подключаемых конечных устройств;
- создать VPN-интерфейс для организации туннеля.

Предоставление доступа для VPN-соединений

Откройте доступ к сервису VPN в свойствах зоны, из которой будут подключаться конечные устройства.

В параметрах зоны, из которой будут подключаться конечные устройства (например, Untrusted), активируйте доступ к сервису VPN. Для этого в веб-консоли UserGate NGFW перейдите в раздел **Настройки → Сеть → Зоны**, затем в параметрах контроля доступа зоны поставьте флажок для сервиса VPN. Подробнее о создании и настройках параметров зон — в разделе [«Настройка зон»](#).

Создание зоны для VPN-подключений

Создайте зону, которой будут принадлежать подключаемые по VPN конечные устройства. Эту зону в дальнейшем можно будет использовать в правилах политик безопасности.

В веб-консоли UserGate NGFW зоны создаются в разделе **Настройки → Сеть → Зоны**. Подробнее о создании и настройках зон — в разделе [«Настройка зон»](#).

Создание VPN-интерфейса

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения конечных устройств. Такой тип интерфейса является кластерным — он будет автоматически создаваться на всех узлах UserGate NGFW, входящих в кластер конфигурации. Если настроен кластер отказоустойчивости, конечные устройства будут автоматически переключаться на резервный узел в случае обнаружения проблем с активным узлом.

В веб-консоли UserGate NGFW VPN-интерфейс создается в разделе **Настройки → Сеть → Интерфейсы**. Для создания интерфейса нажмите **Добавить** и выберите **Добавить VPN**. Подробнее о создании VPN-интерфейса — в разделе [«Настройка интерфейсов»](#).

Настройка параметров аутентификации

Порядок аутентификации в сценарии remote access VPN описывается [правилами аутентификации](#).

Чтобы настроить правила аутентификации, сначала необходимо создать набор средств аутентификации (например, общие ключи, сертификаты или профили клиентских сертификатов), которые затем будут использоваться в правилах в зависимости от выбранного метода аутентификации.

При настройке защищенного IPsec-соединения могут понадобиться следующие средства аутентификации узлов:

- Общий ключ (pre-shared key, PSK). Применяется при использовании протокола IKEv1 для организации защищенного соединения со встроенными VPN-клиентами операционных систем. Общий ключ задается в параметрах [правил подключения](#) на VPN-сервере и в настройках VPN-клиента на устройстве пользователя. Для успешного установления соединения значения ключа на обеих сторонах должны совпадать.
- Сертификат. Используется при выборе протоколов IKEv2 или DTLS для организации защищенного соединения. В этом случае необходимо заранее создать сертификаты для VPN-сервера и конечных устройств, а затем импортировать их в UserGate NGFW и на конечные устройства. Подробнее о правилах импорта сертификатов в UserGate NGFW — в разделе «[Управление сертификатами](#)».
- Профили клиентских сертификатов. Позволяют идентифицировать конечное устройство по определенному атрибуту его сертификата, а также проверить цепочку доверия и подлинность сертификата с учетом списков отозванных сертификатов. При создании профиля используются сертификаты корневых и промежуточных удостоверяющих центров, участвовавших в выдаче сертификатов конечным устройствам. Подробнее о профилях клиентских сертификатов — в разделе «[Профили клиентских сертификатов](#)».

Для аутентификации VPN-пользователей необходимо создать соответствующий профиль аутентификации. Он настраивается в разделе **Настройки → Пользователи и устройства → Профили аутентификации**. Допускается использование того же профиля, который применяется для аутентификации пользователей при доступе в интернет. При этом следует учитывать, что для VPN-аутентификации не поддерживаются методы прозрачной аутентификации, такие как Kerberos, NTLM и SAML IDP. Подробнее о профилях аутентификации — в разделе «[Профили аутентификации](#)».

i Примечание

Если авторизация пользователей происходит в различных поддоменах, на вкладке «Домены LDAP» в настройках LDAP-коннектора необходимо указывать все варианты таких поддоменов. Подробнее о настройке LDAP-коннектора читайте в разделе «[Серверы аутентификации](#)».

Для аутентификации пользователей VPN вы также можете использовать метод многофакторной аутентификации. Значение второго фактора аутентификации может быть получено через одноразовые коды TOTP. VPN с TOTP работает для клиента UserGate Client с протоколами IKEv2 или DTLS (код вводится в отдельном окне), для других клиентов — только с протоколом IKEv1 (код вводится в пароле через двоеточие: `пароль_пользователя:totp_code`).

i Примечание

При установлении L2TP/IPsec VPN-соединения с аутентификацией пользователей через Multifactor RADIUS Adapter повторное переподключение к VPN-серверу в течении 30-секундного тайм-аута с момента предыдущего успешного подключения произойдет без обращением к RADIUS-серверу. Если переподключение будет выполняться за пределами 30-секундного тайм-аута, обращение к RADIUS-серверу произойдет.

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом и завершается ответом VPN-сервера — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Для создания правила подключения в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила подключения** и нажмите **Добавить**.
2. Выберите протокол подключения (**IKE** или **DTLS**).

3. На вкладке **Общие** в свойствах выбранного протокола укажите:

- Для протокола IKE:
 - Укажите название и описание правила;
 - Выберите версию протокола IKE:
 - **IKEv1PSK.** Укажите режим работы IKEv1 (основной или агрессивный) и значение общего ключа (pre-shared key). Ключ должен совпадать на VPN-сервере и на VPN-клиенте;
 - **IKEv2.**
- Для протокола DTLS укажите название и описание правила.

4. На вкладке **Источник** укажите зоны и адреса, с которых разрешено принимать подключения к VPN:

- Укажите зону инициатора подключения;
- Укажите адрес инициатора подключения:
 - выберите или создайте список IP-адресов;
 - выберите или создайте список доменов;
 - выберите GeoIP.

Примечание

Обработка трафика происходит по следующей логике:

- условия объединяются по логическому ИЛИ, если указаны несколько списков IP-адресов или доменов;
- условия объединяются по логическому И, если указаны GeoIP и списки IP-адресов или доменов.

5. На вкладке **Назначение** выберите или создайте список IP-адресов или доменных имен интерфейса, на который будут приходить запросы на VPN-подключения от конечных устройств. Интерфейс должен принадлежать зоне, указанной на этапе [контроля доступа зоны](#).

6. На вкладке **Фаза 1** укажите криптографические параметры фазы 1 согласования защищенного соединения:

- Укажите время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1.
- Укажите параметры работы механизма Dead Peer Detection (DPD) для проверки работоспособности канала и его своевременного отключения или переподключения при обрыве связи. DPD периодически отправляет сообщения **R - U - THERE** для проверки доступности IPsec-соседа. Возможны три режима работы механизма:
 - **Отключено** — механизм отключен. DPD-запросы не отсылаются.
 - **Всегда включено** — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD-запросов. Если ответ не пришел, соединение завершается.
 - **При отсутствии трафика** — DPD-запросы не отсылаются, пока есть ESP-трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в поле **Неудачных попыток**. Если нет ни одного ответа, соединение завершается.
- В разделе **Безопасность** выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.
- Для протокола IKE выберите группы Диффи-Хеллмана, которые будут использоваться для обмена ключами.

О создании правил подключения с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа VPN-клиента на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

Для создания правила аутентификации в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Правила аутентификации** и нажмите **Добавить**.
2. Выберите сценарий **Удаленный доступ** и затем протокол установления защищенного соединения:
 - IPsec/L2TP;
 - IKEv2;
 - DTLS.
3. На вкладке **Общие** в свойствах выбранного протокола укажите:
 - Для протокола IPsec/L2TP:
 - Укажите название и описание правила;
 - Выберите созданный ранее [профиль аутентификации](#);
 - Выберите одно или несколько созданных ранее [правил подключения](#).
 - Для протоколов IKEv2 и DTLS:
 - Укажите название и описание правила;
 - Укажите импортированный ранее [сертификат сервера](#) и созданный ранее [профиль аутентификации](#);
 - Выберите режим аутентификации (AAA, PKI или любой):
 - Для аутентификации с помощью ключей (PKI) укажите [профиль клиентских сертификатов](#).
 - В режиме аутентификации с помощью методов EAP, PEAP (AAA) VPN-клиент обменивается с VPN-сервером EAP-

пакетами. VPN-сервер транслирует пакеты на внешний доменный RADIUS-сервер, который принимает решение об авторизации. После получения разрешения от RADIUS-сервера, VPN-сервер по полученному логину запрашивает у сервера домена информацию о пользователе, после чего принимает решение о подключении пользователя к VPN.

- Выберите одно или несколько созданных ранее [правил подключения](#).

4. На вкладке **Фаза 2** укажите криптографические параметры фазы 2 согласования защищенного соединения:

- Укажите максимальный размер данных, шифруемых одним ключом.
- При необходимости включите параметр NAT keepalive. NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону VPN-клиента для поддержания сессии NAT активной.
- Дополнительно для протоколов IKEv2 и IKEv1/L2TP:
 - Укажите время жизни ключа. По истечению этого времени узлы должны сменить ключ шифрования.

Примечание

Если заданы значения обоих параметров (время жизни ключа и максимальный размер данных, шифруемых одним ключом), то первый достигнувший предела счетчик запустит пересоздание ключей сессии.

- Выберите алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка переместите нужную пару алгоритмов вверх или вниз.

О создании правил аутентификации с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации VPN-клиента и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Для создания политики VPN в веб-консоли UserGate NGFW:

1. Перейдите в раздел **Настройки → VPN-сервер → Политики VPN** и нажмите **Добавить**.
2. Выберите сценарий **Удаленный доступ** и затем тип VPN-клиента:
 - **Clients** — для встроенных VPN-клиентов известных операционных систем;
 - **UserGate Client** — для VPN-клиента UserGate Client.
3. На вкладке **Общие** в свойствах удаленного доступа:
 - Укажите название и описание правила;
 - Выберите одно или несколько созданных ранее [правил аутентификации](#).
4. На вкладке **Пользователи** выберите локальную или доменную учетную запись или группу, которые будут использоваться для аутентификации пользователей.
5. На вкладке **Подсети для VPN**:
 - Укажите VPN-интерфейс, который будет использоваться для подключения.
 - Укажите диапазон IP-адресов, которые будут использованы для подключения. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
 - Укажите маску сети VPN.
 - Укажите DNS-серверы, которые будут переданы VPN-клиенту, или поставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены локальные DNS-серверы, которые использует UserGate NGFW.

6. Для встроенных VPN-клиентов операционных систем на вкладке **Маршруты VPN** укажите маршруты, передаваемые конечному устройству в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.

7. Для UserGate Client укажите параметры настройки функции раздельного туннелирования (split tunneling). Подробнее — в разделе «[Настройка раздельного туннелирования для UserGate Client](#)».

О создании политик VPN с помощью команд интерфейса командной строки — в разделе «[Настройка серверных правил](#)».

Настройка доступа к ресурсам

Клиенты подключаются к VPN с использованием протокола Point-to-Point. Чтобы трафик мог ходить из созданной ранее зоны для VPN-подключений, создайте правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Настройки → Политики сети → NAT и маршрутизация**. Подробнее о правилах NAT — в разделе «[NAT и маршрутизация](#)». Для примера в веб-консоли UserGate NGFW создано правило NAT from VPN for remote access to Trusted and Untrusted, разрешающее подмену IP-адресов из зоны VPN for remote access в зоны Trusted и Untrusted.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в веб-консоли UserGate NGFW в разделе **Настройки → Политики сети → Межсетевой экран** создайте правило межсетевого экрана, разрешающее трафик из зоны для VPN-подключений в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана — в разделе «[Межсетевой экран](#)».

Для примера в веб-консоли UserGate NGFW создано правило межсетевого экрана VPN for remote access to Trusted and Untrusted, разрешающее весь трафик из зоны VPN for remote access в зоны Trusted и Untrusted. Правило отключено по умолчанию.

Настройка параметров VPN-клиента

После настройки правил VPN-сервера необходимо настроить параметры подключения VPN-клиентов. В качестве клиентского ПО на устройствах пользователей может использоваться UserGate Client, также поддерживаются встроенные клиенты большинства известных операционных систем.

Настройка параметров VPN-клиента зависит от типа клиента и протокола установления VPN-подключения.

Настройка параметров VPN-подключения UserGate Client

О настройках VPN-подключений с помощью UserGate Client для Windows — в разделе «[Установка VPN-соединения с помощью UserGate Client для Windows](#)».

О настройках VPN-подключений с помощью UserGate Client для Linux — в разделе «[Настройка VPN-соединения на устройстве пользователя с помощью UserGate Client для Linux](#)».

О настройках VPN-подключений с помощью UserGate Client для macOS — в разделе «[Настройка VPN-соединения на устройстве пользователя с помощью UserGate Client для macOS](#)».

Настройка параметров VPN-подключения встроенных VPN-клиентов

О настройках VPN-подключений с помощью встроенных VPN-клиентов операционных систем — в разделе «[VPN для удаленного доступа клиентов \(remote access VPN\)](#)».

Журналирование событий VPN-сервера

Записи о работе VPN-сервера UserGate NGFW сохраняются в системном журнале событий (Event log).

Записи содержат информацию:

- об изменениях параметров правил VPN;
- статусе VPN-подключений;
- ошибках VPN-подключений.

В веб-консоли UserGate NGFW в разделе **Журналы и отчеты → Журналы → Журнал событий** записи событий VPN-сервера можно отфильтровать, выбрав в меню журнала компонент «VPN» и нужные типы событий.

Журнал событий

Сегодня (07 Окт 2025 г.) Важность: Все Компоненты и события: VPN Ещё Сброс Поиск Расширенный

Узел	Время	Компонент	Тип события	Детали события
utm...	13:24:07	VPN	Пользователь	Логин: vpn_client1, Продолжительность: 28м
utm...	13:23:59	VPN	Сервер	Название: VR1, —, Старые значения, Маршрут
utm...	12:54:47	VPN	Пользователь	Логин: vpn_client1, Продолжительность: 5м 2
utm...	12:49:10	VPN	Сервер	Название: VR1, —, Старые значения, Пользов
utm...	12:48:13	VPN	Сервер	Название: AR1, —, Старые значения, —, Новы
utm...	12:43:37	VPN	Сервер	Название: AR1, —, Старые значения, ID initiat
utm...	12:21:25	VPN	Сервер	Название: VR1, Описание: Серверная полити
utm...	12:19:50	VPN	Сервер	Название: AR1, Описание: Серверное правил
utm...	12:17:38	VPN	Сервер	Название: CR1, Описание: Серверное правил
utm...	12:15:45	VPN	Сервер	Название: CR1 IKE, Тип правила подключения
utm...	12:15:36	VPN	Сервер	Название: AR1, Описание: Test auth rule, Тип
utm...	12:15:33	Сервер	Серверное правило аутентификации VPN удалено	Название: Auth rule 1, Тип правила аутентифи
utm...	12:15:30	Сервер	Серверное правило аутентификации VPN удалено	Название: 111, Тип правила аутентификации

Компонент

Тип события

Также записи событий можно отфильтровать с помощью запросов в строке расширенного поиска.

Журнал событий

event = vpn

Узел	Время	Компонент	Тип события	Детали события
utm...	13:24:07	VPN	Пользователь	Логин: vpn_client1, Продолжительность: 28м
utm...	13:23:59	VPN	Сервер	Название: VR1, —, Старые значения, Маршрут
utm...	12:54:47	VPN	Пользователь	Логин: vpn_client1, Продолжительность: 5м 2
utm...	12:49:10	VPN	Сервер	Название: VR1, —, Старые значения, Пользов
utm...	12:48:13	VPN	Сервер	Название: AR1, —, Старые значения, —, Новы
utm...	12:43:37	VPN	Сервер	Название: AR1, —, Старые значения, ID initiat
utm...	12:21:25	VPN	Сервер	Название: VR1, Описание: Серверная полити
utm...	12:19:50	VPN	Сервер	Название: AR1, Описание: Серверное правил
utm...	12:17:38	VPN	Сервер	Название: CR1, Описание: Серверное правил
utm...	12:15:45	VPN	Сервер	Название: CR1 IKE, Тип правила подключения
utm...	12:15:36	VPN	Сервер	Название: AR1, Описание: Test auth rule, Тип
utm...	12:15:33	Сервер	Серверное правило аутентификации VPN удалено	Название: Auth rule 1, Тип правила аутентифи
utm...	12:15:30	Сервер	Серверное правило аутентификации VPN удалено	Название: 111, Тип правила аутентификации

Примечание

События VPN-сервера не реплицируются на другой узел кластера.

Ошибки подключений на VPN-сервере

Ошибки, связанные с неудачными попытками подключения к VPN-серверу или с разрывом существующих VPN-соединений, записываются в журнал событий UserGate NGFW.

Вы можете отсортировать ошибки подключений в журнале событий по компоненту «VPN», типу события «Ошибка сервера», времени возникновения ошибки, названию клиентского правила или IP-адресу VPN-клиента.

В таблице приведены варианты сообщений об ошибках VPN-подключений, отображаемые в журнале событий веб-интерфейса UserGate NGFW, и возможные причины их возникновения.

Детали события	Event details	Возможная причина ошибки
Клиент не отвечает	No response from client	При согласовании параметров безопасности фазы 1 защищенного соединения не получен ответ от VPN-клиента в установленный промежуток времени. Возможные причины: • Произошла потеря пакетов. • VPN-клиент выключен. • VPN-клиент инициировал новое подключение
Настройки параметров безопасности фазы 1 на сервере несовместимы с настройками на клиенте	The server's Phase 1 security settings are incompatible with the client's settings	На этапе согласования параметров безопасности фазы 1 защищенного соединения не найдены совпадения в параметрах: • групп Диффи-Хеллмана; • алгоритмов шифрования; • алгоритмов аутентификации
Ошибка подключения VPN-клиента: неверный общий ключ	VPN client connection error: incorrect pre-shared key	На этапе установления фазы 1 защищенного соединения VPN-сервер не может расшифровать сообщение от VPN-клиента или подтвердить его подлинность. Возможная причина ошибки: несовпадение значения общего ключа в настройках параметров VPN-сервера и VPN-клиента
Настройки параметров безопасности фазы 2 на сервере несовместимы с настройками на клиенте	The server's Phase 2 security settings are incompatible with the client's settings	На этапе согласования параметров безопасности фазы 2 защищенного соединения не найдены совпадения: • алгоритмов шифрования; • алгоритмов аутентификации
Для клиента не был найден свободный IP-адрес, подключение отклонено	No Available IP Address Found for the Client, Connection Rejected	Диапазон адресов, предназначенный для VPN-клиентов, слишком мал для имеющегося количества одновременных подключений
Не получен код двухфакторной аутентификации	MFA code not received	На этапе аутентификации не получен код второго фактора аутентификации от VPN-клиента

Детали события	Event details	Возможная причина ошибки
Неверный код двухфакторной аутентификации	MFA verification failed	На этапе аутентификации получен неверный код второго фактора аутентификации от VPN-клиента. Возможные причины получения неверного кода: • Рассинхронизация времени между сервером и клиентом. • Неверно введенный пользователем код. • Устаревший код
Цифровая подпись в сертификате клиента не соответствует подписи, вычисленной VPN-сервером	The digital signature in the client certificate does not match the signature computed by the VPN server	Ошибка аутентификации на этапе IKE_AUTH в IKEv2. VPN-сервер использует открытый ключ из сертификата клиента для проверки цифровой подписи, которую клиент создал своим закрытым ключом. Если подписи не совпадают, сервер немедленно разрывает соединение, так как не может подтвердить подлинность клиента. Возможные причины: • Несоответствие пары ключей. • Повреждение данных или неправильный расчет хеш-суммы. • Проблемы с цепочкой доверия сертификатов. Сервер не может проверить подпись удостоверяющего центра на клиентском сертификате
В сертификате отсутствует альтернативное имя (SAN) или оно указано неверно	Certificate SAN empty or certificate SAN mismatch	Ошибка при установлении VPN-подключения в сценарии Site-to-Site с аутентификацией посредством сертификатов. Возможной причиной ошибки является некорректный сертификат клиента, в котором либо отсутствует расширение Subject Alternative Name (SAN), либо в нем указан некорректный IP-адрес или FQDN клиента
Несовпадение подсетей клиента и VPN-сервера	Client and server VPN subnets do not match	В сценарии Site-to-site с протоколом IPsec/IKEv2 в ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет ни одного совпадения в адресах локальных и удаленных подсетей, соединение разрывается и выдается сообщение об ошибке

Детали события	Event details	Возможная причина ошибки
Клиент не поддерживает NAT-T	Client does not support NAT-T	При установлении VPN-подключения с протоколом IPsec IKEv1 VPN-сервер не находит в сообщении от клиента идентификатор Vendor ID
Отсутствует KE-пакет, обмен ключами DH невозможен	Missing KE payload, DH key exchange not possible	Критическая ошибка в процессе обмена ключами при установлении VPN-подключения. Возможные причины: • Ошибки в конфигурации DH-групп на одной из сторон соединения. • Устаревшая версия VPN-клиента. • Блокировки IKE-пакетов на сети
Сбой согласования IKE: не получен nonce (Ni payload) от клиента	IKE negotiation failed: the initiator's nonce was not received	Ошибка в процессе обмена ключами при установлении VPN-подключения. Возможные причины: • Потери пакетов или фрагментация пакетов. • Блокировки IKE-пакетов на сети. • Ошибки конфигурации: разные версии IKE на клиенте и сервере. • Рассинхронизация времени между клиентом и сервером
Сбой аутентификации клиента: хеш-код HASH_I не получен.	Client authentication failed: HASH_I not received	Ошибка аутентификации клиента в процессе установления IKE-соединения. Возможные причины: • Некорректные учетные данные (неправильный общий ключ, недействительный сертификат). • Несовместимость алгоритмов шифрования или аутентификации на клиенте и сервере. • Рассинхронизация времени между клиентом и сервером
Соединение разорвано по алгоритму DPD	VPN connection closed by Dead Peer Detection algorithm	Разрыв VPN-подключения по причине неактивности противоположной стороны соединения в пределах установленного интервала. Причинами отсутствия ответа противоположной стороны соединения могут быть: • Проблемы с сетевой связностью. • Высокая загрузка сети или сторон соединения.

Детали события	Event details	Возможная причина ошибки
		Слишком агрессивные настройки параметров протокола DPD
VPN-туннель закрыт по причине срабатывания защиты от перехвата	VPN tunnel closed due to anti-replay protection trigger	Срабатывание защиты от перехвата и повторной передачи VPN-пакетов. Нарушение последовательности или повторяемость номеров (sequence number) получаемых пакетов. Возможные причины: - Проблемы с сетью (большая потеря пакетов, большая вариация задержек, неправильная очередность доставки пакетов). - Перегрузка VPN-сервера или клиента. - Рассинхронизация времени между клиентом и сервером

Следующие ошибки VPN-подключений не фиксируются в журнале событий UserGate NGFW:

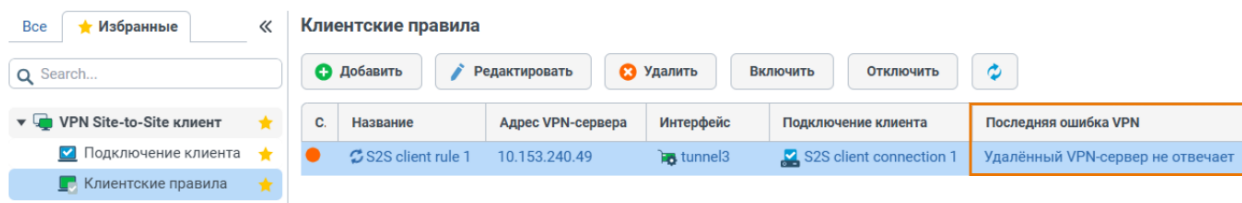
- Несовпадение параметров первого пакета. Если параметры инициирующего пакета от VPN-клиента не соответствуют ни одному из настроенных на VPN-сервере правил подключения.
- Отсутствие активной VPN-политики. Если параметры инициирующего пакета VPN-клиента соответствует условиям одного из правил подключения, но это правило не связано ни с одной из активных политик VPN.
- Промежуточные этапы IKEv2. Отдельные итерации в процессе согласования группы Диффи-Хеллмана по протоколу IKEv2, если в итоге соединение устанавливается успешно.

Ошибки подключений на VPN-сервере (инициаторе соединения)

В сценарии site-to-site VPN UserGate NGFW может выступать в роли инициатора VPN-соединения. При неудачной попытке установления соединения с удаленным VPN-сервером или при разрыве установленного соединения в журнал событий будут записываться сообщения об ошибках VPN-подключения.

В журнале событий веб-интерфейса вы можете отсортировать ошибки подключений по компоненту «VPN», типу события «Ошибка клиента» или времени возникновения ошибки.

Последняя ошибка подключения по активному правилу также отображается в разделе клиентских правил веб-интерфейса (**Настройки → VPN Site-to-Site клиент → Клиентские правила**) в поле **Последняя ошибка VPN**.



В таблице приведены варианты сообщений об ошибках, отображаемые в веб-интерфейсе UserGate NGFW (инициатора соединения), и возможные причины их возникновения.

Детали события	Event details	Возможная причина ошибки
Сервер не отвечает	No response from server	1. Инициатор VPN-соединения отправляет запрос на подключение к VPN-серверу и не получает ответ в течение настроенного времени ожидания. Возможные причины: • Некорректный IP-адрес VPN-сервера в настройках клиентских правил на инициаторе соединения. • Неверный адрес VPN-сервера определяется на DNS-сервере. • На VPN-сервере не открыты порты 500, 4500. • На VPN-сервере не найдено активное правило подключения, подходящее по параметрам: ◦ протокол; ◦ режим IKE; ◦ IP-адрес источника или назначения; ◦ пользователь. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети 2. После истечения таймера механизма DPD система отправляет первоначальный DPD-запрос. В случае отсутствия ответа и исчерпания всех попыток проверки клиент фиксирует недоступность VPN-сервера.

Детали события	Event details	Возможная причина ошибки
		Возможные причины: • На VPN-сервере не открыты порты 500, 4500. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети. 3. Ошибка в процессе пересоздания ключей (rekeying) для IKE- или ESP-туннеля: VPN-сервер не ответил на запрос. Возможные причины: • Потеря сетевой связности. • Высокая загрузка VPN-сервера. • Произошла перезагрузка VPN-сервера без сохранения состояния IKE_SA. • Потеря пакетов из-за перегрузки сети
Ошибка подключения: некорректное имя сервера	Invalid server name	Доменное имя VPN-сервера, указанное в параметрах подключения инициатора VPN-соединения, не определяется DNS-сервером. Вероятные причины: • Неверно указано доменное имя VPN-сервера в параметрах подключения на узле-инициаторе соединения. • На DNS-сервере не определено доменное имя VPN-сервера
Ошибка подключения: некорректные параметры аутентификации клиента	VPN client connection error — wrong client auth	Ошибка подключения по IKEv2. Узел-инициатор соединения не прошел аутентификацию на VPN-сервере. Возможные причины: • неверно указан общий ключ (PSK) в настройках подключения; • VPN-сервер сопоставил идентификатор клиента с другой политикой, где задан другой общий ключ
Тайм-аут фазы 1. Используется неверный общий ключ	Phase 1 timeout. Incorrect shared key	Ошибка установления IPsec-соединения с использованием протоколов IPsec/L2TP

Детали события	Event details	Возможная причина ошибки
		Возможные причины: • В параметрах VPN-подключения указано неверное значение общего ключа. • Не совпадают параметры фазы 1 IKE
Ошибка подключения по протоколу IPsec/L2TP: неверный пароль	VPN client connection error IPsec/L2TP: incorrect password	Ошибка при установлении соединения с протоколами IPsec/L2TP. Возможные причины: • На VPN-сервере создана, но не включена учетная запись для аутентификации узла-инициатора соединения. • Учетная запись для аутентификации узла-инициатора соединения на VPN-сервере не связана с политикой VPN. • На VPN-сервере не настроен профиль аутентификации с локальным пользователем для аутентификации узла-инициатора соединения . • Несовпадение пароля учетной записи на VPN-сервера и в параметрах соединения на узле-инициаторе. • На VPN-сервере нет свободного IP-адреса для клиента
Настройки безопасности VPN-клиента несовместимы с настройками сервера	VPN client and VPN server security settings are not compatible	Ошибка при установлении соединения с протоколами IKEv2 и IPsec/L2TP. Возможные причины: • Несовпадение параметров соединения на VPN-сервере и узле-инициаторе соединения: ◦ Группы Диффи-Хеллмана не совпадают. ◦ Настройки безопасности первой фазы не совпадают. ◦ Настройки безопасности второй фазы не совпадают
Ошибка подключения VPN-клиента — некорректные параметры аутентификации сервера	VPN client connection error — wrong server auth	Ошибка при установлении соединения с протоколами IKEv2. Неуспешная проверка цифровой подписи VPN-сервера в сообщении IKE_AUTH, в результате чего подлинность сервера не подтверждена

Детали события	Event details	Возможная причина ошибки
Аутентификация клиента невозможна: не получен HASH_I	Client authentication failed: HASH_I not received	Ошибка при установлении соединения по протоколу IKEv1. Значение HASH_DATA, полученное от VPN-сервера, не совпадает со значением, вычисленным на стороне инициатора соединения. Возможные причины: - повреждение пакета при передаче; - потеря предыдущего сообщения, влияющего на вычисление HASH_DATA; - использование некорректного значения общего ключа; - попытка подмены или иного вмешательства в процесс обмена сообщениями
Отсутствие ключевой информации в ответе сервера. Вероятно не совпадает общий ключ	Missing key exchange in server response. Highly likely incorrect shared key	Ошибка при установлении соединения по протоколу IKEv2. В сообщении, полученном от VPN-сервера, отсутствует обязательный payload Key Exchange (KE)
Ошибка декодирования сообщения сервера, хэш неверный	Error decoding server message, hash is invalid	Ошибка при установлении соединения по протоколу IKEv2. Инициатор соединения выполняет проверку целостности сообщения, полученного от VPN-сервера, путем вычисления значения Integrity Check Value (ICV) и сравнения его с полученным значением. При несовпадении значений проверка целостности завершается неуспешно, и соединение не устанавливается. Возможные причины: - повреждение или потеря пакетов при передаче (в том числе при фрагментации); - потеря предыдущего сообщения, влияющего на состояние обмена
Настройки безопасности VPN-клиента несовместимы с настройками сервера	VPN client and VPN server security settings are not compatible	Ошибка при установлении соединения по протоколу IKEv1. Параметры защищаемых подсетей (local/remote networks), настроенные на VPN-сервере и узле-инициаторе соединения, не совпадают, в результате чего не удастся согласовать параметры IPsec-туннеля

Детали события	Event details	Возможная причина ошибки
Несовпадение идентификаторов	Incompatible identifiers	Ошибка при установлении соединения по протоколу IKEv2. На этапе согласования IPsec SA клиент отправляет сообщение IKE_AUTH с селекторами трафика (TSi/TSr). VPN-сервер сверяет полученные TSi/TSr с настройками локальных подсетей. Если ни одна подсеть не может быть согласована, VPN-сервер отправляет сообщение INFORMATIONAL со значением Notify payload TS_UNACCEPTABLE, и соединение не устанавливается. Причина: Подсети, настроенные на узле-инициаторе соединения и VPN-сервере, не совпадают
Отсутствие идентификатора в ответе сервера	Missing identifier in server response	Ошибка при установлении соединения по протоколу IKEv1. Узел-инициатор соединения не получил обязательный идентификатор VPN-сервера (IDr) в ответном пакете IKE. В результате невозможна проверка подлинности VPN-сервера, и соединение не устанавливается. Возможные причины: - повреждение или потеря пакетов при передаче; - несоответствие режима IKE в параметрах соединения на узле-инициаторе и на VPN-сервере; - неправильное значение общего ключа в параметрах подключения
Ошибка выделения IP-адреса на сервере	Error allocating IP address from VPN server	Не удалось получить IP-адрес от VPN-сервера. Узел-инициатор соединения не получил свободный IP-адрес от VPN-сервера, поэтому соединение не может быть установлено. Проверьте параметры подключения на VPN-сервере и наличие свободных IP-адресов в пуле

VPN в режиме полного туннелирования

VPN в режиме полного туннелирования (full tunnel) — это способ подключения, при котором весь сетевой трафик со стороны VPN-клиента, включая обращения к корпоративным системам и к внешним интернет-ресурсам, передается через защищенный VPN-туннель и обрабатывается на VPN-сервере. При таком

подходе трафик не разделяется на корпоративный и интернет-трафик — весь поток данных проходит через VPN.

В UserGate NGFW режим полного туннелирования может применяться в сценариях site-to-site VPN с использованием протокола IPsec/IKEv2.

Администратору филиала не нужно поддерживать список корпоративных подсетей — весь трафик по умолчанию передается в туннель, а дальнейшую маршрутизацию VPN-сервер головного офиса выполняет самостоятельно: в свои локальные сети, в другие филиалы или в интернет.

Основные преимущества режима полного туннелирования:

- Полный контроль трафика.
- Единая политика безопасности.
- Централизованное журналирование.

К недостаткам сценария можно отнести повышенную нагрузку на VPN-сервер головного офиса и возможное увеличение сетевых задержек.

Принцип работы

На этапе согласования защищенного канала узел-инициатор соединения (VPN-клиент) запрашивает для селектора трафика VPN-сервера (TSr) значение 0.0.0.0/0, которое принимается VPN-сервером. На узле-инициаторе изменяется таблица маршрутизации: маршрут по умолчанию назначается через VPN-интерфейс, и весь исходящий трафик направляется через корпоративный VPN-сервер. При этом доступ к самому VPN-серверу сохраняется по прямому маршруту вне туннеля.

При разрыве VPN-соединения — по инициативе пользователя, по команде сервера или по иной причине — узел-инициатор завершает VPN-сессию и восстанавливает исходный маршрут по умолчанию.

Настройка режима полного туннелирования на UserGate NGFW

Для создания VPN-подключения необходимо выполнить настройку обоих граничных узлов защищенного соединения: VPN-сервера и узла-инициатора соединения (VPN-клиента).

Настройка VPN-сервера

Настройку VPN-сервера выполните по алгоритму, описанному в разделе [«Настройка UserGate NGFW в качестве узла-ответчика»](#).

Особенности настройки для режима полного туннелирования:

- На VPN-сервере должны быть настроены маршруты в корпоративные сети, сети филиалов и в интернет.
- Должны быть созданы правила сетевых политик, разрешающие доступ к необходимым сетевым ресурсам.
- Настроено правило подключения site-to-site с протоколом IKEv2 с ограничением по IP-адресам. Разрешена соответствующая зона источника.
- Создано правило аутентификации site-to-site IKEv2, в котором:
 - TSr (Local subnets) = 0.0.0.0/0 — VPN-сервер принимает весь трафик по умолчанию от удаленных шлюзов, использующих такую политику.
 - Для удаленных сетей может быть активирована опция «Не проверять сети инициатора», при которой VPN-сервер принимает любые TSr (Remote subnets). Это упрощает конфигурацию.
 - Если опция «Не проверять сети инициатора» отключена, необходимо явно указать подсети, которые VPN-сервер будет проверять при получении трафика от узла-инициатора. Эти подсети добавятся в таблицу маршрутизации VPN-сервера. В этом случае VPN-сервер согласует только те подсети, объявленные узлом-инициатором, которые полностью совпадают с указанными.

Настройка узла-инициатора (VPN-клиента)

Настройку узла-инициатора выполните по алгоритму, описанному в разделе [«Настройка UserGate NGFW в качестве узла-инициатора подключения»](#).

Особенности настройки для режима полного туннелирования:

- До установления VPN-соединения VPN-сервер должен быть доступен согласно текущей таблице маршрутизации (через шлюз по умолчанию, другой L3-шлюз или по L2 — в зависимости от выбранного варианта).

- Должно быть создано правило подключения с протоколом IKEv2 со
- следующими параметрами:
 - Remote subnets (TSr): 0.0.0.0/0;
 - Local subnets (TSi): указываются только те подсети, которые разрешены на VPN-сервере согласно действующей политике.
 - VPN-клиент выполняет роль шлюза по умолчанию для всех локальных подсетей.

Раздельное туннелирование для UserGate Client

Режим раздельного туннелирования (split tunnel) — это способ удаленного подключения, при котором трафик VPN-клиента разделяется на два потока:

- Часть трафика идет через VPN-туннель (например, доступ к корпоративным ресурсам).
- Остальной трафик идет напрямую через обычное интернет-соединение, минуя VPN.

Принцип работы

Таблица маршрутизации устройства пользователя с установленным ПО UserGate Client модифицируется при установлении VPN-соединения в соответствии с настроенными на VPN-сервере UserGate NGFW параметрами маршрутизации клиента. После завершения VPN-сессии локальные настройки маршрутизации на компьютере пользователя возвращаются в исходные.

При установлении VPN-соединения в таблицу маршрутов клиента добавляются два новых маршрута. Они необходимы для сохранения подключения к VPN-серверу во всех сценариях:

- Маршрут к шлюзу локальной сети. Добавляется через IP-адрес локального интерфейса в качестве шлюза.
- Маршрут к VPN-серверу.
 - Добавляется через IP-адрес локального интерфейса в качестве шлюза, если адрес VPN-сервера находится в адресном пространстве локальной сети.

- Добавляется через IP-адрес шлюза локальной сети в качестве шлюза в случае если адрес VPN-сервера не находится в адресном пространстве локальной сети.

Локальные маршруты в обход VPN, изначально прописанные на устройстве пользователя, удаляются на время работы VPN. После отключения VPN-соединения эти маршруты возвращаются.

Настройка режима раздельного туннелирования на UserGate NGFW

В веб-консоли UserGate NGFW вы можете настроить различные сценарии работы режима раздельного туннелирования. Для этого перейдите в раздел **Настройки → VPN-сервер → Политики VPN**. В свойствах политики удаленного доступа для UserGate Client выберите вкладку **Маршруты для UserGate Client**.

Рассмотрим подробнее возможные сценарии настроек раздельного туннелирования.

а) Если поставлен флажок **Все маршруты**, в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию (default route) вида **0.0.0.0/0 → VPN-шлюз**. Имеющийся ранее маршрут по умолчанию будет удален из таблицы.

Свойства удаленного доступа UserGate client

Общие Пользователи Подсети для VPN **Маршруты для UserGate Client**

☒ Все маршруты

Включить маршруты

+ Добавить Ещё...

Название списка	Владелец
-----------------	----------

Исключить маршруты

+ Добавить Ещё...

Название списка	Владелец
-----------------	----------

☐ Ограничить доступ к локальной сети

Сохранить Отмена

b) Если в поле **Включить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида $n.n.n.n/c \rightarrow \text{VPN-шлюз}$ с гарантированно минимальной метрикой 2.

Свойства удаленного доступа UserGate client

Общие Пользователи Подсети для VPN **Маршруты для UserGate Client**

☐ Все маршруты

Включить маршруты

+ Добавить Ещё...

	Название списка	Владелец
✓	IP-list1	вы
✓	IP-list2	вы

Исключить маршруты

+ Добавить Ещё...

	Название списка	Владелец
--	-----------------	----------

☐ Ограничить доступ к локальной сети

Сохранить Отмена

c) Если в поле **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию вида $0.0.0.0/0 \rightarrow \text{VPN-шлюз}$. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

Свойства удаленного доступа UserGate client

Общие

Пользователи

Подсети для VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+ Добавить

Ещё...

	Название списка	Владелец

Исключить маршруты

+ Добавить

Ещё...

	Название списка	Владелец
	IP-list3	Вы
	IP-list4	Вы

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

д) Если в обоих полях **Включить маршруты** и **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида $n.n.n.n/c \rightarrow \text{VPN-шлюз}$ с гарантированно минимальной метрикой 2. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.

Свойства удаленного доступа UserGate client

Общие

Пользователи

Подсети для VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+ Добавить

Ещё...

	Название списка	Владелец
	IP-list1	Вы
	IP-list2	Вы

Исключить маршруты

+ Добавить

Ещё...

	Название списка	Владелец
	IP-list3	Вы
	IP-list4	Вы

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

е) Если на вкладке нет никаких настроек, то в таблицу маршрутизации клиента добавляется VPN-маршрут вида **0.0.0.0/0 → VPN-шлюз** с метрикой больше, чем у имеющегося маршрута по умолчанию. Имеющийся маршрут по умолчанию при этом не удаляются и маршруты для UserGate MC, UserGate NGFW, VPN-сервера не создаются.

ф) Если поставлен флажок **Ограничить доступ к локальной сети**, то для каждой подсети локального интерфейса создается копия маршрута через VPN-шлюз с гарантированно минимальной метрикой 2. Такие же копии маршрутов создаются для всех адресов, которые имеют тип `local interface`.

В зависимости от сценариев настроек метрики для VPN-маршрутов broadcast- и multicast-адресов получают следующие значения:

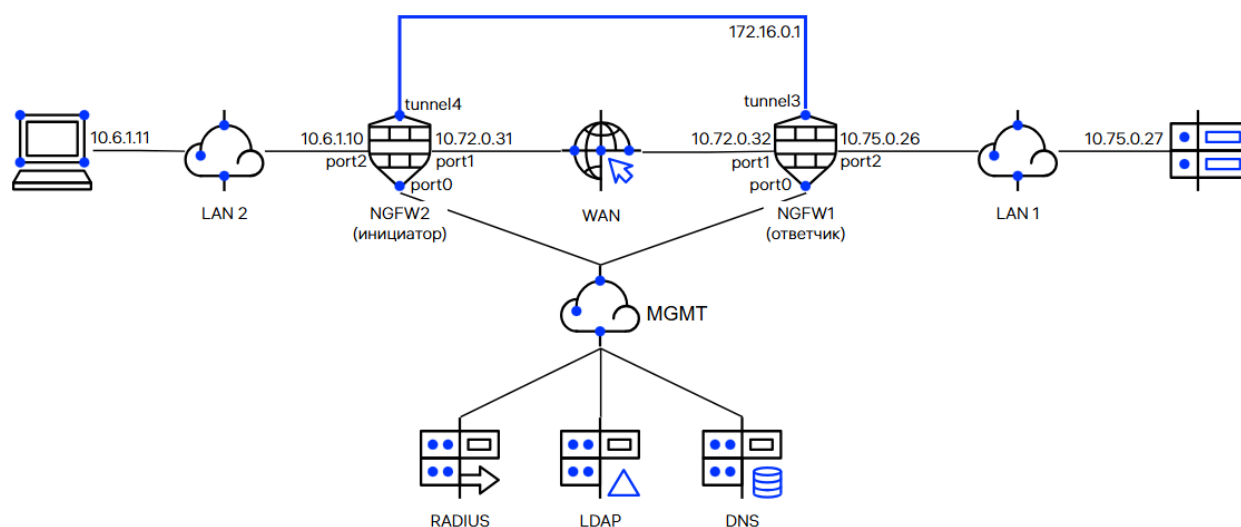
- Лучшая метрика среди соответствующих адресов — для сценариев [a\)](#) и [c\)](#);
- Гарантированно худшая метрика 10 000 — для сценариев [b\)](#) и [d\)](#).

В зависимости от режима работы устройство пользователя с установленным ПО UserGate Client осуществляет коммуникацию либо с UserGate MC, либо с UserGate NGFW. С этой целью создается отдельный маршрут для соответствующего IP-адреса в обход VPN. Такой маршрут не создается для сценария [e\)](#) и в случае, когда VPN-клиент и UserGate MC или UserGate NGFW находятся в одной сети.

ПРИМЕРЫ НАСТРОЙКИ

Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1)

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема.



Настройка VPN-сервера

Для настройки NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

В разделе **Настройки → Сеть → Зоны** создайте зону **WAN** и активируйте сервис **VPN** в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе [«Настройка зон»](#).

2. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройке зон — в разделе [«Настройка зон»](#).

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

В этом примере воспользуемся созданным по умолчанию интерфейсом **tunnel3**. Подробнее о создании и настройке сетевых интерфейсов — в разделе [«Настройка интерфейсов»](#).

4. Настройте параметры аутентификации.

- Создайте локальную учетную запись, которая будет использоваться для аутентификации узла-инициатора соединения (NGFW2) при установлении L2TP-туннеля. В веб-консоли NGFW1 в разделе **Настройки → Пользователи и устройства → Пользователи** создана локальная учетная запись **User for S2S** (логин **vpn_user_s2s**). Для удобства использования все созданные подобные учетные записи могут быть помещены в имеющуюся группу **VPN servers**, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп — в разделе [«Пользователи и группы»](#).
- Создайте профиль аутентификации. Для примера в разделе **Настройки → Пользователи и устройства → Профили аутентификации** создан профиль **local user auth profile**, на вкладке метода аутентификации выбран **Локальный пользователь**. Подробнее о профилях аутентификации — в разделе [«Профили аутентификации»](#).

5. Создайте правило подключения.

В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол IKE. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила подключения.
 - Выберите протокол подключения **IKEv1PSK**.
 - Выберите режим IKE: **Основной**.
 - Укажите значение общего ключа для аутентификации удаленного узла при установлении защищенного соединения IPsec.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Название:

ikev1 conn rule

Описание:

Протокол:

IKEv1PSK

Режим IKE:

Основной

Общий ключ:

Общий ключ (повтор):

Сохранить

Отмена

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны **WAN**.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Зона источника

☐ Cluster
☐ DMZ
☐ LAN1
☐ Management
☐ MGMT
☐ Trusted
☐ Tunnel inspection zone
☐ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site
☒ WAN
☐ WAN1

Создать и добавить новый объект

Адрес источника

+ Добавить

Ещё...

Название списка	Владелец
Создать и добавить новый объект	

Сохранить

Отмена

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
 - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
 - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Время жизни ключа:

1

часов

Dead peer detection:

Всегда включена

29

секунд

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site → IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила аутентификации.
 - Выберите профиль аутентификации удаленного сервера-инициатора соединения, созданный на шаге 4.
 - Выберите тип идентификации узлов (**IPv4**).
 - Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.

- В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

Свойства Site-to-Site IPSec/L2TP

ОбщиеФаза 2

Название:

s2s ipsec-l2tp auth rule

Описание:

Профиль аутентификации:

local user auth profile

URL инициализации TOTP

Initiator

Тип

IPv4

идентификации:

Значение

10.72.0.31

идентификации:

Responder

Тип

IPv4

идентификации:

Значение

10.72.0.32

идентификации:

Правила подключения

Добавить

Удалить

Название	Протокол
ikev1 conn rule	IKEv1PSK

Сохранить

Отмена

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

Свойства Site-to-Site IPsec/L2TP

Общие

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

☐ Включить NAT keepalive

Время жизни NAT:

0

секунд

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

7. Создайте политику VPN-подключения.

В разделе **Настройки** → **VPN-сервер** → **Политики VPN** нажмите **Добавить** и выберите **Site-to-Site** → **IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название политики VPN-подключения.
 - В блоке **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

Свойства Site-to-Site IPSec/L2TP

Общие

Пользователи

Подсети для VPN

Маршруты VPN

☒ Включено

Название: S2S IPSec/L2TP example VPN policy

Описание:

Правила аутентификации

+ Добавить

✖ Удалить

Название	Протокол
s2s ipsec-l2tp auth rule	IPSec/L2TP

Сохранить

Отмена

- На вкладке **Пользователи** вы можете указать учетные записи или группы, созданные для серверов, которым разрешено подключаться по VPN.
- На вкладке **Подсети для VPN**:
 - Выберите VPN-адаптер, который будет использоваться для установления соединения (`tunnel3`).
 - Укажите диапазон IP-адресов и маску подсети, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW1 (172.16.0.1), используемому совместно с этой сетью.
 - Оставьте флажок **Использовать системные DNS-серверы**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW1.

Свойства Site-to-Site IPSec/L2TP

Общие

Пользователи

Подсети для VPN

Маршруты VPN

VPN адаптер:

tunnel3

Диапазон IP:

172.16.0.2-172.16.0.254

Маска:

255.255.255.0

☒ Использовать системные DNS-серверы

Серверы DNS

+ Добавить

✎ Редактировать

✕ Удалить

IP-адрес

Сохранить

Отмена

- На вкладке **Маршруты VPN** вы можете указать маршруты к подсетям за VPN-сервером, передаваемые узлу-инициатору.

Свойства Site-to-Site IPSec/L2TP

Общие Пользователи Подсети для VPN Маршруты VPN

+ Добавить

✎ Редактировать

✖ Удалить

	Название списка ↑	Владелец
IP	10.75.0.0/16	

Создать и добавить новый объект

Сохранить

Отмена

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в свойствах виртуального маршрутизатора VPN-сервера (**Настройки → Сеть → Виртуальные маршрутизаторы**), указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

Свойства виртуального маршрутизатора

Статические маршруты

+ Добавить

✎ Редактировать

✖ Удалить

Включить

Отключить

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
def1	unicast	10.6.0.0/16	172.16.0.2	Автоматически	0

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался

клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной **VPN for Site-to-Site** и зоной **LAN1**.

#	Журналирование	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи
Локальные правила								
8	Начало сессии	allow_lan1_s2s	Разрешить	LAN1 VPN for Site-to-Site	Любой	LAN1 VPN for Site-to-Site	Любой	Любой

Подробнее о создании и настройке правил межсетевого экрана — в разделе «[Межсетевой экран](#)».

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN подключений.

В этом примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс **tunnel4**. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону **VPN for Site-to-Site**.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной **VPN for Site-to-Site** и зоной **LAN2**.

#	Журналирование	Название	Теги	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
Локальные правила										
8	Начало сесс...	allow_lan2_s2s		Разрешить	LAN2 VPN for Site-to-Site	Любой	LAN2 VPN for Site-to-Site	Любой	Любой	Любой

4. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила подключения.
 - Выберите режим IKE: **Основной**.
 - Укажите значение общего ключа для аутентификации узлов. Ключи на VPN-сервере и узле-инициаторе соединения должны совпадать.
 - Выберите параметр идентификации узлов: **IPv4**.
 - Укажите в качестве значений параметров идентификации IP-адреса интерфейсов NGFW2 и NGFW1 из зоны **WAN**.
 - Укажите логин и пароль учетной записи, созданной [на шаге 4](#) при настройке NGFW1 для аутентификации NGFW2 в процессе установления L2TP-туннеля.

Свойства IPSec/L2TP

Общие

Фаза 1

Фаза 2

Название:

ipsec/l2tp

Описание:

Режим IKE:

Основной

Общий ключ:

Общий ключ (повтор):

Initiator

Тип идентификации:

IPv4

Значение идентификации:

10.72.0.31

Responder

Тип идентификации:

IPv4

Значение идентификации:

10.72.0.32

Аутентификация

Логин:

vpn_user_s2s

Пароль:

Сохранить

Отмена

- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
 - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
 - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

Свойства IPSec/L2TP

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Dead peer detection:

Всегда включена

20

секунд

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала. Для этого примера оставим значения криптографических параметров, заданные по умолчанию.

Свойства IPSec/L2TP

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

5. Создайте клиентское правило.

В разделе **Настройки** → **VPN Site-to-Site клиент** → **Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (ipsec/l2tp).
- Выберите в качестве туннельного интерфейса интерфейс `tunnel4`, созданный на шаге 2.
- Укажите IP-адрес VPN-сервера (10.72.0.32).

Свойства клиентского правила

☐ Включено

Название:

ipsec/l2tp

Описание:

Подключение клиента:

ipsec/l2tp

Интерфейс:

tunnel4

Адрес VPN-сервера:

10.72.0.32

Сохранить

Отмена

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

Клиентские правила

+

Добавить

✎

Редактировать

✖

Удалить

Включить

Отключить

↺↻

С.	Название	Адрес VPN-сервера	Интерфейс	Подключение клиента	Последняя ошибка VPN
●	ipsec/l2tp	172.26.157.218	🔌 tunnel4	🔌 ipsec/l2tp	

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг** → **Мониторинг** → **VPN** появится информация о новом туннеле.

VPN

NGFW1

Пользователь	Роль этого устройства	Политики VPN	Время сессии	Туннельный IP	IP адрес	Шифрование	Geo IP
User for S2S	🖨 Сервер	S2S IPSec/L2TP example VPN policy	03 февраля 2026 г., 11:34 (4м 10с)	172.16.0.2	172.26.157.217	aes	?

VPN

NGFW2

Пользователь	Роль этого устройства	Политики VPN	Время сессии	Туннельный IP	IP адрес	Шифрование	Geo IP
vpn_user_s2s	👤 Клиент	—	03 февраля 2026 г., 11:34 (2...	172.16.0.2	172.26.157.218	aes256	?

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW2 добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс **tunnel4**.

Маршруты

Узел: Виртуальный маршрутизатор:

NGFW2 ▾ Все ▾  |  Маршруты ▾

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 01:54:30
K>* 10.75.0.0/16 [0/0] via 172.16.0.1, tunnel4, src 172.16.0.2, 00:00:07
K>* 172.16.0.1/32 [0/0] is directly connected, tunnel4, 00:00:12

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

C>* 10.6.0.0/16 is directly connected, port2, 01:54:30
C>* 10.72.0.0/16 is directly connected, port1, 01:54:30
C>* 172.16.0.2/32 is directly connected, tunnel4, 00:00:12
C>* 172.26.0.0/16 is directly connected, port0, 01:54:30

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW1.

Ping host: TTL: Интерфейс:

Счётчик: ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

```

PING 172.16.0.2 (172.16.0.2) from 172.16.0.1 : 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_req=1 ttl=64 time=1.69 ms
64 bytes from 172.16.0.2: icmp_req=2 ttl=64 time=4.35 ms
64 bytes from 172.16.0.2: icmp_req=3 ttl=64 time=2.61 ms
64 bytes from 172.16.0.2: icmp_req=4 ttl=64 time=0.706 ms
64 bytes from 172.16.0.2: icmp_req=5 ttl=64 time=2.75 ms
64 bytes from 172.16.0.2: icmp_req=6 ttl=64 time=4.32 ms

--- 172.16.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.706/2.740/4.357/1.315 ms

```

Со стороны NGFW2.

Ping host: TTL: Интерфейс:

Счётчик: ☐ Показывать временные метки ☐ Не распознавать IP в доменные имена

Вывод ответа

```

PING 172.16.0.1 (172.16.0.1) from 172.16.0.2 : 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_req=1 ttl=64 time=1.50 ms
64 bytes from 172.16.0.1: icmp_req=2 ttl=64 time=1.05 ms
64 bytes from 172.16.0.1: icmp_req=3 ttl=64 time=1.96 ms
64 bytes from 172.16.0.1: icmp_req=4 ttl=64 time=3.97 ms
64 bytes from 172.16.0.1: icmp_req=5 ttl=64 time=1.96 ms
64 bytes from 172.16.0.1: icmp_req=6 ttl=64 time=0.820 ms

--- 172.16.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 0.820/1.881/3.977/1.030 ms

```

Сервер и компьютер в сетях обоих офисов доступны друг для друга.

```

Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff

```

```

altname enp19s0
inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
    valid_lft forever preferred_lft forever
inet6 fe80::254:54ff:fea8:7c91/64 scope link
    valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=5.13 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.64 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=3.37 ms
^C
--- 10.6.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.370/4.043/5.126/0.772 ms

```

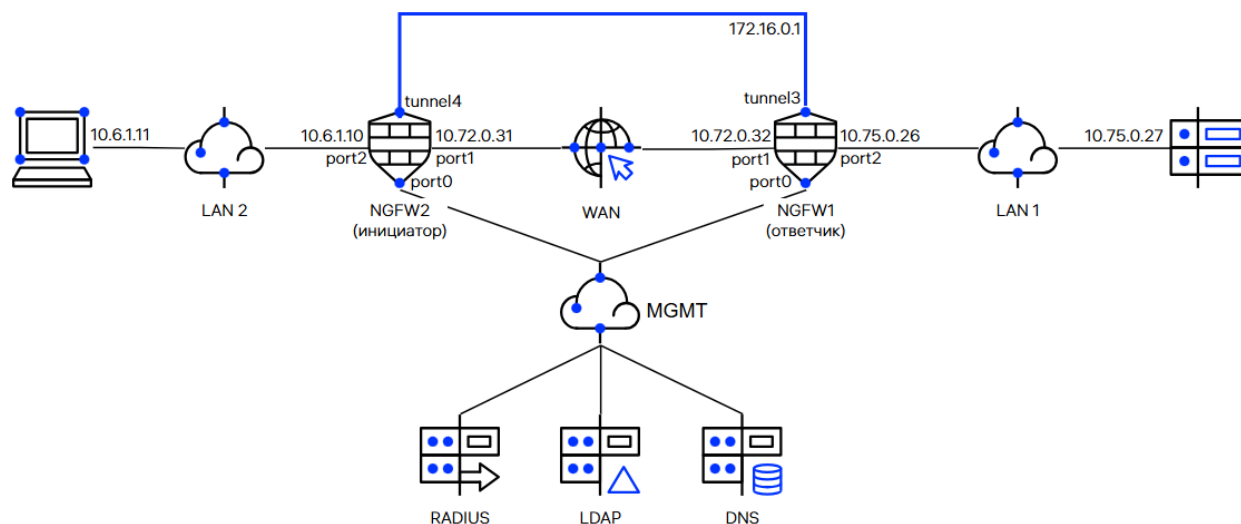
```

Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
        valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.29 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.17 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=8.40 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.169/6.952/8.402/1.026 ms

```


Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1) с помощью интерфейса CLI

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.



Настройка VPN-сервера

Для настройки узла NGFW 1 в качестве VPN-сервера выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

```
Admin@NGFW1# create network zone name WAN enabled-services [ VPN ]
```

Подробнее о командах и параметрах для создания и редактирования зон в CLI — в разделе «[Зоны](#)».

2. Создайте зону для VPN-подключений.

На узле уже создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@NGFW1# show network zone "VPN for Site-to-Site"
```

```
name : VPN for Site-to-Site
```

```

antispoof-enable           : off
antispoof-negate           : off
dos-protection-syn         :
    enabled                 : on
    aggregate               : off
    alert-threshold         : 3000
    drop-threshold          : 6000
dos-protection-udp         :
    enabled                 : on
    aggregate               : off
    alert-threshold         : 3000
    drop-threshold          : 6000
dos-protection-icmp        :
    enabled                 : on
    aggregate               : off
    alert-threshold         : 100
    drop-threshold          : 200
services-access            :
    service                 : Any ICMP
    allowed-addresses       : Any
    enabled                 : on

    service                 : reponse_pages
    allowed-addresses       : Any
    enabled                 : on

    service                 : DNS
    allowed-addresses       : Any
    enabled                 : on

    service                 : HTTP Proxy
    allowed-addresses       : Any
    enabled                 : on

    service                 : Endpoint connect
    allowed-addresses       : Any
    enabled                 : on

```

```
sessions-limit-enabled      : off
sessions-limit-threshold    : 0
```

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

Для создания VPN-интерфейса используется команда:

```
Admin@ug# create network interface vpn <parameters>
```

Подробнее о порядке создания VPN-интерфейса в CLI — в разделе «[Интерфейсы](#)».

На узле изначально уже создан VPN-интерфейс `tunnel3`, который может быть использован для настройки site-to-site VPN. Установите статический IP-адрес `172.16.0.1` для этого примера.

```
Admin@NGFW1# set network interface vpn tunnel3 ip-addresses
[ 172.16.0.1/24 ]
Admin@NGFW1# show network interface vpn tunnel3

type                : vpn
node_name           : cluster
interface-name      : tunnel3
description         : Interface for site-to-site vpn
enabled             : on
netflow-profile     : Undefined
iface-mode          : static
mtu                 : 1420
mss                 : 0
speed               : 0
zone                : VPN for Site-to-Site
running             : off
master              : off
ip-addresses        : 172.16.0.1/24
```

4. Настройте параметры аутентификации.

- **Создайте локальную учетную запись для аутентификации узла-инициатора соединения при установлении L2TP-туннеля.**

Пример создания учетной записи **User for s2s** с логином **vpn_user_s2s**, входящего в группу **VPN servers**:

```
Admin@NGFW1# create users user name "User for s2s" login
vpn_user_s2s groups [ "VPN servers" ] enabled on
```

Подробнее о командах и параметрах для создания локальных пользователей в CLI — в разделе «[Настройки пользователей](#)».

- **Создайте профиль аутентификации для VPN-пользователей.**

Пример создания профиля аутентификации **local user auth profile** с аутентификацией по базе данных локально заведенных пользователей:

```
Admin@NGFW1# create users auth-profile name "local user auth
profile" auth-methods local-user-auth on
```

Подробнее о порядке создания профилей аутентификации для пользователей в CLI — в разделе «[Настройка профилей аутентификации](#)».

5. Создайте правило подключения.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW1# create vpn-server connection-rules ike name
ikev1_test_rule protocol ikev1 ike-mode main src-zones [ WAN ] dh-
groups [ "Group 2 Prime 1024 bit" "Group 14 Prime 2048 bit" ] security
[ SHA1/AES256 SHA256/AES256 ] psk 123321
```

Repeat preshared key:

```
Admin@NGFW1# show vpn-server connection-rules ike ikev1_test_rule
```

```
name                : ikev1_test_rule
type                : ike
protocol            : ikev1
ike-mode            : main
src-zones            : WAN
dh-groups           : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
security            :
```

```

authentication      : SHA1
encryption          : AES256

authentication      : SHA256
encryption          : AES256

key-lifetime        : 1 h
dpd-state           : off
dpd-interval        : 60
dpd-max-failures    : 5

```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе «[Настройка серверных правил VPN](#)».

6. Создайте правило аутентификации.

Пример создания правила подключения для протокола **l2tp-ipsec**:

```

Admin@NGFW1# create vpn-server authentication-rules site-to-site l2tp-
ipsec name "s2s ipsec-l2tp auth rule" connection-rules [ "ikev1 conn
rule" ] initiator-type ipv4 initiator-value 10.72.0.31 responder-type
ipv4 responder-value 10.72.0.32 auth-profile "local user auth profile"
Admin@NGFW1# show vpn-server authentication-rules site-to-site l2tp-
ipsec "s2s ipsec-l2tp auth rule"

```

```

name                  : s2s ipsec-l2tp auth rule
connection-rules      : ikev1 conn rule
initiator-type        : ipv4
initiator-value       : 10.72.0.31
responder-type        : ipv4
responder-value       : 10.72.0.32
auth-profile          : local user auth profile
key-lifetime          : 1 h
key-lifetime-enabled  : off
key-lifetime-size     : 100.0 MB
nat-keepalive         : 0
security              :
  authentication      : SHA1
  encryption          : AES256

```

```
authentication      : SHA256
encryption          : AES256
```

Подробнее о командах и параметрах для создания правила аутентификации в CLI — в разделе «[Настройка серверных правил VPN](#)».

7. Создайте политику VPN-подключения.

Политики VPN создаются с помощью синтаксиса языка [UASL](#).

Пример создания правила подключения для протокола `l2tp-ipsec`:

```
Admin@NGFW1# create vpn-server vpn-policy 7 upl-rule \
...OK
...auth_rules("s2s ipsec-l2tp auth rule") \
...vpn_routes(10.75.0.0/16) \
...ip_range("172.16.0.2-172.16.0.254") \
...desc("VPN server policy for S2S IPSec/L2TP connection.") \
...mask(255.255.255.0) \
...use_system_dns(true) \
...enabled(true) \
...type(s2s_l2tp) \
...interface(tunnel3) \
...name("S2S IPSec/L2TP example VPN policy")
```

Подробнее о создании политик VPN в CLI — в разделе «[Настройка серверных правил VPN](#)».

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в виртуальном маршрутизаторе VPN-сервера, указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

```
Admin@NGFW1# set network virtual-router default routes new name route1
destination-ip 10.6.0.0/16 gateway 172.16.0.2 enabled on
Admin@NGFW1# show network virtual-router default routes

route1
  name          : route1
```

```

enabled      : on
destination-ip : 10.6.0.0/16
gateway      : 172.16.0.2
interface    : auto
metric       : 0

```

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе Настройки → Политики сети → Межсетевой экран правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1:

```

Admin@NGFW1# create network-policy firewall 8 upl-rule \
...PASS \
...src.zone = (LAN1, "VPN for Site-to-Site") \
...dst.zone = (LAN1, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan1_s2s)

```

Подробнее о порядке настройки правил межсетевого экрана в CLI — в разделе [«Настройка правил межсетевого экрана»](#).

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону, которой будет принадлежать интерфейс, используемый для подключения по VPN.

На узле изначально создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@NGFW2# show network zone "VPN for Site-to-Site"
```

```

name                               : VPN for Site-to-Site
antispoof-enable                   : off
antispoof-negate                   : off
dos-protection-syn                 :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 3000
    drop-threshold                 : 6000
dos-protection-udp                 :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 3000
    drop-threshold                 : 6000
dos-protection-icmp               :
    enabled                        : on
    aggregate                      : off
    alert-threshold                : 100
    drop-threshold                 : 200
services-access                    :
    service                       : Any ICMP
    allowed-addresses              : Any
    enabled                        : on

    service                       : reponse_pages
    allowed-addresses              : Any
    enabled                        : on

    service                       : DNS
    allowed-addresses              : Any
    enabled                        : on

    service                       : HTTP Proxy
    allowed-addresses              : Any
    enabled                        : on

    service                       : Endpoint connect
    allowed-addresses              : Any

```



```

enabled                : on

sessions-limit-enabled  : off
sessions-limit-threshold : 0

```

2. Создайте VPN-интерфейс.

Пример создания VPN-интерфейса `tunnel4`:

```

Admin@NGFW2# create network interface vpn interface-name 4 iface-mode
dynamic zone "VPN for Site-to-Site" enabled on
Admin@NGFW2# show network interface vpn tunnel4

```

```

type                : vpn
node_name           : cluster
interface-name      : tunnel4
enabled             : on
netflow-profile     : Undefined
iface-mode          : dynamic
mtu                 : 1420
mss                 : 0
speed              : 0
zone                : VPN for Site-to-Site
running            : off
master              : off

```

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону **VPN for Site-to-Site**.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной **VPN for Site-to-Site** и зоной **LAN2**.

```

Admin@NGFW2# create network-policy firewall 8 upl-rule \
...PASS \

```

```
...src.zone = (LAN2, "VPN for Site-to-Site") \
...dst.zone = (LAN2, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan2_s2s)
```

4. Создайте правило подключения к VPN.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW2# create vpn-client connections l2tp-ipsec name ipsec/l2tp
ike-mode main authentication-login vpn_user_s2s authentication-password
123456 initiator-type ipv4 initiator-value 10.72.0.31 responder-type
ipv4 responder-value 10.72.0.32 psk 123456
```

Repeat preshared key:

```
Admin@NGFW2# show vpn-client connections l2tp-ipsec ipsec/l2tp
```

```
name                : ipsec/l2tp
ike-mode            : main
authentication-login : vpn_user_s2s
phase1-key-lifetime : 1 h
phase2-key-lifetime : 1 h
key-lifesize-enabled : off
key-lifesize        : 100.0 MB
initiator-type      : ipv4
initiator-value     : 10.72.0.31
responder-type      : ipv4
responder-value     : 10.72.0.32
dpd-state           : off
dpd-interval        : 60
dpd-max-failures    : 5
dh-groups           : Group 2 Prime 1024 bit; Group 14 Prime 2048
bit
phase1-security     :
  authentication    : SHA1
  encryption        : AES256

  authentication    : SHA256
  encryption        : AES256
```

```

phase2-security      :
  authentication     : SHA1
  encryption         : AES256

  authentication     : SHA256
  encryption         : AES256

```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе «[Настройка клиентских правил VPN](#)».

5. Создайте клиентское правило.

Клиентские правила создаются с помощью синтаксиса языка [UASL](#).

Пример создания клиентского правила для протокола `l2tp-ipsec`:

```

Admin@NGFW2# create vpn-client rules 4 upl-rule \
...OK \
...server_address("10.72.0.32") \
...connection("ipsec/l2tp") \
...interface(tunnel4) \
...enabled(false) \
...name("ipsec/l2tp")

```

Подробнее о командах и параметрах для создания клиентского правила в CLI — в разделе «[Настройка клиентских правил VPN](#)».

Для инициации соединения включите клиентское правило.

```

Admin@NGFW2# set vpn-client rules 4 upl-rule \
...enabled(true)

```

Проверка VPN-соединения

Проверка доступности соседнего узла и маршрута в сеть удаленного офиса.

Со стороны NGFW 1:

```
Admin@NGFW1> show network route
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b -
backup
       t - trapped, o - offload failure
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:12:57
K>* 10.6.0.0/16 [0/0] via 172.16.0.2, tunnel3, 00:00:16
C>* 10.72.0.0/16 is directly connected, port1, 00:12:57
C>* 10.75.0.0/16 is directly connected, port2, 00:12:57
C>* 10.153.0.0/16 is directly connected, port3, 00:12:57
C>* 172.16.0.0/24 is directly connected, tunnel3, 00:12:57
C>* 172.26.0.0/16 is directly connected, port0, 00:12:57
C>* 172.30.250.0/24 is directly connected, tunnel1, 00:12:57
C>* 172.30.255.0/24 is directly connected, tunnel2, 00:12:57
```

```
Admin@NGFW1> ping host 172.16.0.2
```

```
PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_req=1 ttl=64 time=1.32 ms
64 bytes from 172.16.0.2: icmp_req=2 ttl=64 time=3.89 ms
64 bytes from 172.16.0.2: icmp_req=3 ttl=64 time=1.71 ms

--- 172.16.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.327/2.311/3.893/1.129 ms
```

Со стороны NGFW 2:

```
Admin@NGFW2> show network route
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b -
backup
       t - trapped, o - offload failure
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:08:41
```

```

C>* 10.6.0.0/16 is directly connected, port2, 00:08:41
C>* 10.72.0.0/16 is directly connected, port1, 00:08:41
K>* 10.75.0.0/16 [0/0] via 172.16.0.1, tunnel4, src 172.16.0.2,
00:01:18
K>* 172.16.0.1/32 [0/0] is directly connected, tunnel4, 00:01:23
C>* 172.16.0.2/32 is directly connected, tunnel4, 00:01:23
C>* 172.26.0.0/16 is directly connected, port0, 00:08:41

```

```
Admin@NGFW2> ping host 172.16.0.1
```

```

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_req=1 ttl=64 time=2.70 ms
64 bytes from 172.16.0.1: icmp_req=2 ttl=64 time=1.76 ms
64 bytes from 172.16.0.1: icmp_req=3 ttl=64 time=3.35 ms

--- 172.16.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.763/2.609/3.359/0.655 ms

```

Проверка установления L2TP-туннеля в журналах узлов.

На NGFW1.

```

Admin@NGFW1> show logs log vpn-server static | grep "LCP connected" -BA
0:23
2026-02-04 13:36:47.063149<0.1074.0> [info][vpn]
lcp_fsm:send_connected/1:256 LCP connected
2026-02-04 13:36:47.063159<0.1073.0> [info][vpn]
ppp_protocol:decode_packet/1:62 PAPResponse with password
2026-02-04 13:36:47.063180<0.1074.0> [info][vpn]
lcp_fsm:send_auth_challenge/1:226 PAP protocol selected - wait for
client
2026-02-04 13:36:47.064482<0.1074.0> [info][xmlrpc]
database:process_server_policy_phase/2:380 server policy "S2S IPSec/
L2TP example VPN policy"
2026-02-04 13:36:47.064547<0.1074.0> [warning][xmlrpc]
database:login_user_v2/5:449 login user "vpn_user_s2s" ip "10.72.0.31"
token
"35a447c5-a03f-49f4-83d5-3493cd4b983a" guid "c9202ee4-

```

```

cb35-4d18-91fb-62a67f72aa0e"
2026-02-04 13:36:47.066152<0.1074.0> [info][vpn]
lcp_fsm:STATE_OPENED_9/2:984 auth succeed, username <<"vpn_user_s2s">>,
guid
                "c9202ee4-cb35-4d18-91fb-62a67f72aa0e", parent pid
<0.1073.0>
2026-02-04 13:36:47.066526<0.1074.0> [info][vpn]
lcp_fsm:send_auth_response_pap/4:210 send PAP response ID 1 code 2
<<"Willkommen">>
2026-02-04 13:36:47.066581<0.1074.0> [info][vpn]
lcp_fsm:send_ccp_configure/2:750 Send CCP configure packet
<<1,1,0,6,4,2>>
2026-02-04 13:36:47.066953<0.1074.0> [info][vpn]
lcp_fsm:send_ipcp_configure/4:735 Send IPCP configure packet
{172,16,0,1}/{[{10,75,0,0},{255,255,0,0}]}
2026-02-04 13:36:47.067352<0.1073.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
                {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',
1,1,[{'IPCPOpt_Address',<<0,0,0,0>>},{ 'IPCPOpt_PriDNS',<<0,0,0,0>>}]}]}
2026-02-04 13:36:47.067440<0.1073.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',255,3,49185,
{'LCPProtocolReject',8,1,257}}
2026-02-04 13:36:47.067498<0.1074.0> [error][vpn]
lcp_fsm:STATE_OPENED_9/2:1054 Protocol 257 rejected!
2026-02-04 13:36:47.067821<0.1073.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
                {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',
2,1,[{'IPCPOpt_Routes',[{10,75,0,0},{255,255,0,0}]}],
{'IPCPOpt_Address',<<172,16,0,1>>}]}]}
2026-02-04 13:36:47.068119<0.1073.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
                {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',
1,2,[{'IPCPOpt_Address',<<172,16,0,2>>},
{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}]}
2026-02-04 13:36:47.068174<0.1074.0> [critical][vpn]
lcp_fsm:analyze_ipcp_option/2:785 IPClientSuggested {172,16,0,2}
IPClientReqTuple {172,16,0,2}
2026-02-04 13:36:47.068258<0.1074.0> [critical][vpn]
lcp_fsm:send_ipcp_response/2:881 IPCP ACK! Great deal

```

```

        {'IPCPHeader',1,2,[{'IPCP0pt_Address',<<172,16,0,2>>},
{'IPCP0pt_PriDNS',<<172,16,0,1>>}]]
2026-02-04 13:36:47.069245<0.1073.0> [warning][vpn]
l2tp_fsm:handle_info/3:750 NewIPs [{client_ip,{172,16,0,2}},{server_ip,
{172,16,0,1}}] Routes
        [{10,75,0,0},{255,255,0,0}]

```

Ha NGFW2.

```

Admin@NGFW2> show logs log vpn-client static | grep "LCP connected" -BA
0:19
2026-02-04 13:36:47.052244<0.1069.0> [info][vpn]
lcp_client:send_connected/1:155 LCP connected, send auth
2026-02-04 13:36:47.056257<0.1066.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,
49187,{pap_success,1}}
2026-02-04 13:36:47.056341<0.1069.0> [info][vpn]
lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip
undefined dns undefined
2026-02-04 13:36:47.056330<0.1066.0> [info][vpn]
ppp_protocol:decode_ccp/1:387 {'CCPHeader',1,1,<<4,2>>}}
2026-02-04 13:36:47.056408<0.1066.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,
33021,{'CCPHeader',1,1,<<4,2>>}}
2026-02-04 13:36:47.056668<0.1069.0> [info][vpn]
lcp_client:encode_protocol_reject/2:125 send LCP reject protocol
"010100060402"
2026-02-04 13:36:47.056903<0.1066.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',
1,1,[{'IPCP0pt_Routes',[{10,75,0,0},{255,255,0,0}]}],
{'IPCP0pt_Address',<<172,16,0,1>>}]]}}
2026-02-04 13:36:47.056958<0.1069.0> [critical][vpn]
lcp_client:send_ipcp_response/2:628 IPCP ACK! Server ip <<172,16,0,1>>,
routes
        [{10,75,0,0},{255,255,0,0}]
2026-02-04 13:36:47.057046<0.1066.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',

```

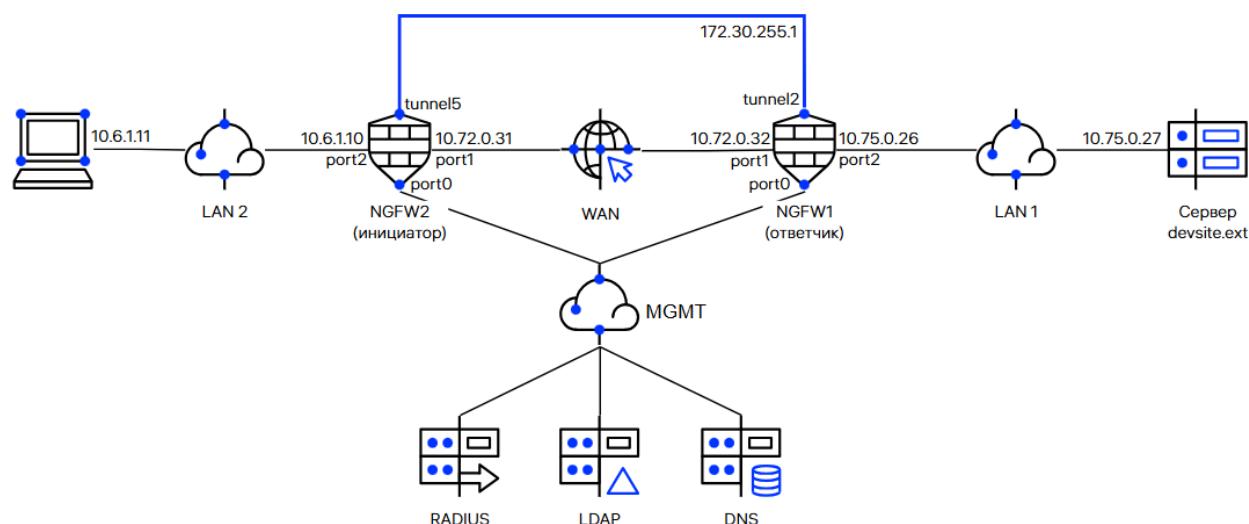
```

3,1,[{'IPCP0pt_Address',<<172,16,0,2>>},
{'IPCP0pt_PriDNS',<<172,16,0,1>>}]]}
2026-02-04 13:36:47.057072<0.1069.0> [warning][vpn]
lcp_client:send_ipcp_response/2:689 Send IPCP answer
      {'IPCPHeader',2,1,[{'IPCP0pt_Routes',[{10,75,0,0},
{255,255,0,0}]]},{'IPCP0pt_Address',<<172,16,0,1>>}]]}
2026-02-04 13:36:47.057355<0.1069.0> [info][vpn]
lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip
<<172,16,0,2>> dns <<172,16,0,1>>
2026-02-04 13:36:47.060539<0.1066.0> [info][vpn]
ppp_protocol:decode_packet/1:64 PPP:
      {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',
2,2,[{'IPCP0pt_Address',<<172,16,0,2>>},
{'IPCP0pt_PriDNS',<<172,16,0,1>>}]]}
2026-02-04 13:36:47.060650<0.1069.0> [critical][vpn]
lcp_client:send_ipcp_response/2:660 IPCP ACK! Client IP <<172,16,0,2>>
dns <<172,16,0,1>>
2026-02-04 13:36:47.061877<0.1069.0> [info][vpn]
lcp_client:send_ipcp_response/2:672 AuthToken
"a270d112-428f-4d28-8727-354510f99325"
2026-02-04 13:36:47.062790<0.1066.0> [info][vpn]
l2tp_client:handle_info/3:729 configure device "tunnel4" static
undefined dynamic <<172,16,0,2>>

```

Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.



Настройка VPN-сервера

Для настройки узла NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

В разделе **Настройки → Сеть → Зоны** создайте зону **WAN** и активируйте сервис **VPN** в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе [«Настройка зон»](#).

2. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройке зон — в разделе [«Настройка зон»](#).

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

В этом примере воспользуемся созданным по умолчанию интерфейсом **tunnel2**. Подробнее о создании и настройке сетевых интерфейсов — в разделе [«Настройка интерфейсов»](#).

4. Настройте параметры аутентификации.

- Импортируйте созданный заранее сертификат VPN-сервера и корневой сертификат. О примерах создания самоподписанных сертификатов — в [Приложении](#).

В разделе **Настройки → Консоль администратора →**

Сертификаты нажмите **Импорт**. В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

- Создайте профиль клиентского сертификата в веб-консоли NGFW1. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите поле **Subject altname IPv4** для получения из сертификата узла-инициатора соединения (NGFW2) его IP-адреса.

Профиль клиентского сертификата

Название:

Cert profile 1

Описание:

Получать имя пользователя из:

Subject altname IPv4

Сертификаты УЦ

Добавить

Импорт

Удалить

Название	Издатель	Истекает
ca	VPN root CA	15 Июль 2033 г.

Наверх

Выше

Низе

Вниз

Проверка отозванных сертификатов:

Не проверять

Таймаут проверки:

1

(в секундах)

Сохранить

Отмена

5. Создайте правило подключения.

В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила подключения.
 - Выберите протокол подключения **IKEv2**.

The screenshot shows a dialog box titled "Свойства IKE" (IKE Properties) with a close button (X) in the top right corner. The dialog has four tabs: "Общие" (General), "Источник" (Source), "Назначение" (Destination), and "Фаза 1" (Phase 1). The "Общие" tab is selected. It contains the following fields:

- Название:** A text input field containing "ikev2 wan".
- Описание:** A larger text input field, currently empty.
- Протокол:** A dropdown menu with "IKEv2" selected.
- Режим IKE:** A dropdown menu with "Основной" (Main) selected.
- Общий ключ:** A text input field with six dots (password mask).
- Общий ключ (повтор):** A text input field with six dots (password mask).

At the bottom right of the dialog are two buttons: "Сохранить" (Save) and "Отмена" (Cancel).

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны **WAN**.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Зона источника

☐ Cluster
☐ DMZ
☐ LAN1
☐ Management
☐ MGMT
☐ Trusted
☐ Tunnel inspection zone
☐ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site
☒ WAN
☐ WAN1

Создать и добавить новый объект

Адрес источника

+ Добавить

Ещё...

Название списка	Владелец

Создать и добавить новый объект

Сохранить

Отмена

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Время жизни ключа:

1

часов

Dead peer detection:

Отключена

60

секунд

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

6. Создайте правило аутентификации.

В разделе **Настройки** → **VPN-сервер** → **Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site** → **IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила аутентификации.
 - Выберите режим аутентификации посредством сертификатов (**PKI**).
 - Выберите импортированный на шаге 4 сертификат VPN-сервера.
 - Выберите созданный на шаге 4 профиль клиентского сертификата.
 - Выберите тип идентификации узлов (**IPv4**).

- Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.
- В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

Свойства Site-to-Site IKEv2

Общие Фаза 2

Название:

s2s ikev2 auth rule pki

Описание:

Режим аутентификации:

PKI

Общий ключ:

.....

Общий ключ (повтор):

.....

Сертификат сервера:

server cert

Профиль клиентского сертификата:

Cert profile 1

Initiator

Тип идентификации:

IPv4

Значение идентификации:

10.72.0.31

Responder

Тип идентификации:

IPv4

Значение идентификации:

10.72.0.32

Правила подключения

+ Добавить

✖ Удалить

Название	Протокол
ikev2 wan	IKEv2

Сохранить

Отмена

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

Свойства Site-to-Site IKEv2

Общие

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

☒ Включить NAT keepalive

Время жизни NAT:

25

секунд

PEER networks

☐ Включить динамическую маршрутизацию

+ Добавить

Ещё...

Локальная подсеть

10.75.0.0/16

+ Добавить

Ещё...

Удалённая подсеть

☒ Не проверять сети инициатора

Безопасность

+ Добавить

✎ Редактировать

✖ Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

7. Создайте политику VPN-подключения.

В разделе **Настройки** → **VPN-сервер** → **Политики VPN** нажмите **Добавить** и выберите **Site-to-Site** → **IPsec**. Укажите следующие ключевые параметры:

- Укажите название правила аутентификации.
- Выберите VPN-адаптер, созданный на шаге 2 (**tunnel2**).
- В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

718

Свойства Site-to-Site IPSec

☒ Включено

Название: S2S IPSec example VPN policy

Описание: Пример политики VPN.

VPN адаптер: tunnel2

Правила аутентификации

Добавить

Удалить

Название	Протокол
s2s ikev2 auth rule pki	IKEv2

Сохранить

Отмена

8. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону **VPN for Site-to-Site**.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной **VPN for Site-to-Site** и зоной **LAN1**.

#	Журналирование	Название	Теги	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
Локальные правила										
8	Начало сесс...	allow_lan3_s2s		Разрешить	LAN1 VPN for Site-to-Site	Любой	LAN1 VPN for Site-to-Site	Любой	Любой	Любой

Подробнее о создании и настройке правил межсетевого экрана — в разделе [«Межсетевой экран»](#).

719

Настройка VPN-клиента

Для настройки узла NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс **tunnel5**. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте параметры аутентификации.

Импортируйте созданный заранее сертификат VPN-клиента.

В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импорт**. В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа.

4. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону **VPN for Site-to-Site**.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной **VPN for Site-to-Site** и зоной **LAN2**.

#	Журналирование	Название	Теги	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
Локальные правила										
8	Начало сесс...	allow lan2 s2s		Разрешить	LAN2 VPN for Site-to-Site	Любой	LAN2 VPN for Site-to-Site	Любой	Любой	Любой

5. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила подключения.
 - Выберите режим аутентификации с помощью сертификата (**PKI**).
 - Выберите импортированный на шаге 3 сертификат клиента.
 - Выберите параметр идентификации узла (**IPv4**).
 - Укажите в качестве значения параметра идентификации узла IP-адрес интерфейса из зоны **WAN (10.72.0.31)**.

Свойства IKEv2

×

Общие

Фаза 1

Фаза 2

Название:

ikev2 pki

Описание:

☐ Проверять IP на VPN сервере

Режим аутентификации:

PKI

▼

Общий ключ:

Общий ключ (повтор):

Сертификат клиента:

client cert

▼

Initiator

Тип идентификации:

IPv4

▼

Значение идентификации:

10.72.0.31

Сохранить

Отмена

- На вкладке **Фаза 1** укажите параметры фазы 1 для установления защищенного канала IKE SA: Для этого примера оставим значения параметров, заданные по умолчанию

Свойства IKEv2

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Dead peer detection:

Отключена

60

секунд

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала IPsec SA.
 - Для этого примера оставим значения криптографических параметров, заданные по умолчанию.
 - В разделе **Peer networks** укажите адреса локальных и удаленных подсетей для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В этом примере указываются адреса подсетей **LAN2** и **LAN1** соответственно

Свойства IKEv2

ОбщиеФаза 1Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

PEER networks

☐ Включить динамическую маршрутизацию

Добавить

Ещё...

Локальная подсеть

10.6.1.0/16

Добавить

Ещё...

Удалённая подсеть

10.75.0.0/16

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

6. Создайте клиентское правило.

В разделе **Настройки → VPN Site-to-Site клиент → Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (`ikev2 pki`).
- Выберите в качестве туннельного интерфейса интерфейс `tunnel3`.
- Укажите адрес VPN-сервера (`vpntest.net`).

Свойства клиентского правила

☐ Включено

Название:

ikev2 pki

Описание:

Example VPN client rule for IPSec only/IKEv1 connection. It can be changed or deleted if necessary.

Подключение клиента:

ikev2 pki

Интерфейс:

tunnel5

Адрес VPN-сервера:

vpntest.net

Сохранить

Отмена

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

Клиентские правила

+

Добавить

✎

Редактировать

✖

Удалить

Включить

Отключить

↺↻

С	Название	Адрес VPN-сервера	Интерфейс	Подключение клиента	Последняя ошибка VPN
●	ikev2 pki	vpntest.net	🌐 tunnel5	🔒 ikev2 pki	

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг** → **Мониторинг** → **VPN** появится информация о новом туннеле.

VPN

NGFW1

Пользователь	Роль этого устройства	Политики VPN	Время сессии	Туннельный ...	IP адрес	Шифрован...	Geo IP
-	🖨 Сервер	S2S IPSec example VPN policy	04 февраля 2026 г., 07:29 (23м 14с)	—	10.72.0.31	aes	?

VPN

NGFW2

Пользователь	Роль этого устройства	Политики VPN	Время сессии	Туннельный IP	IP адрес	Шифрование	Geo IP
-	👤 Клиент	—	04 февраля 2026 г., 07:29 (24м 57с)	192.168.0.0	vpntest.net	aes256	?

На узле NGFW1 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.6.0.0/16 через туннельный интерфейс tunnel2.

Узел: Виртуальный маршрутизатор:

NGFW1 Все  |  **Маршруты** ▼

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:13:04
K>* 10.6.0.0/16 [0/0] is directly connected, tunnel2, 00:00:05

VRF default

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
> - selected route, * - FIB route, q - queued, r - rejected, b - backup
t - trapped, o - offload failure

VRF default:

C>* 10.72.0.0/16 is directly connected, port1, 00:13:04
C>* 10.75.0.0/16 is directly connected, port2, 00:13:04
C>* 10.153.0.0/16 is directly connected, port3, 00:13:04
C>* 172.16.0.0/24 is directly connected, tunnel3, 00:13:04
C>* 172.26.0.0/16 is directly connected, port0, 00:13:04
C>* 172.30.250.0/24 is directly connected, tunnel1, 00:13:04
C>* 172.30.255.0/24 is directly connected, tunnel2, 00:13:04

На узле NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс tunnel5.

Узел: Виртуальный маршрутизатор:

NGFW2 ▾ Все ▾  |  Маршруты ▾

VRF default
 Codes: K - kernel route, C - connected, S - static, R - RIP,
 O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
 > - selected route, * - FIB route, q - queued, r - rejected, b - backup
 t - trapped, o - offload failure

VRF default:
 C>* 10.6.0.0/16 is directly connected, port2, 00:13:44
 C>* 10.72.0.0/16 is directly connected, port1, 00:13:44
 C>* 172.26.0.0/16 is directly connected, port0, 00:13:44
 C>* 192.168.0.0/32 is directly connected, tunnel5, 00:00:51
 Codes: K - kernel route, C - connected, S - static, R - RIP,
 O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
 > - selected route, * - FIB route, q - queued, r - rejected, b - backup
 t - trapped, o - offload failure

VRF default:
 K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:13:44
 K>* 10.75.0.0/16 [0/0] is directly connected, tunnel5 00:00:51

Узлы в сетях обоих офисов доступны друг для друга.

```
Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c91/64 scope link
        valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=3.54 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.99 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=4.85 ms
^C
--- 10.6.1.11 ping statistics ---
```

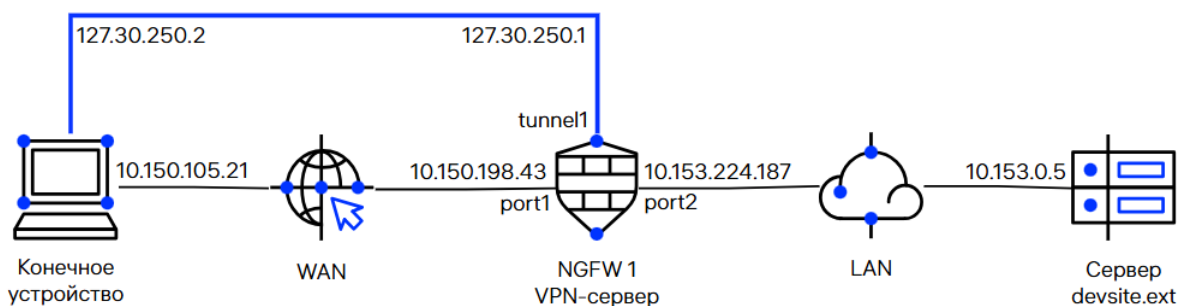


```
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.536/4.124/4.851/0.545 ms
```

```
Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
        valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.81 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.78 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=4.68 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.677/6.089/6.808/0.998 ms
```

Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux

Пример создания VPN-подключения между конечным устройством с операционной системой Astra Linux и UserGate NGFW версии 7.5.0.



В этом примере UserGate NGFW выступает в роли VPN-сервера, а компьютер пользователя на Astra Linux с установленным ПО UserGate Client — в роли

конечного устройства. Аутентификация пользователя будет происходить с помощью сертификата X.509. Конечному устройству будет передан маршрут к сети за VPN-сервером.

Сначала настройте VPN-сервер, затем настройте VPN-клиент на конечном устройстве и иницилируйте подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки UserGate NGFW в качестве VPN-сервера выполните следующие шаги:

1. Разрешите сервис VPN в контроле доступа зоны, из которой будут подключаться конечные устройства.

В веб-консоли UserGate NGFW в разделе **Настройки → Сеть → Зоны** создайте зону WAN. В параметрах контроля доступа зоны разрешите сервис VPN. Подробнее о создании и настройке зон — в разделе [«Настройка зон»](#).

2. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной по умолчанию зоной VPN for remote access. Подробнее о создании и настройке параметров зон — в разделе [«Настройка зон»](#).

3. Создайте VPN-интерфейс для организации туннеля.

В этом примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом `tunnel1`, который может быть использован для настройки remote access VPN. Изначально этот интерфейс не активен, его необходимо включить в свойствах интерфейса.

4. Настройте параметры аутентификации:

- Импортируйте созданные заранее сертификаты: сертификат VPN-сервера и корневой сертификат. Примеры создания самоподписанных сертификатов приведены в [Приложении](#).

В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импортировать**. В открывшемся окне укажите название сертификата и добавьте созданные ранее файлы сертификата VPN-сервера и его

закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

- Создайте профиль клиентского сертификата в веб-консоли UserGate NGFW. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя.

Профиль клиентского сертификата

Название:

Cert_profile 1

Описание:

Получать имя пользователя из:

Common-name

Сертификаты УЦ

Добавить

Импорт

Удалить

Название	Издатель	Истекает
са	VPN root CA	15 Июль 2033 г.

Наверх

Выше

Ниже

Вниз

Проверка отозванных сертификатов:

Не проверять

Таймаут проверки:

1

(в секундах)

Сохранить

Отмена

- Создайте профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации — в разделе «[Профили аутентификации](#)». Для этого примера был создан профиль аутентификации в домене **ADTEST1** через LDAP-коннектор **ad16**:

Свойства профиля аутентификации

ОбщиеМетоды аутентификации

+ Добавить

✗ Удалить

⬆ Выше

⬆ Ниже

Название
Сервер LDAP/Active Directory: ad16

Сохранить

Отмена

Свойства коннектора LDAP

НастройкиДомены LDAPKerberos keytabПути поиска

☒ Включено

☐ Использовать для соединений SSL

Название:

ad16

Описание:

Доменное имя LDAP или IP-адрес:

192.168.117.11

Привязать DN («логин»):

ADTEST1\user

Пароль:

Время жизни кэша:

28800

секунд

Проверить соединение

Сохранить

Отмена

5. Создайте правило подключения.

В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила подключения.
 - Выберите протокол подключения **IKEv2**.

Свойства IKE

Общие | Источник | Назначение | Фаза 1

Название: IKEv2 Connection phase

Описание: Пример правила подключения.

Протокол: IKEv2

Режим IKE: Основной

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

Свойства IKE

×

Общие

Источник

Назначение

Фаза 1

Зона источника

☐ CLUSTER
☐ Cluster
☐ DMZ
☐ LAN
☐ Management
☐ MGMT
☐ Trusted
☐ Tunnel inspection zone
☐ Untrusted
☐ VPN for remote access
☐ VPN for Site-to-Site
☒ WAN

Создать и добавить новый объект

Адрес источника

+ Добавить

Ещё...

Название списка	Владелец
Создать и добавить новый объект	

Сохранить

Отмена

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения от конечных устройств.
- На вкладке **Фаза 1** укажите криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

Свойства IKE

Общие

Источник

Назначение

Фаза 1

Время жизни ключа:

1

часов

Dead peer detection:

Отключена

60

секунд

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Группа 14 Prime 2048 бит

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Удаленный доступ → IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Укажите название правила аутентификации.
 - Выберите импортированный на шаге 4 сертификат VPN-сервера.
 - Выберите созданный на шаге 4 профиль аутентификации пользователя.
 - Выберите режим аутентификации посредством сертификатов (PKI).
 - Выберите созданный на шаге 4 профиль клиентского сертификата.

- В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

Свойства удаленного доступа IKEv2

Общие

Фаза 2

Название:

RA ikev2 auth phase pki

Описание:

Пример правила аутентификации.

Сертификат сервера:

server

Профиль аутентификации:

Auth_profile1

URL инициализации TOTP

Режим аутентификации:

PKI

Профиль клиентского сертификата:

Cert_profile 1

Правила подключения

+ Добавить

✕ Удалить

Название	Протокол
IKEv2 Connection phase	IKEv2

Сохранить

Отмена

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

Свойства удаленного доступа IKEv2

Общие

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

☐ Включить NAT keepalive

Время жизни NAT:

0

секунд

Безопасность

Добавить

Редактировать

Удалить

Аутентификация	Шифрование
SHA1	AES256
SHA256	AES256

Сохранить

Отмена

7. Создайте политику VPN-подключения.

В разделе **Настройки** → **VPN-сервер** → **Политики VPN** нажмите **Добавить** и выберите **Удаленный доступ** → **UserGate Client**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
 - Поставьте флажок для включения политики VPN.
 - Укажите название правила аутентификации.
 - В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

Свойства удаленного доступа UserGate client

Общие

Пользователи

Подсети для VPN

Маршруты для UserGate Client

☒ Включено

Название:

RA UserGate client example VPN policy

Описание:

Пример политики VPN-подключения.

Правила аутентификации

+ Добавить

✖ Удалить

Название	Протокол
RA ikev2 auth phase pki	IKEv2

Сохранить

Отмена

- На вкладке **Пользователи** вы можете добавить локальную или доменную учетную запись или группу, которые будут использоваться для аутентификации пользователей.
- На вкладке **Подсети для VPN**
 - Укажите VPN-интерфейс `tunnel1`, который будет использоваться для подключения.
 - Укажите диапазон IP-адресов, которые будут использованы для подключения. Исключите из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с данной сетью.
 - Укажите маску сети VPN.
 - Оставьте флажок **Использовать системные DNS-серверы** для передачи клиенту туннельного адреса UserGate NGFW в качестве DNS-сервера.

Свойства удаленного доступа UserGate client

Общие

Пользователи

Подсети для VPN

Маршруты для UserGate Client

VPN адаптер:

tunnel1

Диапазон IP:

172.30.250.2-172.30.250.254

Маска:

255.255.255.0

☒

Использовать системные DNS-серверы

Серверы DNS

+ Добавить

✎ Редактировать

✕ Удалить

IP-адрес

Сохранить

Отмена

- На вкладке **Маршруты для UserGate Client** укажите параметры маршрутов, передаваемых на конечное устройство с помощью функции раздельного туннелирования.
 - В этом примере на конечном устройстве будет добавлен маршрут к тестовому серверу `devsite.ext` (10.153.0.5).

Свойства удаленного доступа UserGate client

Общие

Пользователи

Подсети для VPN

Маршруты для UserGate Client

☐ Все маршруты

Включить маршруты

+ Добавить

Ещё...

	Название списка	Владелец
IP	10.153.0.5/32	

Исключить маршруты

+ Добавить

Ещё...

	Название списка	Владелец
--	-----------------	----------

☐ Ограничить доступ к локальной сети

Сохранить

Отмена

8. Настройте контроль доступа к ресурсам.

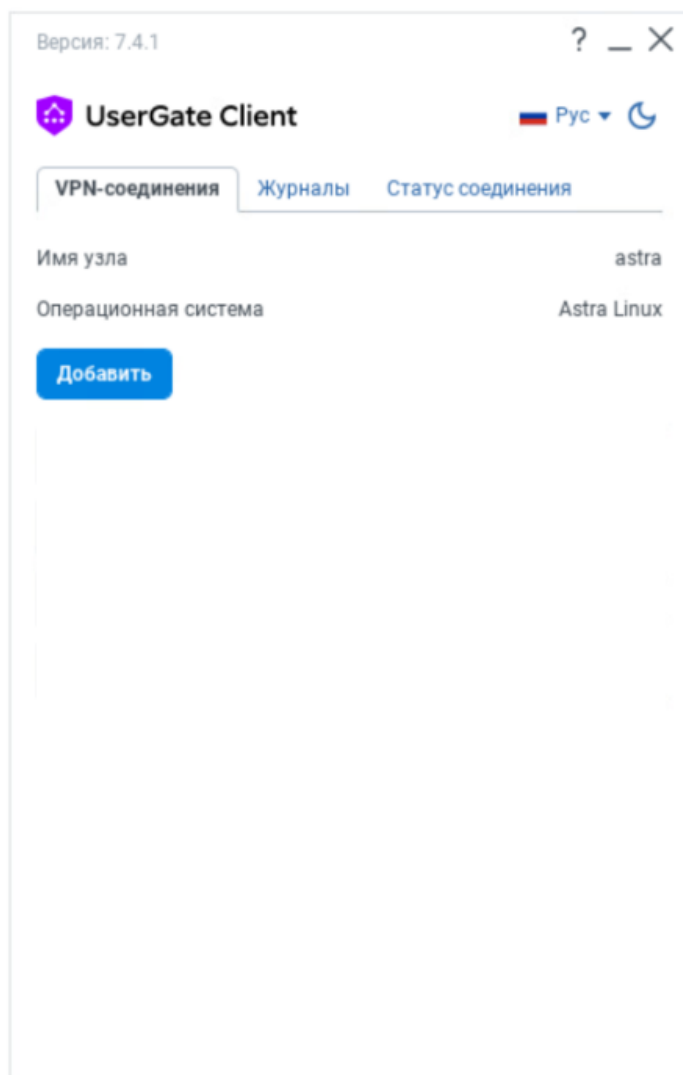
- Создайте правило NAT, выполняющее трансляцию IP-адресов при поступлении трафика из зоны VPN for remote access в зону LAN. Правило создается в разделе **Политики сети → NAT и маршрутизация**.
- При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Настройки → Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны. Для этого примера создано правило межсетевого экрана, разрешающее весь трафик из зоны VPN for remote access в зону LAN.

Настройка VPN-клиента

Предполагается, что ПО UserGate Client уже установлено на конечном устройстве. Подробнее об установке ПО — в разделе «[Настройка VPN-соединения на конечном устройстве](#)».

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Откройте окно настройки приложения UserGate Client и на вкладке VPN-соединения нажмите **Добавить**.



2. Настройте параметры профиля VPN-соединения:

- Укажите название соединения.
- Укажите IP-адрес или доменное имя VPN-сервера. В этом примере указано доменное имя сервера **vpntest.net**. Адрес должен быть прописан в серверном сертификате, импортированном на шаге 4 настройки VPN-сервера.
- Выберите протокол для установления VPN-соединения. В этом примере используется протокол **IKEv2**.
- Выберите один из способов аутентификации. В этом примере используется аутентификация посредством сертификатов.

- Выберите заранее созданные файл сертификата пользователя
- ADTEST1\user, закрытый ключ и введите пароль закрытого ключа.

Версия: 7.4.1

UserGate Client

Добавить VPN-соединение

Название соединения*

Доменное имя или IP-адрес сервера*

Протокол*

Способ аутентификации*

☐ Логин и пароль ☒ Сертификат

Файл сертификата в форматах DER, PEM, PKCS12

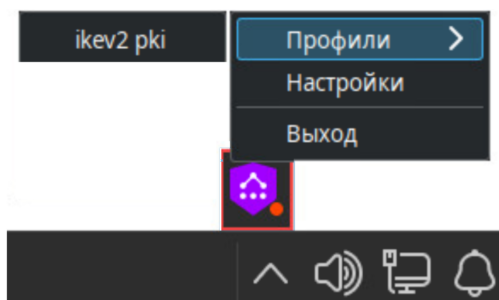
Закрытый ключ

Пароль закрытого ключа

3. Сохраните параметры профиля, нажав **Сохранить**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения в строке состояния в правом нижнем углу нажмите на значок UserGate Client и в появившемся меню выберите профиль соединения **ikev2 pki**.



В случае успешного подключения на значке UserGate Client появится символ установленного соединения.



Проверка подключения

После установлении VPN-соединения в веб-консоли UserGate NGFW на вкладке **Диагностика и мониторинг** в разделе **Мониторинг → VPN** появилась информация о новом VPN-соединении.

VPN

NGFW 1

Пользователь ↑	Роль этого устройства	Время сессии	Политики VPN	Туннельный ...	IP адрес	Шифрование	Geo IP
user (adtest1.net\user)	Сервер	26 января 2026 г., 11:52 (4м 24с)	RA UserGate client example VPN policy	172.30.250.2	10.150.105.21	aes	?

В **Журнале событий** на вкладке **Журналы и отчеты** появилась соответствующая запись.

Журнал событий

date >= 2026-01-26T00:00:00 AND date <= 2026-01-26T23:59:59 AND component = 'vpn'

Узел	Время	Компоне...	Тип события	Пользователь	IP источника	Модуль	Детали события
NGFW 1	11:52:41	VPN	Подключение пользователя к VPN прошло успешно	user (adtest1.net\user)	10.150.105.21	VPN сервер	Логин: ADTEST1\user, Серверное правило VPN: RA UserGate client example VPN policy

На конечном устройстве в таблице маршрутизации добавился маршрут к серверу `devsite.ext` (10.153.0.5) через туннельный интерфейс. Сервер доступен с конечного устройства..

```

admin1@astra:~$ ip r show table 777
default via 172.26.0.1 dev ens192
default via 172.26.0.1 dev ens192 proto dhcp src 172.26.116.132 metric 100
10.150.0.0/16 dev ens224 proto kernel scope link src 10.150.105.21
10.150.198.43 dev ens224 metric 1
10.153.0.5 via 172.30.250.2 dev ugtun metric 2
172.26.0.0/16 dev ens192 proto kernel scope link src 172.26.116.132 metric 100
172.26.0.1 dev ens192 proto dhcp scope link src 172.26.116.132 metric 100
172.30.250.1 via 172.30.250.2 dev ugtun
admin1@astra:~$ curl devsite.ext
<html>
<body>

<h1>DEVSITE.EXT</h1>

<p>For functional testing</p>

BODY

BODY

BODY

</body>
</html>

```

БИБЛИОТЕКИ ЭЛЕМЕНТОВ

Общие сведения

Библиотеки элементов содержит в себе все записи, адреса сайтов, IP-адреса, шаблоны, сигнатуры и прочие элементы, которые используются при настройке правил UserGate NGFW.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, обновляются автоматически при наличии специальной лицензии. Подробнее о лицензировании — в разделе «[Лицензирование UserGate NGFW](#)».

Морфология

Морфологический анализ — механизм, который распознает отдельные слова и словосочетания на веб-сайте. Если в тексте содержится достаточное для блокировки количество указанных слов и словосочетаний, то доступ к сайту блокируется.

Морфологический анализ выполняется как при проверке запроса пользователя, так и при получении ответа от веб-сервера и до его передачи пользователю. Получив ответ от веб-сервера, NGFW просматривает текст на странице и подсчитывает его суммарный «вес», исходя из «весов» слов, указанных в морфологических категориях. Если «вес» страницы превышает «вес» морфологической категории, правило срабатывает. При подсчете «веса» страницы учитываются все словоформы (леммы) запрещенных слов. Для поиска словоформ NGFW использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые UserGate. Данные словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

Наименование	Описание
Соответствие списку запрещенных материалов Министерством Юстиции Российской Федерации	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции Российской Федерации.
Соответствие списку запрещенных материалов республики Казахстан	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции республики Казахстан.
Суицид	Морфологический словарь, содержащий перечень слов и фраз суицидальной направленности.
Терроризм	Морфологический словарь, содержащий перечень слов и фраз террористической направленности.
Нецензурная лексика	Морфологический словарь, содержащий перечень слов и фраз, относящихся к нецензурной лексике.
Азартные игры	Морфологический словарь, содержащий перечень слов и фраз, относящихся к азартным играм.
Наркотики	Морфологический словарь, содержащий перечень слов и фраз наркотической направленности.

Наименование	Описание
Соответствие ФЗ-436 (Защита детей)	Морфологический словарь, содержащий перечень слов и фраз тематик, нежелательных для детей.
Порнография	Морфологический словарь, содержащий перечень слов и фраз порнографической направленности.
Бухгалтерия (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в бухгалтерии.
Маркетинг (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в маркетинге.
Персональные данные (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, встречающихся в персональных данных.
Финансы (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в финансах.
Юридический (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в юриспруденции.

Для фильтрации по морфологическому содержанию страницы требуется:

Наименование	Описание
Шаг 1. Создать одну или несколько морфологических категорий и указать вес каждой категории.	Нажать на кнопку Добавить , задать название новой категории и ее вес.
Шаг 2. Указать список запрещенных фраз с весами.	Нажать на кнопку Добавить и указать необходимые слова или фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки.
Шаг 3. Создать правило фильтрации контента, содержащее одну или несколько морфологических категорий.	Смотрите раздел Фильтрация контента .

Администратор имеет возможность создать свой словарь и централизованно распространять его на все межсетевые экраны UserGate, имеющиеся в организации. Для создания такой морфологической базы необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми фразами.	создать файл list.txt со списком слов в следующем формате: !word1 !word2 !word3 word4 50 ... Lastword Вес словаря в таком случае равен 100, вес слова можно указать. По умолчанию он равен 100.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией словаря.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать морфологическую категорию указать URL для обновления словаря.	На каждом UserGate создать морфологическую базу. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в

Наименование	Описание
	следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Примечание

При создании морфологических словарей не рекомендуется добавлять фразы, содержащие более трех слов, без использования символа «!» перед словами. Необходимо помнить, что при построении морфологической базы каждое из слов будет преобразовано во все существующие формы (склонения, спряжения, множественные числа, времена и т.д.), и результирующее количество фраз будет достаточно большим. При добавлении длинных фраз необходимо использовать модификатор «!» перед словами, модификация которых не нужна, как правило, это различные предлоги и союзы. Например, фразу «как уйти из жизни безболезненно» правильно добавить в виде «!как уйти !из !жизни безболезненно». Это сократит количество возможных вариантов фраз, но при этом оставит все фразы с требуемым смыслом.

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

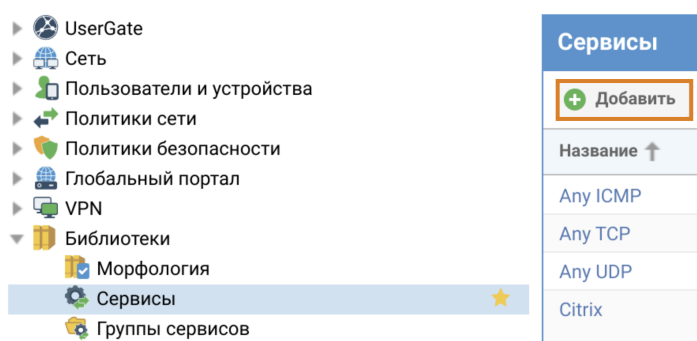
```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Сервисы

Раздел **Сервисы** содержит список общеизвестных сервисов, основанных на протоколах TCP/IP, например, таких как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил NGFW. Первоначальный список сервисов поставляется вместе с NGFW.

Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

1. В веб-консоли администратора перейти в раздел **Библиотеки → Сервисы** и нажать кнопку **Добавить**.



2. В открывшемся окне свойств сервиса указать название и его краткое описание (опционально):

Свойства сервиса

Название: Test

Описание: Test service

+ Добавить ✎ Редактировать ✖ Удалить

Сетевой протокол	Порты назначения	Порты источника	Application level gateway

Сохранить Отмена

3. Нажать кнопку **Добавить**, выбрать необходимый сетевой протокол и указать порты сервиса. Порты можно указывать диапазонами, например, 33333-33355:

Свойства сервиса

Название: Test

Описание: Test service

+ Добавить ✎ Редактировать ✖ Удалить

Сетевой протокол	Порты назначения	Порты источника	Application level gateway

Выбор протокола и портов

Сетевой протокол: tcp

Порты назначения:

Порты источника: Например, 80-88

Application level gateway: Нет

- Нет
- sip
- h323
- ftp

При выборе сетевых протоколов TCP или UDP можно также выбрать шлюз прикладного уровня (Application Layer Gateway — ALG).

Некоторые протоколы используют отдельные потоки для обмена сигнальной информацией и передачи данных. Примерами таких протоколов являются FTP, SIP или H.323. Параметры установления потока передачи данных (например, IP-

адреса или порты) у таких протоколов не настраиваются заранее, а согласуются при обмене сигнальными сообщениями между устройствами на этапе активации сервиса. Для управления такими протоколами в NGFW используются шлюзы прикладного уровня (ALG).

ALG работает как посредник между сетью и сервером приложений, который "понимает" прикладной протокол. Например, ALG может разрешать клиентским приложениям использовать динамические порты TCP/UDP для взаимодействия с известными портами, используемыми серверными приложениями, даже в тех случаях, когда настройки межсетевого экрана разрешают трафик только через ограниченное число портов. Без ALG порты будут блокироваться, либо администраторам придётся открывать в межсетевом экране большое количество портов, что ослабляет безопасность сети и открывает возможность для потенциальных атак через эти порты. Также ALG может распознавать конкретные команды приложения и получать адресную информацию сетевого уровня, которая находится в пэйлоаде пакетов приложения. ALG может синхронизировать несколько потоков или сеансов между хостами.

При создании нового сервиса с протоколом TCP можно выбрать шлюзы прикладного уровня для следующих протоколов:

- FTP;
- SIP;
- H.323.

При создании нового сервиса с протоколом UDP можно выбрать шлюзы прикладного уровня для протоколов:

- SIP;
- TFTP.

FTP использует несколько потоков для передачи файлов — первичный сигнальный поток и вторичные потоки данных для списков каталогов и передачи файлов. Поскольку эти потоки данных могут подключаться к любому порту, сложно создать статическую политику межсетевого экрана, которая бы разрешала эти потоки данных и при этом обеспечивала адекватную защиту. FTP ALG автоматически решает эту проблему путём мониторинга сигнального потока FTP, поиска команд порта FTP, которые указывают, какие порты источника и назначения запрашиваются. ALG динамически открывает определённую комбинацию IP-портов источника и назначения в политике межсетевого экрана, которая позволяет установить сессию. Как только сессия завершена, шлюз немедленно закрывается. В случае, если FTP-сессия проходит через NAT, ALG

анализирует пакеты на прикладном уровне, заменяя внутренний IP на адрес интерфейса NAT.

SIP ALG — шлюз прикладного уровня, который позволяет голосовому VoIP-трафику (RTP) проходить через устройство с функцией NAT. Если на межсетевом экране присутствует и активирован SIP ALG, то не нужно дополнительно настраивать проброс портов для этого типа трафика. Для беспрепятственного прохождения SIP-трафика через устройство с NAT необходимо транслировать адресацию в SIP-пакетах. SIP-пакет анализируется на прикладном уровне, и в нем изменяются IP-адреса. Так SIP ALG позволяет реализовать услуги SIP-телефонии в сети с трансляцией адресов без использования вспомогательных внешних устройств.

H.323 ALG поддерживает набор протоколов H.225.0 и H.245 для обеспечения сеанса аудиовизуальной связи в сети. ALG позволяет трафику проходить через устройство с функцией NAT, анализируя пакеты на уровне приложения, и заменяя в них IP-адреса.

По умолчанию шлюзы прикладного уровня отключены в настройках устройства. Включить их можно в интерфейсе командной строки (CLI) с помощью следующей команды:

```
Admin@nodename# set settings device <sip|h323|tp-alg> on
```

Подробнее в статье [Настройка параметров устройства](#).

Группы сервисов

В данном разделе пользователь может управлять (создавать/обновлять/удалять) группами объектов сервисов. Группы сервисов могут быть использованы при настройке политик безопасности NGFW.

Для создания группы сервисов:

Наименование	Описание
Шаг 1. Создать группу.	На панели Группы сервисов нажать на кнопку Добавить , указать название и, опционально, описание группы сервисов.

Наименование	Описание
Шаг 2. Добавить сервисы в группу.	На панели Элементы нажать Добавить и выбрать сервисы для добавления в группу. Для добавления всех сервисов использовать кнопку Добавить все .

IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил NGFW. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели Группы нажать на кнопку Добавить : • Дать название списку IP-адресов. • Добавить описание списка (опционально). • Указать уровень угрозы адресов в списке (параметр для визуального отображения, какие адреса не представляют собой угрозы, а какие лучше запретить). • Выбрать тип списка (локальный или обновляемый по URL обновления).
Шаг 2. Указать адрес обновления списка (для обновляемых списков).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить IP-адреса.	На панели Адреса из выбранной группы нажать на кнопку Добавить и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
	Создать файл list.txt со списком адресов.

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: <pre> x.x.x.x y.y.y.y z.z.z.z </pre>
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом NGFW создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.  Примечание URL списка задается в формате: http://x.x.x.x/, https://x.x.x.x/ или ftp://x.x.x.x/. При использовании протокола HTTPS требуется использовать сертификат, подписанный доверенным УЦ. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную.

Наименование	Описание
	При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Useragent браузеров

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список Useragent.	В панели Категории нажать на кнопку Добавить и задать название нового списка UserAgent, опционально, описание списка и URL обновления.
Шаг 2. Добавить необходимые Useragent браузеров в новый список.	В панели Шаблоны useragent добавить необходимый Useragent. Исчерпывающий список строк Useragent представлен тут: http://www.useragentstring.com/pages/useragentstring.php
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Фильтрация контента .

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл list.txt со списком Useragent .
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом NGFW создать список Useragent. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно.

Наименование	Описание
	• Ежедневно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Типы контента

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа *.doc.

Существует возможность подписки на типы контента, предоставляемые разработчиками UserGate. Данные списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

Для фильтрации по типу контента необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3.	В панели Категории нажать на кнопку Добавить , задать название нового списка типа контента, опционально, описание списка и URL обновления.
Шаг 2. Добавить необходимые типы контента в новый список.	Добавить необходимый тип контента в данный список в формате MIME. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml . Например, для блокировки документов типа *.doc необходимо добавить тип контента «application/msword».
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Фильтрация контента .

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл list.txt со списком типов контента.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .

Наименование	Описание
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом NGFW создать список типа контента. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**,

содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Списки URL

Списки URL используются в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет ряд собственных обновляемых списков. Для использования этих списков необходима соответствующая лицензия.

Подробнее о лицензировании UserGate NGFW — в разделе «[Лицензирование](#)».

Наименование списка	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля
Соответствие списку запрещенных URL Министерства Юстиции РФ	Список содержит URL, запрещенные Министерством Юстиции Российской Федерации
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ
Список фишинговых сайтов	Список содержит URL фишинговых сайтов

Наименование списка	Описание
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен на сайте http://eais.rkn.gov.ru
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен на сайте http://eais.rkn.gov.ru

Вы также можете создать собственные списки URL в веб-консоли или в [интерфейсе командной строки](#) UserGate NGFW.

Для создания списка в веб-консоли:

1. В разделе **Настройки → Библиотеки → Списки URL** нажмите **Добавить** и задайте название и описание нового списка.
2. Выберите тип списка (локальный или обновляемый). Для обновляемого списка укажите URL обновления и настройте [расписание скачивания обновлений](#).
3. Установите категорию создаваемого списка в поле **Чувствительность к регистру**:
 - **Чувствительный к регистру** — список URL-адресов, чувствительных к регистру букв в адресе.
 - **Нечувствительный к регистру** — список URL-адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах.
 - **Домен** — список адресов доменов. При добавлении в этот список записи вида `http://test.ru`, она будет преобразована в запись вида `test.ru`.

Важно!

Категория списка задается при его создании. Изменить категорию после создания списка нельзя.

i Примечание

При использовании URL-списка ищется весь URL запроса; при использовании доменного списка — только имя узла. При сохранении URL в доменный список в процессе преобразования из него удаляется все лишнее, остается только имя узла.

4. Добавьте необходимые записи в новый список.

В списках можно использовать некоторые специальные символы. Значения специальных символов в списках:

- * — любое количество любых символов;
- ^ — начало строки;
- \$ — конец строки.

Символы «?» и «#» не могут быть использованы в списках.

Правило фильтрации контента может содержать один или несколько списков. Подробнее — в разделе [«Фильтрация контента»](#).

i Внимание!

Спецсимволы не работают в списках исключений для блокировки рекламы. Не рекомендуется использовать спецсимволы в записях таких списков.

Если необходимо заблокировать строго определенный адрес, используйте символы начала (^) и конца (\$) строки. Например:

```
^http://domain.com/exacturl$
```

Если необходимо заблокировать адрес и все страницы внутри него, используйте символ ^ в начале строки, без символа \$ в конце. Например:

```
^http://domain.com/exacturl/
```

Чтобы заблокировать домен со всеми возможными URL, укажите только имя домена без специальных символов:

domain.com

Примеры интерпретации URL-записей приведены в таблице.

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
yahoo.com или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com; mail.yahoo.com; а также: qweryahoo.com	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyyahoo.com/	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyyahoo.com/ Не блокируются вхождения типа: https://ya.ru/YAHoo.cOM	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyyahoo.com/ https://ya.ru/YAHoo.cOM
^mail.yahoo.com\$	Заблокирован только mail.yahoo.com	Заблокированы: http://mail.yahoo.com; https://mail.yahoo.com; а также любые ссылки на этом домене, например: http://mail.yahoo.com/personal-finance Т. е., блокируется весь домен mail.yahoo.com и	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
		все URL этого домена		
^mail.yahoo.com/\$	Ничего не заблокировано	Заблокированы: http://mail.yahoo.com; https://mail.yahoo.com; и любые ссылки на этом домене, например: https://mail.yahoo.com/personal-finance т. к. при преобразовании списка остается только домен, слеш в этом случае удалится и реально в списке будет: ^mail.yahoo.com\$ т. е. блокируется весь домен mail.yahoo.com и все URL этого домена	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола
^https://finance.yahoo.com/personal-finance/\$	Ничего не заблокировано	Заблокированы: http://finance.yahoo.com; https://finance.yahoo.com; и любые ссылки на этом домене, например: http://finance.yahoo.com	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ Не заблокируется: http://finance.yahoo.com/personal-finance/ и любое изменение	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ и любое изменение регистра букв в URL: https://finance.yahoo.com/Personal-finance/.

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
		m/personal-finance/ т.к. после преобразования в списке останется только: ^finance.yahoo.com\$ Т. е. блокируется весь домен finance.yahoo.com и все URL этого домена	регистр букв в URL: https://finance.yahoo.com/personal-financeE/	Не заблокируется: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не заблокировано	Заблокированы: http://yahoo.com/12345/whatever/; https://yahoo.com/12345/whatever/; т.к. после преобразования в списке будет: ^yahoo.com Т. е. заблокируется домен yahoo.com и все URL этого домена	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола

Администратор имеет возможность создавать собственные обновляемые списки и централизованно распространять их на все узлы UserGate NGFW. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, `list.txt`) со списком URL в следующем формате:

```
www.site1.com/url1
```

```
www.site2.com/url2
```

...

`www.siteend.com/urlN`

2. Создайте архив, содержащий этот файл (например, `list.zip`).
3. Создайте файл с версией списка (например, `version.txt`). Внутри файла укажите номер версии списка (например, 3). Необходимо инкрементировать это значение при каждом обновлении списка.
4. Разместите файлы архива и версии (например, `list.zip` и `version.txt`) на веб-сервере, чтобы они были доступны для скачивания.
5. На каждом UserGate NGFW создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate NGFW будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

 Примечание

URL списка задается в формате: `http://x.x.x.x/`, `https://x.x.x.x/` или `ftp://x.x.x.x/`.
При использовании протокола HTTPS требуется использовать сертификат, подписанный доверенным УЦ.

В свойствах списка можно настроить расписание обновления.

Вы можете выбрать одно из предустановленных значений или указать время вручную в спон-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

UserGate NGFW может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в Linux можно с помощью команды:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется с расширением `.md5`. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах NGFW. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели Группы нажать на кнопку Добавить , указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели Элементы нажать на кнопку Добавить и добавить интервал. Дать название интервалу и указать время.

Полосы пропускания

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую возможно в дальнейшем использовать в правилах управления полосой пропускания. Более подробно о правилах управления полосой пропускания смотрите в главе [Пропускная способность](#).

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать полосу пропускания.	Нажать на кнопку Добавить , дать название, описание.
Шаг 2. Указать скорость.	Указать скорость в Кбит/сек.
Шаг 3. Указать значение DSCP для QoS.	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

Шаблоны страниц

С помощью шаблонов страниц вы можете настраивать отображение страниц блокировки, авторизации, предупреждений и сетевых ошибок. Список шаблонов страниц, которые поставляются с UserGate NGFW, — см. в таблице ниже. Вы можете использовать эти шаблоны в качестве основы для создания пользовательских шаблонов в фирменном стиле компании или на другом языке.

По умолчанию шаблоны страниц настроены на отображение минимальной информации в стандартном оформлении. Но в HTML-коде этих шаблонов содержатся дополнительные блоки информации или интерактивных элементов, которые по умолчанию закомментированы. Вы можете раскомментировать их: например, на страницу блокировки вывести дату блокировки или форму ввода логина и пароля администратора для снятия блокировки.

Чтобы создать пользовательский шаблон страницы:

1. В разделе **Шаблон страниц** нажмите **Добавить** и создайте шаблон страницы нужного типа.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу, найдите закомментированные блоки для отображения дополнительных сведений и раскомментируйте нужные.

i Примечание

Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

Шаблон	Описание
Blockpage (EN) и Blockpage (RU)	Стандартные шаблоны блокировки на английском и русском языках
Captive portal user auth (EN) и Captive portal user auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль). При успешной авторизации пользователь получает доступ в интернет
Captive portal user auth + policy (EN) и Captive portal user auth + policy (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принять правила политики доступа. При успешной авторизации пользователь получает доступ в интернет
Captive portal: email auth (EN) и Captive portal: email auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе, подтвердив указанную электронную почту. Для корректной работы шаблонов необходимо настроить параметры раздела Оповещения в Captive-профиле
Captive portal: SMS auth (EN) и Captive portal: SMS auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы шаблонов необходимо настроить параметры раздела Оповещения в Captive-профиле
Captive portal policy (EN) и Captive portal policy (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принять правила политики доступа. При согласии с политикой доступа пользователь получает доступ в

Шаблон	Описание
	интернет. Для работы шаблона требуется установить метод Принять политику в качестве метода аутентификации в Captive-профиле
Captive portal user session (EN) и Captive portal user session (RU)	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps
Content warning (EN) и Content warning (RU)	Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием Предупредить
FTP client (EN) и FTP client (RU)	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP
SSL VPN (EN) и (RU)	Шаблоны на английском и русском языках для отображения страницы веб-портала
SSL VPN RDP (EN) и (RU)	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал
SSL VPN SSH (EN) и (RU)	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал
TOTP INIT PAGE (EN) и TOTP INIT PAGE (RU)	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей
NETWRK ERROR PAGE (RU) и NETWORK ERROR PAGE (EN)	Шаблоны на русском и английском языках для отображения страницы сетевых ошибок от прокси-сервера. Доступны в версии ПО 7.4.0 и выше

Категории URL

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, администратор может создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Для использования категорий UserGate URL filtering требуется наличие специальной лицензии.

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы.

Наименование	Описание
Threats	Набор категорий, рекомендованных для блокировки в целях обеспечения безопасности сети.
Parental Control	Набор категорий, рекомендованных для блокировки в целях защиты детей от нежелательного контента.
Productivity	Набор категорий, рекомендованных для блокировки в целях повышения эффективности работы сотрудников.
Safe categories	Набор категорий, считаемых безопасными для посещения. Рекомендуется отключать морфологическую проверку, перехват HTTPS-трафика для данной группы категорий в целях уменьшения количества ложных срабатываний.
Recommended for morphology checking	Набор категорий, рекомендованных для проверки с помощью морфологического анализа. Из этого набора исключены такие категории, как «Новости», «Финансы», «Правительство», «Информационная безопасность», «Детские сайты» и ряд других в целях уменьшения количества ложных срабатываний. Этот же набор категорий рекомендуется использовать для перехвата трафика HTTPS.
Recommended for virus check	Набор категорий, рекомендованных для антивирусной проверки.

Для добавления новой группы категорий необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу категорий.	В панели Группы URL категорий нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить категории.	Выделить созданную группу и в панели Категории , нажать на кнопку Добавить и выбрать необходимые категории из списка.

В системе определены следующие категории URL:

ID	Уровень риска	Название	Описание
0	Высокий (4)	Неизвестная тематика / Unknown	Сайты без принадлежности к какой-либо категории.
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Pop-Ups	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхода средств веб-фильтрации и т.д.
4	Очень низкий (1)	Искусство / Arts	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
5	Очень низкий (1)	Бизнес / Business	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности.
6	Очень низкий (1)	Транспорт / Transportation	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров,

ID	Уровень риска	Название	Описание
			сайты с обзорами, сообщества, клубы автолюбителей и т.д.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени.
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
10	Очень высокий (5)	Заражённые сайты / Compromised	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.
11	Очень низкий (1)	Компьютеры и технологии / Computers and Technology	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
12	Средний (3)	Преступная деятельность / Criminal Activity	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как

ID	Уровень риска	Название	Описание
			совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения.
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.
15	Очень низкий (1)	Образование / Education	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие пользователю

ID	Уровень риска	Название	Описание
			телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
17	Низкий (2)	Финансы / Finance	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
20	Очень низкий (1)	Правительство / Government	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны,

ID	Уровень риска	Название	Описание
			служб борьбы с терроризмом и больниц.
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т.д.
23	Низкий (2)	Наркотики / Illegal Drug	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
25	Средний (3)	Военные сайты / Military	

ID	Уровень риска	Название	Описание
			Информация о военных организациях, военной истории.
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.
27	Очень низкий (1)	Новости / News	Новостные сайты: онлайн-журналы, новостные ленты и т.д.
28	Низкий (2)	Некоммерческие и неправительственные организации / Non-profits and NGOs	Сайты, посвященные клубам, сообществам, союзам и некоммерческим организациям. Значительное число данных структур созданы в образовательных или благотворительных целях.
29	Низкий (2)	Нудизм / Nudity	Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие или продающие нижнее белье, интимную одежду или купальные костюмы.
30	Средний (3)	Персональные сайты / Personal Sites	Персональные сайты, созданные отдельными людьми или группами лиц, блоги.
31	Очень высокий (5)	Фишинг и мошенничество / Phishing and Fraud	Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи

ID	Уровень риска	Название	Описание
			финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных законных ресурсов, что вводит в заблуждение пользователей.
32	Очень низкий (1)	Политика / Politics	Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые предлагают сведения о правах и их защите.
33	Очень высокий (5)	Порнография и насилие / Pornography/Sexually Explicit	Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать эротические рассказы и текстовые описания половых актов.
34	Низкий (2)	Недвижимость / Real Estate	Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду,

ID	Уровень риска	Название	Описание
			улучшению жилищных условий.
35	Низкий (2)	Религия / Religion	Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.
36	Очень низкий (1)	Рестораны и еда / Restaurants and Dining	Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина.
37	Очень низкий (1)	Поисковые системы и порталы / Search Engines and Portals	Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы.
38	Низкий (2)	Покупки / Shopping	Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина.
39	Средний (3)	Социальные сети / Social Networking	Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.

ID	Уровень риска	Название	Описание
40	Очень высокий (5)	Спам-сайты / Spam Sites	Сайты, продвижение которых основано на использовании спам-рассылок.
41	Очень низкий (1)	Спорт / Sports	Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.
42	Очень высокий (5)	Вредоносное ПО / Malware	Сайты, содержащие нежелательные программы, автоматически загружающиеся и устанавливающиеся на ПК пользователей. Вирусы вносят изменения в систему и позволяют злоумышленникам получить данные с компьютера без ведома и согласия его владельца.
43	Низкий (2)	Фондовый рынок / Stock trading	Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировкам и новостям.
44	Очень низкий (1)	Переводчики / Translators	Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных ограничений, так как просмотр сайтов

ID	Уровень риска	Название	Описание
			осуществляется с URL сайта онлайн-переводчика.
45	Очень низкий (1)	Путешествия / Travel	Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино.
46	Низкий (2)	Насилие / Violence	Сайты, содержащие изображения, текстовые описания и пропаганду физического насилия против людей, животных или организаций\сообществ. Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику.
47	Низкий (2)	Оружие / Weapons	Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом.
48	Высокий (4)	Веб-почта / Web-based Email	Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем.
49	Средний (3)	Общие / General	Сайты, которые не попадают в другие категории, например, пустые веб-страницы.

ID	Уровень риска	Название	Описание
50	Низкий (2)	Отдых и оздоровление / Leisure and Recreation	Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечений и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т.д.
51	Низкий (2)	Онлайн обучение / Online training and tools	Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации.
52	Низкий (2)	Юриспруденция / Legal	Сайты юридических фирм, обсуждение и анализ юридических вопросов.
53	Низкий (2)	Местные достопримечательности / Local Information	Путеводители и информация для туристов, в том числе о ресторанах и местных достопримечательности.
54	Низкий (2)	Справочная информация / Reference and Research	Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации.
55	Очень низкий (1)	Форумы с технической или бизнес информацией / Technical or business forums and news groups	Сайты с обсуждениями, относящимся к деловой или технической тематикам.
56	Очень низкий (1)	Техническая информация / Technical information and documentation	Сайты, которые предоставляют информацию к

ID	Уровень риска	Название	Описание
			технической документации и информации.
57	Высокий (4)	Персональные хранилища / Personal Storage	Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных.
58	Низкий (2)	CDNs	Сети предоставления контента
59	Низкий (2)	Нецензурная лексика / Profanity	Сайты, содержащие нецензурную лексику
60	Низкий (2)	Профессиональные социальные сети / Professional social networks	Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный исключительно для бизнеса и профессионалов.
61	Очень высокий (5)	Ботнеты / Botnets	Сайты, которые управляют сетями ботов через командно-контрольные центры.
62	Низкий (2)	Религиозные культы / Cults	Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера.
63	Низкий (2)	Мода и красота / Fashion and Beauty	Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает

ID	Уровень риска	Название	Описание
			отзывы, сравнения, а также общую информацию, полезную потребителю.
64	Низкий (2)	Поздравительные открытки / Greeting cards	Сайты, которые позволяют людям получать и отправлять поздравительные открытки.
65	Очень высокий (5)	Хакерство / Hacking	Сайты, которые способствуют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации.
66	Очень высокий (5)	Криптомайнеры / Cryptocurrency Mining	Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя.
67	Очень высокий (5)	Нелегальное ПО / Illegal Software	Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей.
68	Высокий (4)	Обмен картинками / Image Sharing	Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники.

ID	Уровень риска	Название	Описание
69	Низкий (2)	Информационная безопасность / Information Security	Сайты, которые предоставляют информацию о законной защите данных, в том числе о новых угрозах и способах борьбы с ними.
70	Средний (3)	Сервисы мгновенных сообщений / Instant Messaging	Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т.п.
71	Очень низкий (1)	Сетевые ошибки / Network Errors	Сайты, которым не присвоен IP-адрес.
72	Средний (3)	Паркованные домены / Parked Domains	К паркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя сайты, находящиеся на реконструкции, папки и базовые страницы веб-серверов.
73	Высокий (4)	Пиринговые сети / Peer-to-Peer	Сайты, которые позволяют осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера.
74	Высокий (4)	Частные IP-адреса / Private IP Addresses	Включает наборы IP-адресов, определенные в RFC 1918.

ID	Уровень риска	Название	Описание
75	Низкий (2)	Школьные мошенничества / School Cheating	Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами.
76	Низкий (2)	Половое воспитание / Sex Education	Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборты, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность.
77	Средний (3)	Сайты сомнительного содержания / Tasteless	Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса", ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными.
78	Низкий (2)	Жестокое обращение с детьми / Child Abuse Images	Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми.
79	Очень низкий (1)	Нетрадиционная сексуальная ориентация / Gay, Lesbian or Bisexual	Сайты, содержащие материалы о геях, лесбиянках, трансгендерах.
80	Низкий (2)	Литература и книги / Literature and Books	Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии.
81	Низкий (2)	Здоровое питание и диеты / Nutrition and Diet	Сайты, посвященные правильному питанию, снижению веса, диетам.

ID	Уровень риска	Название	Описание
82	Низкий (2)	Домашние животные / Pets and Animals	Сайты, посвященные продуктам и сервисам для домашних и других животных.
84	Низкий (2)	Обновления / Updates	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
85	Средний (3)	Чат-боты искусственного интеллекта / Chat-bot AI	Сайты, предоставляющие доступ к чат-ботам искусственного интеллекта, подобным Chat GPT.
97	Низкий (2)	Репутация: Низкий риск / Reputation: Low risk	Сайты с низким репутационным риском. Как правило это сайты, не имеющие известных уязвимостей, но относящиеся к категориям, где риск нарушения безопасности возможен.
98	Средний (3)	Репутация: Средний риск / Reputation: Medium risk	Сайты со средним репутационным риском. Как правило это сайты, которые могут содержать уязвимости и относящиеся к категориям, где риск нарушения безопасности возможен.
99	Очень высокий (5)	Репутация: Высокий риск / Reputation: High risk	Сайты с высоким репутационным риском. Сайты с известными уязвимостями.

Измененные категории URL

Элемент библиотеки **Измененные категория URL** позволяет администратору назначить определенным сайтам категории, отличные от категорий, назначенных техническими специалистами UserGate. Такая потребность может возникнуть в случае некорректного категорирования сайтов или в случае, если требуемый сайт не имеет назначенной ему категории. Для переопределения категории сайта необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Проверить первоначальную категорию сайта.	В разделе Библиотеки → Измененные категории URL ввести требуемый адрес сайта в строку проверки и нажать на кнопку Проверить категорию .
Шаг 2. Назначить новую категорию.	Если полученная категория не совпадает с требуемой, то необходимо нажать на кнопку Добавить и назначить до двух новых категорий.

После успешного изменения категории сайт будет отображаться в списке сайтов с измененными категориями. Для него также будет указаны дата изменения категории, администратор, выполнивший данное изменение, его оригинальные и новые категории.

При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями — **Переопределенные пользователем категории**.

Администратор может экспортировать списки сайтов с измененными категориями или импортировать любые списки сайтов и назначить им требуемые категории.

Приложения

Сигнатуры приложений представляют собой совокупность семантических выражений, с помощью которых описываются характерные признаки определенных сетевых приложений. Сигнатуры используются для анализа трафика на 7 уровне модели OSI.

Типы сигнатур приложений

В UserGate NGFW могут использоваться два типа сигнатур приложений:

- проприетарные;
- пользовательские.

Проприетарные сигнатуры приложений создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В библиотеке приложений они помечаются выражением «@UserGate» в колонке **Владелец**.

Пользовательские сигнатуры приложений создаются самими пользователями. Для создания пользовательской сигнатуры в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Приложения** и нажать **Добавить**. Далее необходимо задать параметры приложения и описать его признаки с помощью синтаксиса [UASL](#).

Параметры пользовательской сигнатуры приложения.

Наименование	Описание
Тип	Тип сигнатуры; • Приложение, • Протокол, • Поддержка — вспомогательная сигнатура.
Id	Идентификатор сигнатуры. Если поле оставить пустым, то будет выдан свободный id из пользовательского пула.
Название	Название сигнатуры.
Описание	Описание сигнатуры.
Уровень угрозы	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.

Наименование	Описание
Технология	Технология приложения: • browser-based — браузерное веб-приложение; • client-server — клиент-серверное приложение; • network-protocol — сетевой протокол; • peer-to-peer — приложение точка-точка.
Категория	Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен. • Media streaming; • Email; • Coin Miners; • Tunneling; • Games; • Remote access; • Conferencing; • Trojan Horses; • Business; • Mobile; • Proxies and anonymizers; • Standard networks; • VOIP; • Web posting; • Software update; • File storage and backup; • Web browsing; • File sharing P2P; • Instant messaging • Social networking
UASL	Описание признаков сигнатуры с помощью синтаксиса UASL.

О создании сигнатур приложений в интерфейсе командной строки — в разделе «[Настройка библиотек](#)».

Сигнатуры приложений, зависимые от типа протокола

Для корректной работы некоторых сигнатур приложений в профилях необходимо наличие сигнатур определенного протокола.

В следующей таблице представлены такие зависимости.

Сигнатура протокола	ID зависимых сигнатур
SSL/TLS (id=19)	185, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 198, 199, 200, 201, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 267, 268, 269, 270, 271, 272, 273, 275, 276, 277, 278, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 437, 439, 440, 441, 443, 444, 445, 446, 449, 450, 451, 458, 459, 465, 466, 470, 471, 472, 474, 475, 477, 481, 482, 485, 486, 487, 490, 492, 494, 495, 496, 501, 502, 504, 505, 511, 512, 513, 515, 516, 517, 518, 521, 524, 525, 526, 527, 528, 531, 532, 535, 536, 537, 538, 539, 544, 549, 550, 552, 554, 556, 557, 560, 563, 564, 566, 567, 568, 576, 577, 579, 581, 585, 589, 590, 592, 595, 596, 597, 600, 601, 603, 604, 606, 607, 610, 612, 613, 617, 621, 622, 623, 625, 627, 632, 635, 636, 638, 710, 730, 731, 734, 738, 739, 744, 746, 748, 752, 753, 754, 755, 756, 759, 760, 761, 762, 763, 766, 769, 770, 771, 772, 773, 774, 775, 776, 781, 783, 785, 788, 790, 795, 797, 800, 801, 807, 808, 810, 811, 813, 815, 817, 818, 820, 822, 825, 826, 831, 832, 833, 835, 836, 837, 841, 842, 846, 847, 848, 850, 851, 852, 853, 854, 858, 859, 860, 863, 864, 867, 869, 872, 874, 875, 877, 878, 879, 880, 883, 885, 887, 888, 891, 893, 894, 895, 897, 898, 899, 902, 903, 904, 905, 908, 909, 1967, 2027, 4062, 4082, 4437, 4459, 5294, 5301, 5317, 5321, 5323, 5324, 5385, 5395, 5407, 5431, 5506, 5637, 5641, 5644, 5645, 5649, 5650, 5652, 5654, 5656, 5658, 5668, 5671, 5673, 5674, 5675, 5676, 5678, 5679, 5680, 5681, 5688, 5692, 5693, 5695, 5699, 5710, 5711, 5715, 5719, 5730, 5736, 5739, 5740, 5742, 5744, 5750, 5762, 5765, 5769, 5770, 5773, 5776, 5777, 5778, 5786, 5791, 5792, 5794, 5795, 5800, 5804, 5809, 5810, 5812, 5813, 5815, 5816, 5820, 5822, 5823, 5825, 5826, 5827, 5828, 7688, 7689, 7690, 7691, 7692, 7694, 7695, 7698, 7699, 7704, 7705, 7707, 7708, 7740, 7843, 7864, 7865, 7867, 7868, 8000, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8009, 8010, 8011, 8012, 8014, 8015, 8016, 8017, 8018, 8019, 8022, 8024, 8026, 8027, 8028, 8031, 8032, 8033, 8034, 8035, 8036, 8037, 8038, 8039, 8040, 8041, 8043, 8044, 8045, 8048, 8049, 8053, 8054, 8055, 8056, 8057, 8058, 8059, 8060, 8063, 8064, 8066, 8067, 8069, 8070, 8071, 8075, 8077, 8078, 8079, 8080, 8081, 8082, 8083, 8084, 8086,

Сигнатура протокола	ID зависимых сигнатур
	8087, 8088, 8089, 8090, 8091, 8092, 8094, 8095, 8096, 8098, 8099, 8101, 8102, 8103, 8104, 8105, 8106, 8107, 9003, 9007, 9008, 9016, 9019, 9030, 9042, 9044, 9048, 9050, 9051, 9052, 9053, 9054, 9055, 9056, 9057, 9058, 9059, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9068, 9069, 9071, 9072, 9074, 9075, 9076, 9077, 9078, 9079, 9080, 9081, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9090, 9091, 9092, 9094, 9096, 9097, 9098, 9099, 9100, 9101, 9102, 9103, 9104, 9105, 9114, 9128, 9141, 9147, 9148, 9150, 9529, 9543, 9544, 9553, 9563, 9566, 9572, 9573, 9575, 9579, 9580, 9622, 9625, 9627, 9628, 9641, 9650, 9655, 9657, 9714, 9733, 10514, 11011, 11024, 11025, 11044, 11504, 12001, 12002, 12003, 12006, 12007, 12008, 12009, 12010, 12011, 12012, 12013, 12014, 12015, 12016, 12017, 12018, 12019, 12020, 12021, 12022, 12023, 12024, 12025, 12026, 12027, 12028, 12033, 12034, 12035, 12036, 12044, 12045, 12501, 14002, 14003
HTTP (id=3)	196, 239, 261, 475, 532, 535, 610, 612, 627, 710, 1967, 4133, 4340, 4441, 5323, 5395, 5506, 5655, 5672, 5674, 5676, 5693, 5728, 5730, 5750, 5754, 5763, 5769, 5770, 5773, 5778, 5788, 5792, 5823, 5830, 7867, 8002, 8013, 8048, 9777, 9823, 9824, 9845, 11027, 12032, 12033
DNS (id=5)	1967, 5395, 5672, 5815
IKE (id=11041)	11056

Связанные сигнатуры

Ряд сигнатур приложений зависят не только от сигнатур протокола, но и от других связанных сигнатур.

Список связанных сигнатур приложений приведен в следующей таблице.

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
218	Yandex.Disk	SSL/TLS (id=19)	—	Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
7707	Yandex.Disk download	SSL/TLS (id=19)	Yandex.Disk (id=218), Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044).
7708	Yandex.Disk upload	SSL/TLS (id=19)	Yandex.Disk (id=218), Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044).
12044	Yandex Services	SSL/TLS (id=19)	—	Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).
16020	Yandex Tracker	SSL/TLS (id=19)	Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
				(id=19), а также связанную сигнатуру (id=12044).
12045	Yandex Cloud	SSL/TLS (id=19)	Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанную сигнатуру (id=12044).

Пользовательские тайм-ауты приложений

В UserGate NGFW для приложений можно установить пользовательские значения тайм-аута бездействия (`idle timeout`) — времени, в течение которого сессия будет сохраняться открытой, если в ней не производится обмен пакетами.

Значение тайм-аута по умолчанию для приложения зависит от протокола транспортного уровня, который использует приложение. Для TCP это значение равно 18 000 сек., для UDP — 60 сек.

Значение пользовательского тайм-аута задается в настройках сигнатуры приложения.

Пользовательский тайм-аут бездействия назначается на установившуюся сессию, как только сигнатура приложения определилась (сработала) в текущем трафике:

- Для протокола TCP — после того, как соединение переходит в состояние ESTABLISHED.
- Для протокола UDP — после того, как соединение переходит в состояние ASSURED. Состояние ASSURED возникает при обработке пакета (третьего по счету на соединении) после установки состояния REPLIED.

Значение пользовательского тайм-аута настраивается в интерфейсе командной строки (CLI) на уровне `libraries application-signature`. Подробнее — в разделе [Настройка библиотек](#).

Профили приложений

Назначение профиля приложений

Профиль приложений позволяет создавать динамический набор [сигнатур приложений](#), предназначенный для анализа трафика на 7 уровне модели OSI. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. При изменении библиотеки сигнатур приложений профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определяться действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами, и действия, которые должны быть применены к трафику, который не удалось идентифицировать.

Создание профиля приложений в веб-консоли администратора

В веб-консоли администратора профили приложений создаются в разделе **Библиотеки → Профили приложений**.

В консоли администратора по умолчанию созданы два профиля приложений:

- Default application profile — профиль, содержащий все сигнатуры приложений, за исключением относящихся к категории ICS/IoT.
- Pass ICS/IoT applications — профиль, содержащий только сигнатуры приложений с категорией ICS/IoT (приложения, относящиеся к АСУ ТП).

Для создания собственного профиля необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля приложений:

Свойства профиля приложений

Общие Совпавшие сигнатуры

Название: Test profile

Описание:

Фильтры

Добавить Редактировать Удалить Включить Отключить

Фильтры	Включено	Действие	PCAP включен

Наверх Выше Ниже Вниз

Настройки сигнатуры неопределенных приложений

Действие: Применить к: Журналировать: Файл PCAP:

Пропустить Оба Включить Отключить

Сохранить Отмена

1. В поле **Название** указать название создаваемого профиля.
2. В поле **Описание** опционально указать назначение профиля.
3. В области **Фильтры** добавляются фильтры для выбора необходимых сигнатур из библиотеки и настраиваются действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами.
4. В области **Настройки сигнатуры неопределенных приложений** определяются действия с трафиком, который не был определен сигнатурами данного профиля.
5. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур приложений, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над приложениями, отфильтрованными этими сигнатурами.

Настройка фильтров сигнатур в профиле приложений

Для создания фильтра сигнатур приложений необходимо в области **Фильтры** нажать **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции отбора в панели инструментов. Ниже в окне будут отображаться сигнатуры из библиотеки, попадающие под действие этого фильтра:

Свойства фильтра

☒ Вкл

Состояние сигнатур: Включить Действие: Отбросить

Журналировать: Включить Файл PCAP: Отключить Применить к: Оба Продолжительность: 5 минут

Сработавшие сигнатуры

очень высокий Владелец: Все Ещё Сброс Расширенный

Тип: app ✕ Технология: Peer-to-Peer ✕ Категория: Media strea... ✕

	Id	Название ↑	Категории приложен...	Технология приложе...	Владелец
5	116	Zona	☐ Media streaming ☐ File sharing P2P	Peer-to-Peer	© UserGate

« < | Страница 1 из 1 | > » ↻ Всего: 1857 (найдено: 1)

Сохранить Отмена

Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого необходимо нажать **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:

Свойства фильтра

☒ Вкл

Состояние сигнатур: Включить Действие: Отбросить

Журналировать: Включить Файл PCAP: Отключить Применить к: Оба Продолжительность: 5 минут

Сработавшие сигнатуры

✓ threat = 'very high' AND (type = 'app') AND (technology = 'Peer-to-Peer') AND (category = 'Media streaming') ✕ ✎ ? 🔍 Простой

	Id	Название ↑	Категории приложен...	Технология приложе...	Владелец
5	116	Zona	☐ Media streaming ☐ File sharing P2P	Peer-to-Peer	© UserGate

« < | Страница 1 из 1 | > » ↻ Всего: 1857 (найдено: 1)

Сохранить Отмена

В каждом фильтре могут настраиваться состояния сигнатур и действия, которые применяются ко всем сигнатурам, попадающим под него:

- включение/отключение сигнатуры;
- включение/отключение журналирования сигнатуры;
- запись в рсар-файл, если сигнатура сработала;
- предпринимаемое действие над трафиком, если сигнатура сработала, т.е. приложение было найдена в трафике; действия могут быть следующие: пропустить, отбросить, отбросить с разрывом TCP соединения, блокировать IP-адрес источника и/или назначения.

Свойства фильтра

☒ Вкл

Состояние сигнатур: Включить Действие: Отбросить

Журналировать: Включить Файл РСАР: Отключить Применить к: Оба Продолжительность: 5 минут

Сработавшие сигнатуры

	Id	Название ↑	Категории приложен...	Технология приложе...	Владелец
5	116	Zona	☐ Media streaming ☐ File sharing P2P	Peer-to-Peer	© UserGate

« < | Страница 1 из 1 | > » | C Всего: 1857 (найдено: 1)

Сохранить Отмена

Для сохранения созданного фильтра необходимо нажать **Сохранить**.

В одном профиле может быть создано сразу несколько фильтров.

Фильтры в профиле работают по правилу логического ИЛИ.

Порядок фильтров сигнатур в профиле важен – настройки верхнего фильтра имеют высший приоритет. Например, если в библиотеку сигнатур приложений будут добавлены новые сигнатуры и они попадут под действие сразу нескольких фильтров одного профиля, им будет присвоено настроенное действие первого фильтра, под который они попадают.

Настройка действий для трафика, который не удалось идентифицировать

В профиле приложений может быть настроено действие, которое применяется к трафику, который не удалось идентифицировать с помощью набора сигнатур профиля.

В области **Настройки сигнатуры неопределенных приложений** настраивается действие, включается/отключается журналирование и запись в файл pcap.

Свойства профиля приложений

Общие Совпавшие сигнатуры

Название: Test profile

Описание:

Фильтры

Добавить Редактировать Удалить Включить Отключить

Фильтры	Включено	Действие	PCAP включен
---------	----------	----------	--------------

Наверх Выше Ниже Вниз

Настройки сигнатуры неопределенных приложений

Действие: Пропустить Применить к: Оба Журналировать: Включить Файл PCAP: Отключить

Сохранить Отмена

Действия могут быть следующие: пропустить, отбросить, отбросить с разрывом TCP соединения.

Работа с профилями приложений в интерфейсе командной строки описана в разделе [Настройка библиотек](#) Руководства администратора.

Примеры настроек профилей приложений

Пример 1. Профиль приложения с сигнатурой, зависимой от сигнатуры протокола

Списки сигнатур, зависящих от сигнатур протоколов, приведены в разделе [Приложения](#).

Создадим профиль для приложения Kontur Talk, которое определяется соответствующей сигнатурой (id=14002). Чтобы запретить весь трафик, кроме трафика приложения Kontur Talk, профиль приложений должен выглядеть следующим образом:

Свойства профиля приложений

Общие Совпавшие сигнатуры

Название: Пример 1

Описание: Пример профиля с сигнатурой приложения, зависимой от сигнатуры протокола.

Фильтры

Добавить Редактировать Удалить Включить Отключить

Фильтры	Включено	Действие	PCAP включен
id = 14002 or id = 19	Включено	Пропустить	Отключено

Настройки сигнатуры неопределенных приложений

Действие: **Отбросить** Применить к: Оба Журналировать: Включить Файл PCAP: Отключить

Сохранить Отмена

Свойства профиля приложений

Общие Совпавшие сигнатуры

Переопределить Включить Отключить Восстановить по умолчанию Выделить все Показать Все

Все Владелец: Все Ещё Сброс Q Расширенный

	Id	Название	Действие	Категории прило...	Технология прило...	PCAP включен	Владелец
3	14002	Kontur Talk	Пропустить	Conferencing	Client-server	Отключено	© UserGate
4	19	SSL/TLS	Отбросить	Standard net...	Network-protocol	Отключено	© UserGate

« « Страница 1 из 1 » » Всього: 1880 (найдено: 2)

Сохранить Отмена

Сигнатура SSL/TLS (id=19) необходима для работы сигнатуры Kontur Talk, поэтому она добавляется в профиль, но для нее выставляется действие **Отбросить**, чтобы не пропускать посторонний трафик по протоколам SSL/TLS. Для неидентифицированного трафика также устанавливается действие **Отбросить**.

Пример 2. Профиль для белого списка со связанными сигнатурами

Списки связанных сигнатур приведены в разделе [Приложения](#).

Создадим профиль для случая, когда необходимо разрешить загрузку файлов на Yandex Disk. Для того, чтобы сигнатура Yandex.Disk upload работала, необходимо учесть её зависимость от сигнатуры протокола SSL/TLS (id=19) и связанность с сигнатурами Yandex.Disk (id=218) и Yandex Services (id=12044). В данном примере профиль приложений будет выглядеть следующим образом:

Свойства профиля приложений

Общие Совпавшие сигнатуры

Название: Пример 2

Описание: Пример профиля для белого списка со связанными сигнатурами.

Фильтры

Добавить Редактировать Удалить Включить Отключить

Фильтры	Включено	Действие	PCAP включен
id = 19 or id = 12044 or id = 218 or id = 7708	Включено	Пропустить	Отключено

Наверх Выше Ниже Вниз

Настройки сигнатуры неопределенных приложений

Действие: **Отбросить** Применить к: Оба Журналировать: Включить Файл PCAP: Отключить

Сохранить Отмена

Свойства профиля приложений

Общие Совпавшие сигнатуры

Переопределить Включить Отключить Восстановить по умолчанию Выделить все Показать Все

Все Владелец: Все Ещё Сброс Поиск Расширенный

	Id	Название	Действие	Категории приложения	Технология приложе...	PCAP включен	Владелец
4	19	SSL/TLS	Отбросить	Standard networks	Network-protocol	Отключено	© UserGate
4	12044	Yandex Services	Пропустить	Web browsing	Client-server	Отключено	© UserGate
4	218	Yandex.Disk	Пропустить	File storage and b...	Browser-based	Отключено	© UserGate
4	7708	Yandex.Disk upload	Пропустить	Standard networks	Browser-based	Отключено	© UserGate

« « Страница 1 из 1 » » ↺ Всего: 1880 (найдено: 4)

Сохранить Отмена

Таким образом разрешается доступ и загрузка файлов на Yandex Disk, а весь остальной трафик помечается как неидентифицированный и отбрасывается либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

Пример 3. Профиль для черного списка со связанными сигнатурами

В данном примере разрешается весь трафик, кроме попадающего под сигнатуру Yandex.Disk upload (id=7708). Для этого случая необходимо учесть зависимость сигнатуры Yandex.Disk upload от сигнатуры протокола SSL/TLS (id=19). Связанность с сигнатурами Yandex.Disk и Yandex Services **в случае блокировки не учитывается**. Профиль приложений в данном примере будет выглядеть следующим образом:

Свойства профиля приложений

Общие

Совпавшие сигнатуры

Название:

Пример 3

Описание:

Пример профиля для черного списка со связанными сигнатурами.

Фильтры

Добавить

Редактировать

Удалить

Включить

Отключить

Фильтры	Включено		Действие	PCAP включен
id = 7708 or id = 19	Включено		Пропустить	Отключено

Наверх

Выше

Ниже

Вниз

Настройки сигнатуры неопределенных приложений

Действие:

Применить к:

Журналировать:

Файл PCAP:

Пропустить

Оба

Включить

Отключить

Сохранить

Отмена

Свойства профиля приложений

Общие

Совпавшие сигнатуры

Переопределить

Включить

Отключить

Восстановить по умолчанию

Выделить все

Показать Все

Все

Владелец: Все

Ещё

Сброс

Расширенный

	Id ↑		Название	Действие	Категории приложения	Технология приложе...	PCAP включен	Владелец
4	19		SSL/TLS	Пропустить	☐ Standard networks	Network-protocol	Отключено	© UserGate
4	7708		Yandex.Disk upload	Отбросить	☐ Standard networks	Browser-based	Отключено	© UserGate

«

«

Страница

1

из 1

»

»

↺

Всего: 1880 (найдено: 2)

Сохранить

Отмена

Таким образом запрещается загрузка файлов на Yandex Disk, а весь остальной трафик разрешается либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

Применение профилей приложений

Администратор может создать необходимое количество профилей.

Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль приложения применяется в разрешающем правиле [межсетевого экрана](#).

Внимание!

Для корректной работы системы анализа трафика COB/L7 через NGFW должен проходить как прямой, так и обратный трафик. На асимметричном трафике система работать не будет.

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем (адреса/зоны источника/назначения, пользователи итд.). После попадания под разрешающее правило с профилем приложений, трафик начинает анализироваться с помощью сигнатур профиля. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в фильтрах профиля и произведена соответствующая запись в [Журнале трафика](#), если была включена опция журналирования. Если ни одна из сигнатур не была найдена, то к трафику будет применено действие, настроенное в профиле для неопределённых приложений.

Примечание

При выбранном действии «Пропустить» для неопределённых приложений, попадающий под это условие, трафик будет безусловно разрешаться, не переходя дальше в обработку цепочки нижестоящих правил Межсетевого экрана.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе

Заблокированные COB/L7 IP-адреса (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

Виджеты сработавших приложений

Администратор может настроить отображение виджетов приложений на информационной панели — дашборде. В виджеты попадает информация о сработавших в правилах сигнатурах приложений, которые были определены в соответствующих профилях.

На NGFW predetermined 3 шаблона виджетов для приложений:

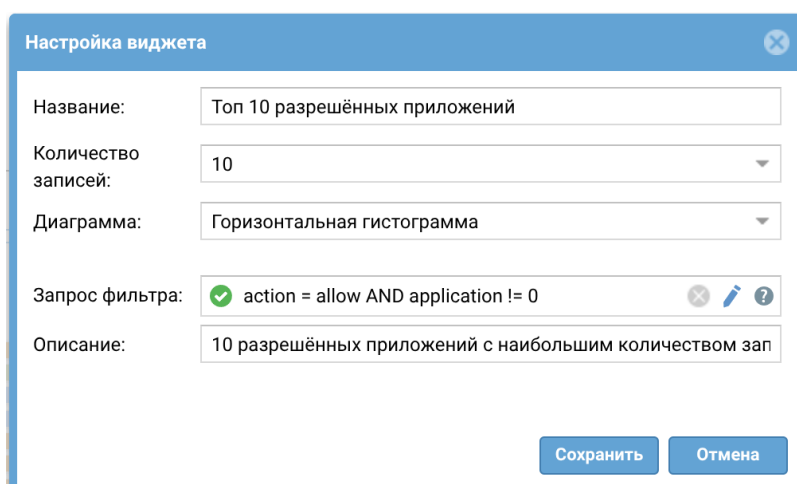
- Топ 10 приложений;
- Топ 10 разрешённых приложений;
- Топ 10 заблокированных приложений.

Виджеты можно добавлять на страницы дашборда и настраивать.

В настройках виджетов можно изменять:

- название;
- количество отображаемых записей;
- способ отображения информации (гистограмма или таблица);
- фильтр поиска информации для отображения;
- описание виджета.

Пример настройки виджета в шаблоне "Топ 10 разрешённых приложений":



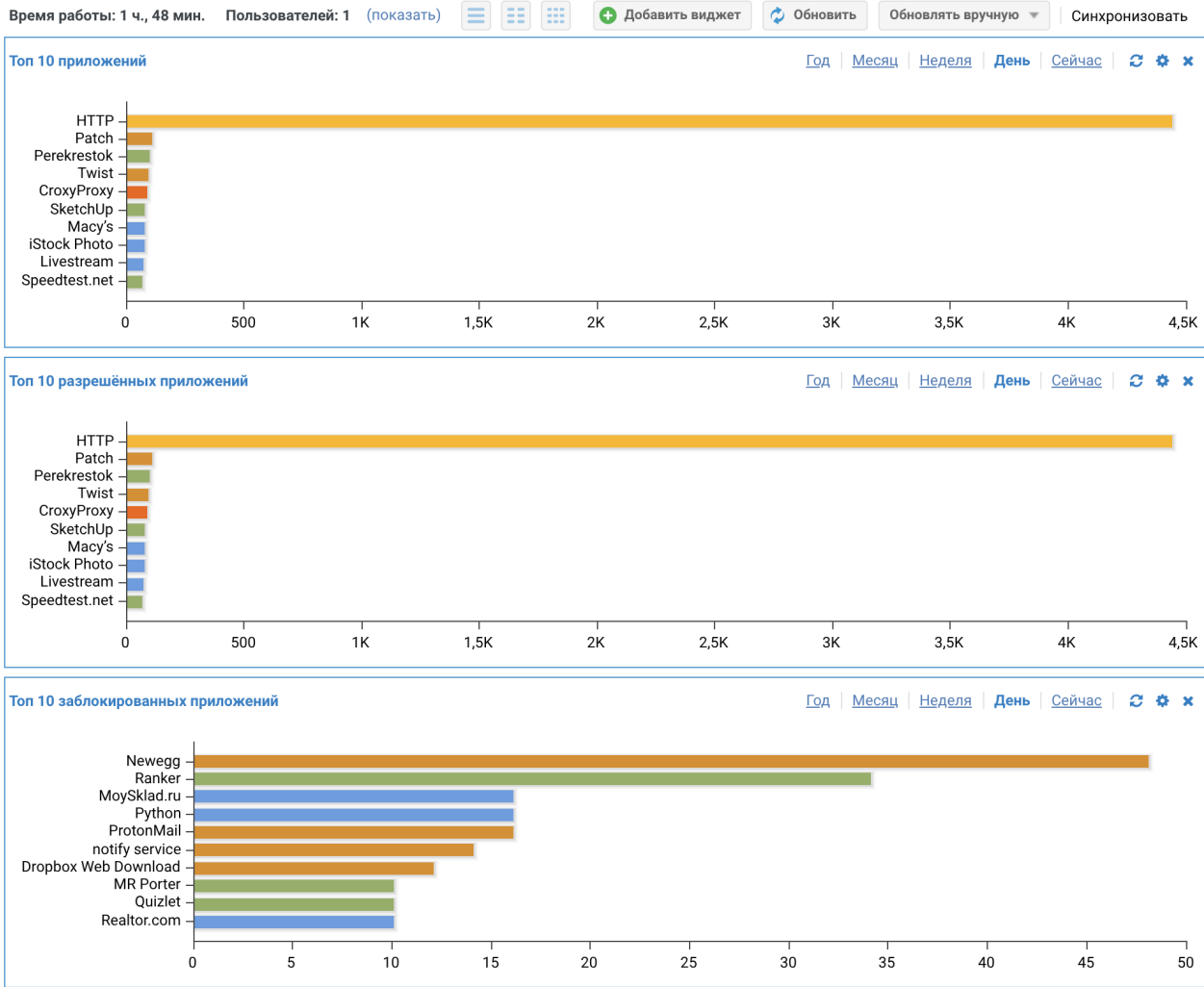
The screenshot shows a 'Настройка виджета' (Widget Settings) dialog box. It contains the following fields and values:

- Название:** Топ 10 разрешённых приложений
- Количество записей:** 10
- Диаграмма:** Горизонтальная гистограмма
- Запрос фильтра:** action = allow AND application != 0
- Описание:** 10 разрешённых приложений с наибольшим количеством зап

At the bottom, there are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).

Подробнее о работе с виджетами на дашборде читайте в статье [Дашборд](#) руководства администратора.

Пример отображения настроенных виджетов приложений с гистограммами на дашборде:



Пример отображения настроенных виджетов приложений с таблицами на дашборде:

Топ 10 приложений		Год	Месяц	Неделя	День	Сейчас	↺	⚙	×
	↓								
3	HTTP	4 430							
4	Patch	98							
1	Perekrestok	88							
4	Twist	84							
5	CroxyProxy	78							
2	iStock Photo	68							
2	Macy's	68							

Топ 10 заблокированных приложений		Год	Месяц	Неделя	День	Сейчас	↺	⚙	×
	↓								
4	Newegg	48							
1	Ranker	34							
4	ProtonMail	16							
2	Python	16							
2	MoySklad.ru	16							
4	notify service	14							
4	Dropbox Web Download	12							

Топ 10 разрешённых приложений		Год	Месяц	Неделя	День	Сейчас	↺	⚙	×
	↓								
4	Twist	84							
5	CroxyProxy	78							
2	iStock Photo	68							
2	Macy's	68							
1	SketchUp	68							
2	Livestream	62							
1	Speedtest.net	56							

Группы приложений

В данном разделе пользователь может управлять (создавать/обновлять/удалять) группами приложений. Группы приложений могут быть использованы при настройке правил управления пропускной способности.

Для создания группы приложений:

Наименование	Описание
Шаг 1. Создать группу.	В разделе Библиотеки → Группы приложений нажать на кнопку Добавить , указать название и, опционально, описание группы приложений.
Шаг 2. Добавить сигнатуры приложений в группу.	На панели Приложения нажать Добавить и выбрать сигнатуры приложений для добавления в группу. Для добавления всех сигнатур приложений использовать кнопку Добавить все .

Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу, в панели Почтовые адреса нажать на кнопку Добавить и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом NGFW создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.

Наименование	Описание
	Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу, в панели Группа телефонных номеров нажать на кнопку Добавить и добавить необходимые номера.

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом NGFW создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.

Наименование	Описание
	Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.

Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Сигнатуры COB

Сигнатуры COB представляют собой выражения на языке UASL и содержат описания паттернов (строк), которые COB распознает в сетевом трафике.

Для использования сигнатуры COB устройством необходимо [создать профиль COB](#), включающий эту сигнатуру, и добавить созданный профиль в [разрешающее правило межсетевого экрана](#).

Сигнатуры COB в UserGate NGFW делятся на пользовательские сигнатуры, которые вы можете [создавать в веб-консоли устройства](#), и проприетарные сигнатуры, разрабатываемые компанией UserGate и поставляемые [в рамках лицензии на модуль Security Updates](#).

Для проприетарных сигнатур вы можете настраивать [некоторые параметры](#) (например, изменять действие при срабатывании сигнатуры). Это может понадобиться для адаптации таких сигнатур под сетевую инфраструктуру организации. При необходимости вы можете восстановить исходные значения параметров проприетарных сигнатур, установленные экспертами UserGate.

Просмотр списка сигнатур

В разделе **Настройки** → **Библиотеки** → **Сигнатуры COB** отображается список доступных сигнатур COB.

UserGate NGFW

Дашборды

Диагностика и мониторинг

Журналы и отчеты

Настройки

Гостевой портал

Введите IP или текст...

Admin

Py

Все

Избранное

Библиотека

Морфология

Список

Группы сервисов

IP-адреса

UserAgent браузеров

Типы контента

Списки URL

Календари

Полночные приложения

Шаблоны страниц

Категории URL

Изменяемые категории URL

Приложения

Профили приложений

Группы приложений

Почтовые адреса

Номера телефонов

Сигнатуры COB

Профили COB

Профили приложений

Профили L7-8

Сигнатуры COB

Добавить

Удалить

Включить

Отключить

Восстановить по умолчанию

Включить все

Уменьшить угрозы: все

Действие: все

Владельцы: все

Паи

Сброс

Расширенный

Уровень угрозы	ID	Статус	Журналирование	Название сигнатуры	Действие	Операционная система	Протокол	Класс	Влияемость	Категория	PCAP включен	Владелец
1000000	По умолчанию	Журналируется	Example signature	Пропустить	Нет	Нет	Нет	Нет	Нет	Нет	Отключено	You
6017	Изменено	Журналируется	Possible Windows NFS4.1 Buffer Overflow	Отбросить	Windows	Tcp	arbitrary-code-execution	CVE-2023-24941	exploit	Отключено	© UserGate	
6012	Изменено	Журналируется	Altegrity Power Control Software C1.2.5 RCE	Пропустить	Нет	Tcp	arbitrary-code-execution	CVE-2023-28343	exploit	Отключено	© UserGate	
6122	По умолчанию	Журналируется	Realtek Jungle SDK CI	Пропустить	Нет	udp	arbitrary-code-execution	CVE-2023-33384 BDU-2021-04677	exploit	Отключено	© UserGate	
6078	Изменено	Журналируется	Juniper JunOS PHP environment variable manipulation RCE	Пропустить	BSD Linux	Tcp	arbitrary-code-execution	CVE-2023-36844 BDU-2023-04993	exploit	Отключено	© UserGate	
6015	Изменено	Не журналируется	Zynga Zynga/VPN/ATP RCE	Отбросить (znc)	Нет	Tcp	arbitrary-code-execution	CVE-2023-27992	exploit	Включено	© UserGate	
6016	По умолчанию	Журналируется	Barracuda ESG Mail Tar RCE	Пропустить	Нет	Tcp	arbitrary-code-execution	CVE-2023-2868	exploit	Отключено	© UserGate	
6125	Изменено	Журналируется	ShakeFarm Constructor Insecure Deserialization	Блокировать IP (both, int)	Нет	Tcp	arbitrary-code-execution	CVE-2022-1471 BDU-2023-00013	exploit	Отключено	© UserGate	
9664	По умолчанию	Журналируется	Unauthenticated File upload WordPress plugin RCE	Пропустить	Нет	http	arbitrary file access	CVE-2020-24186	broken access control	Отключено	© UserGate	

«

Страница 1 из 115

»

Всего 11462

Для каждой сигнатуры в таблице отображаются следующие параметры.

Параметр	Описание
Уровень угрозы	Уровень опасности угрозы (от 1 до 5, где 1 — очень низкий уровень), который определяет степень потенциального ущерба ИТ-инфраструктуре при срабатывании сигнатуры
Id	Идентификатор сигнатуры
Статус	Статус параметров проприетарной сигнатуры: • По умолчанию — значения параметров сигнатуры соответствуют значениям, установленным экспертами UserGate; • Изменено — значения параметров сигнатуры изменены администратором устройства
Журналирование	Статус журналирования срабатываний сигнатуры: • Журналируется — журналирование включено в свойствах сигнатуры, записи о ее срабатывании отображаются в Журнале СОВ; • Не журналируется — журналирование отключено в свойствах сигнатуры
Свойства сигнатуры	По нажатию на значок в столбце параметра открывается карточка выбранной сигнатуры
Название сигнатуры	Название сигнатуры, указанное при ее создании
Действие	Действие при срабатывании сигнатуры: • Нет — маркировка пакета или проверка наличия метки, установленной другой сигнатурой. Используется для сигнатур, связанных через конструкцию <code>.mark set test</code>. Подробнее — в разделе «Работа с метками». • Пропустить — разрешение передачи трафика. • Отбросить — запрет передачи трафика. • Сбросить — запрет передачи трафика и разрыв TCP-соединения с его источником. • Блокировать IP — блокирование IP-адреса источника и (или) назначения трафика
Операционная система сигнатуры	Операционная система, для которой разработана сигнатура
Протокол	Сетевой протокол соединений, к которым применима сигнатура

Параметр	Описание
Дата создания	Дата создания сигнатуры. Параметр доступен начиная с версии 7.5.0
Дата модификации	Дата изменения сигнатуры. Параметр доступен начиная с версии 7.5.0
Класс	Класс сигнатуры, который определяет тип угрозы по срабатыванию этой сигнатуры. Ниже в этом разделе перечислены классы сигнатур в UserGate NGFW
References	Идентификаторы уязвимости, на которую указывает срабатывание сигнатуры, согласно реестрам CVE и BDU
Категория	Категория сигнатуры, в которую объединяются сигнатуры с общими параметрам. Ниже в этом разделе перечислены категории сигнатур в UserGate NGFW
PCAP включен	Запись копии трафика (трассировка) при срабатывании сигнатуры: • Включено — трассировка выполняется, результат записывается в файл формата PCAP; • Отключено — трассировка не выполняется
Владелец	Разработчик сигнатуры. Для проприетарных сигнатур отображается UserGate , для пользовательских — You
Описание	Описание сигнатуры, указанное при ее создании. Для проприетарных сигнатур отображается описание угрозы, на которую указывает срабатывание сигнатуры. Описание может включать сведения об уязвимостях в инфраструктуре организации, а также механику проведения и последствия атаки, использующей эти уязвимости. По умолчанию в таблице сигнатур столбец Описание скрыт

В таблице сигнатур вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;

- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Кроме того, вы можете фильтровать данные в таблице, выбрав один из следующих режимов:

- **Простой** — с помощью доступных параметров. Например, фильтрация по состоянию сигнатур (**true** — включено, **false** — отключено), уровню опасности угрозы, действию при срабатывании, а также владельцу сигнатур. Для выбора параметров используются соответствующие кнопки в панели инструментов. В раскрывающемся списке по кнопке **Еще** вы также можете выбирать дополнительные параметры фильтрации, устанавливая соответствующие флажки.
- **Расширенный** — с помощью специальных запросов [на языке фильтрации](#). Для ввода запросов используется строка фильтрации.

Вы можете управлять сигнатурами в таблице:

- Включать и отключать их состояние (по кнопкам **Включить** и **Отключить** соответственно).
- Создавать пользовательские сигнатуры (по кнопке **Добавить**).
- Изменять параметры сигнатур (по кнопке **Редактировать**). После изменения параметров проприетарных сигнатур вы можете восстановить значения этих параметров, установленные по умолчанию (по кнопке **Восстановить по умолчанию**).
- Просматривать информацию о сигнатуре в ее карточке (по нажатию на значок в столбце **Свойства сигнатуры** для выбранной сигнатуры).

Создание пользовательской сигнатуры

Примечание

Ниже приведена инструкция по созданию пользовательской сигнатуры в веб-консоли UserGate NGFW, аналогичная инструкция для интерфейса командной строки устройства приведена в разделе «[Настройка библиотек](#)».

Чтобы создать сигнатуру:

1. В разделе **Настройки → Библиотеки → Сигнатуры СОВ** нажмите **Добавить**.

2. На вкладке **Общие** выполните следующие действия:

- Активируйте сигнатуру, установив флажок **Включено**.
- Если необходимо, укажите идентификатор сигнатуры, выбрав одно из доступных значений. При незаполненном поле идентификатор будет сгенерирован автоматически.
- Укажите название и при необходимости описание сигнатуры.
- Выберите уровень опасности угрозы по срабатыванию сигнатуры (от 1 до 5, где 1 — очень низкий уровень).
- При необходимости выберите класс сигнатуры, определяющий тип угрозы по срабатыванию этой сигнатуры. Ниже в этом разделе перечислены [классы сигнатур в UserGate NGFW](#).
- При необходимости выберите категорию сигнатуры, в которую объединяются сигнатуры с общими параметрам. Ниже в этом разделе перечислены [категории сигнатур в UserGate NGFW](#).
- При необходимости укажите ОС, для которой создается сигнатура. Вы можете выбрать несколько значений.
- При необходимости укажите идентификатор уязвимости, на которую указывает срабатывание сигнатуры, согласно реестру CVE.
- При необходимости укажите идентификатор уязвимости, на которую указывает срабатывание сигнатуры, согласно реестру BDU.
- При необходимости укажите адрес ресурса с описанием уязвимости, на которую указывает срабатывание сигнатуры, в формате `https://<адрес ресурса>`, например `https://example.com`.

3. На вкладке **UASL и настройки** выполните следующие действия:

- В поле **UASL** укажите параметры сигнатуры [с помощью синтаксиса UASL](#).

- Выберите действие, выполняемое при срабатывании сигнатуры.

Для сигнатуры с действием **Нет** вы можете указывать параметры только в поле **UASL**, остальные поля недоступны для настройки.

- Если не требуется записывать информацию о срабатываниях сигнатуры [в Журнал СОВ](#), отключите журналирование. По умолчанию журналирование включено.

Если при срабатывании сигнатуры требуется

- сохранять копию трафика в виде файла формата PCAP, включите трассировку трафика в поле **Файл PCAP**. По умолчанию трассировка отключена.
- Для сигнатуры с действием **Сбросить** или **Блокировать IP** выберите направление трафика, к которому будет применяться сигнатура:
 - **Источник** — от клиента к серверу;
 - **Назначение** — от сервера к клиенту;
 - **Оба** — в обоих направлениях.
- Для сигнатуры с действием **Блокировать IP** выберите режим блокировки IP-адресов при срабатывании сигнатуры:
 - **Всегда** — постоянная блокировка;
 - **На время** — блокировка в течение указанного времени.

4. Нажмите **Проверить сигнатуру** для проверки синтаксиса UASL.

Результат проверки отобразится в отдельном окне.

5. Нажмите **Заккрыть**.

6. Если в синтаксисе UASL содержатся ошибки, исправьте их и повторите проверку.

7. Нажмите **Сохранить**.

Настройка проприетарной сигнатуры

Чтобы настроить проприетарную сигнатуру:

1. Выберите сигнатуру в таблице и нажмите **Редактировать**.
2. Настройте параметры сигнатуры:
 - Состояние сигнатуры.
 - Действие, выполняемое при срабатывании.
 - Журналирование срабатываний.
 - Трассировку трафика при срабатывании.

Направление трафика, к которому применяется сигнатура.

- Доступно только для действий **Сбросить** и **Блокировать IP**.
- Время блокировки IP-адресов при срабатывании. Доступно только для действия **Блокировать IP**. Для постоянной блокировки необходимо установить значение 0.

В некоторых проприетарных сигнатурах указаны параметры агрегации (суммирования) срабатываний этих сигнатур:

- **Частота срабатывания** — количество срабатываний сигнатуры за указанный период времени (в секундах). Например, если указано «5 срабатываний за 10 секунд», UserGate NGFW пропустит первые четыре срабатывания сигнатуры и выполнит выбранное действие только при пятом срабатывании.
- **Направление** — направление агрегирования срабатываний сигнатуры:
 - **IP источника** — суммируются срабатывания сигнатуры для каждого уникального IP-адреса клиента (источника трафика).
 - **IP назначения** — суммируются срабатывания сигнатуры для каждого уникального IP-адреса сервера (назначения трафика).

При необходимости вы можете изменить параметры агрегации. Это может понадобиться для снижения количества ложных срабатываний сигнатур, которые обнаруживают массовые атаки, например такие, как брутфорс (см. сигнатуру с `id = 17002`) или DoS (см. сигнатуру с `id = 3040443`).

3. Нажмите **Сохранить**.

Классы сигнатур в UserGate NGFW

Сигнатуры COB в UserGate NGFW классифицируются по типу угрозы, на которую указывают их срабатывания (например, запуск произвольного кода, сетевая разведка или атака на веб-приложение). Эта классификация определяет, как именно срабатывание сигнатуры влияет на ИТ-инфраструктуру, и позволяет администраторам эффективно управлять безопасностью.

В таблице ниже перечислены классы, используемые в проприетарных сигнатурах UserGate. При создании пользовательских сигнатур вы можете использовать только основные классы из этого перечня.

Класс сигнатуры	Описание угрозы
arbitrary-code-execution	Попытка выполнения произвольного кода
arbitrary file access	Попытка доступа к произвольным файлам
attempted-admin	Попытка получения прав администратора
attempted-dos	Попытка DoS-атаки
attempted-recon	Попытка сетевой разведки
attempted-user	Попытка получения прав пользователя
authentication bypass	Попытка обхода аутентификации
backdoor	Обход стандартных механизмов аутентификации
bad-unknown	Потенциально вредоносный трафик
bruteforce	Атака брутфорс
buffer overflow	Атака через переполнение буфера
c2-activity	Активность, указывающая на подключение к командному центру злоумышленника
code injection	Попытка внедрения кода
command injection	Попытка внедрения системных команд
command-and-control	Попытка подключения к командному центру злоумышленника
csrf	Попытка выполнения несанкционированных действий от имени авторизованного пользователя
default-login-attempt	Попытка входа с учетными данными по умолчанию
denial-of-service	DoS-атака
deserialization	Попытка удаленного выполнения кода (RCE), связанного с десериализацией параметров
evasion	Попытка обхода злоумышленником механизмов защиты COB

Класс сигнатуры	Описание угрозы
exploit-kit	Использование злоумышленником набора инструментов для эксплуатации уязвимостей
file transfer	Попытка передачи файлов определенных типов
hardcoded credentials	Попытка использования злоумышленником встроенных учетных данных
information disclosure	Попытка получения конфиденциальных данных
local file inclusion	Попытка доступа к локальным файлам сервера
memory corruption	Попытка атаки через повреждение памяти
misc	Активность, не относящаяся к другим классам
misc activity	Потенциально опасная или опасная активность, не относящаяся к другим классам
misc attack (или misc-attack)	Попытка атаки, не относящейся к другим классам
misc scan	Попытка сканирования сети и поиска уязвимостей
network scan (или network-scan)	Сканирование сети на наличие активных узлов и открытых портов
null pointer dereference	Попытка атаки через ошибки обращения к памяти
out of bounds access	Попытка атаки через переполнение или чтение памяти
path traversal	Попытка атаки через обход пути к файлам на сервере
policy-violation	Нарушение сетевых политик
privilege escalation	Попытка повышения привилегий
protocol-command	Попытка использования нестандартных или вредоносных команд протокола
protocol-command-decode	Попытка использования команд протокола в закодированном виде
remote file inclusion	Попытка удаленного внедрения файлов
service scan	Попытка сканирования сетевых сервисов и их версий

Класс сигнатуры	Описание угрозы
shellcode	Попытка передачи шелл-кода для получения управления системой
shellcode-detect	Попытка использования исполняемого кода (шелл-кода)
sql injection	Попытка SQL-внедрения
ssrf	Попытка подделки запросов на стороне сервера
string-detect	Использование подозрительных строк
successful-recon-limited	Сетевая разведка ограниченного масштаба
suspicious-filename-detect	Использование подозрительного имени файла
suspicious-login	Попытка входа с использованием подозрительного имени пользователя
system-call-detect	Попытка использования системных вызовов
targeted-activity	Активность, указывающая на проведение целенаправленной атаки
trojan	Активность, указывающая на работу вредоносного ПО
trojan-activity	Использование вредоносного ПО
uncaught exception	Попытка вызова программных ошибок
uncontrolled resource consumption	Попытка исчерпания системных ресурсов
use after free	Попытка обращения к освобожденным участкам памяти
vulnerability scan	Сканирование сети на наличие уязвимостей
web-application-activity	Активность, связанная с работой веб-приложений
web-application-attack	Атака через уязвимости веб-приложений
worm	Активность, указывающая на работу самораспространяющегося вредоносного ПО (сетевых червей)
xml injection	Попытка XML-внедрения

Класс сигнатуры	Описание угрозы
xss	Попытка внедрения вредоносного сценария в веб-приложение

Список классов сигнатур постоянно пополняется экспертами UserGate.

Категории сигнатур в UserGate NGFW

В UserGate NGFW сигнатуры с общими параметрами объединяются в категории по их функциональному назначению.

В таблице ниже перечислены категории, используемые в проприетарных сигнатурах UserGate. При создании пользовательских сигнатур вы можете использовать только основные категории из этого перечня.

Категория сигнатур	Функциональное назначение
activex	Защита от использования уязвимостей ActiveX
adware pup	Поиск рекламного и нежелательного ПО
attack response	Выявление в ответах сервера признаков проведенных атак
authentication-failures	Обнаружение подбора учетных данных
authentication-failures,Apache	Обнаружение подбора учетных данных к веб-серверу Apache
authentication-failures,ICS/IoT	Обнаружение подбора учетных данных в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
broken-access-control	Выявление обхода прав доступа
broken-access-control,ICS/IoT	Выявление обхода прав доступа в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
bruteforce	Обнаружение брутфорса
coinminer	Выявление скрытого майнинга
dns	Обнаружение угроз в трафике DNS
dos	Обнаружение DoS-атак
dos,Apache	Обнаружение DoS-атак на веб-сервер Apache

Категория сигнатур	Функциональное назначение
dos,ICS/IoT (или ICS/IoT,dos)	Обнаружение DoS-атак на промышленные системы управления (ICS) и устройства интернета вещей (IoT)
dos,smtp	Обнаружение DoS-атак на почтовые серверы
exploit	Обнаружение использования известных уязвимостей
exploit kit	Выявление наборов инструментов для эксплуатации уязвимостей
ftp	Обнаружение угроз в трафике FTP
icmp	Обнаружение угроз в трафике ICMP
ICS/IoT	Обнаружение угроз в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
imap	Обнаружение угроз в трафике IMAP
info	Выявление утечки конфиденциальных данных
injection	Обнаружение внедрения данных
injection,Apache	Обнаружение внедрения данных на стороне веб-сервера Apache
injection,ftp	Обнаружение внедрения данных в трафике FTP
injection,ICS/IoT	Обнаружение внедрения данных в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
injection,scan	Выявление сканирования сети на наличие уязвимостей, используемых для внедрения данных
injection,smb	Обнаружение внедрения данных в трафике SMB
injection,smtp	Обнаружение внедрения данных в трафике SMTP
integrity-failures	Выявление нарушений целостности данных или ПО
integrity-failures,Apache	Выявление нарушений целостности данных или конфигурации веб-сервера Apache
integrity-failures,ICS/IoT	Выявление нарушений целостности данных или ПО в промышленных системах управления (ICS) и устройствах интернета вещей (IoT)

Категория сигнатур	Функциональное назначение
integrity-failures,injection	Обнаружение внедрений, нарушающих целостность данных или ПО
ldap	Обнаружение угроз в трафике LDAP
malware	Обнаружение вредоносного ПО
malware,wmi	Обнаружение вредоносной активности, использующей инструменты WMI
misc	Обнаружение прочих угроз
misc,ICS/IoT	Обнаружение прочих угроз в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
misc,smtp	Обнаружение прочих угроз в трафике SMTP
netbios	Обнаружение угроз в трафике NetBIOS
p2p	Обнаружение активности пиринговых сетей и протоколов
phishing	Обнаружение активности, связанной с фишингом
policy	Выявление нарушения политик безопасности
pop3	Обнаружение угроз в трафике POP3
request-forgery	Обнаружение подделки запросов
request-forgery,ICS/IoT	Обнаружение подделки запросов в трафике промышленных систем управления (ICS) и устройств интернета вещей (IoT)
rpc	Обнаружение угроз в трафике RPC
scada	Обнаружение угроз в трафике систем управления SCADA
scan	Обнаружение активности по сканированию сети и поиску уязвимостей
shellcode	Обнаружение внедрения шелл-кода
sip	Обнаружение угроз в трафике SIP
smb	Обнаружение угроз в трафике SMB
smtp	Обнаружение угроз в трафике SMTP

Категория сигнатур	Функциональное назначение
snmp	Обнаружение угроз в трафике SNMP
sql	Обнаружение угроз в трафике баз данных
telnet	Обнаружение угроз в трафике Telnet
tftp	Обнаружение угроз в трафике TFTP
user agents	Выявление подозрительных идентификаторов браузеров и приложений
voip	Обнаружение угроз в трафике протоколов IP-телефонии (VoIP)
web client	Обнаружение атак на веб-браузеры и клиентские приложения
web server	Обнаружение атак на веб-серверы и серверные приложения
web specific apps	Обнаружение атак на веб-приложения
worm	Обнаружение самораспространяющегося вредоносного ПО (сетевое червя)

Список категорий сигнатур постоянно пополняется экспертами UserGate.

Профили COB

Назначение профиля COB

С помощью профилей COB администратор может создать динамические наборы [сигнатур COB](#), предназначенные для обнаружения вторжений и защиты определенных сервисов. Динамичность профилей достигается за счет использования фильтров, с помощью которых автоматически собирается необходимый набор сигнатур. Для фильтрации используются как описательные поля, так и параметры сигнатур. При изменении сигнатур в библиотеке профили динамически обновят наборы сигнатур в соответствии с настроенными фильтрами.

В профилях COB также можно настроить действия, которые будут выполняться над трафиком, отфильтрованным сигнатурами.

Создание профиля COB в веб-консоли администратора

В веб-консоли администратора профили COB создаются в разделе **Настройки → Библиотеки → Профили COB**.

Нажмите **Добавить** и заполните соответствующие поля в свойствах профиля:

Свойства профиля COB

Общие Совпавшие сигнатуры

Название: Test 1

Описание: Тестовый профиль №1

Фильтры

+ Добавить ✎ Редактировать ✕ Удалить Включить Отключить

Фильтры	Включено		Действие	РСАР включен
threat IN ('high';very h...	По умолчанию	📄	🚫 Отбросить	По умолчанию

Наверх Выше Ниже Вниз

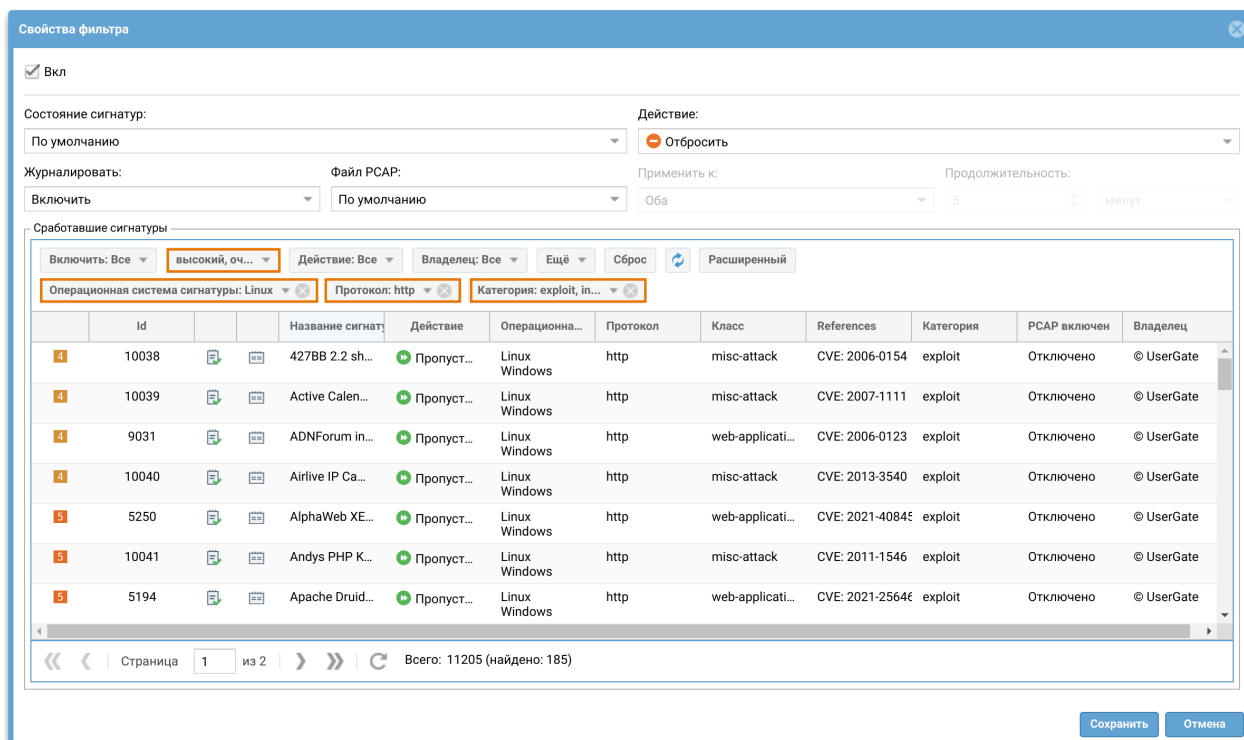
Сохранить Отмена

1. В поле **Название** укажите название создаваемого профиля.
2. В поле **Описание** укажите назначение профиля.
3. В области **Фильтры** добавьте фильтры для выбора необходимых сигнатур из библиотеки.
4. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур COB, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над трафиком, отфильтрованным этими сигнатурами.

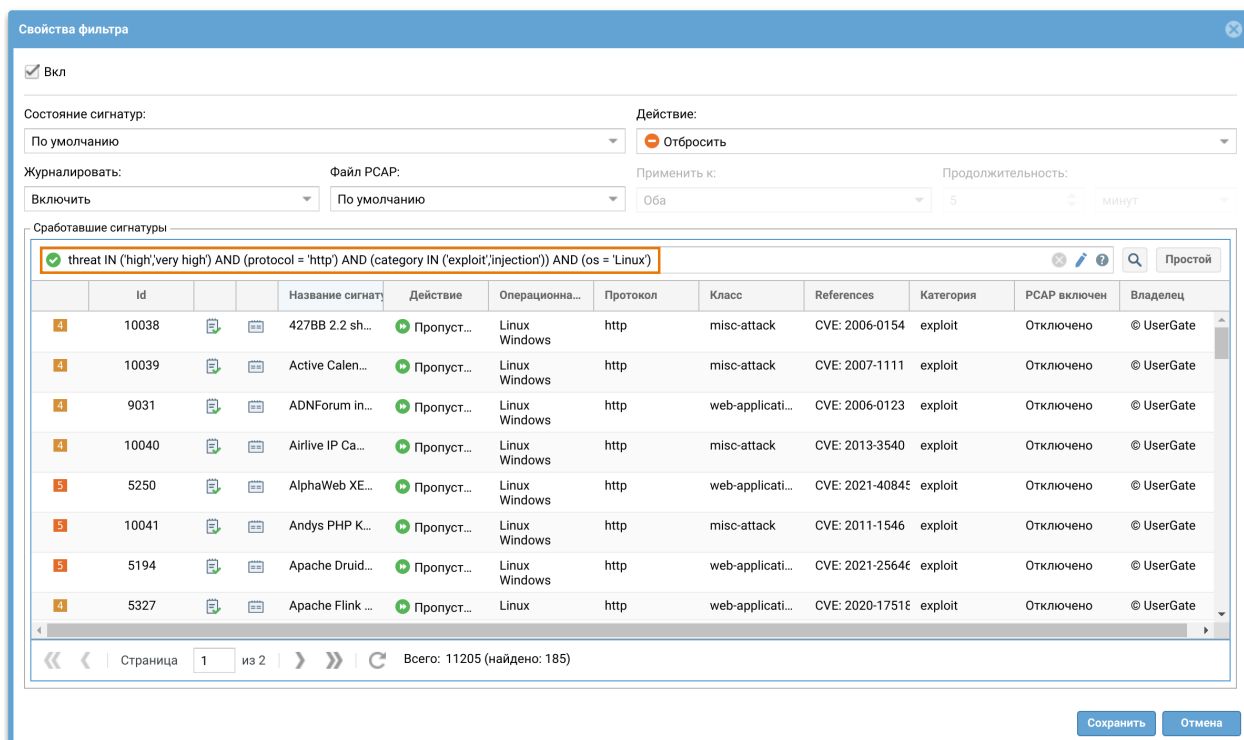
Настройка фильтров сигнатур в профиле COB

Для создания фильтра сигнатур в области **Фильтры** нажмите **Добавить**. Откроется окно свойств фильтра.

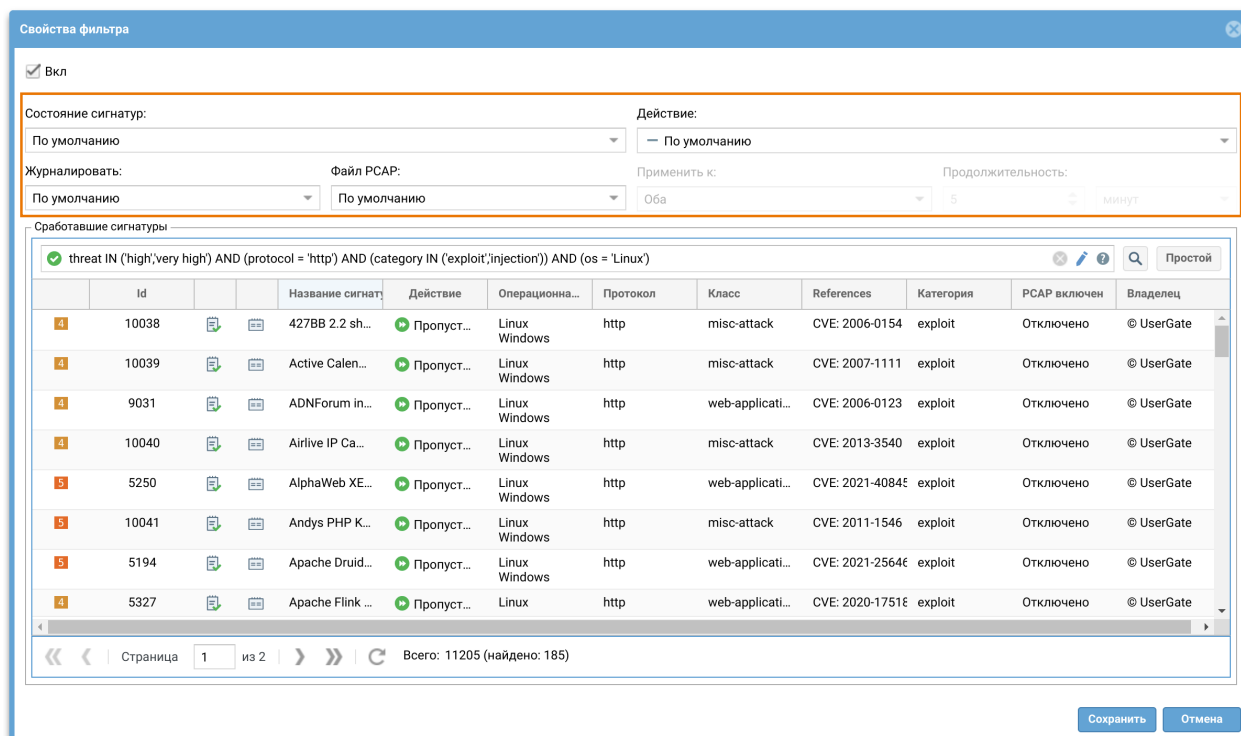
Фильтр можно создать, выбирая опции фильтрации в панели инструментов. В окне под панелью инструментов будут отображаться сигнатуры, отбираемые этим фильтром:



Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого нажмите **Расширенный** в панели инструментов и в открывшейся строке опишите свойства выбора фильтра:



Начиная с версии ПО 7.3.0 в свойствах фильтров доступна возможность перенастройки параметров всех сигнатур, отбираемых фильтром:



Вы можете перенастроить следующие параметры отфильтрованных сигнатур:

- **Состояние сигнатуры** — возможность включить или выключить сигнатуры. Значение «По умолчанию» оставляет состояние всех сигнатур таким, как было определено в самих сигнатурах по умолчанию.
- **Действие** — предпринимаемое действие, если сигнатура сработала, т. е. была найдена в трафике. Действия могут быть следующие: пропустить пакет, отбросить пакет, сбросить пакет с разрывом TCP-соединения, заблокировать IP-адрес источника или назначения. Значение «По умолчанию» оставляет для всех сигнатур то действие, которое было определено в самих сигнатурах по умолчанию.
- **Журналировать** — включение или отключение журналирования срабатывания сигнатуры. Значение «По умолчанию» оставляет настройку журналирования для всех сигнатур, как она была определена в самих сигнатурах по умолчанию.
- **Файл PCAP** — включение или отключение записи в PCAP-файл, если сигнатура сработала. Значение «По умолчанию» оставляет настройку записи в PCAP-файл для всех сигнатур, как она была определена в самих сигнатурах по умолчанию.

- Применить к** — настраивается, если параметр «Действие» выставлен в значения «Сбросить» или «Блокировать IP». Параметр имеет следующие значения:
- Источник;
 - Назначение;
 - Оба.
- **Продолжительность** — можно настроить, если параметр «Действие» имеет значение «Блокировать IP». Число, указывающее срок блокировки IP-адреса. Если значение равно нулю, IP-адрес блокируется бесконечно.

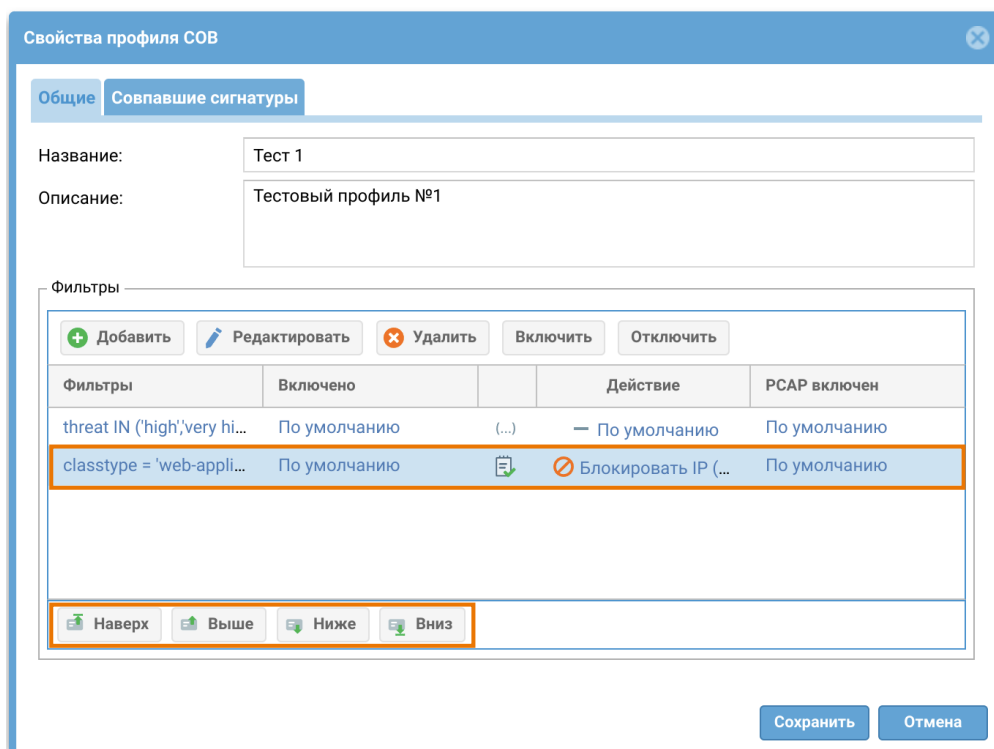
Для сохранения созданного фильтра нажмите **Сохранить**.

В одном профиле можно использовать сразу несколько фильтров.

Фильтры в профиле работают по логическому ИЛИ. Например, если в профиле добавлено два фильтра: `category = injection` и `threat = low`, они эквивалентны одному фильтру: `category = injection OR threat = low`.

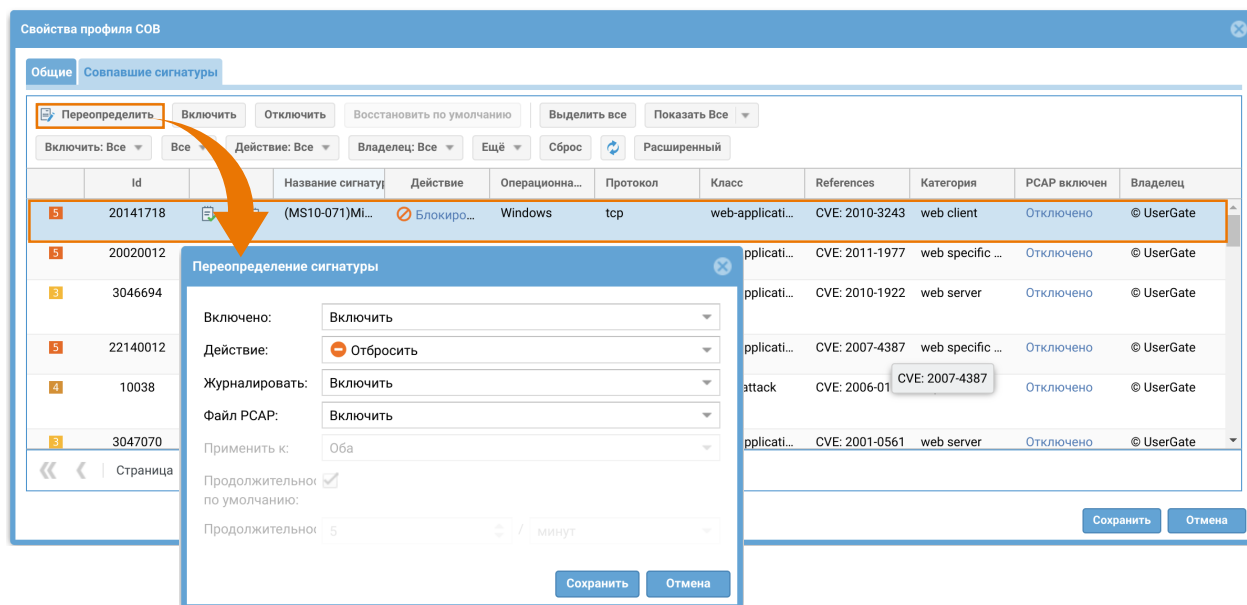
Если одна и та же сигнатура попала в несколько фильтров, приоритет настроек параметров сигнатуры определяется настройками в верхнем фильтре в списке.

Фильтры в профиле можно перемещать вверх или вниз:



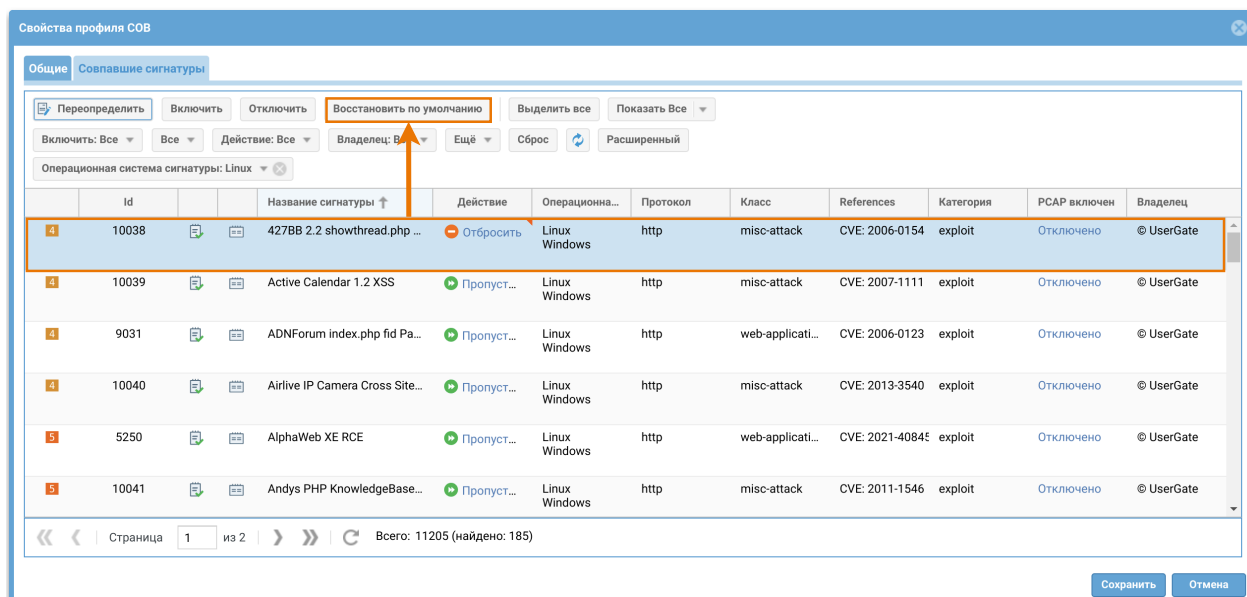
Точечное переопределение параметров сигнатур в профиле COB

На вкладке профиля **Совпавшие сигнатуры** можно произвести точечное переопределение параметров сигнатуры. Для этого выберите нужные сигнатуры в списке совпавших сигнатур и нажмите **Переопределить** в панели инструментов.



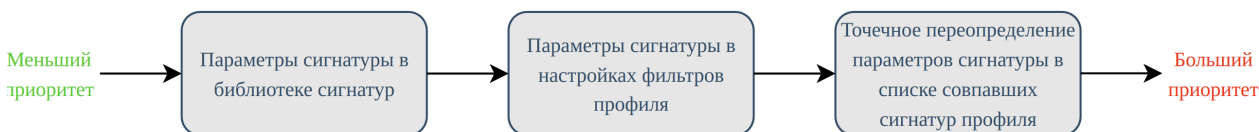
Переопределение настроек сигнатур в профиле COB имеет более высокий приоритет, чем настройки этих же сигнатур в библиотеке сигнатур COB.

Измененные настройки сигнатур COB можно вернуть в первоначальное состояние, для этого выделите сигнатуру в списке сигнатур профиля и нажмите в панели инструментов профиля **Восстановить по умолчанию**.



Приоритет значений параметров сигнатуры COB

Приоритет назначений параметров сигнатуры COB определяется согласно следующей диаграмме:



- В библиотеке сигнатур COB (**Настройки → Библиотеки → Сигнатуры COB**) представлен общий перечень сигнатур с определенными по умолчанию параметрами. Администратор может [самостоятельно переопределить](#) некоторые параметры (например, состояние, действие, журналирование, запись в файл PCAP и т. д.) в настройках параметров сигнатуры.
- При создании профиля COB администратор может [переопределить параметры](#) сигнатур при настройке конкретного фильтра. Эти изменения будут актуальны только для профиля, в котором они определены.
- При создании профиля COB администратор может точно переопределить параметры сигнатур в списке всех совпавших сигнатур профиля (подробнее — в главе «[Точечное переопределение параметров сигнатур в профиле COB](#)»). Изменения применяются к результату фильтрации. Изменения параметров сигнатуры при точечном переопределении сохраняются до тех пор, пока сигнатура попадает в профиль.

i Примечание

Если в фильтре профиля задан поиск по свойствам сигнатур, этот поиск будет осуществляться с учетом свойств, заданных в библиотеке сигнатур («Настройки» → «Библиотеки» → «Сигнатуры COB»). Переопределения на этапе задания свойств фильтра, а также точечные переопределения на факт попадания сигнатуры в фильтр не влияют.

Применение профилей COB

Администратор может создать необходимое количество профилей. Рекомендуется ограничивать количество сигнатур в профиле только теми,

которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль COB применяется в разрешающем правиле [межсетевого экрана](#).

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем. После попадания под правило с профилем COB, трафик начинает анализироваться с помощью определенного в профиле набора сигнатур. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в профиле и произведена соответствующая запись в [Журнале COB](#), если была включена опция журналирования. Если ни одна из сигнатур профиля не была найдена, то трафик пропускается дальше.

Важно!

Для корректной работы системы анализа трафика COB/L7 через NGFW должен проходить как прямой, так и обратный трафик. На асимметричном трафике система работать не будет.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные COB/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

Работа с сигнатурами COB в интерфейсе командной строки описана в разделе [Настройка библиотек](#) Руководства администратора.

Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.

- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Авторизация	Включает авторизацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL -- 3550.

Наименование	Описание
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Профили Netflow

Netflow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

NGFW может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс NGFW, необходимо выполнить следующие действия:

1. Создать профиль Netflow.
2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.

Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили Netflow** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля Netflow.
Описание	Описание профиля Netflow.
IP-адрес Netflow коллектора	IP-адрес сервера, куда сенсор будет отправлять статистику.
Порт Netflow коллектора	UDP порт, на котором коллектор будет принимать статистику.
Версия протокола	Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе.
Таймаут активного потока (сек)	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд.
Таймаут неактивного потока (сек.)	Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд.
Количество потоков	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения.
Отправлять информацию NAT	Отправлять информацию о NAT преобразованиях в статистику Netflow.
Частота отправки шаблона (пакетов)	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
Период отправки старого шаблона (сек.)	Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Профили LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

Наименование	Описание
Название	Название профиля LLDP.
Описание	Описание профиля LLDP.
Статус порта	Режим: • Приём и передача данных LLDP — NGFW будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • Только приём данных LLDP — NGFW не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • Только передача данных LLDP — NGFW будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей.

Профили SSL

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в правилах инспектирования SSL, в настройках веб-консоли, страницы авторизации, страницы блокировки, веб-портале.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля SSL.

Наименование	Описание
Описание	Описание профиля SSL.
Протоколы SSL	Минимальная версия TLS — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. Максимальная версия TLS — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем.
Наборы алгоритмов шифрования	Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384

Наименование	Описание
	• TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256 • TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS GOST2012256 WITH 28147 CNT IMIT • TLS GOSTR341001 WITH 28147 CNT IMIT • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле Выберите протокол для установки алгоритмов необходимые версии протоколов TLS, нажать на кнопку Применить, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно

Наименование	Описание
	последовательно добавить несколько версий протокола TLS.

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили SSL:

Наименование	Описание
Default SSL profile	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время. Данный профиль используется по умолчанию в: • Правилах инспектирования трафика SSL. • Для страницы авторизации Captive-портала. • Для страницы блокировки. • В веб-портале.
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется.
Default SSL profile (GOST)	Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов, например, для веб-портала. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется.
Default SSL profile (web console)	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль. Важно! Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!

Профили пересылки SSL

Профили пересылки SSL работают совместно с правилами инспектирования SSL и позволяют указать устройства, на которые необходимо отправить копию

расшифрованного трафика. Копия трафика будет отправлена в случае успешной расшифровки передаваемого трафика в соответствии с правилом инспектирования и выбранным профилем SSL.

Для создания профиля пересылки необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили пересылки SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля пересылки SSL.
Описание	Описание профиля пересылки SSL.
Тип пересылки	Доступные типы пересылки: • L2. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • L3 туннель: копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.
MAC-адрес назначения	MAC-адрес устройства, на которое необходимо переслать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.
Пересылать на интерфейс	Название интерфейса, на который необходимо пересылать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.
GRE IP-адрес источника	IP-адрес источника туннеля GRE. Параметр указывается при выборе типа пересылки L3.
GRE IP-адрес назначения	IP-адрес назначения туннеля GRE. Параметр указывается при выборе типа пересылки L3.

NIP объекты

Объекты NIP позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

i Примечание

После подключения к NGFW конечное устройство будет отправлять телеметрию с периодичностью в 1 минуту.

i Примечание

Для указания некоторых условий требуется наличие лицензированного модуля *Security Updates*, необходимого для скачивания обновлений библиотек.

Для добавления объекта необходимо указать:

Наименование	Описание
Название	Название объекта HIP.
Описание	Описание объекта HIP (опционально).
Версия ОС	Версия операционной системы устройства пользователя. При использовании операторов = и != необходимо указывать полную версию Windows.
Версия UserGate Client	Версия ПО UserGate Client.
Безопасность	Статусы компонентов безопасности конечного устройства: • Межсетевой экран; • Антивирус; • Автоматическое обновление; • BitLocker. Важно! BitLocker считается включенным, если он включен хотя бы на одном из дисков.
Продукты	Проверка соответствия программного обеспечения, установленного на конечном устройстве: • Антивирус. Проверка соответствия антивирусного ПО на устройстве пользователя. ◦ Включено: проверка статуса ПО (да, нет, не проверять); ◦ Базы антивируса обновлены: проверка актуальности баз (да, нет, не проверять) — производится только в случае, когда в предыдущем пункте включена проверка статуса антивируса в явном виде;

Наименование	Описание
	◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Межсетевой экран. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: ◦ Установлен: проверка наличия установленного ПО; ◦ Включено: проверка статуса ПО (да, нет, не проверять); ◦ Версия ПО; ◦ Вендор: производитель и название продукта; • Резервное копирование. Проверка ПО для резервного копирования: ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Шифрование диска. Проверка установленных на конечном устройстве программ для шифрования диска: ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • DLP. Проверка соответствия системы предотвращения утечек информации. ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Управление обновлениями. Проверка актуальности обновлений. ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта.
Процессы	Проверка процессов, запущенных на конечном устройстве.
Запущенные службы	Проверка служб, запущенных на конечном устройстве.
Ключи реестра	

Наименование	Описание
	Ключ реестра Microsoft Windows - каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце. • REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys).
Установленные обновления	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.

HIP-профили

Host Information Profile (HIP) позволяет производить сбор и анализ информации о степени защиты конечного устройства с установленным ПО UserGate Client. HIP профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). С использованием профилей HIP можно настроить гибкие политики доступа к зоне сети или приложению.

Примечание

Для проверки комплаенса и работы правил межсетевого экрана, в которых в качестве одного из условий указан профиль HIP, необходимо наличие лицензии на модуль *Контроль доступа в сеть на уровне МЭ*.

При создании профиля необходимо указать:

Наименование	Описание
Включено	Включение/отключение использования профиля. Если профиль используется в правилах межсетевого экрана, то в случае его выключения, он будет помечен серым цветом. Важно! В случае выключения профиля правило межсетевого экрана продолжает работать без условия проверки комплаенса.
Название	Название профиля HIP.
Описание	Описание профиля HIP (опционально).
Объекты HIP	Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP. Подробнее о создании объектов читайте в разделе Объекты HIP .

Примечание

Максимальное количество одновременно активных профилей не может превышать 32.

Профили BFD

BFD (Bidirectional Forwarding Detection) — протокол, работающий на уровне интерфейса и протокола маршрутизации и предназначенный для быстрого обнаружения сбоев между двумя соседними маршрутизаторами, включая интерфейсы, каналы передачи данных и механизмы пересылки.

BFD работает поверх любого протокола передачи данных (сетевой уровень, канальный уровень, туннели и т.д.), передаваемого между двумя системами. Пакеты BFD передаются в качестве полезной нагрузки инкапсулирующего протокола, который подходит для данной среды и сети. BFD может работать на нескольких уровнях в системе.

Маршрутизаторы с BFD отправляют пакеты друг другу с согласованной скоростью. Если пакеты от маршрутизатора, поддерживающего BFD, не поступают, то этот маршрутизатор объявляется неработающим. BFD передает

эту информацию соответствующим протоколам маршрутизации, и информация о маршрутизации обновляется. BFD помогает обнаружить односторонний отказ устройства и используется для быстрой конвергенции протоколов маршрутизации.

Профиль BFD — это конфигурация или набор параметров, используемых в протоколах динамической маршрутизации (BGP, OSPF), для определения работы функции обнаружения двунаправленной переадресации. Профиль обычно включает такие параметры, как желаемое время обнаружения, время удержания и другие параметры, определяющие скорость обнаружения и реагирования сетевых устройств на сбой в канале связи.

Настройка и использование профилей обеспечивают оперативное обнаружение сбоев в сети, что позволяет ускорить перенаправление трафика на интерфейсы и повысить надежность сети.

Настройка BFD для OSPF позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF.

В случае протокола BGP, BFD также может быть использован для регулирования времени обнаружения сбоев. Настройка BFD на более быстрое обнаружение неисправностей соединений позволяет оперативней реагировать и улучшать конвергенцию маршрутизации BGP.

Чтобы создать профиль BFD, необходимо в разделе **Библиотеки → Профили BFD** нажать **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля BFD
Описание	Опциональное описание профиля.
Определить множитель	Множитель времени обнаружения. Локальная система рассчитывает время обнаружения неисправностей соединения как произведение множителя времени обнаружения, полученного от удалённой системы, и согласованного интервала передачи удалённой системы. Если BFD не получит управляющий пакет до истечения времени обнаружения, то считается, что произошел сбой соединения. Например, если интервал передачи равен 300 мс, а множитель — 3, то локальная система будет обнаруживать сбои только через 900 мс отсутствия приёма пакетов.
Интервал приёма	Интервал приёма управляющих пакетов BFD (минимальное время, которое требуется между пакетами). Для определения интервала каждый из узлов сравнивает свой

Наименование	Описание
	интервал передачи с интервалом приема соседа — большее из двух значений принимается в качестве интервала передачи для этого узла. Значение по умолчанию — 50 мс.
Интервал передачи	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами. Значение по умолчанию — 50 мс.
Время получения echo	Минимальный интервал, через который система способна принимать echo-пакеты. Значение по умолчанию — 50 мс.
Время отправки echo	Минимальный интервал передачи, через который система будет способна отправлять echo-пакеты BFD. Значение по умолчанию — 50 мс.
Echo режим	Включение/отключение режима передачи Echo. По умолчанию этот режим отключён. Когда функция Echo активна, поток пакетов BFD Echo передается на удалённую систему, которая возвращает их обратно по тому же маршруту пересылки. Если некоторое количество пакетов Echo-потока данных не получено, сессия объявляется нерабочей. Echo-пакеты отличаются от control-пакетов (обычный режим) тем, что пакеты имеют адрес назначения равный адресу источника. Попадая на соседнюю систему, они проходят весь обычный транзитный путь, обеспечивая таким образом более полное тестирование работоспособности системы соседа. Учитывая специфику обработки и фильтрации пакетов в UserGate NGFW, для работы Echo-режима BFD необходимо создавать правило межсетевого экрана с разрешением соответствующего сервиса, иначе Echo-режим работать не будет. Например, для работы в Echo-режиме с Cisco IOS нужно создать сервис с разрешением UDP src port 49152 и dst port 3785.
Пассивный режим	Включение/отключение пассивного режима. При работе в пассивном режиме система ждёт управляющие пакеты от соседей и отвечает на них в случае их получения. Эта функция полезна, когда маршрутизатор выступает в роли центрального узла звездообразной сети, и требуется избежать отправки ненужных управляющих пакетов BFD. По умолчанию используется активный режим.

Наименование	Описание
	При работе в активном режиме узел отправляет управляющие пакеты соседнему узлу. Оба узла не могут работать в пассивном режиме; хотя бы один из них (или оба) должны работать в активном режиме.
Минимальное время жизни	Только для сеансов с несколькими переходами. Настройка минимального значения времени жизни (количество переходов), которое BFD будет принимать в управляющем пакете BFD. Может принимать значения от 1 до 254. Все пакеты с меньшим значением TTL будут отброшены. Установка данного значения необходима для ужесточения требований к проверке пакетов во избежание получения управляющих пакетов BFD от других сессий. Значение по умолчанию равно 254 (это означает, что ожидается только один переход между этой системой и аналогом).

Syslog-фильтры UserID агента

При использовании syslog в качестве источников событий UserGate производит фильтрацию событий в соответствии с указанными syslog-фильтрами UserID агента. Фильтры syslog представляют из себя стандартные Regexp выражения, которые пользователь может писать и сам. В стандартной поставке представлены три вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей по протоколу SSH в журналах syslog.
Unix PAM Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей посредством технологии Pluggable Authentication Modules (PAM) в журналах syslog.
UserGate WEC Agent	Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов. (Доступно начиная с релиза ПО 7.2.0).

Примечание

Используя правила Regexp, возможно написание дополнительных правил. Таким образом фильтры syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

Сценарии

Для чего нужны сценарии

UserGate NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря концепции SOAR (Security Orchestration, Automation and Response). NGFW реализует данную концепцию с помощью механизма сценариев. Сценарий является дополнительным условием в правилах межсетевого экрана, пропускной способности, контентной фильтрации, PBR, правилах защиты DoS, позволяя администратору настроить реакцию NGFW на определенные события, произошедшие за некое продолжительное время.

Примером работы сценария может быть задача по ограничению на определенное время пропускной способности для пользователя, который выбрал установленный лимит трафика.

Настройка сценариев

Для начала работы со сценариями необходимо выполнить следующие шаги:

1. Создать сценарий.
2. Применить созданный сценарий в правилах межсетевого экрана, пропускной способности, контентной фильтрации, PBR, правилах защиты DoS.

В веб-консоли администратора сценарии создаются в разделе **Библиотеки элементов → Сценарии**.

При создании сценария необходимо указать следующие параметры:

Свойства сценария

Общие | Условия

Включено: ☒

Название: Scenario1

Описание:

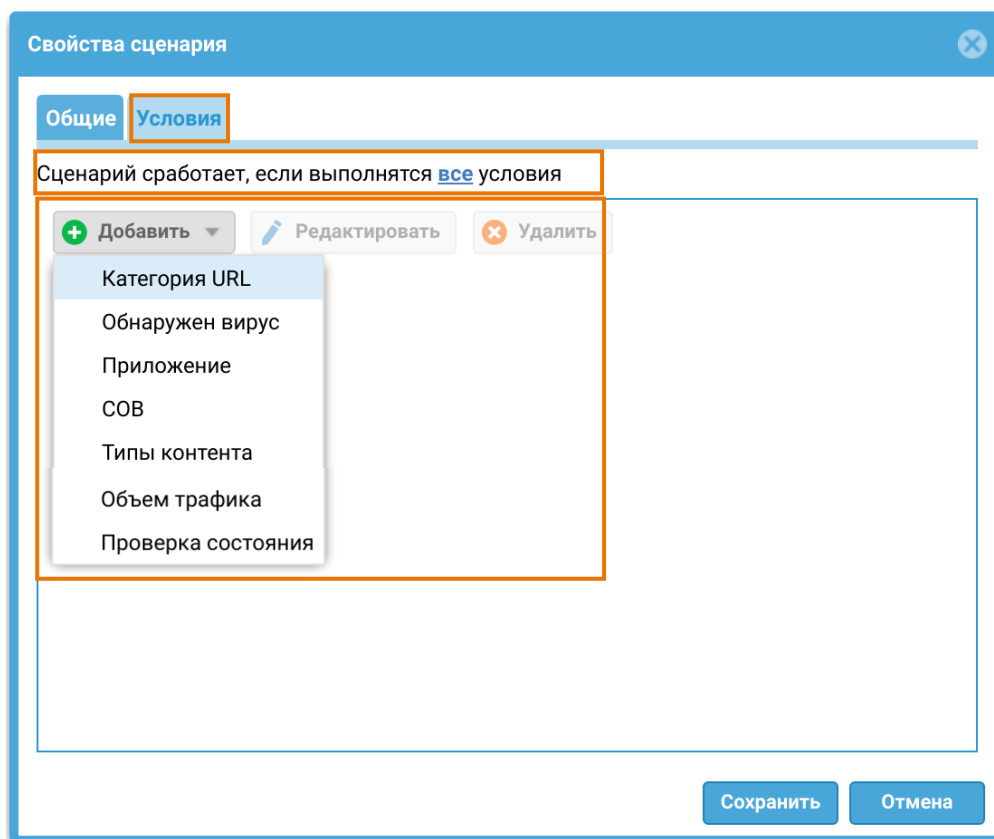
Применить для: одного пользователя

Продолжительность: 1 минут

Сохранить Отмена

- **Включено** — Включает или отключает сценарий.
- **Название** — Название сценария.
- **Описание** — Описание сценария.
- **Применить для** — Параметр, отвечающий за количество пользователей в правиле, к которым будет применен сценарий. Возможны варианты:
 - **Одного пользователя** — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий.
 - **Всех пользователей** — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в поле Пользователи/Группы правила.
- **Продолжительность** — длительность работы ограничивающего правила, в котором сработал сценарий.

На вкладке **Условия** задаются условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, то необходимо указать механизм срабатывания сценария — совпадение хотя бы одного из указанных условий, или всех условий.



Настройка условий срабатывания сценариев

Возможны следующие условия срабатывания для использования в сценарии:

- **Категория URL** — совпадения указанных категорий UserGate URL в трафике пользователя.
- **Обнаружен вирус** — факт обнаружения вируса.
- **Приложение** — обнаружено указанное приложение в трафике пользователя.
- **СОВ** — срабатывание системы обнаружения вторжений.
- **Типы контента** — обнаружены указанные типы контента в трафике пользователя.
- **Объем трафика** — объем трафика пользователя превысил определенный лимит за указанную единицу времени.
- **Проверка состояния** — проверка состояния какого-либо ресурса, который должен быть доступен с NGFW. Проверка может осуществляться с помощью команды icmp ping, запроса DNS или выполнения HTTP GET.

Категория URL

Условие срабатывания в данном случае является совпадения указанных категорий UserGate URL в трафике пользователя.

Выберите категории сайтов

Количество срабатываний:

0

За интервал:

0

Интервал времени в минутах

Добавить

Редактировать

Удалить

Название списка ↑	Владелец
 Threats	© UserGate

Создать и добавить новый объект

Необходимо наличие действующей лицензии Advanced Threat Protection для проверки

Проверить URL

Сохранить

Отмена

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор категорий сайтов из библиотеки элементов или создание списка с категориями сайтов из имеющихся в библиотеке элементов.
- **Проверить URL** — возможность проверки конкретного URL на соответствие той или иной категории.

Обнаружен вирус

Свойства сценария

Общие

Условия

Сценарий сработает, если выполнятся все условия

+

Добавить

Редактировать

×

Удалить

Обнаружен вирус

Сохранить

Отмена

Условием срабатывания в данном случае является обнаружение вируса в трафике пользователя.

Приложение

Условием срабатывания в данном случае является обнаружение определенных приложений в трафике пользователя.

Выберите приложения

Количество срабатываний:

0

За интервал:

0

Интервал времени в минутах

+

Добавить

✎

Редактировать

✕

Удалить

+

Добавить группу приложений 'Все приложения'

+

Добавить группы приложений

+

Добавить категории приложений

Создать и добавить новый объект

Найти:

Сохранить

Отмена

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор групп или категорий приложений из библиотеки элементов.

COB

Свойства сценария

Общие **Условия**

Сценарий сработает, если выполнятся **все** условия

+ Добавить ✎ Редактировать ✕ Удалить

Уровень угрозы COB: очень высокий

Уровень угрозы COB

Уровень угрозы: **очень высокий**

- очень высокий
- очень низкий
- низкий
- средний
- высокий
- очень высокий

Сохранить Отмена

Условием срабатывания в данном случае является детектирование системой COB угрозы определенного уровня.

Типы контента

Выберите типы контента

Количество срабатываний:

За интервал: Интервал времени в минутах

+ Добавить ✎ Редактировать ✕ Удалить

Название списка	Владелец
 Видео	© UserGate

Создать и добавить новый объект

Сохранить Отмена

В данном условии настраиваются следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор типов контента из библиотеки элементов.

Объем трафика

Условие срабатывания сценария по объему прошедшего трафика через NGFW.

Свойства сценария

Общие Условия

Сценарий работает, если выполняются все условия

+ Добавить ✎ Редактировать ✕ Удалить

Объем трафика достиг: 1 ГБ / день

Выберите ограничение объема трафика

Введите размер: 1 ГБ

Период: день

Сохранить Отмена

Сохранить Отмена

В данном условии настраиваются параметры:

- **Введите размер** — предельный объем трафика, прошедшего через NGFW, при котором сработает сценарий.
- **Период** — промежуток времени за который будет посчитан объем проходящего трафика.

Т.е. если будет выбран 5 ГБ за день, то при превышении 5 ГБ трафика пользователем за 1 день, сработает данный сценарий.

Проверка состояния

Условия срабатывания сценарии зависят от состояния сервера, запрос к которому идет с NGFW.

Возможны следующие методы проверки состояния сервера:

- Ping;
- DNS;
- HTTP GET.

Метод **Ping**.

Выберите тип проверки

Метод: ping

Адрес: 192.168.100.100

FQDN запроса:

Шлюз: По умолчанию

Результат: Отрицательный

Таймаут подключения, (сек): 2

Таймаут ответа, (сек):

Тип DNS запроса: a

Количество срабатываний: 0

За интервал: 0 Интервал времени в минутах

Сохранить

Отмена

В данном условии настраиваются следующие параметры:

- **Адрес** — IP-адрес для выполнения ICMP ping с NGFW.
- **Шлюз** — шлюз.
- **Результат** — отрицательный или положительный. Определяет, какой результат будет ожидаться от пинга сервера. Отрицательный — нет ответа по ping, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Метод **DNS**.

Выберите тип проверки

Метод: DNS

Адрес: 192.168.100.100

FQDN запроса: test.loc

Шлюз: По умолчанию

Результат: Отрицательный

Таймаут подключения, (сек): 4

Таймаут ответа, (сек):

Тип DNS запроса: a

Количество срабатываний: 0

За интервал: 0 Интервал времени в минутах

Сохранить

Отмена

В данном условии настраиваются следующие параметры:

- **Адрес** — это ip адрес DNS сервера, на который посылаем DNS запросы с NGFW.
- **FQDN запроса** — доменное имя сервера, которое разрешается в рамках проверки доступности.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.
- **Тип DNS-запроса** — тип DNS-запроса (a, aaaa, cname, ns, ptr).

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Тип HTTP GET

Выберите тип проверки

Метод:

HTTP GET

Адрес:

192.168.100.100

FQDN запроса:

test.loc

Шлюз:

По умолчанию

Результат:

Отрицательный

Таймаут подключения, (сек):

5

Таймаут ответа, (сек):

10

Тип DNS запроса:

a

Количество срабатываний:

0

За интервал:

0

Интервал времени в минутах

Сохранить

Отмена

В данном условии настраиваются следующие параметры:

- **Адрес** — домен для выполнения HTTP GET с NGFW.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидать от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — максимальное время, в течение которого клиент готов ждать ответа от сервера после успешного установления соединения.
- **Тайм-аут ответа** — тайм-аут ответа для проверки выполнением HTTP GET.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.

- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Пример использования сценариев

Как пример, сценарии могут использоваться в правилах межсетевого экрана для ограничения доступа в сеть, если происходит какое-либо событие, описанное в сценарии.

В данном примере реализуется следующий сценарий: для подключенных к NGFW узлов должно работать правило межсетевого экрана, блокирующее доступ в сеть на 5 минут, если на этом узле было скачано за 1 минуту 250 МБ трафика и более. В ином случае доступ в сеть через NGFW должен быть разрешен.

Создан сценарий с условием срабатывания по объему прошедшего трафика:

Сценарии				
+ Добавить ✎ Редактировать ✖ Удалить Включить Отключить Показать Все ↺				
Название	Описание	Продолжительность	Применить для	Условия
250Mb_per_min		5м	Триггер для одного пользователя	Сценарий сработает, если выполняются все условия Объем трафика достиг: 250 МБ / минута

В межсетевом экране создано блокирующее правило, в которое добавлен созданный сценарий:

Межсетевой экран										
+ Добавить ✎ Редактировать ✖ Удалить Переместить Копировать Включить Отключить 📄 Скопировать ID правила 🔍 Открыть логи										
✓										
#	С...	Название	Действие	Зона источн...	Адрес и...	Зона назначения	Адре...	Пользов...	Сервис	Сценарий
Локальные правила										
4	(...)	Block by traffic	🚫 Запретить	Trusted	Любой	Untrusted	Любой	Любой	Любой	250Mb_per_min
5	(...)	Allow all	✓ Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	—
По умолчанию										
6	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой	—

Верхнее блокирующее правило **Block by traffic** в межсетевом экране имеет более высокий приоритет по отношению к нижнему разрешающему правилу **Allow all**, но оно сработает только в случае срабатывания сценария по объему прошедшего трафика. В остальных случаях трафик будет разрешен правилом **Allow all**.

Теги

Тегами называются специализированные маркеры, которые могут назначаться объектам в веб-интерфейсе для удобства их отображения, группирования и фильтрации.

Примечание

Использование тегов доступно в версии 7.3.0 и выше.

В UserGate NGFW теги могут быть присвоены интерфейсам и всем типам правил — правилам межсетевого экрана, NAT и маршрутизации, пропускной способности, фильтрации контента, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, защиты почтового трафика, ICAP, защиты от DoS-атак, reverse-прокси, серверным и клиентским правилам VPN.

В веб-консоли администратора UserGate NGFW список всех созданных на устройстве тегов находится в **Библиотеке элементов**:

UserGate NGFW | Дашборд | Диагностика и мониторинг | Журналы и отчёты |

Библиотеки

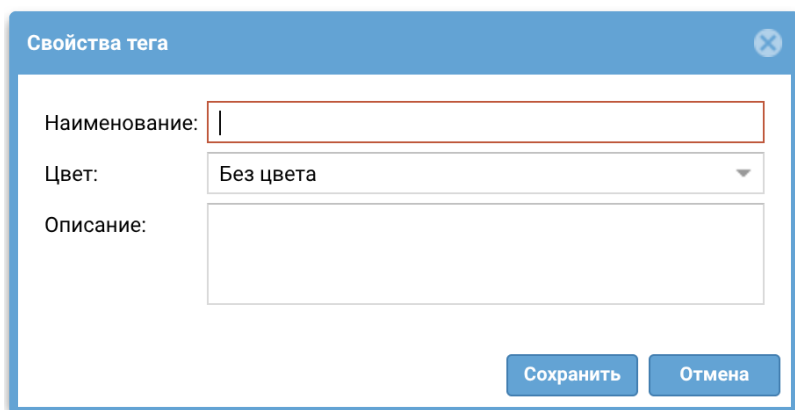
- Теги

Теги

 Добавить
  Редактировать
  Удалить
  Обновить

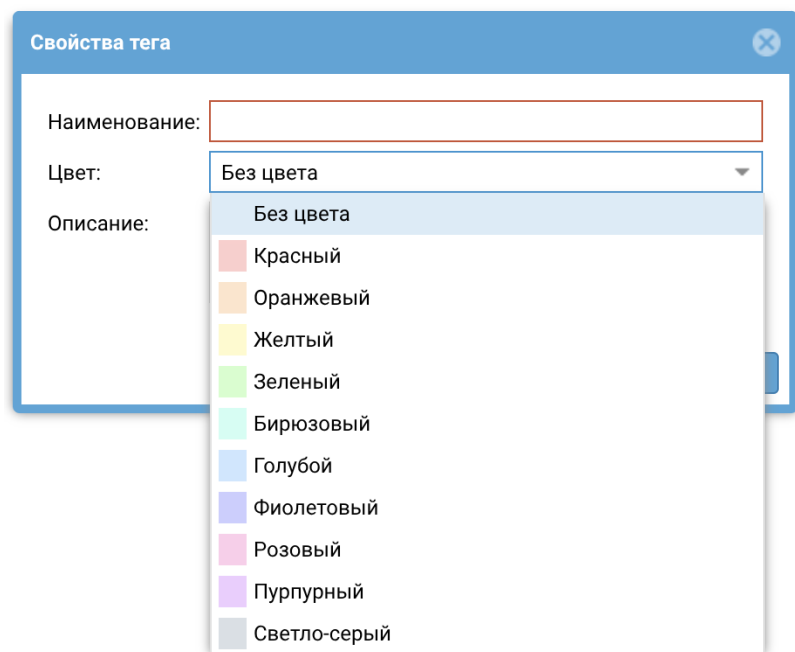
Наименование и цвет ↑	Описание
Tag 1	Test tag #1
Tag 2	Test tag #2
Tag 3	Test tag #3
Tag 4	Test tag #4
Tag 5	Test tag #5

Для создания нового тега нажмите **Добавить** и заполните поля настроек тега в окне свойств:



Укажите наименование тега. Оно может иметь не более 64 символов, начинаться с символа буквы или цифры, иметь в своём составе пробел и символы: , . () _ + - : / @.

При необходимости для тега можно выбрать цветовую маркировку из десяти имеющихся цветов:



Опционально добавьте описание создаваемому тегу.

Помимо библиотеки элементов теги можно создавать непосредственно в свойствах маркируемых объектов — интерфейсов или правил, выбрав в поле **Теги** опцию **Добавить новый Тег**. Откроется такое же диалоговое окно создания тега, как описано выше.

Пример создания тега непосредственно в свойствах правила межсетевого экрана:

Свойства правила межсетевого экрана

Общие

Источник

Пользователи

Назначение

Сервис

Время

НIP профили

Использование

История

Включено:

Название:

Теги:

Описание:

Действие:

Профиль приложений:

Профиль COB:

Отбросить и:

Сценарий:

Журналирование:

☒

Правило 1

Tag 1

Tag 2

Tag 3

Tag 4

Tag 5

Добавить новый тэг

Не выбран

Не использовать сценарии

Журналировать начало сессии

Теги могут присваиваться интерфейсам устройства. Каждому интерфейсу может быть присвоено множество тегов:

UserGate NGFW

Дашборд

Диагностика и мониторинг

Журналы и отчёты

Настройки

Гостевой портал

Интерфейсы

Добавить

Редактировать

Удалить

Включить

Отключить

Управление тегами

Показать Все

Тип	Название	Теги	Режим	IP интерфейса	MAC-адрес	Зона	MTU
Узел кластера:cluster							
Текущий Узел кластера:utmcore@nalonaspeest							
Сетевой адаптер	port0	Tag 1	DHCP	192.168.56.174/255.255.255.0	08:00:27:51:03:12	Management	1500
Сетевой адаптер	port1	Tag 2	Статический	10.10.0.1/255.255.255.0	08:00:27:06:27:0a	Trusted	1500
Сетевой адаптер	port2	Tag 4 Tag 5	Статический	172.16.1.0/255.255.255.0	08:00:27:12:19:bb	Untrusted	1500
Сетевой адаптер	port3	Tag 1 Tag 2 Tag 3 Ещё 2...	DHCP	10.0.3.23/255.255.255.0	08:00:27:7e:d9:33	Test Zone	1500

Теги могут присваиваться любым типам правил в NGFW. Пример использования тегов в правилах межсетевого экрана:

UserGate NGFW

Дашборд

Диагностика и мониторинг

Журналы и отчёты

Настройки

Гостевой портал

Admin

Py

Межсетевой экран

Управление тегами

Скопировать ID правила

Открыть логи

Все

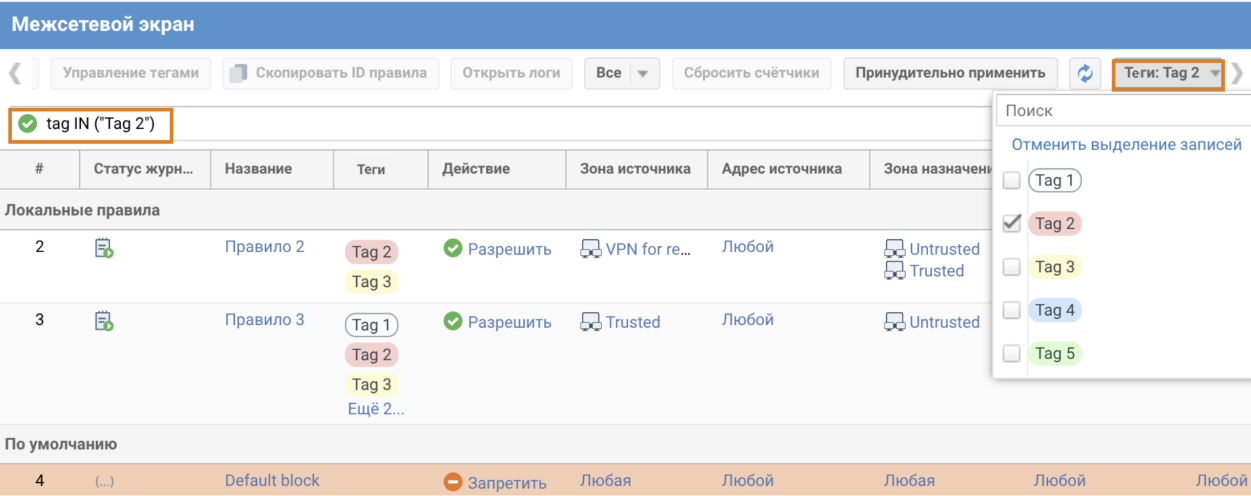
Сбросить счётчики

Принудительно применить

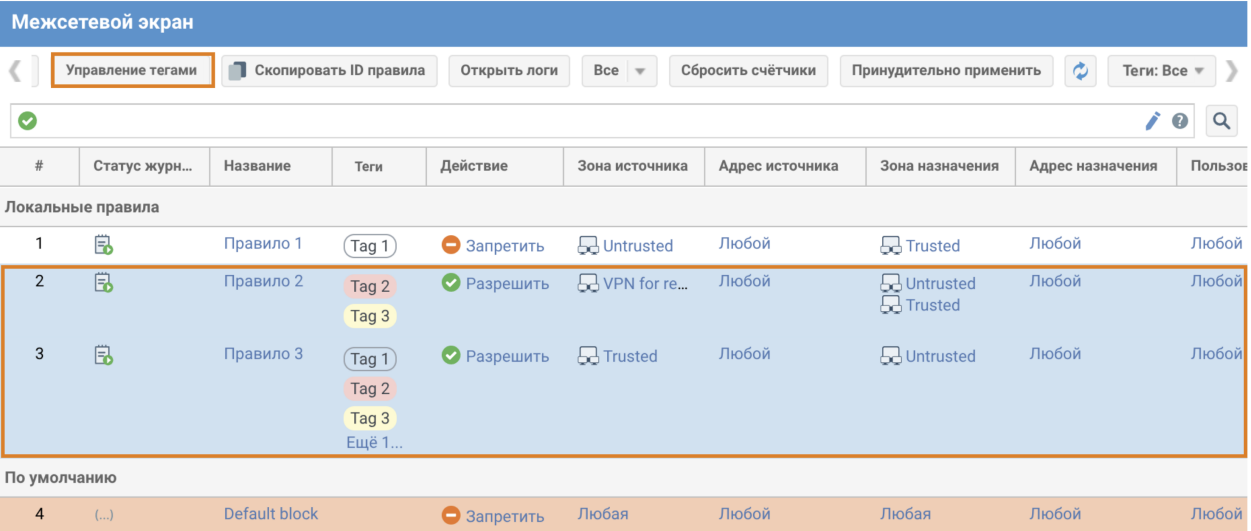
Теги: Все

#	Статус журн...	Название	Теги	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользов
Локальные правила									
1		Правило 1	Tag 1	Запретить	Untrusted	Любой	Trusted	Любой	Любой
2		Правило 2	Tag 2 Tag 3	Разрешить	VPN for re...	Любой	Untrusted Trusted	Любой	Любой
3		Правило 3	Tag 1 Tag 2 Tag 3 Ещё 2...	Разрешить	Trusted	Любой	Untrusted	Любой	Любой
По умолчанию									
4	(...)	Default block		Запретить	Любая	Любой	Любая	Любой	Любой

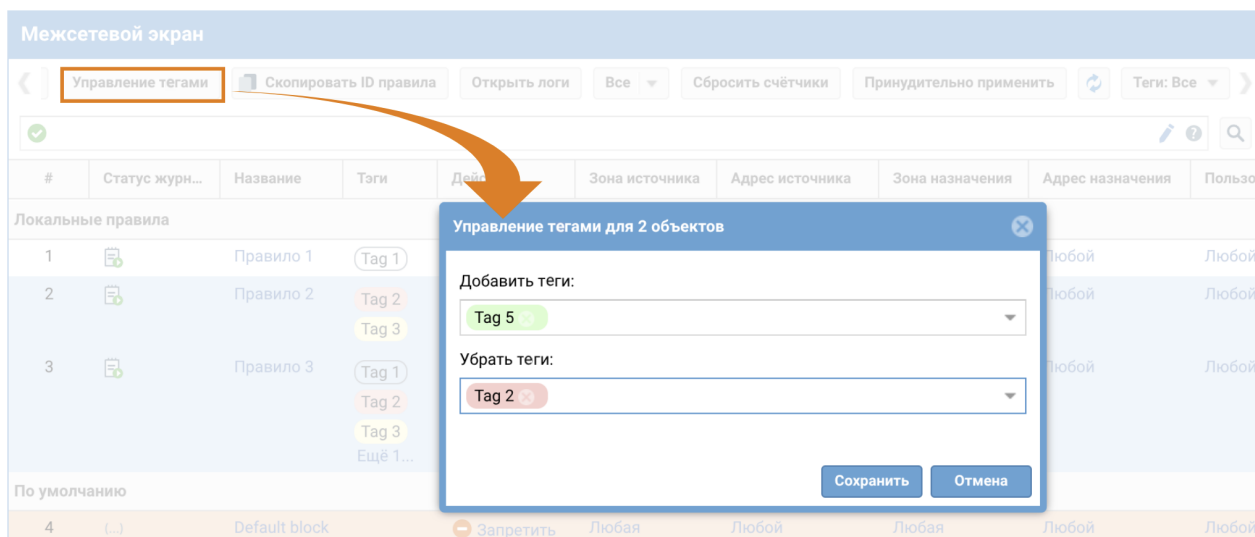
Благодаря использованию тегов объекты в веб-интерфейсе можно визуально группировать. Поддерживается фильтрация объектов в веб-интерфейсе по тегам как с помощью кнопки в меню инструментов, так и с помощью команд в строке поиска:



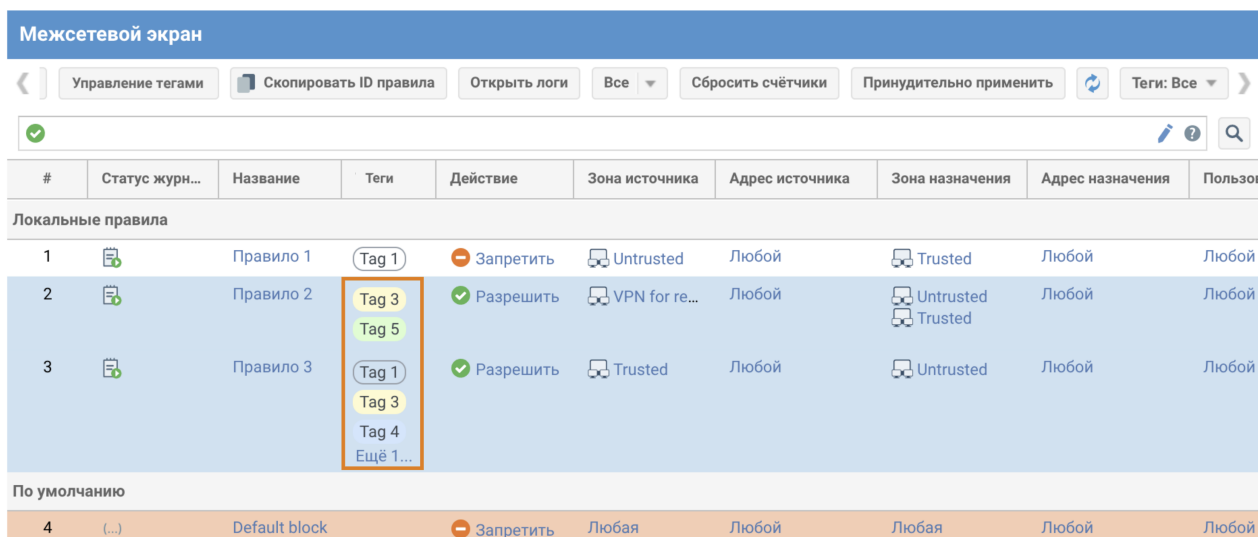
В разделах настроек правил или интерфейсов есть инструмент для групповой работы с тегами. При выделении сразу нескольких объектов становится активной кнопка **Управление тегами** в панели инструментов:



С помощью инструмента управления тегами можно добить и удалить теги множеству объектов одновременно:



Результат одновременного массового добавления и удаления тегов в правилах межсетевого экрана:



Работа с тегами также поддерживается в интерфейсе командной строки. Подробнее о работе с тегами в CLI читайте в статье [Настройка библиотек](#).

ДИАГНОСТИКА И МОНИТОРИНГ

Мониторинг трафика

Раздел **Мониторинг трафика** позволяет получить список всех пользовательских соединений, установленных через UserGate NGFW в реальном времени. Соединением считается уникальное сочетание адреса источника, адреса

назначения и пользователя (если определен). Для каждого соединения отображаются мгновенные значения скорости передачи (TX) и скорости приема (RX). Имеется возможность сортировки выводимых данных по каждому столбцу, а также возможность создать блокирующее правило межсетевого экрана или правило ограничения пропускной способности для выбранного из списка IP-адреса источника.

Примечание

Процесс построения данного отчета требует большего количества вычислительных ресурсов NGFW и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на МЭ.

Маршруты

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate и на определенном виртуальном маршрутизаторе на узле кластера. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **С** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **К** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **О** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **В** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

OSPF

Раздел **OSPF** позволяет получить отчет о состоянии канала маршрутизации. С использованием соответствующих фильтров можно отобразить информацию о протоколе на определенном узле UserGate и определенном виртуальном маршрутизаторе узла кластера. Представлена следующая информация:

- **protocol** — отображает информацию о параметрах, необходимых для настройки и функционирования OSPF на маршрутизаторах. (Router ID, настройки интерфейсов, области OSPF, маршруты, соседи OSPF, информация о пересылаемых OSPF сообщениях и состоянии интерфейсов, секреты аутентификации, параметры времени и таймаутов)
- **border-routers** — отображает записи таблицы маршрутизации OSPF для пограничного маршрутизатора зоны (ABR) и пограничного маршрутизатора автономной системы (ASBR).
- **database** — отображает информацию о состоянии и топологии сети, собранной протоколом OSPF. База данных хранит информацию о маршрутах, соседях, состояниях интерфейсов и других параметрах.
- **route** — отображает информацию о всех маршрутах в таблице маршрутизации OSPF.
- **neighbor** — отображает сведения о соседнем маршрутизаторе OSPF для каждого интерфейса. (Neighbor ID, приоритет, состояние, время жизни, интервал простоя, IP-адрес, интерфейс)

VPN

Раздел **VPN** отображает всех пользователей и все серверы, подключенные по VPN к данному серверу. Для каждого соединения отображается следующая информация:

- **Пользователь** — имя пользователя, под которым произошла аутентификация соединения.
- **Роль этого сервера** — клиент или сервер.
- **Время сессии** — продолжительность установленного соединения.
- **Туннельный IP** — адрес, назначенный данному клиенту в виртуальной частной сети.

- **IP-адрес** — адрес, с которого инициировано соединение VPN.
- **Geo IP** — страна по Geo IP, откуда установлено соединение.
- **Шифрование** — тип шифрования

Веб-портал

Раздел **Веб-портал** отображает всех пользователей и все серверы, подключенные через веб-портал к данному серверу. Для каждого соединения отображается следующая информация:

- **Имя** — имя пользователя, под которым произошла аутентификация соединения.
- **Начало сессии** — время, когда пользователь подключился к сервису.
- **Продолжительность** — продолжительность соединения.
- **IP источника** — IP-адрес пользователя.
- **Useragent** — useragent пользовательского браузера.

Можно задать период обновления данного окна от 3-х секунд до одной минуты или установить обновление вручную.

Администратор имеет возможность принудительно закрыть определённую сессию. Для этого надо выделить её и нажать кнопку **Заккрыть** сессию.

Заблокированные COB/L7 IP-адреса

COB отслеживает и блокирует атаки в режиме реального времени. Мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал мониторинга.

Раздел **Заблокированные COB/L7 IP-адреса** отображает список всех заблокированных IP-адресов. Кластерные узлы имеют одну общую таблицу **Заблокированных COB/L7 IP-адресов**.

Запись в журнале отображает:

- **Заблокированный IP-адрес** — отображает заблокированный IP-адрес, возможность разблокировать и удалить IP-адрес из списка.
- **Дата блокировки** — дата и время блокировки.
- **Угроза сигнатуры** — уровень угрозы.
- **Статус журналирования** — возможность перехода в раздел журналирования:
 - для приложений trafficlog;
 - для ips сигнатуры idpslog.
- **Свойство сигнатуры/название сигнатуры** — информация о сработавшей сигнатуре.
- **IP назначения** — адрес атакованного узла.
- **Продолжительность блокировки** — время блокировки.
- **Время для снятия блокировки** — отсчет оставшегося времени, окончание блокировки.

Для разблокирования заблокированных IP-адресов необходимо выделить их в списке и нажать кнопку **Разблокировать**.

Захват пакетов

Раздел **Захват пакетов** позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, wireshark. Это бывает необходимо для диагностирования сетевых проблем.

Раздел состоит из трех частей:

- **Фильтры** — здесь определяются условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть [по ссылке](#).

- **Правила** — в правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** — сюда помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Чтобы записать трафик, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимый фильтр.	Опционально. Можно воспользоваться предустановленными фильтрами или писать весь трафик, не фильтруя его.
Шаг 2. Создать правило.	Создать правило, в котором указать имя правила, имя файла, максимальный размер записываемого файла и необходимые фильтры.
Шаг 3. Выбрать необходимое правило и начать запись.	Выбрать необходимое правило и нажать на кнопку Начать запись . По окончании прекратить запись, нажав на кнопку Остановить запись .
Шаг 4. В разделе Файлы , скачать полученный файл.	Скачать рсар-файл для анализа.

Запросы в белый список

При блокировке сайтов с помощью правил контентной фильтрации пользователь получает страницу блокировки с указанием причины блокировки, на которой указаны имя правила, категория сайта и/или морфологическая база, черный список, из-за которых сайт был заблокирован. Кроме этого, страница блокировки предлагает пользователю сделать запрос на добавление данного сайта в белый список в случае, если пользователь не согласен с блокировкой ресурса. При нажатии на кнопку **Добавить в белый список** запрос на добавление появляется в списке запросов в разделе **Запросы в белый список**. Администратор может осуществить следующие действия с запросом пользователя:

Наименование	Описание
Добавить в белый список	Добавить данный URL в белый список. Администратору будет предложено изменить URL и выбрать белый список, в который необходимо добавить данный ресурс.

Наименование	Описание
Удалить	Удалить данный запрос из списка запросов.
Отклонить URL	Добавить запрошенный URL в список отклоненных запросов. При последующих блокировках данного URL страница блокировки не будет содержать кнопки Добавить в белый список . Список отклоненных доменов и URL отображается в Окне отклоненных запросов .
Отклонить домен	Добавить домен запрошенного URL в список отклоненных запросов. При последующих блокировках любого URL данного домена страница блокировки не будет содержать кнопки Добавить в белый список . Список отклоненных доменов и URL отображается в Окне отклоненных запросов .

Администратор может проверить категорию интернет-ресурса с помощью формы **Проверить URL**. В случае, если ресурс относится к некорректной категории, администратор может сделать запрос на смену категории или изменить категорию самостоятельно локально на своем устройстве.

Для того, чтобы сделать запрос на смену категории, необходимо нажать на кнопку **Предложить категорию**. Запрос на смену категории будет отправлен в компанию UserGate, где будет проверен, и в случае подтверждения будет внесен в ближайшее обновление базы категорий сайтов UserGate URL filtering.

Для того, чтобы сменить категории локально, необходимо нажать на кнопку **Изменить категорию** и назначить до двух новых категорий. Посмотреть все сайты с измененными категориями можно в разделе **Библиотеки → Измененные категории URL**. При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями - **Переопределенные пользователем категории**. Более подробно об изменении категорий для определенных сайтов описано в разделе руководства [Запросы в белый список](#).

Трассировка правил

С помощью трассировки правил администратор может посмотреть, какие правила срабатывают при обработке пользовательских HTTP(S)-запросов. Это может быть полезно при определении проблем с доступом к определенным сайтам.

Чтобы выполнить трассировку правил:

1. На странице **Диагностика и мониторинг** в разделе **Трассировка правил** нажмите **Настроить** и укажите параметры фильтра диагностической информации:

- **Строка** — строка в запросе пользователя, например имя домена, URL, правила контентной фильтрации.
- **Пользователь** — пользователь, обработку запросов которого необходимо продиагностировать.
- **IP-адрес источника** — IP-адрес, с которого пользователь выполняет запрос.
- **IP-адрес назначения** — IP-адрес веб-сервиса, которому направлен запрос.

Примечание

Если фильтр не настроен, то могут быть также отображены результаты обработки запросов других пользователей.

2. Сохраните изменения.

3. Нажмите **Начать**.

4. Попросите пользователя открыть проблемный сайт и посмотрите, какие правила срабатывают при открытии сайта. Будут указаны все правила, которые выполняются во время обработки пользовательского запроса.

Примечание

При трассировке отображаются сработавшие правила ICAP, инспекции SSL и контентной фильтрации.

Администратор может проверить содержание отображаемого в трассировке интернет-ресурса с помощью формы **Открыть сайт**. С помощью формы **Добавить в белый список** администратор может поместить выбранный ресурс в один из существующих в системе списков URL.

Ping

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать timestamp	Добавляет timestamp в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	С какого сетевого интерфейса выполнять команду.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

LLDP-соседи

В разделе **Диагностика и мониторинг** → **Сеть** → **LLDP-соседи** отображается список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. Подробнее о настройке отправки данных по протоколу LLDP — в разделе «[Настройка интерфейсов](#)».



Примечание

Отображение LLDP-совместимых устройств доступно, только когда в разделе «Настройки» → «Usergate» → «Настройки» включен модуль «Настройка LLDP».

Параметр	Описание
Chassis ID	Идентификатор шасси; является обязательной TLV-записью LLDP-кадра. У каждого устройства UserGate есть только один Chassis ID. В качестве Chassis ID используется MAC-адрес интерфейса управления
SysName	Имя системы.
SysDescr	Описание системы, содержит информацию об оборудовании и операционной системе устройства
Management	Адрес соседнего устройства. Содержит информацию: • IP-адреса интерфейса управления (IPv4 и IPv6). • Номер интерфейса указанного адреса управления

Параметр	Описание
Capability	Функции устройства (например, маршрутизатор, коммутатор и т.п.)
Port ID	Идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit); является обязательной TLV-записью LLDP-кадра. В качестве идентификатора используется MAC-адрес интерфейса
PortDescr	Описание порта
TTL	Время жизни передаваемых пакетов LLDP; является обязательной TLV-записью LLDP-кадра. TTL задаётся в разделе UserGate → Настройки → Модули в поле Настройка LLDP

Статистика LLDP

Данная вкладка отображает статистику интерфейсов, в настройках которых был указан профиль LLDP. Отображается следующая информация:

Наименование	Описание
Interface	Название интерфейса.
Transmitted	Общее количество кадров LLDP, переданных через интерфейс.
Received	Общее количество кадров LLDP, полученных на интерфейсе.
Discarded	Число полученных на этом интерфейсе кадров LLDP, которые были отброшены.
Unrecognized	Количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе.
Ageout	В каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется.
Inserted	Количество добавлений записей с информацией о соседях LLDP.

Наименование	Описание
Deleted	Количество удалений записей о соседях LLDP.

ОПОВЕЩЕНИЯ

Правила оповещений

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или отправке пароля пользователю по SMS. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения.	Смотрите раздел Профили оповещений .
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов .
Шаг 3. Создать правило оповещения.	Во вкладке Диагностика и мониторинг в разделе Оповещения → Правила оповещений добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.

Наименование	Описание
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

SNMP

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SNMP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.
2. Создать правило SNMP

Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Название правила	Название правила.

Наименование	Описание
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
Комьюнити	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
События	Выбор типов параметров, доступных для мониторинга по правилу.



Примечание

Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования — в профиле безопасности SNMP) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Актуальные mib-файлы UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого необходимо перейти на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения → SNMP** нажать **Скачать MIB**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.
- UTM-TEMPERATURE-MIB.

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на "not_clean".
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.

Наименование	Описание
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружение атаки системой COB.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора (95%).
trapLowMemory	Высокая загрузка памяти (95%).
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загрузке $\geq 95\%$ за 5 минут хотя бы на одном из дисковых устройств.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.
trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C .

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	integer	

Наименование	Тип данных	Описание
		Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmDataPartionFSStatus	integer	Состояние файловой системы. • 0 — clean. • 1 — not clean.
utmHASStatus	integer	Текущий статус узла кластера отказоустойчивости: • 0 — master-узел. • 1 — slave-узел. • 3 — fault.
utmHASStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • 1 — связь с узлом потеряна. • 2 — HTTP прокси-сервер недоступен. • 3 — ни один из шлюзов недоступен. • 4 — DNS-сервер недоступен. • 5 — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора (%).
utmMemory	integer	Использование оперативной памяти (%).
utmLogdiskSpace	integer	

Наименование	Тип данных	Описание
		Пространство на диске, используемое под журналы (%).
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • no_raid • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • 2 — partialDegraded — полный или частичный выход из строя одного из дисков.

Наименование	Тип данных	Описание
		• 3 — failed — не работает из-за наличия ошибки. • 4 — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: • 1 — один блок питания. • 2 — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: • no_power_supplies. • 0 — off. • 1 — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • 1 — кабель подключен. • 2 — кабель не подключен.
utmDiskIOUtilization	integer	Текущая утилизация диска (%).
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.
utmThermSensor	string	Название температурного сенсора.
utmThermValue	integer	Значение температуры, измеренное сенсором.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается фактическое число загруженных виртуальных процессоров.
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)
tcpsessionsCounter	integer	Количество активных TCP сессий на текущий момент времени. (*)
udpsessionsCounter	integer	Количество активных UDP сессий на текущий момент времени. (*)
icmpsessionsCounter	integer	Количество активных ICMP сессий на текущий момент времени. (*)
sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд. (*)
sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее

Наименование	Тип данных	Описание
		значение за последние 60 секунд. (*)
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	

Наименование	Тип данных	Описание
		Общее количество HTTP запросов. (*)
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы.
haStatus	integer	Текущее состояние узла кластера.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
powerSupply1Status	string	Состояние первого источника питания: • no_power_supplies. • on. • off.
powerSupply2Status	string	Состояние второго источника питания: • no_power_supplies. • on. • off.
raidType	string	Тип RAID массива.
raidStatus	string	

Наименование	Тип данных	Описание
		Текущий статус RAID (Redundant Array of Independent Disks): • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.
diskIOUtilization	integer	Текущая утилизация диска (%).
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд.
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд.

Примечание

Метрики, отмеченные в описании символом (*) не актуальны для UGMC и LogAn.
Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.

Наименование	Тип данных	Описание
ifDescr	string	Информация об интерфейсе, которая может включать в себя название производителя, имя продукта, аппаратную версию интерфейса.
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • 1 — other — неизвестный тип. • 2 — regular1822 — определён в BBN Report 1822. • 3 — hdh1822 — определён в BBN Report 1822. • 4 — ddn-x25 — определён в BBN Report 1822. • 5 — определён в стандарте канального уровня сетевой модели OSI X.25. • 6 — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • 7 — iso88023-csmacd — определён в IEEE 802.3. • 8 — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • 9 — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.

Наименование	Тип данных	Описание
		• 10 — iso88026-man — определён в стандарте ISO 88026 "MAN". • 11 — starLan — определён в стандарте IEEE 802.3e. • 12 — proteon-10Mbit — Proteon 10 Mbit • 13 — proteon-80Mbit — Proteon 80 Mbit. • 14 — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • 15 — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • 16 — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • 17 — sdlc — протокол канального уровня для системной сетевой архитектуры IBM. • 18 — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1 • 19 — e1 — европейский аналог T1. • 20 — basicISDN — для связи аппаратуры абонента и ISDN-станции.

Наименование	Тип данных	Описание
		• 21 — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • 22 — propPointToPointSerial — определён в стандарте RFC1213. • 23 — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • 24 — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • 25 — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • 26 — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • 27 — nsip — XNS over IP — предназначен для использования в разнообразных

Наименование	Тип данных	Описание
		средах передачи данных. • 28 — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 29 — ultra — ULTRA Technologies. • 30 — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • 31 — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 32 — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	

Наименование	Тип данных	Описание
		Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • 1 — up — готов для передачи пакетов. • 2 — down — не работает. • 3 — testing — в режиме тестирования; рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: • 1 — up — интерфейс готов для передачи пакетов. • 2 — down — интерфейс не может передавать пакеты данных. • 3 — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. • 4 — unknown — интерфейс находится в неизвестном состоянии. • 5 — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. • 6 — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего

Наименование	Тип данных	Описание
		компонента, обычно аппаратного. • 7 — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.

Наименование	Тип данных	Описание
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передаче. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Длина выходной очереди (в пакетах).
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.

Наименование	Тип данных	Описание
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOctets	counter64	Смысл одинаков со смыслом объекта ifOutOctets — количество байтов, переданное данным

Наименование	Тип данных	Описание
		интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOOutUcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled — включено. • 2 — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.

Наименование	Тип данных	Описание
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • 1 — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • 2 — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров.
ifAlias	string	Название интерфейса, заданное администратором при настройке интерфейса.
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса.

UTM-TEMPERATURE-MIB

Наименование	Тип данных	Описание
termNumber	integer	Количество температурных сенсоров на данной платформе.
thermLowerThreshold	integer	Нижний предел рабочей температуры.
thermUpperThreshold	integer	Верхний предел рабочей температуры.
thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry).

Наименование	Тип данных	Описание
thermEntry	sequence	Информация о конкретном сенсоре: • thermName (string) — название сенсора. • thermValue (integer) — показание сенсора. • thermUnit (string) — единица измерения показаний сенсора.

Примечание

Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание

Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учётом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

Данный раздел используется для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP. Параметры SNMP задаются для каждого узла индивидуально.

Наименование	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP.
SNMP локация системы	Информация о физическом расположении SNMP-агента.

Наименование	Описание
SNMP описание системы	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text. Engine ID может быть сформирован в формате: • IPv4 (ip4). • IPv6 (ipv6). • MAC-адрес (mac). • Текст (text). • Октеты (octets).

Профили безопасности SNMP

В данном разделе производится настройка профилей безопасности для аутентификации SNMPv3-менеджера.

Примечание

Настройки аутентификации для SNMP v3 (имя пользователя, пароль, тип и алгоритм аутентификации, алгоритм и пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate

Наименование	Описание
Название	Название профиля безопасности SNMP
Описание	Описание профиля безопасности SNMP
Пользователь	Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv).

Наименование	Описание
	• С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: • SHA1; • MD5; • SHA224; • SHA256; • SHA384; • SHA512.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.

ЖУРНАЛЫ И ОТЧЕТЫ

ЖУРНАЛЫ

Общие сведения

UserGate NGFW регистрирует события, возникающие в процессе его функционирования, и сохраняет их в следующих журналах:

- **Журнал событий** — содержит события, связанные с изменением параметров UserGate NGFW, авторизацией пользователей, обновлениями различных списков и т. п.

- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate NGFW.
- **Журнал DNS** — содержит события, связанные с DNS-трафиком.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, правил подмены портов и правил маршрутизации на основе политик (PBR). Для регистрации этих событий необходимо включить функцию журналирования в соответствующих правилах.
- **Журнал COB** — содержит события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации этих событий необходимо включить функцию журналирования.
- **История поиска** — содержит сведения о поисковых запросах пользователей в популярных поисковых системах.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в параметрах которых включена функция журналирования.
- **Агент UserID** — содержит описание событий, отражающих результат работы UserID-агента.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных отображаются в журнале событий. В случае, если узел интегрирован с UserGate Log Analyzer, записи будут отображаться в журнале событий UserGate Log Analyzer. Ротация записей журнала событий никогда не производится.

Примечание

В релизе 7.5.0 и выше при изменении имени узла в настройках кластера конфигурации его новое имя будет отображаться как в веб-консоли, так и во всех журналах и отчетах.

Журнал событий

Журнал событий отображает события, связанные с изменением настроек NGFW, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал или VPN, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал веб-доступа

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).

- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User-agent браузер.

i Примечание

В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик после срабатывания всех правил на этом запросе.

Если правила требуют анализа ответа от веб-сервера, то трафик ответа также будет подсчитан и учтён одинаковый, в том числе у первого сработавшего на этом запросе правила (bypass captive, decrypt). Таким образом, учитывается весь прошедший трафик и указывается одно и то же значение каждому правилу, сработавшему на этом запросе.

Если анализ ответа от веб-сервера для правил не требуется, то весь остальной трафик не учитывается.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал DNS

Журнал DNS отображает события, связанные с DNS трафиком. Для журналирования событий DNS на NGFW должна быть включена DNS-фильтрация в настройках DNS-прокси и разрешено журналирование в правилах контентной фильтрации, в которые будет попадать DNS трафик.

Отображается следующая информация:

- Узел.
- Время.
- Пользователь.
- Правило.

- Причины.
- Имя домена.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Сетевой протокол.
- Категория URL.
- Информация.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал трафика

Журнал трафика отображает события срабатывания правил межсетевого экрана и правил NAT, в настройках которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.

- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.
- NAT IP-адрес источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP-адрес назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов отправлено/получено.

i Примечание

В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила. Если в настройках журналирования в правиле выбрано: “Журналировать каждый пакет”, то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.

Если в настройках журналирования в правиле выбрано: “Журналировать начало сессии”, будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал СОВ

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел NGFW, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие.

- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал инспектирования SSH

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH, для которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.

- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

История поиска

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на

любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал защиты почтового трафика

Журнал защиты почтового трафика отображает события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время срабатывания.
- Пользователь.
- Отправитель.
- Получатель
- Правило.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Приложение.
- Протокол прикладного уровня.

- Байт отправлено/получено.
- Пакетов отправлено/получено.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

UserID-агент

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные UserID агентом с помощью коннектора "Microsoft Active Directory" с серверов AD. В журнале отображаются события с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). В журнале отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, которым зафиксировано событие.
Время	Время произошедшего события.
Запись журнала событий конечных устройств	Ссылка на событие.
Конечное устройство\сенсор	UserID конектор.
Уровень лога	Поле "Keywords" из журнала AD.
Данные	Содержание события из журнала AD.

Наименование	Описание
Источник журнала событий	Поле "Источник" из журнала AD.
Категория журнала	Код категории инцидента (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и тд)
Категория инцидента	Поле "Тип задачи" из журнала AD
Имя компьютера	узел Windows на котором произошло событие.
Пользователь	Поле "Пользователь"из журнала AD.
Код события лога	Поле "Код события" из журнала AD (EventCode).
Идентификатор события лога	Поле "Идентификатор события" из журнала AD (EventID).
Тип события лога	Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.).
Файл журнала лога	файл журнала Windows.

Syslog (Журнал)

Журнал Syslog отображает события, собранные UserID агентом с помощью коннектора "Отправитель syslog" с серверов-источников данных syslog. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отобрана следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.
Запись журнала syslog	Ссылка на событие.
Правило	Правило под которое попало Syslog сообщение.
Критичность	Уровень события Syslog.
Объект	Представление процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и тд)
Имя компьютера	Имя компьютера на котором произошло событие.

Наименование	Описание
Приложение	Приложение вызвавшее событие.
Идентификатор процесса	PID процесса вызвавшего событие.
Данные	Описание события.

UserID (Журнал)

Журнал UserID содержит описание событий отражающие результат работы UserID агента. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.
Содержание события	Открыть подробное описание события.
Действие	Действие примененное к событию.
Источник логов	Источник полученного события.
Пользователь	Пользователь UG, который вызвал событие.
IP-адрес	IP-адрес узла на котором произошло событие.
Информация	Описание события.

RADIUS (Журнал)

Журнал RADIUS отображает события, собранные UserID агентом с помощью коннектора "RADIUS" из данных RADIUS accounting. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.

Наименование	Описание
Идентификатор правила	Идентификатор правила, срабатывание которого создало событие
Пользователь	Пользователь, который вызвал событие.
Группы	Строка групп в которых состоит пользователь.
Статус	Статус пользователя.
IP источника	IP-адрес источника, откуда пришло сообщение.
IP адрес NAS	IP-адрес NAS, авторизовавшего пользователя.
IP-адрес пользователя	IP-адрес пользователя (framed ip address).

Экспорт журналов

Функция экспортирования журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал COB.
- Журнал трафика.
- Журнал инспектирования SSH.
- Журнал DNS.
- Журнал почтового трафика.
- Журнал UserID.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

i Примечание

Если в настройках указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Оptionальное поле для описания правила.
Параметры разового экспорта	Выбор диапазона экспорта журналов. Опция доступна в версии ПО 7.2.0 и выше.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал COB. • Журнал трафика. • Журнал инспектирования SSH. • Журнал DNS. • Журнал почтового трафика. • UserID. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • CEF Compact. • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.

Наименование	Описание
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения.
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6.

Наименование	Описание
	• Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а

Наименование	Описание
	выражение <code>"*/2"</code> в поле "часы" будет означать "каждые два часа".
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.

Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. NGFW предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требуется полного совпадения значения поля указанному значению, например, <code>ip=172.16.31.1</code> будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, <code>ip!=172.16.31</code> будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равно указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, <code>portSource</code> , <code>portDest</code> , <code>statusCode</code> и т.п., например, <code>date<='2019-03-28T20:59:59' AND statusCode=303</code>
>=	Больше либо равно. Значение поля должно быть больше либо равно указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, <code>portSource</code> , <code>portDest</code> , <code>statusCode</code> и т.п., например, <code>date>='2019-03-13T21:00:00' AND statusCode=200</code>
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, <code>portSource</code> , <code>portDest</code> , <code>statusCode</code> и т.п., например, <code>date < '2019-03-28T20:59:59' AND statusCode=404</code>
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, <code>portSource</code> , <code>portDest</code> , <code>statusCode</code> и т.п., например, <code>(statusCode>200 AND statusCode<300) OR (statusCode=404)</code>

Наименование	Описание
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH '{"module":"threats"}' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH '{"module":"threats"}' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

При составлении расширенного запроса NGFW показывает возможные варианты названия полей, применимых к ним операторов и возможных

значений, облегчая оператору системы формирование сложных запросов. Список полей и их возможных значений может отличаться для каждого из журналов.

При переключении режима поиска с основного на расширенный NGFW автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Описание форматов журналов

Экспорт журналов в формате CEF

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 1 — информационные; • 4 — предупреждения; • 7 — ошибки; • 10 — критичные.

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Тип события.	login_successful
	suser	Имя пользователя.	Admin
	src	IPv4-адрес источника.	192.168.117.254
	cat	Компонент, в котором произошло событие.	console_auth
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"name": "MIME_BUILTIN_COMPOSITE", "module": "nlist_import"}

Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id": 39, "name": "Social Networking", "threat_level": 3}
	proto	Используемый протокол 4-го уровня.	TCP
	app	Протокол прикладного	HTTP/1.1

Тип поля	Название поля	Описание	Пример значения
		уровня и его версия.	
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0

Тип поля	Название поля	Описание	Пример значения
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для	Destination Zone

Тип поля	Название поля	Описание	Пример значения
		индикации зоны назначения.	
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в	3

Тип поля	Название поля	Описание	Пример значения
		направлении источник — назначение.	
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302

Формат журнала веб-доступа **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10

Тип поля	Название поля	Описание	Пример значения
			(установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id": 39, "name": "Social Networking", "threat_level": 3}
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0

Тип поля	Название поля	Описание	Пример значения
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	flexString1Label	Поле указывает на категорию	URLCats

Тип поля	Название поля	Описание	Пример значения
		запрашиваемого URL-адреса.	
	flexString1	Категория URL.	Computers & Technology
	cn1Label	Поле указывает исходный ответ сервера.	Response
	cn1	Код ответа HTTP.	302

Примечание

Общее правило для компактного формата — значения некоторых полей обрезаются по длине до 80 символов. Например, список url-категорий, url, имя пользователя, имя правила, имя зоны, и т.д.

Формат журнала DNS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	block
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id": 37,"name":"Search Engines & Portals","threat_level":1}]}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country

Тип поля	Название поля	Описание	Пример значения
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания передаваемых данных.	Data
	cs6	Передаваемые данные.	<pre>{ "question": [{ "domain": "google.com", "type": "A", "class": "IN" }], "answer": [{ "domain": "google.com", "type": "TXT", "class": "IN", "ttl": 5, "data": "Blocked" }, { "domain": "google.com", "type": "A", "class": "IN", "ttl": 5, "data": "10.10.0.1" }] }</pre>
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories

Тип поля	Название поля	Описание	Пример значения
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала DNS **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	act	Действие, принятое устройством в соответствии с	block

Тип поля	Название поля	Описание	Пример значения
		настроенными политиками.	
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id": 37,"name":"Search Engines & Portals","threat_level":1}]}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS об

Тип поля	Название поля	Описание	Пример значения
			ычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Поле используется для указания передаваемых данных.	Data
	cs4	Передаваемые данные.	{ "question": [{ "domain": "google.com", "type": "A", "class": "IN" }], "answer": [{ "domain": "google.com", "type": "TXT", "class": "IN", "ttl": 5, "data": "Blocked" }, { "domain": "google.com", "type": "A", "class": "IN" }] }

Тип поля	Название поля	Описание	Пример значения
			":IN","ttl":5,"data":"10.10.0.1"]}] }
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21

Тип поля	Название поля	Описание	Пример значения
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1		

Тип поля	Название поля	Описание	Пример значения
		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent

Тип поля	Название поля	Описание	Пример значения
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный

Тип поля	Название поля	Описание	Пример значения
			уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08

Тип поля	Название поля	Описание	Пример значения
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)

Тип поля	Название поля	Описание	Пример значения
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted

Формат журнала COV

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Формат журнала COB **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example

Формат журнала инспектирования SSH

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app		SSH или SFTP

Тип поля	Название поля	Описание	Пример значения
		Протокол прикладного уровня.	
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для	Source Country

Тип поля	Название поля	Описание	Пример значения
		указания страны источника.	
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала инспектирования SSH **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source		ssh

Тип поля	Название поля	Описание	Пример значения
		Название журнала.	
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	

Тип поля	Название поля	Описание	Пример значения
			Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Указание на команду, передаваемую по SSH.	Command

Тип поля	Название поля	Описание	Пример значения
	cs4	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала защиты почтового трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einersonstal
	act	Действие, выполненное устройством в	mark

Тип поля	Название поля	Описание	Пример значения
		соответствии с настроенными политиками.	
	app	Протокол прикладного уровня.	SMTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule

Тип поля	Название поля	Описание	Пример значения
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	Source Zone
	cs2	Зона источника.	Untrusted
	cs3Label	Поле используется для индикации страны источника трафика.	Source Country
	cs3	Страна источника трафика.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения трафика.	Destination Zone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для индикации страны назначения трафика.	Destination Country
	cs5	Страна назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания почтового адреса получателя.	To

Тип поля	Название поля	Описание	Пример значения
	cs6	Email получателя.	receiver@example.com
	flexString1Label	Поле используется для указания почтового адреса отправителя.	From
	flexString1	Email отправителя.	sender@example.com
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1

Формат журнала защиты почтового трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einersonstal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark
	app	Протокол прикладного уровня.	SMTP
	suser	Имя пользователя.	user_example (Unknown, если

Тип поля	Название поля	Описание	Пример значения
			пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	SrcZone

Тип поля	Название поля	Описание	Пример значения
	cs2	Зона источника.	Untrusted
	cs4Label	Поле используется для указания зоны назначения трафика.	DstZone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для указания почтового адреса отправителя.	From
	cs5	Email отправителя.	sender@example.com
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com

Формат журнала Windows Active Directory

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	endpoint_log
	Name	Тип источника.	log

Тип поля	Название поля	Описание	Пример значения
	Threat Level	Уровень угрозы.	Может принимать значения от 1 до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	suser	Имя пользователя.	user1.dep.local
	msg	Описание события в журнале AD.	Group membership information Subject: Security ID: S-1-0-0 Account Name: — Account Domain: — Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-21-379587013 3-5220325-2125745 684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: % {S-1-5-21-379587013 33-5220325-21257 45684-513} % {S-1-1-0} % {S-1-5-32-544} % {S-1-5-32-555} % {S-1-5-32-545} %

Тип поля	Название поля	Описание	Пример значения
			{S-1-5-32-554} % {S-1-5-2} % {S-1-5-11} % {S-1-5-15} % {S-1-5-21-37958701 33-5220325-21257 45684-512} % {S-1-5-21-37958701 33-5220325-21257 45684-572} % {S-1-5-64-10} % {S-1-16-12288} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as

Тип поля	Название поля	Описание	Пример значения
			well as to any other security audit events generated during this logon session.
	cn1Label	Поле используется для указания кода события из журнала AD.	logEventCode
	cn1	Код события.	4627
	cn2Label	Поле используется для указания номера идентификатора события из журнала AD.	logEventId
	cn2	Идентификатор события.	4627
	cn3Label	Поле используется для указания типа события журнала Windows (Система\Безопасность\Приложение и т. д.).	logEventType
	cn3	Тип события журнала Windows.	4
	cs1Label	Поле используется для указания идентификатора конечного устройства — источника события.	endpointId
	cs1	Идентификатор конечного устройства.	16535060-5a1a-4e92-8331-239406ec34da

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для указания имени конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	endpointName
	cs2	Имя конечного устройства.	dep.local
	cs3Label	Поле используется для указания уровня важности события в журнале AD.	logLevel
	cs3	Уровень важности события.	Audit Success
	cs4Label	Поле используется для указания кода категории события (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и тд)	logCategoryString
	cs4	Категория события.	Group Membership
	cs5Label	Поле используется для указания файла журнала Windows.	logFile
	cs5	Файл журнала Windows	Security
	cs6Label	Поле используется для указания	sourceName

Тип поля	Название поля	Описание	Пример значения
		источника из журнала AD.	
	cs6	Источник из журнала AD.	Microsoft-Windows-Security-Auditing
	flexString1Label	Поле используется для указания содержания события из журнала AD.	insertionString
	flexString1	Параметры события из журнала AD после парсинга сообщения.	<pre>['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-37958701 33-5220325-21257 45684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\ \\t% {S-1-5-21-37958701 33-5220325-21257 45684-513}\\r\\n\\ \\t\\t%{S-1-1-0}\\r\\ \\n\\t\\t% {S-1-5-32-544}\\r\\ \\n\\t\\t% {S-1-5-32-555}\\r\\ \\n\\t\\t% {S-1-5-32-545}\\r\\ \\n\\t\\t% {S-1-5-32-554}\\r\\ \\n\\t\\t%{S-1-5-2}\\ \\r\\n\\t\\t% {S-1-5-11} \\r\\n\\t\\t% {S-1-5-15}\\r\\n\\t\\ \\t% {S-1-5-21-37958701 33-5220325-21257 45684-512}\\r\\n\\ \\t\\t% {S-1-5-21-37958701 33-5220325-21257 45684-572}\\r\\n\\ \\t\\t% {S-1-5-64-10}\\r\\</pre>

Тип поля	Название поля	Описание	Пример значения
			\n\\t\\t% {S-1-16-12288}']

Формат журнала Syslog

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: • 0 — emergencies; • 1 — alerts; • 2 — critical; • 3 — errors; • 4 — warnings; • 5 — notifications; • 6 — informational; • 7 — debugging.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	msg	Описание события.	[3603:3603:1128/175000.938565:ERROR:CONSOLE(6)] "console.assert", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
	cn1Label	Поле используется для указания типа источника событий syslog. Подробнее о значениях syslog facility смотрите в RFC 5424 .	Facility
	cn1	Тип источника событий syslog. Например, user-level messages.	1
	cs1Label	Поле используется для указания имени устройства, на котором произошло событие.	Hostname
	cs1	Имя компьютера, на котором произошло событие.	node1
	cs2Label	Поле используется для указания	Tag

Тип поля	Название поля	Описание	Пример значения
		приложения, вызвавшего событие.	
	cs2	Приложение, вызвавшее событие.	org.gnome.Shell.desktop
	cs3Label	Поле используется для указания идентификатора процесса события.	ProcessID
	cs3	PID процесса вызвавшего событие.	3036
	cs4Label	Поле используется для указания срабатывания правила.	Rule
	cs4	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages

Формат журнала RADIUS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	radius

Тип поля	Название поля	Описание	Пример значения
	Name	Тип источника.	log
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	act	Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
	suser	Имя пользователя.	Unknown, если пользователь неизвестен.
	src_ip	IP-адрес источника, откуда пришло сообщение.	192.168.57.4
	dst	IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
	dvc	IP-адрес пользователя (framed ip address).	192.168.57.29
	cs1Label	Поле используется для указания группы, в которой состоит пользователь.	user groups
	cs1	Строка групп в которых состоит пользователь.	test_group

Формат журнала UserID

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	userid
	Name	Тип источника.	log
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorere aeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	login
	reason	Причина, по которой было создано событие.	{ "user_groups_sids": ["S-1-5-21-3795870133-5220325-2125745684-513", "S-1-5-21-3795870133-5220325-2125745684-512"], "user_sid": "S-1-5-21-3795870133-5220325-2125745684-1103", "login": "user1",

Тип поля	Название поля	Описание	Пример значения
			domain":"DEV","event_id":4624}
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	dev.local

Экспорт журналов в формате JSON

Описание журнала событий

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
ip_address	IPv4-адрес источника события.	192.168.174.134

Название поля	Описание	Пример значения
attributes	Детали события в формате JSON.	<code>{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}}</code>
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth
user	Имя пользователя.	<code>{"guid":"37333739-3733-3734-3635-366400000000","name":"System","groups":[]}}</code>

Описание журнала веб-доступа

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
reasons	Причина, по которой было создано событие, например, причина блокировки сайта.	<code>"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]</code>

Название поля	Описание	Пример значения
proto	Используемый протокол 4-го уровня.	TCP
host	Имя хоста.	www.google.com
action	Действие, принятое устройством в соответствии с настроенными политиками.	block
bytes_sent	Количество байтов, переданных в направлении источник — назначение.	52
bytes_recv	Количество пакетов, переданных в направлении назначение — источник.	100
packets_sent	Количество пакетов, переданных в направлении источник — назначение.	2
packets_recv	Количество байтов, переданных в направлении назначение — источник.	5
request_method	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url	Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
media_type	Тип контента.	application/json
status_code	Код ответа HTTP.	302
http_referer	URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted	Поле указывает было ли содержимое расшифровано.	true, false
useragent	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0

Название поля			Описание	Пример значения	
application			id	Идентификатор приложения.	20
			name	Название приложения.	Youtube
			threat_level	Уровень угрозы приложения.	0
			app_protocol	Протокол прикладного уровня и его версия.	HTTP\1.1"
url_categories	id		Идентификатор категории, к которой относится URL.	39	
	threat_level		Уровень угрозы категории URL.	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.	
	name		Название категории, к которой относится URL.	Social Networking	
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47	
		name	Название зоны источника.	Trusted	
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)	
	ip		IPv4-адрес источника.	10.10.10.10	
	port		Порт источника.	Может принимать значения от 0 до 65535.	
	mac		MAC-адрес источника	01:23:45:67:89:AB	
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0	
		name	Название зоны назначения трафика.	Untrusted	

Название поля			Описание	Пример значения
	country		Страна назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		Название правила.	Default allow
	type		Тип сработавшего правила.	
user	guid		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала DNS

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	00000000-0000-0000-0000-000000000000
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda

Название поля		Описание	Пример значения
reasons		Причина, по которой было создано событие, например, url категория, на которых сработало правило.	<code>{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}</code>
proto		Используемый протокол 4-го уровня.	UDP
host		Имя хоста.	google.com
data		Поле используется для указания передаваемых данных.	<code>{"question":[{"domain":"google.com","type":"A","class":"IN"}], "answer":[{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}]}</code>
url_categories	id	Идентификатор сработавшей URL-категории.	37
	threat_level	Уровень угрозы сработавшей категории.	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.
	name	Название сработавшей категории.	Search Engines & Portals
action		Действие, принятое устройством в соответствии с настроенными политиками.	block
application	id	Идентификатор приложения.	5
	name	Название приложения.	

Название поля		Описание		Пример значения
		threat_level	Уровень угрозы приложения.	0
		app_protocol	Протокол прикладного уровня.	DNS
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	mac		MAC-адрес назначения	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f

Название поля			Описание	Пример значения
	name		Название правила, срабатывание которого вызвало событие.	Rule1
	Type		Тип сработавшего правила.	
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user1
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto		Используемый протокол 4-го уровня.	TCP или UDP
action		Действие, принятое устройством в соответствии с настроенными политиками.	accept

Название поля			Описание	Пример значения
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
json_data			Дополнительные данные.	null
application	id		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.
	app_protocol		Протокол прикладного уровня.	HTTP
	name		Название приложения.	Youtube
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10

Название поля			Описание	Пример значения
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
nat	source	ip	Адрес источника после переназначения (если настроены правила NAT).	192.168.117.85 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
	destination	ip	Адрес назначения после переназначения (если настроены правила NAT).	64.233.164.198 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown,	a7a3cd49-8232-4f1a-962a-3659af89e96f

Название поля		Описание	Пример значения
		то идентификатор: 00000000-0000-0000-0000-000000000000.	
	name	Имя пользователя.	Admin
	groups	guid Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name Название группы, в которой состоит пользователь.	Default Group

Описание журнала COB

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto		Используемый протокол 4-го уровня.	TCP или UDP
action		Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv		Количество байтов, переданных в направлении назначение — источник.	6

Название поля		Описание	Пример значения
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv		Количество пакетов, переданных в направлении назначение — источник.	1
json_data		Дополнительные данные.	null
application	id	Идентификатор приложения.	195
	threat_level	Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.
	name	Название приложения.	Youtube
	app_protocol	Протокол прикладного уровня.	HTTP
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.
		name	Название группы, в которой состоит пользователь.
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Allow trusted to untrusted

Название поля		Описание	Пример значения
signatures		Название правила, срабатывание которого вызвало событие.	
	type	Тип сработавшего правила	idps
	id	Идентификатор сработавшей сигнатуры.	999999
signatures	threat_level	Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 — очень низкий; • 2 — низкий; • 3 — средний; • 4 — высокий; • 5 — очень высокий.
	name	Название сработавшей сигнатуры.	BlackSun Test
source	zone	guid	Уникальный идентификатор зоны источника трафика.
		name	Название зоны источника трафика.
	country		Название страны источника. RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.
	port		Порт источника. Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.
			01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
		name	Название зоны назначения трафика.
	country		Название страны назначения. RU (отображается двухбуквенный код страны)

Название поля		Описание	Пример значения
	ip	IPv4-адрес назначения трафика.	104.19.197.151
	port	Порт назначения.	Может принимать значения от 0 до 65535.
	mac	MAC-адрес назначения.	01:23:45:67:89:AB

Описание журнала инспектирования SSH

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command		Команда, передаваемая по SSH.	whoami
action		Действие, принятое устройством в соответствии с настроенными политиками.	block
application	id	Идентификатор приложения.	195
	name	Название приложения.	
	threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
	app_protocol	Протокол прикладного уровня.	SSH или SFTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.
		name	Название зоны источника трафика.

Название поля		Описание	Пример значения
	country	Название страны источника.	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес источника трафика.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.
	mac	MAC-адрес источника.	FA:16:3E:65:1C:B4
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
		name	Название зоны назначения трафика.
	country		Название страны назначения.
	ip		IPv4-адрес назначения трафика.
	port		Порт назначения.
	mac		MAC-адрес назначения.
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.
	name		Название правила, срабатывание которого вызвало событие.
	type		Тип сработавшего правила.
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.
	name		Имя пользователя.

Название поля		Описание	Пример значения
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.
		name	Название группы, в которой состоит пользователь.

Описание журнала защиты почтового трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
action		Действие, принятое устройством в соответствии с настроенными политиками.	mark
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	0
bytes_rcv		Количество байтов, переданных в направлении назначение — источник.	0
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	0
packets_rcv		Количество пакетов, переданных в направлении назначение — источник.	0
decrypted		Поле указывает было ли содержимое расшифровано.	true, false
from		Почтовый адрес отправителя.	sender@example.com

Название поля		Описание		Пример значения
to		Почтовый адрес получателя.		receiver@example.com
application	id	Идентификатор приложения.		9
	name	Название приложения.		
	threat_level	Уровень угрозы приложения.		Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
	app_protocol	Сетевой протокол прикладного уровня.		SMTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	10.10.10.10
	port		Порт назначения.	Может принимать значения от 0 до 65535.

Название поля		Описание	Пример значения	
	port	MAC-адрес назначения.	01:23:45:67:89:AB	
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f	
	name	Название правила, срабатывание которого вызвало событие.	Mail security rule	
	type	Тип сработавшего правила.	Mail security rule	
user	guid	Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f	
	name	Имя пользователя.	user_name	
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала Windows Active Directory

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node_name		Имя, которое однозначно идентифицирует устройство UserGate, генерирующее это событие.	utmcore@ntoorereaeda
endpoint_id		Идентификатор конечного устройства — источника события.	16535060-5a1a-4e92-8331-239406ec34da
endpoint_name		Имя конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	dep.local
user_name			user1.dep.local

Название поля	Описание	Пример значения
	Поле «Пользователь» из журнала AD.	
log_level	Поле «Keywords» из журнала AD.	Audit Success
log_category_string	Код категории события из журнала AD.	Group Membership
log_file	Файл журнала Windows.	Security
source_name	Поле «Источник» из журнала AD.	Microsoft-Windows-Security-Auditing
data	Описание события в журнале AD.	Group membership information.\r\n\r\nSubject:\r\n\tSecurity ID:\tS-1-0-0\r\n\tAccount Name:\t\t\r\n\tAccount Domain:\t\t\r\n\tLogon ID:\t0x0\r\n\r\nLogon Type:\t\t3\r\n\r\nNew Logon:\r\n\tSecurity ID:\tS-1-5-21-3795870133-5220325-2125745684-1103\r\n\tAccount Name:\t\tuser1\r\n\tAccount Domain:\t\tDEP\r\n\tLogon ID:\t0x7A25A21\r\n\r\nEvent in sequence:\tt1 of 1\r\n\r\nGroup Membership:\tt%\{S-1-5-21-3795870133-5220325-2125745684-513}\r\n\t\t%\{S-1-1-0}\r\n\t\t%\{S-1-5-32-544}\r\n\t\t%\{S-1-5-32-555}\r\n\t\t%\{S-1-5-32-545}\r\n\t\t%\{S-1-5-32-554}\r\n\t\t%\{S-1-5-2}\r\n\t\t%\{S-1-5-11}\r\n\t\t%\{S-1-5-15}\r\n\t\t%\{S-1-5-21-3795870133-5220325-2125745684-512}\r\n\t\t%\{S-1-5-21-3795870133-5220325-2125745684-572}\r\n\t\t%\{S-1-5-64-10}\r\n\t\t%\{S-1-16-12288}\r\n\r\nThe subject fields indicate the

Название поля	Описание	Пример значения
		account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThis event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.
computer_name	Узел Windows из журнала AD, на котором произошло событие.	DC1.dep.local
insertion_string	Параметры события из журнала AD после парсинга сообщения.	<pre>['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\ \n\\t\\t%' {S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\ \t%{S-1-1-0}\\r\\n\\t\\t% {S-1-5-32-544}\\r\\n\\t\\t% {S-1-5-32-555}\\r\\n\\t\\t% {S-1-5-32-545}\\r\\n\\t\\t% {S-1-5-32-554}\\r\\n\\t\\t% {S-1-5-2}\\r\\n\\t\\t%{S-1-5-11} \\r\\n\\t\\t%{S-1-5-15}\\r\\n\ \t\\t% {S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\ \t% {S-1-5-21-3795870133-522032</pre>

Название поля	Описание	Пример значения
		5-2125745684-572}\\r\\n\\t\\ \\t%{S-1-5-64-10}\\r\\n\\t\\t% {S-1-16-12288}'
error	Код ошибки из журнала AD, которая произошла при получении данных.	0
status	Описание ошибки из журнала AD, которая произошла при получении данных.	
counter_id	Идентификатор счетчика WMI сенсора.	login_logout
log_event_code	Поле «Код события» из журнала AD.	4627
log_event_id	Поле «Идентификатор события» из журнала AD.	4627
log_event_type	Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.).	4

Описание журнала Syslog

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
syslog_facility	Тип источника события syslog. Например, user-level messages. Подробнее о значениях syslog facility смотрите в RFC 5424 .	1

Название поля		Описание	Пример значения
syslog_severity		Уровень важности события syslog. Например, warning. Подробнее о значениях syslog severity смотрите в RFC 5424 .	4
computer_name		Имя устройства, на котором произошло событие.	node1
app_name		Приложение, вызвавшее событие.	org.gnome.Shell.desktop
process_id		PID процесса, вызвавшего событие.	3036
data		Описание события.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"console.assert\", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages
	type	Тип сработавшего правила.	

Описание журнала RADIUS

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
event_type		Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off

Название поля		Описание	Пример значения
action		Действие, принятое устройством в соответствии с настроенными политиками.	login
src_ip		IP-адрес источника, откуда пришло сообщение.	192.168.57.4
nas_ip		IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
framed_ip		IP-адрес пользователя.	192.168.57.29
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b00000044f
	name	Имя пользователя.	user_name
	groups	Название группы, в которой состоит пользователь.	test_group

Описание журнала UserID

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons	Причина, по которой было создано событие.	{"user_groups_sids\": [\"S-1-5-21-3795870133-5220325-2125745684-513\", \"S-1-5-21-3795870133-5220325-2125745684-512\",

Название поля			Описание	Пример значения
				\S-1-5-21-3795870133-5220325-2125745684-572\], \"user_sid\": \"S-1-5-21-3795870133-5220325-2125745684-1103\", \"login\": \"user1\", \"domain\": \"DEV\", \"event_id\": 4624}
action			Действие, принятое устройством в соответствии с настроенными политиками.	login
src_ip			IPv4 источника события.	10.10.0.11
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name		Название правила, срабатывание которого вызвало событие.	dev.local
	type		Тип сработавшего правила.	syslog
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b00000044f
	name		Имя пользователя.	user1
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local

ОТЧЕТЫ

Описание

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел **Отчеты** состоит из трех подразделов — **Шаблоны**, **Правила отчётов** и **Созданные отчеты**. Чтобы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет.	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе Созданные отчеты .

Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

Примечание

В отчетах по трафику (кроме отчетов веб-доступа) используются данные из компонента Netflow. Отчеты веб-доступа по трафику используют данные из журналов (домены, URL-категории и т.п.).

Шаблоны отчетов

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список шаблонов отчетов, сгруппированных по категориям:

- **Пользовательский** — группа шаблонов по обобщенной статистике срабатывания правил отчетов.
- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **Приложения конечных устройств** — группа шаблонов со списками приложений, которые когда-либо запускались на конечных устройствах.
- **Журнал правил конечных устройств** — группа шаблонов по событиям срабатывания правил межсетевого экрана конечных устройств.
- **Журнал событий конечных устройств** — группа шаблонов по событиям, полученным от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **COB** — группа шаблонов по событиям, регистрируемым в журнале COB.
- **Защита почтового трафика** — группа шаблонов по событиям, регистрируемым в журнале защиты почтового трафика.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.
- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **UserID** — группа шаблонов для создания отчетов по работе UserID агента.
- **VPN** — группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Правила отчетов

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. Важно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Для шаблонов Подробный список всех посещенных URL и Подробный список всех посещенных сайтов автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задаёт пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.

Наименование	Описание
Расписание	Выбор расписания для создания отчетов. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7 • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23" Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа."
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: • Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. • От — имя отправителя письма. • Тема письма — тема письма (subject). • Тело письма — содержимое письма. • Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки Почтовые адреса.

i Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

i Примечание

Для того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку Запустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

Созданные отчеты

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо кликнуть на файл с созданным отчетом, для удаления — **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию — 60 дней.

ГОСТЕВОЙ ПОРТАЛ

Управление гостевыми пользователями

UserGate NGFW позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей

интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или email.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать администратора гостевых пользователей (опционально).	- В разделе Администраторы нажать кнопку Добавить и создать профиль администратора, разрешающий Гостевой портал для чтения и записи в закладке Разрешения для веб-консоли. Данный профиль дает доступ в консоль управления временными пользователями. - Создать учетную запись администратора и назначить ей созданную роль. Более подробно о создании администраторов NGFW смотрите соответствующий раздел руководства.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Подключиться к консоли управления Гостевого портала.	В браузере перейти на адрес https://IP_NGFW:8001/ta Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1.
Шаг 4. Создать список пользователей.	В консоли нажать на кнопку Добавить и заполнить поля: - Количество пользователей. - Комментарий. Дата и время окончания — время, когда учетная запись гостевого пользователя будет отключена. Длина пароля — определяет длину пароля для создаваемого пользователя. Сложность пароля — определяет сложность пароля для создаваемого пользователя. Возможны варианты: - Цифры. - Буквы + цифры.

Наименование	Описание
	• Буквы + цифры + спецсимволы. • Время жизни — продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена. • Группа — созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи.

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через email).	В разделе Библиотеки → Профили оповещений нажать кнопку Добавить и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений .
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей.	В консоли NGFW в разделе Группы нажать на кнопку Добавить и создать группу, отметив поле Группа для гостевых пользователей . Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи.	В разделе Пользователи и устройства в подразделе Captive-профили создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон Captive portal: email auth или Captive portal: SMS auth , в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времени действия учетной записи. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений .

Наименование	Описание
Шаг 4. Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль.	В разделе Пользователи и устройства → Captive-портал создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства Настройка Captive-портала .

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения (Описание)

UserGate NGFW поддерживает работу через интерфейс командной строки (CLI).

С помощью CLI вы можете:

- просматривать конфигурацию устройства;
- выполнять диагностику работы устройства;
- настраивать параметры конфигурации устройства;
- перезагружать или выключать устройство.

Подключение к интерфейсу командной строки

К интерфейсу командной строки можно подключиться с помощью стандартных портов для монитора и клавиатуры (при наличии таких портов на устройстве), с помощью терминала через консольный порт или удаленно с помощью протокола SSH.

i Примечание

Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — usergate.

Для подключения с помощью монитора и клавиатуры:

1. Подключите монитор к разъему VGA (HDMI), клавиатуру — к разъему USB.
2. Войдите в CLI, используя имя и пароль пользователя с правами администратора (по умолчанию — Admin и usergate).

Для подключения с помощью консольного порта:

1. Подключите компьютер к устройству с помощью кабеля для консольного порта.
2. Запустите программу — эмулятор терминала, например **Putty** для Windows или **minicom** для Linux. Установите подключение через последовательный порт, указав параметры подключения: **115200, 8 n 1**.
3. Введите логин и пароль для доступа в интерфейс (по умолчанию — Admin и usergate).

Для подключения с помощью протокола SSH:

1. Разрешите доступ для протокола CLI по SSH в параметрах зоны, к которой вы собираетесь подключаться (доступ по порту TCP 2200). Подробнее о настройке зоны в CLI — в разделе «[Зоны](#)».
2. Запустите на компьютере SSH-терминал, например **SSH** для Linux или **Putty** для Windows.
3. Укажите IP-адрес устройства, порт для подключения (по умолчанию — 2200), имя пользователя с правами администратора (по умолчанию — Admin).

Пример команды подключения для Linux: `ssh Admin@<IP-address> -p 2200`.

3. Войдите в CLI, используя пароль пользователя, указанного на предыдущем шаге.

В версии 7.4.0 и выше для подключения к CLI по SSH поддерживаются следующие алгоритмы:

- Kex: diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256;
- Public key: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-256, rsa-sha2-512, ssh-rsa;
- Ciphers: aes128-ctr, aes192-ctr, aes256-ctr;
- MAC: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-256.

Режимы работы интерфейса командной строки

CLI имеет два основных режима работы — режим диагностики и режим конфигурации.

После авторизации вы попадаете в режим диагностики.

В режиме диагностики доступны команды:

- проверки доступности сетевых ресурсов;
- просмотра статистики и информации об интерфейсах;
- просмотра информации о записях ARP;
- отслеживания пакетов по установленным правилам;
- мониторинга трафика;
- просмотра информации о маршрутах;
- просмотра состояния кластера;
- просмотра заблокированных COB IP-адресов;
- отображения системной информации;
- диагностики работы протоколов динамической маршрутизации;
- просмотра информации об авторизованных пользователях.

Приглашение командной строки в режиме диагностики имеет следующий вид:

```
Admin@nodename>
```

Настройка параметров устройства выполняется в режиме конфигурации.

Для переключения на режим конфигурации используется команда **configure**. В режиме конфигурации символ приглашения в командной строке меняется на **#**. Вернуться в режим просмотра можно с помощью команды **exit**.

```
Admin@nodename> configure
Admin@nodename#
Admin@nodename# exit
Admin@nodename>
```

Если система находится в состоянии до первичной инициализации, в CLI доступны команды режима диагностики и ограниченный набор команд режима конфигурации, позволяющий выполнить настройку сетевых параметров устройства. Приглашение командной строки в режиме диагностики по умолчанию имеет вид: **<user-name>@<product-type>** (например, **Admin@NGFW**), а в режиме конфигурации — **<user-name>@<product-type>#** (например, **Admin@NGFW#**). Подробнее — в разделе «[Команды, доступные до первичной инициализации узла](#)».

Если система находится в аварийном состоянии, для восстановления рабочего состояния в неё можно войти в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации устройства. Обычно это учетная запись **Admin**. Для входа необходимо указать имя в виде **Admin@emergency**, в качестве пароля — пароль корневого администратора. Приглашение командной строки в режиме emergency по умолчанию имеет вид: **<user-name>@emergency@<product-type>#** (например, **Admin@emergency@NGFW#**). Подробнее о режиме emergency — в разделе «[Настройка устройства](#)».

Формат команд

Команды интерфейса командной строки имеют следующий формат:

```
<action> <level> <filter> <configuration_info>
```

- **<action>** — действие, которое необходимо выполнить (**create**, **set**, **show**, **delete**).

- `<level>` — уровень контекста конфигурации. Соответствует одному из разделов структуры конфигурации в веб-интерфейсе NGFW (`network`, `network-policy`, `security-policy`, `users`, `settings`, `libraries`, `logs` и т. д.).
- `<filter>` — идентификатор объекта, к которому происходит обращение для выполнения действия `<action>`.
- `<configuration_info>` — значения параметров, которые необходимо применить к объекту `<filter>`.

Поддерживается ввод команды в несколько строк (многострочный ввод). Примером таких команд могут быть команды описания правил, использующих [синтаксис UPL](#). Для перехода на новую строку необходимо добавить символ «\» в конце строки. Начиная со второй строки ввод символа «\» необязателен. Чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@nodename# set users user example \
... name username1
... enabled on
... groups [ "Default Group" ]
...
Admin@nodename#
```

В версии 7.5.0 и выше поддерживается последовательное исполнение нескольких команд, вставленных из буфера обмена. Исключением являются многострочные команды, например команды, написанные с помощью синтаксиса UPL. Импортировать многострочные команды можно с помощью [команды import](#).

Фильтрация вывода команд

В версии 7.5.0 и выше в интерфейсе командной строки поддерживается функция фильтрации вывода команд. С помощью функции фильтрации вы можете управлять отображением результатов выполнения команд в соответствии с заданными критериями.

Фильтрация может применяться к различным типам команд просмотра, включая:

- команды отображения состояния устройства;
- команды просмотра конфигурации;

- команды просмотра системных журналов;
- команды с динамическим выводом данных (такие, как `show traffic capture` и `show network trace`).

Формат команд с фильтрацией вывода:

```
<cli-command> | grep <pattern> -f <include|exclude> -BA <Num>:<Num>
```

- `<cli-command>` — команда CLI, вывод которой нужно отфильтровать.
- `<pattern>` — искомое выражение. Поддерживается формат выражений RegExp.
- `-f <include|exclude>` — включение или исключение искомого выражения из вывода команды.
- `-BA <Num>:<Num>` — отображение строк, соседних с совпадением (<количество отображаемых строк до совпадения>:<количество отображаемых строк после совпадения>).

Пример фильтрации вывода команд просмотра состояния интерфейсов:

```
Admin@nodename> show network interface
```

```
+-----+-----+-----+-----+
+-----+
|  Name  |          IP          | Link status | Mode |
Zone      |
+-----+-----+-----+-----+
+-----+
| tunnel1 | 172.30.250.1/24 | DOWN      |      | VPN for remote
access |
| tunnel2 | 172.30.255.1/24 | DOWN      |      | VPN for Site-to-
Site |
| tunnel3 |                  | DOWN      |      | VPN for Site-to-
Site |
| port0   | 172.26.147.146/16 | 10000     | main |
MGMT      |
| port1   | 10.150.185.119/16 | 10000     | main |          [MC]
LAN        |
```

```

| port2 | 10.153.219.236/16 | 10000 | main | [MC]
WAN |
+-----+-----+-----+-----+
+-----+
Admin@nodename> show network interface | grep VPN
| tunnel1 | 172.30.250.1/24 | DOWN | | VPN for remote
access |
| tunnel2 | 172.30.255.1/24 | DOWN | | VPN for Site-to-
Site |
| tunnel3 | | DOWN | | VPN for Site-to-
Site |
Admin@nodename> show network interface | grep VPN -f exclude
+-----+-----+-----+-----+
+-----+
| Name | IP | Link status | Mode |
Zone |
+-----+-----+-----+-----+
+-----+
| port0 | 172.26.147.146/16 | 10000 | main |
MGMT |
| port1 | 10.150.185.119/16 | 10000 | main | [MC]
LAN |
| port2 | 10.153.219.236/16 | 10000 | main | [MC]
WAN |
+-----+-----+-----+-----+
+-----+

```

Пример фильтрации вывода команд поиска правил межсетевого экрана:

```

Admin@nodename# show network-policy firewall | grep "name\\\\"VPN"
name("VPN for remote access to Trusted and Untrusted")
name("VPN for Site-to-Site to Trusted and Untrusted")
Admin@nodename# show network-policy firewall | grep "name\\\\"VPN" -BA
4:
src.zone = "VPN for remote access" \
dst.zone = (Untrusted, Trusted) \
desc("Example firewall rule which allows traffic from VPN for
remote access zone to Trusted and Untrusted zones. This is an example
rule which can be changed or deleted if necessary.") \

```



```

enabled(false) \
name("VPN for remote access to Trusted and Untrusted")
-----
src.zone = "VPN for Site-to-Site" \
dst.zone = (Untrusted, Trusted) \
desc("Example firewall rule which allows traffic from VPN for Site-
to-Site zone to Trusted and Untrusted zones. This is an example rule
which can be changed or deleted if necessary.") \
enabled(false) \
name("VPN for Site-to-Site to Trusted and Untrusted")
-----

```

Пример фильтрации вывода команды просмотра событий журнала:

```

Admin@nodename> show logs log core static | grep ldap
2025-08-05 11:58:32.861039<0.2336.0> [critical] database:wait_tables/
1:253 'ldap_server' loaded in 0.0ms
2025-08-05 11:58:33.392739<0.3953.0> [critical] database:wait_tables/
1:253 'ldap_server' loaded in 0.0ms
2025-08-05 11:58:33.569880<0.4287.0> [critical] nagent:start_app/1:340
ldap_sync starting ...
2025-08-05 11:58:33.571394<0.4287.0> [critical] nagent:start_app/1:343
[uuid,ldap_sync] started
2025-08-05 11:59:03.889299<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
2025-08-05 11:59:12.366764<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
2025-08-05 12:00:10.162520<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,

```

Пример фильтрации вывода команды с динамическим выводом:

```

Admin@nodename> show traffic capture | grep ICMP

92 0.305709456 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping)
request id=0x0e30, seq=3/768, ttl=30
93 0.305739062 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping)
reply id=0x0e30, seq=3/768, ttl=64 (request in 92)

```

```

706 1.329727201 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping)
request id=0x0e30, seq=4/1024, ttl=30
707 1.329755455 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping)
reply id=0x0e30, seq=4/1024, ttl=64 (request in 706)

```

Горячие клавиши

В интерфейсе командной строки вы можете использовать следующие горячие клавиши:

- Tab — вызов встроенной помощи, автодополнение команды:
 - Если нажать Tab в режиме ожидания ввода, выводится полный список команд, доступных на текущем уровне.
 - Если нажать Tab на этапе ввода команды после пробела, отображается список возможных параметров команды с кратким описанием.
 - Если написать первые несколько букв команды и нажать Tab, команда будет дополнена.
- Ctrl + C — отмена ввода текущей команды.
- ↑, ↓ — прокрутка истории ввода команд.

В выводе встроенной помощи после нажатия клавиши Tab могут использоваться следующие вспомогательные символы:

- * — обязательный параметр в командах **create** и ряде других команд.
- + — опциональный параметр.
- > — вложенные параметры. После введения такого параметра появляется новый список параметров, которые можно указать.

Например:

```

Admin@nodename# set network virtual-router default
+ interfaces          List of network interfaces attached to this
virtual router
> routes              List of static network routes

```

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВОНАЧАЛЬНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла (Описание)

Если устройство еще не прошло первоначальную инициализацию, в CLI доступен минимальный набор команд для настройки сетевых параметров устройства и запуска инициализации.

Примечание

В случае сбоя в работе ядра CLI также может перейти в состояние до первичной инициализации.

Команды режима диагностики

В режиме диагностики доступны команды, позволяющие просмотреть:

- доступность сетевых ресурсов;
- статистику и информацию об интерфейсах;
- информацию о записях ARP;
- информацию о маршрутах;
- системную информацию.

Также в режиме диагностики можно выполнять мониторинг сетевого трафика и диагностику работы протоколов динамической маршрутизации.

Базовые команды управления устройством

Для просмотра текущих даты и времени на узле используется команда:

```
Admin@NGFW> date
```

Для перезагрузки узла используется команда:

```
Admin@NGFW> reboot
```

Для выключения узла используется команда:

```
Admin@NGFW> shutdown
```

Для перехода в режим конфигурации узла используется команда:

```
Admin@NGFW> configure
```

Для выхода из интерфейса CLI используется команда:

```
Admin@NGFW> exit
```

Команды проверки доступности сетевых ресурсов

Команда	Описание
dig	Проверка записи DNS домена: <pre>Admin@NGFW> dig host <hostname> <parameters> Admin@NGFW> dig host <IP-address> <parameters></pre> В команде можно использовать следующие параметры: • reverse-lookup — получение имени устройства по IP-адресу; • dns — указание IP-адреса DNS-сервера; • tcp — использование протокола TCP вместо UDP
netcheck	

Команда	Описание
	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • address — IP-адрес и порт, доменное имя узла — для проверки доступности по TCP; URL — для HTTP; • dns-ip — IP-адрес сервера DNS; • dns-tcp — использование TCP вместо UDP для DNS-запроса; • check-cert — проверка SSL-сертификата; • type — проверка доступности по: ◦ http; ◦ tcp (если порт не указан, то используется порт 80); • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; • timeout — максимальный тайм-аут ожидания ответа от веб-сервера; • user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. <pre>Admin@NGFW> netcheck type tcp address <host-domain-name> data on Admin@NGFW> netcheck address <host-domain-name></pre>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: • host — IP-адрес или доменное имя узла. • count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). • numeric — не определять имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • ttl — время жизни пакета.

Команда	Описание
	• interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — максимальный размер блока данных отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. <pre>Admin@NGFW> ping host <hostname> count <number></pre>
traceroute	Трассировка соединения до определенного узла. Параметры команды: • host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; • interface <iface-name> — интерфейс, с которого будут отправляться пакеты; • not-map-ip — не искать hostname для IP-адреса при отображении; • use-icmp-echo — использовать ICMP echo; • port — указать порт вместо порта по умолчанию (1 — 65535); • min-interval — минимальный интервал между пакетами. <pre>Admin@NGFW> raceroute host <hostname></pre>

Статистика и информация об интерфейсах

Для отображения информации об интерфейсах используется команда:

```
Admin@NGFW> show network interface
```

Для отображения статистики определенного интерфейса и информации о нем используется следующая команда:

```
Admin@NGFW> show network interface <interface-name>
```

Также доступно отображение только информации или только статистики интерфейса:

```
Admin@NGFW> show network interface <interface-name> type info  
Admin@NGFW> show network interface <interface-name> type statistics
```

Для отображения списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов предназначена команда:

```
Admin@NGFW> show network interface-mapping
```

Примечание

Под физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. Изменения MAC-адресов интерфейсов в настройках NGFW данной командой не отображаются. Измененные настройками NGFW MAC-адреса можно посмотреть командой: `show network interface <interface-name>`.

Упорядочивание интерфейсов происходит в соответствии с номером порта в шине PCI.

Для удаления списка используется команда:

```
Admin@NGFW> clear network interface-mapping
```

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенное устройство.

ARP-записи

Для просмотра информации о записях ARP:

```
Admin@NGFW> show network arp
```

Для просмотра ARP-записей вы можете использовать фильтры.

Параметр	Описание
interface	Название интерфейса NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

```
Admin@NGFW> show network arp host <IP-address>
Admin@NGFW> show network arp interface <interface-name>
Admin@NGFW> show network arp mac <MAC-address>
```

Примечание

В режиме диагностики действия производятся с системными записями; в режиме конфигурации – со статическими ARP-записями.

Для удаления системной ARP-записи используется команда:

```
Admin@NGFW> clear network arp interface <iface-name> host <ip>
```

Для удаления всех системных записей на заданном интерфейсе (можно указать несколько интерфейсов) используется команда:

```
Admin@NGFW> clear network arp interfaces [ <iface-name1> <iface-name2>
... ]
```

Отслеживание пакетов

Для включения функции отслеживания пакетов используется команда:

```
Admin@NGFW> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия входящих и исходящих интерфейсов, номера TCP/UDP портов источника и назначения.

Для выхода из режима отслеживания пакетов нажмите комбинацию клавиш **Ctrl + C**.

Мониторинг трафика

Для мониторинга трафика используется команда:

```
Admin@NGFW> show traffic <parameters>
```

Параметры мониторинга трафика.

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Параметры фильтрации: • source-ip — IP-адрес источника; • source-port — порт источника; • dest-ip — IP-адрес назначения; • dest-port — порт назначения; • vlan-tag — тег VLAN; • interface-name — название интерфейса; • node-name — название узла; • protocol — протокол
connections	Отображение информации о соединениях: протокол и его номер; время жизни записи; IP-адреса источника и назначения, порты источника и назначения; IP-адреса источника и назначения, порты источника и назначения, которые ожидаются в ответе; статус сессии (UNREPLIED или ASSURED); количество переданных и принятых пакетов и байтов; зона источника; является ли эта сессия сессией известного NGFW пользователя и т. п.. Возможна фильтрация по параметрам: • protocol — протокол; • source-ip — IP-адрес источника; • dest-ip — IP-адрес назначения; • node-name — название узла; • expect — отображение неустановленных соединений (on/off)

Пример команды мониторинга трафика:

```
Admin@NGFW> show traffic connections dest-ip 192.168.0.100 expect on
```

Просмотр информации LLDP

Для просмотра информации, полученной по LLDP (Link Layer Discovery Protocol) используется команда:

```
Admin@NGFW> show lldp <parameters>
```

Параметры фильтрации.

Параметр	Описание
neighbors	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • Chassis ID — идентификатор шасси. • SysName — имя системы. • SysDescr — описание системы, содержит информацию об оборудовании и операционной системе устройства. • Management — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • Capability — функции устройства (например, маршрутизатор, коммутатор и т. п.). • Port ID — идентификатор порта с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • PortDescr — описание порта. • TTL — время жизни передаваемых пакетов LLDP
statistics	Статистика интерфейсов, в настройках которых был указан профиль LLDP. • Interface — название интерфейса. • Transmitted — общее количество кадров LLDP, переданных через интерфейс. • Received — общее количество кадров LLDP, полученных на интерфейсе. • Discarded — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • Unrecognized — количество кадров LLDP с неподтвержденным содержимым, полученных на этом интерфейсе. • Ageout — в каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в

Параметр	Описание
	течение срока старения новых кадров не принято, информация LLDP удаляется. • Inserted — количество добавлений записей с информацией о соседях LLDP. • Deleted — количество удалений записей о соседях LLDP

Маршруты

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

```
Admin@NGFW> show network route <parameters>
```

Параметры просмотра маршрутов.

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам NGFW. Данные маршруты помечены символом «С» в списке маршрутов
kernel	Отображение маршрутов, добавленных администратором; маршруты помечены символом «К» в списке маршрутов
summary	Количество активных подключений и записей FIB (Forwarding Information Base)
ospf	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации OSPF. Данные маршруты помечены символом «О» в списке маршрутов
bgp	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации BGP; маршруты помечены символом «В» в списке маршрутов
rip	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации RIP; маршруты помечены символом «R» в списке маршрутов
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all)

Мониторинг OSPF

Диагностика и мониторинг OSPF выполняется с помощью команд, представленных ниже. Отображение информации OSPF:

```
Admin@NGFW> show network ospf
...
Admin@NGFW> show network ospf <parameter>
```

Параметр	Описание
virtual-router	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF: (<vrf-name> all)
route	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF
database	Отображена информация: • Router Link States: пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны; используются для передачи информации соседним маршрутизаторам, находящимся в той же зоне, о собственных интерфейсах и своих соседях. • Network Link States: пакеты LSA Type 2 (Network LSA) генерируются выделенным маршрутизатором (Designated Router, DR) для описания всех маршрутизаторов, подключенных к его сегменту напрямую. • Summary Link States: пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • ASBR-Summary Link States: пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора (Autonomous System Border Router, ASBR) в других областях
neighbor	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора).

Параметр	Описание
	• Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором - Designated Router, DR. Если приоритеты маршрутизаторов равны, то будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например, Full/DR, Full/BDR, Full/Drother. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Доступно указание дополнительных параметров: • interface-name — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • all — отображение таблицы со всеми соседях. • detail — отображение подробной информации о соседях
interface	Отображение информации об интерфейсах OSPF. Дополнительно: • interface-name — отображение информации об указанном интерфейсе. • traffic — статистика переданных и принятых пакетов OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment)
border-routers	Отображение информации о пограничных маршрутизаторах

Команда для перезапуска процесса OSPF:

```
Admin@NGFW> clear network ospf <parameter>
```

Параметр	Описание
interface-name	Название интерфейса

Параметр	Описание
<code>virtual-router</code>	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<code><vrf-name> all</code>)
<code>interface</code>	Интерфейс, на котором необходимо перезапустить процесс OSPF (<code><interface-name></code>)
<code>neighbor</code>	Выбор соседей, в отношении которых будет перезапущен процесс

Мониторинг BGP

Для отображения таблиц BGP-маршрутизатора:

```
Admin@NGFW> show network bgp
...
Admin@NGFW> show network bgp <parameter>
```

Параметр	Описание
<code>virtual-router</code>	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<code><vrf-name> all</code>)
<code>ip</code>	IP-адрес, маршрут до которого необходимо отобразить
<code>statistics</code>	Отображение статистики BGP
<code>neighbors</code>	Отображение информации о BGP-соседах (доступно отображение информации об определенном соседе; необходимо указание IP-адреса соседа). Дополнительные параметры, доступные при указании соседа: • received-routes — принятые маршруты до применения к ним входящей политики (Routemap и фильтры). • advertised-routes — маршруты, которые анонсируются указанному соседу
<code>summary</code>	Просмотр краткой информации о соседях

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии):

```
Admin@nodename> clear network bgp <parameter>
```

Параметры команды.

Параметр	Описание
ip	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации
virtual-router	Название виртуального маршрутизатора, которому принадлежит BGP-сосед

В случае, если на соседних устройствах поддерживается метод Route Refresh, то можно избежать полной реинициализации сессии с соседом, отправив специальное сообщение типа ROUTE REFRESH. Отправка данного сообщения позволяет обновить информацию без прерывания в маршрутизации.

Для обновления информации без обрыва сессии с соседом используется команда:

```
Admin@NGFW> clear network bgp ip <neighbor-ip> soft in | out
Admin@NGFW> clear network bgp virtual-router <vrf-name> ip <neighbor-
ip> soft in | out
```

Мониторинг RIP

Для отображения информации RIP из таблицы маршрутизатора по умолчанию (адрес сети, полученный по RIP; адрес Next Hop; метрика маршрута; тэг маршрута, предназначенный для разделения внутренних и внешних маршрутов; интервал времени, по истечении которого маршрут будет признан недействительным, если информация о нем не была получена) используется команда:

```
Admin@NGFW> show network rip
...
Admin@NGFW> show network rip <parameter>
```

Параметры команды.

Параметр	Описание
status	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т. п.
virtual-router	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить: <code><vrf-name> all</code>

Мониторинг мультикаст-трафика

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию используется команда:

```
Admin@NGFW> show network mroute
...
Admin@NGFW> show network mroute <parameter>
```

Параметры команды.

Параметр	Описание
count	Отображение статистики о группе и источнике
virtual-router	Выбор виртуального маршрутизатора: <code><vrf-name> all</code>
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации
fill	Таблица маршрутизации мультикаст-трафика. Доступно указание параметра: • ip — отображение записи для определенного IP-адреса; далее необходимо указать IP-адрес
ip	Отображение записи для определенного IP-адреса; необходимо указать IP-адрес

Мониторинг IGMP

Мониторинг работы протокола IGMP (Internet Group Management Protocol) доступен с использованием следующей команды (указание параметров является обязательным):


```
Admin@NGFW> show network igmp <parameters>
```

Параметры команды.

Параметр	Описание
virtual-router	Выбор виртуального маршрутизатора
statistics	Статистика по сообщениям: • IGMP Membership Query — сообщение сервера клиенту, в котором сервер просит обновить подписку на получаемые клиентом группы иначе, сервер перестанет вещать группу/группы в данный сегмент сети. • IGMP Leave — сообщение клиента серверу; клиент сообщает, что желает убрать мультикаст-группу из списка получаемых. • IGMP Membership Report — сообщение клиента серверу; клиент желает получать трафик этой группы
join	Отображение информации о группах IGMP
sources	Отображение информации об источниках мультикаст-трафика
groups	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: • Общее количество групп. • Интерфейс, через который группа доступна. • Адрес группы. • Режим INCLUDE или EXCLUDE. • Таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report. • Время, в течение которого группа известна
interface	Отображение информации об интерфейсе, связанной с мультикаст-маршрутизацией: • Название интерфейса, его статус и адрес. • Версия IGMP. • Опрашиватель и его адрес (Querier).

Параметр	Описание
	- Таймер, который обнуляется каждый раз, как приходит сообщение Query с меньшим IP-адресом. Доступно указание: <code>interface-name</code> — название интерфейса. <code>detail</code> — подробная информация об интерфейсе

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды:

```
Admin@NGFW> show network pim <parameter>
```

Параметры команды.

Параметр	Описание
<code>virtual-router</code>	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию
<code>vxlان-groups</code>	Информация о группах VXLAN, использующихся в мультитивещании
<code>statistics</code>	Статистика протокола
<code>join</code>	Отображение информации о группах PIM протокола
<code>neighbor</code>	Информация о соседях: - Интерфейс, через который была получена информация о соседе. - Адрес соседа. - Время, с последнего начала работы PIM. - Время, в течении которого сосед доступен. - Приоритет DR
<code>next-hop</code>	Записи о адресах next-hop
<code>state</code>	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List)

Параметр	Описание
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP
interface	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т.п. Также доступно указание параметров: • interface-name — название интерфейса. • traffic — статистика отправленных/полученных сообщений. • detail — подробная информация об интерфейсе
group-type	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Отображение системной информации

Для просмотра версии ПО системы используется команда:

```
Admin@NGFW> show system version
```

Для отображения информации о количестве активных TCP/UDP/ICMP сессий на системе используется команда:

```
Admin@NGFW> show system sessions
```

Для отображения информации о количестве активных сессий по отдельным протоколам или временным интервалам используется команда:

```
Admin@NGFW> show system sessions counters [ parameters ]
```

Очистить статистику:

```
Admin@NGFW> clear system sessions
```

Диагностика работы протоколов динамической маршрутизации

С помощью команд этого раздела можно просматривать события debug-логов протоколов динамической маршрутизации. Включение в debug-лог событий конкретного протокола выполняется командой debug в режиме конфигурации.

Для просмотра записей debug-лога используется команда:

```
Admin@NGFW> show logs log routing <parameters>
```

Далее необходимо указать один из параметров:

Параметр	Описание
all	Все протоколы
rip	Протокол RIP
bgp	Протокол BGP
igmp	Протокол IGMP
pim	Протокол PIM
ospf	Протокол OSPF
bfd	Протокол BFD
msdp	Протокол MSDP
mroute	Таблица мультикаст-маршрутизации mroute
ssmpingd	Инструмент тестирования мультикаст-вещания ssmpingd

Для вывода событий debug-лога в консоль в реальном времени используется команда:

Просмотр системных журналов устройства

Для просмотра событий системных журналов устройства используется команда:

```
Admin@NGFW> show logs log core <static | dynamic>
```

Параметры команды (static или dynamic) определяют режим отображения сообщений журналов в консоли.

Команды режима конфигурации

В режиме конфигурации доступны команды **execute** (команды, которые не относятся к настройке конфигурации устройства — ping, date, traceroute и т.п.), базовые [команды настройки устройства](#) и [команды настройки сети](#) (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, статических ARP-записей).

Команды execute

Команды имеют следующую структуру:

```
Admin@nodename# execute <command-name>
```

Список команд раздела **execute**.

Команда	Описание
date	Просмотр текущих значений даты и времени на узле: <pre>Admin@NGFW# execute date</pre>
dig	Проверка записи DNS домена: <pre>Admin@NGFW# execute dig host <hostname> <parameters> Admin@NGFW# execute dig host <IP-address> <parameters></pre> В команде можно использовать следующие параметры: • reverse-lookup — получение имени устройства по IP-адресу; • dns — указание IP-адреса DNS-сервера; • tcp — использование протокола TCP вместо UDP
factory-reset	Возврат устройства в первоначальное состояние (доступно в версии 7.5.0 и выше):

Команда	Описание
	Admin@NGFW# execute factory-reset Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
install	Первоначальная настройка устройства. Admin@NGFW# execute install <parameter> • master — настройка устройства в качестве главного узла. Задайте логин и пароль администратора. • slave — настройка устройства в качестве дополнительного узла кластера. Укажите следующие параметры: ◦ interface — интерфейса для подключения к кластеру; ◦ master-ip — IP-адрес главного узла; ◦ master-secret — секретный код, необходимый для подключения узла в кластер; ◦ slave-ip — IP-адрес резервного узла, который будет назначен на интерфейс, используемый для подключения к кластеру. Можно указать в виде IP-адреса (например, 192.168.0.1) или в виде IP-адреса и маски подсети (например, 192.168.0.1/24). Доступно в версии 7.4.0 и выше. ◦ gateway-address — IP-адрес шлюза. Шлюз необходимо указать, если узлы кластера находятся в разных подсетях. • mc — настройка устройства через UserGate Management Center. Укажите следующие параметры: ◦ device-code — уникальный код устройства, используемый для подключения узла к UGMC; ◦ mc-ip — IP-адрес UGMC; ◦ login — задать логин администратора NGFW; ◦ password — задать пароль учетной записи администратора NGFW
netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя узла для проверки доступности по TCP или URL — для HTTP; • dns-ip — IP-адрес сервера DNS;

Команда	Описание
	• dns - tcp — использование TCP вместо UDP для DNS-запроса; • check - cert — проверка SSL-сертификата; • type — проверка доступности по: ◦ http; ◦ tcp (если порт не указан, то используется порт 80); • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; • timeout — максимальный тайм-аут ожидания ответа от веб-сервера; • user - agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. <pre>Admin@NGFW# execute netcheck type tcp address <host-domain-name> data on Admin@NGFW# execute netcheck address <host- domain-name></pre>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: • host — IP-адрес или доменное имя узла. • count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). • numeric — не определять имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — максимальный размер блока данных отправляемых пакетов.

Команда	Описание
	• virtual-router — имя виртуального маршрутизатора. <pre>Admin@NGFW# execute ping host <hostname> count <number></pre>
reboot	Перезагрузка устройства: <pre>Admin@NGFW# execute reboot</pre>
restore-mac	Восстановление mac-адреса интерфейса: <pre>Admin@NGFW# execute restore-mac interface <interface-name></pre>
shutdown	Выключение устройства: <pre>Admin@NGFW# execute shutdown</pre>
traceroute	Трассировка соединения до определенного узла. Параметры команды: • host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; • interface <iface-name> — интерфейс, с которого будут отправляться пакеты; • not-map-ip — не искать hostname для IP-адреса при отображении; • use-icmp-echo — использовать ICMP echo; • port — указать порт вместо порта по умолчанию (1 — 65535); • min-interval — минимальный интервал между пакетами. <pre>Admin@NGFW# execute traceroute host <hostname></pre>

Команды настройки устройства

На уровне `settings cli` настраиваются следующие параметры работы интерфейса командной строки:

- вид системного приглашения (prompt) консоли CLI;
- уровень детализации диагностики.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@NGFW# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида: `Admin@nodename#`) на удобное вам.

Например, чтобы поменять вид системного приглашения на `NodeAABBCC`, выполните следующую команду:

```
Admin@NGFW# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@NGFW# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@NGFW#
```

Чтобы задать уровень детализации диагностики используется следующая команда:

```
Admin@NGFW# set settings cli log-level <off | error | debug | warning | info>
```

Вы можете установить следующие уровни детализации:

- **off** — отключить журналирование;
- **error** — только ошибки;
- **warning** — ошибки и предупреждения;
- **info** — ошибки, предупреждения и дополнительная информация;
- **debug** — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:

```
Admin@NGFW# show settings cli
```

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@NGFW# set settings fastpath enabled <on/off>
```

Для просмотра настройки режима ускоренной обработки трафика используется команда:

```
Admin@NGFW# show settings fastpath
```

Команды настройки сетевых параметров устройства

Настройки сетевых параметров выполняются на уровне **network**.

Настройка зон

Для создания зоны используется команда:

```
Admin@NGFW# create network zone <parameter>
```

Параметры настройки зон.

Параметр	Описание
name	Название зоны
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • enabled — включение/отключение защиты. • aggregate — суммирование пакетов: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны; ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold — порог уведомления. Если количество запросов превышает указанный порог, происходит запись события в системный журнал. • drop-threshold — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, UserGate отбрасывает пакеты и записывает это событие в системный журнал. • excluded-ips — список IP-адресов, которые необходимо исключить из защиты
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • enabled — включение/отключение защиты. • aggregate — суммирование пакетов: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны; ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold — порог уведомления. Если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips — список IP-адресов серверов, которые необходимо исключить из защиты
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • enabled — включение/отключение защиты. • aggregate — суммирование пакетов: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны;

Параметр	Описание
	◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold — порог уведомления. Если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips — список IP-адресов серверов, которые необходимо исключить из защиты
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • response-pages: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • rpc: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • ha: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • VRRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "Admin Console": доступ к веб-консоли управления (TCP 8001). • DNS: доступ к сервису DNS-прокси (TCP 53, UDP 53). • "HTTP Proxy": доступ к сервису HTTP(S)-прокси (TCP 8090). • "Authorization agent": доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • "SMTP Proxy": сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "POP3 Proxy": сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.

Параметр	Описание
	• VPN: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • "PROXY PORTAL": сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • L7 DNS: детектирование трафика DNS на уровне приложений. • L7 NTP: детектирование трафика NTP на уровне приложений. • "SAML SERVER": выбор SAML-сервера в списке сервисов зоны и общих настройках UserGate. • "Log Analyzer": сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713). • "Dynamic routing OSPF": сервис динамической маршрутизации OSPF. • "Dynamic routing BGP": сервис динамической маршрутизации BGP. • "SNMP Proxy": сервис используется для построения распределенной системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределенной сетевой инфраструктуры). • "SSH Proxy": сервис, использующийся для инициирования трафика SSH. • Multicast: сервис мультикастинга. • NTP: доступ к сервису точного времени, запущенному на сервере UserGate. • "Dynamic routing RIP": сервис динамической маршрутизации RIP. • UserID agent: сервис для осуществления прозрачной аутентификации. В качестве источника данных аутентификации используются журналы ActiveDirectory и Syslog. • BFD: сервис Bidirectional Forwarding Detection для быстрого обнаружения сетевых ошибок
service-addresses	

Параметр	Описание
	Указание разрешенных IP-адресов для сервисов: • service — выбор сервисов (список соответствует enabled-services); • allowed-addresses — разрешенные адреса: ◦ allowed-ips — указать разрешенные IP-адреса; ◦ geoip — указать код GeoIP; ◦ ip-list — указать заранее созданный в библиотеке элементов список IP-адресов
antispoof-enabled	Включение/отключение защиты от IP-спуфинга
antispoof-negate	При antispoof-negate on адреса источников, указанные в значении ip-spoofing-networks , будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга

Для изменения параметров зоны используется команда:

```
Admin@nodename# set network zone <zone-name> <parameters>
```

Пример изменения параметров зоны:

```
Admin@NGFW# set network zone Test_zone dos-protection-syn enabled on
```

Для удаления зоны или ее параметров используется команда:

```
Admin@nodename# delete network zone <zone-name>
```

Для просмотра параметров зон используется команда:

```
Admin@NGFW# show network zone
```

Настройка интерфейсов

Вы можете настроить следующие типы интерфейсов:

- [bond](#);
- [bridge](#);
- [loopback](#);
- [pppoe](#);
- [tunnel](#);
- [vlan](#);
- [adapter](#).

Для создания bond-интерфейса используется команда:

```
Admin@NGFW# create network interface bond <parameters>
```

Параметры bond-интерфейса.

Параметр	Описание
enabled	Включение/отключение интерфейса
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1)
zone	Зона, которой будет принадлежать бонд-интерфейс
bonding	Дополнительные параметры бонд-интерфейса: • mode — режим работы бонда: ◦ round-robin — режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ active-backup — режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден

Параметр	Описание
	снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). ◦ xor — режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). ◦ broadcast — режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ 802.3ad — режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). ◦ transmit — режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). ◦ load — режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом,

Параметр	Описание
	различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. • mii-monitoring — периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • down-delay — время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. • up-delay — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. • lacp-rate — интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: ◦ slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд; ◦ fast — запрос партнера на передачу LACPDU-пакетов каждую секунду. • failover-mac — определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: ◦ disabled — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. ◦ active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. ◦ follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Параметр	Описание
	• xmit-hash — определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ l2 — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. ◦ l2-3 — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. ◦ l3-4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефраgmentированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, так как отправляются через разные интерфейсы. • interface — интерфейсы, которые будут объединены в бонд
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP; • manual — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. i Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон

Параметр	Описание
mac	MAC-адрес интерфейса
mtu	Указание размер MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение/отключения ретранслятора. • utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего бонд-интерфейса используется команда:

```
Admin@NGFW# set network interface bond <bond-name>
```

Для удаления бонд-интерфейса или его параметров используется команда:

```
Admin@NGFW# delete network interface bond <bond-name>
```

Параметры, доступные для удаления.

Параметр	Описание
ip-addresses	Заданный IP-адрес
dhcp-relay server-address	IP-адрес сервера DHCP
bonding interface	Интерфейсы, объединенные в бонд

Чтобы просмотреть информацию о всех бонд-интерфейсах, используйте команду:

```
Admin@NGFW# show network interface bond
```

или об определенном интерфейсе:

```
Admin@NGFW# show network interface bond <bond-name>
```

Для создания bridge-интерфейса используется команда:

```
Admin@nodename# create network interface bridge
```

Параметры bridge-интерфейса.

Параметр	Описание
enabled	Включение/отключение моста
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет bridge1)
zone	Зона, которой будет принадлежать мост
bridging	Дополнительные параметры моста: • iface-type — режим работы интерфейса: ◦ l2 — Layer 2 (создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security; контентная фильтрация в этом режиме работает). ◦ l3 — Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • interface — интерфейсы, которые будут использованы для создания моста. • stp — включение/отключение использование STP (Spanning Tree Protocol) для защиты от петель. • forward-delay — задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP (указывается в секундах). • max-age — время, по истечении которого STP-соединение считается потерянным (указывается в секундах).

Параметр	Описание
	• bypass-pair — пара интерфейсов, которая будет использована для построения байпас-моста. Необходима поддержка оборудования ПАК UserGate
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP; • manual — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. i Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
mac	MAC-адрес интерфейса
mtu	Указание размера MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение/отключения ретранслятора. • utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bridge-интерфейса используется команда:

```
Admin@NGFW# set network interface bridge <bridge-name>
```

Для удаления bridge-интерфейса или его параметров используется команда:

```
Admin@NGFW# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления.

Параметр	Описание
ip-addresses	Заданный IP-адрес
dhcp-relay server-address	IP-адрес сервера DHCP

Для просмотра информации о всех bridge-интерфейсах используется команда:

```
Admin@NGFW# show network interface bridge
```

или об определенном интерфейсе:

```
Admin@NGFW# show network interface bridge <bridge-name>
```

Для создания loopback-интерфейса используется команда:

```
Admin@NGFW# create network interface loopback <parameters>
```

Параметры loopback-интерфейса.

Параметр	Описание
enabled	Включение/отключение интерфейса
interface-name	Название интерфейса
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: [<ip_address/mask>], маска подсети задается в десятичном виде.

Параметр	Описание
	 Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
<code>iface-mode</code>	Режим назначения IP-адреса: • <code>dhcp</code> — получение динамического IP-адреса по DHCP; • <code>manual</code> — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
<code>zone</code>	Зона, которой будет принадлежать интерфейс
<code>mac</code>	MAC-адрес интерфейса
<code>mtu</code>	Указание размера MTU
<code>dhcp-relay</code>	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • <code>enabled</code> — включение/отключения ретранслятора. • <code>utm-address</code> — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения <code><ip none></code>). • <code>server-address</code> — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего интерфейса используется команда:

```
Admin@NGFW# set network interface loopback <interface-name>
```

Для удаления loopback-интерфейса или его параметров используется команда:

```
Admin@NGFW# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления.

Параметр	Описание
<code>ip-addresses</code>	Заданный IP-адрес
<code>dhcp-relay</code>	IP-адрес сервера DHCP

Для просмотра информации о всех loopback-интерфейсах используется команда:

```
Admin@NGFW# show network interface loopback
```

Об определенном интерфейсе:

```
Admin@NGFW# show network interface loopback <interface-name>
```

Для создания интерфейса PPPoE используется команда:

```
Admin@NGFW# create network interface pppoe
```

Параметры PPPoE-интерфейса.

Параметр	Описание
<code>enabled</code>	Включение/отключение интерфейса PPPoE
<code>interface-name</code>	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет ppp1)
<code>zone</code>	Зона, которой будет принадлежать интерфейс
<code>config</code>	Дополнительные параметры PPPoE интерфейса: • <code>interface</code> — интерфейс, на котором будет создаваться интерфейс PPPoE; • <code>login</code> — имя пользователя для соединения PPPoE; • <code>password</code> — пароль пользователя для соединения PPPoE; • <code>persist-connection</code> — автоматическое переподключение при обрыве связи; • <code>auth-type</code> — тип авторизации: ◦ CHAP;

Параметр	Описание
	◦ PAP; • holdoff — интервал времени в секундах после разрыва соединения перед повторным запуском; • default-route — интерфейс PPPoE в качестве маршрута по умолчанию; • echo-interval — интервал проверки соединения; • echo-failure — количество неуспешных проверок соединения, после которого NGFW считает, что соединение отсутствует и разрывает его; • providers-dns — использование DNS-серверов, выданных провайдером; • connection-attempts — количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены; • service-name — имя сервиса необходимо прописывать в случае предоставления провайдером
mtu	Указание размера MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet

Для изменения существующего интерфейса PPPoE используется команда:

```
Admin@NGFW# set network interface pppoe <pppoe-name>
```

Для удаления интерфейса PPPoE используется команда:

```
Admin@NGFW# delete network interface pppoe <pppoe-name>
```

Для просмотра информации о всех интерфейсах PPPoE используется команда:

```
Admin@NGFW# show network interface pppoe
```

Об определенном интерфейсе:

```
Admin@NGFW# show network interface pppoe <pppoe-name>
```

Для создания туннелей используется команда:

```
Admin@NGFW# create network interface tunnel
```

Параметры туннеля.

Параметр	Описание
<code>enabled</code>	Включение/отключение туннеля
<code>interface-number</code>	Необходимо ввести номер, который будет отображен в названии туннеля (например, 1, тогда название созданного интерфейса будет gre1)
<code>zone</code>	Зона, которой будет принадлежать интерфейс
<code>mtu</code>	Размер MTU для выбранного интерфейса
<code>ip-addresses</code>	IP-адрес, назначенный туннельному интерфейсу. Адрес задается в следующем виде: [<code><ip_address/mask></code>] или [<code><ip_address/mask> <ip_address/mask></code>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
<code>tunnel-config</code>	Дополнительные параметры настройки туннеля: • <code>local-ip</code> — локальный адрес Point-to-Point интерфейса; • <code>remote-ip</code> — удаленный адрес Point-to-Point интерфейса; • <code>iface-mode</code> — режим работы туннеля: ◦ <code>gre</code> — GRE (протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47). ◦ <code>ipip</code> — IPIP (протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP пакета в другой IP пакет, это добавление внешнего заголовка с

Параметр	Описание
	Source IP — точкой входа в туннель, и Destination — точкой выхода из туннеля). ◦ <code>vxlان</code> — VXLAN (протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789). • <code>vxlان-id</code> — Идентификатор VXLAN. Только для типа туннеля VXLAN

Для изменения параметров существующего туннеля используется команда:

```
Admin@NGFW# set network interface tunnel <tunnel-name>
```

Для удаления интерфейса туннель или его параметров используется команда:

```
Admin@NGFW# delete network interface tunnel <tunnel-name>
```

Для просмотра информации о всех туннелях используется команда:

```
Admin@NGFW# show network interface tunnel
```

Об определенном интерфейсе:

```
Admin@NGFW# show network interface tunnel <tunnel-name>
```

Для создания нового VLAN-интерфейса используется команда:

```
Admin@NGFW# create network interface vlan <parameters>
```

Параметры VLAN-интерфейса.

Параметр	Описание
<code>enabled</code>	Включение/отключение VLAN-интерфейса
<code>iface-type</code>	Тип интерфейса: • <code>l3</code> — Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана,

Параметр	Описание
	контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • mirror — интерфейс, работающий в режиме mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа)
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP. • manual — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
tag	Тег VLAN. Допускается создание до 4094 интерфейсов
interface	Физический интерфейс, на котором создается VLAN
zone	Зона, которой будет принадлежать интерфейс
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
mac	MAC-адрес интерфейса
mtu	Указание размера MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение/отключения ретранслятора. • utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего VLAN-интерфейса используется команда:

```
Admin@NGFW# set network interface vlan <vlan-name>
```

Для удаления VLAN-интерфейса или его параметров используется команда:

```
Admin@NGFW# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления.

Параметр	Описание
ip-addresses	Заданный IP-адрес
dhcp-relay server-address	IP-адрес сервера DHCP

Для просмотра информации о всех VLAN-интерфейсах используется команда :

```
Admin@NGFW# show network interface vlan
```

Об определенном интерфейсе:

```
Admin@NGFW# show network interface vlan <vlan-name>
```

Настройка сетевых адаптеров

Сетевые адаптеры создать нельзя, но вы можете настраивать параметры сетевых адаптеров устройства с помощью следующей команды:

```
Admin@NGFW# set network interface adapter <adapter-name>
```

Параметры сетевых адаптеров.

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса

Параметр	Описание
<code>iface-type</code>	Тип интерфейса: • <code>l3</code> — интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • <code>mirror</code> — интерфейс, работающий в режиме mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа)
<code>iface-mode</code>	Режим назначения IP-адреса: • <code>dhcp</code> — получение динамического IP-адреса по DHCP; • <code>manual</code> — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
<code>zone</code>	Зона, которой будет принадлежать интерфейс
<code>ip-addresses</code>	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<code><ip_address/mask></code>] или [<code><ip_address/mask></code> <code><ip_address/mask></code>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
<code>mac</code>	MAC-адрес интерфейса
<code>mtu</code>	Указание размера MTU
<code>rx-ring</code>	Размер буфера RX ring интерфейса типа adapter
<code>tx-ring</code>	Размер буфера TX ring интерфейса типа adapter
<code>dhcp-relay</code>	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • <code>enabled</code> — включение/отключения ретранслятора.

Параметр	Описание
	• utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения <ip none>). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для удаления параметров адаптеров используется команда:

```
Admin@NGFW# delete network interface adapter <adapter-name>
<parameters>
```

Параметры, доступные для удаления.

Параметр	Описание
ip-addresses	Заданный IP-адрес
dhcp-relay server-address	IP-адрес сервера DHCP

Для просмотра параметров сетевых адаптеров используется команда:

```
Admin@NGFW# show network interface adapter <adapter-name>
```

Настройка шлюзов

Для создания шлюза используется команда:

```
Admin@NGFW# create network gateway <parameters>
```

Параметры шлюза.

Параметр	Описание
enabled	Включение/отключение шлюза
interface	Интерфейс, используемый для выхода в Интернет: • port — выбор конкретного порта (port0, port1, port2 и т. д.); • auto — после выбора этого параметра порт определится автоматически. Для узлов, не

Параметр	Описание
	прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0
<code>virtual-router</code>	Виртуальный маршрутизатор, для которого настраивается шлюз
<code>ip</code>	IP-адрес шлюза
<code>weight</code>	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз)
<code>balancing</code>	Включение режима балансировки — весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами
<code>default</code>	Использование данного шлюза в качестве шлюза по умолчанию

Для изменения параметров шлюза используется команда:

```
Admin@NGFW# set network gateway <gateway-name>
```

Для удаления шлюза используется команда:

```
Admin@NGFW# delete network gateway <gateway-name>
```

Для просмотра информации о всех шлюзах используется команда:

```
Admin@NGFW# show network gateway
```

Об определенном шлюзе:

```
Admin@NGFW# show network gateway <gateway-name>
```

Настройка виртуальных маршрутизаторов

Для создания виртуального маршрутизатора используется команда:


```
Admin@NGFW# create network virtual-router <parameters>
```

Параметры виртуального маршрутизатора.

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора
interfaces	Интерфейсы, которые будут использованы в виртуальном маршрутизаторе. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, добавлены быть не могут; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие
routes	Добавление статических маршрутов. • destination-ip — IP-адрес подсети назначения. Указывается в формате <ip/mask>. • type — тип маршрута: ◦ unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. ◦ unreachable — трафик отбрасывается. Источнику отправляется ICMP-сообщение host unreachable (type 3 code 1). ◦ prohibit — трафик отбрасывается. Источнику отправляется ICMP-сообщение host unreachable (type 3 code 13). ◦ blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата. • enabled — включение/отключение использования статического маршрута. • gateway — IP-адрес шлюза, через который будет доступна указанная подсеть. Этот IP-адрес должен быть доступен с устройства. • metric — метрика маршрута. Маршрут с меньшей метрикой более приоритетен

Для изменения параметров виртуального маршрутизатора используется команда:

```
Admin@NGFW# set network virtual-router <virtual-router-name>
```

Для удаления виртуального маршрутизатора или его параметров используется команда:

```
Admin@NGFW# delete network virtual-router <virtual-router-name>  
<parameters>
```

Для просмотра информации о всех виртуальных маршрутизаторах используется команда:

```
Admin@NGFW# show network virtual-router
```

Об определенном виртуальном маршрутизаторе:

```
Admin@NGFW# show network virtual-router <virtual-router-name>
```

Статические ARP-записи

Для добавления статических ARP-записей используется команда:

```
Admin@NGFW# set network arp host <IP-address> interface <interface-  
name> mac <MAC-address>
```

Параметры статических ARP-записей.

Параметр	Описание
interface	Название интерфейса NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

Для удаления статических ARP-записей используется команда:

```
Admin@NGFW# delete network arp host <host-ip-address> interfaces
[ port1 port2 ]
```

Журналирование событий протоколов маршрутизации

Команда `debug` позволяет включить журналирование событий протоколов маршрутизации в режиме отладки. События записываются в `debug-журнал`. Их просмотр также возможен в режиме диагностики консоли CLI.

Для включения журналирования конкретного протокола маршрутизации используется команда:

```
Admin@NGFW# debug <protocol> <parameters>
```

Поддерживаются следующие протоколы:

Параметр	Описание
<code>rip</code>	Протокол RIP
<code>bgp</code>	Протокол BGP
<code>igmp</code>	Протокол IGMP
<code>pim</code>	Протокол PIM
<code>ospf</code>	Протокол OSPF
<code>bfd</code>	Протокол BFD
<code>msdp</code>	Протокол MSDP
<code>mroute</code>	Таблица мультикаст-маршрутизации <code>mroute</code>
<code>ssmpingd</code>	Инструмент тестирования мультикаст-вещания <code>ssmpingd</code>

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация NGFW

При первоначальной инициализации UserGate NGFW в интерфейсе командной строки доступны три режима конфигурации:

- Автономный (главный) узел.
- Дополнительный узел кластера.
- Управление через UserGate Management Center.

Автономный узел

Для настройки UserGate NGFW в качестве автономного узла используется команда:

```
Admin@nodename# execute install master login <login-name> password
<password>
```

Необходимо задать логин и пароль администратора устройства.

Дополнительный узел кластера

Для настройки UserGate NGFW в качестве дополнительного узла кластера используется команда:

```
Admin@nodename# execute install slave <parameters>
```

Укажите дополнительные параметры настройки.

Параметр	Описание
interface	Интерфейс для подключения к кластеру
slave-ip	IP-адрес резервного узла, который будет назначен на интерфейс, использующийся для подключения к кластеру. Возможные опции: • ip — IP-адрес (например, 192.168.0.1); • ip/mask — IP-адрес и маска подсети (например, 192.168.0.1/24). Доступно в версии 7.4.0 и выше

Параметр	Описание
gateway-address	IP-адрес шлюза. Шлюз необходимо указывать, если узлы кластера находятся в разных подсетях
master-ip	IP-адрес мастер-сервера
master-secret	Секретный код, использующийся для подключения узла в кластер
login	Логин администратора UserGate NGFW. Начиная с версии 7.3.0 логин указывать не нужно
password	Пароль учетной записи администратора. Начиная с версии 7.3.0 пароль указывать не нужно

Управление через UserGate Management Center

Для настройки UserGate NGFW с помощью UGMC используется команда:

```
Admin@nodename# execute install mc <parameters>
```

Укажите дополнительные параметры настройки.

Параметр	Описание
login	Логин администратора NGFW
password	Пароль учетной записи администратора
mc-ip	IP-адрес сервера UGMC
device-code	Уникальный код устройства, использующийся для подключения узла к UGMC

Мастер первоначальной настройки узла

Мастер первоначальной настройки (доступен в версии 7.5.0 и выше) позволяет в диалоговом режиме запустить установку UserGate NGFW в качестве автономного (главного) узла, задать логин и пароль учетной записи корневого

администратора, выбрать язык веб-интерфейса и установить IP-адрес интерфейса port0 для подключения к веб-консоли управления.

Чтобы запустить мастер первоначальной настройки:

1. Подключитесь к консоли устройства с помощью монитора и клавиатуры (при наличии соответствующих портов на устройстве) или с помощью эмулятора терминала через консольный порт.
2. Войдите в интерфейс командной строки, указав логин и пароль администратора, используемые по умолчанию.

```
UGOS login: Admin
Password: usergate
Admin@NGFW>
```

3. Перейдите в режим конфигурации интерфейса командной строки.

```
Admin@NGFW> configure
Admin@NGFW#
```

4. Запустите мастер первоначальной настройки узла с помощью команды:

```
Admin@NGFW# execute install master login <admin-login> password <admin-
password> language <en | ru>
```

В команде запуска первоначальной настройки узла вы можете назначить новый логин и пароль корневого администратора и установить язык по умолчанию для веб-консоли устройства.

После запуска мастер первоначальной настройки предложит прочитать и принять условия лицензионного соглашения. Если условия лицензионного соглашения приняты, будет запущен процесс инсталляции устройства в качестве автономного узла NGFW. В процессе инсталляции устройство запустит процедуру получения IP-адреса интерфейса port0 по протоколу DHCP.

```
Admin@NGFW# execute install master login Admin password usergate
language ru
Вы должны принять условия лицензионного соглашения, чтобы продолжить.
```

```
Прочитать условия соглашения сейчас? [Y/n] y
```

```
USERGATE
```

```
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ
```

```
...
```

```
...
```

```
...
```

```
Продолжая, вы принимаете условия лицензионного соглашения. Хотите  
продолжить? [Y/n] y
```

```
Инсталляция началась. Пожалуйста, подождите
```

```
IP-адрес для Port0 192.168.56.252. Используйте этот IP-адрес для  
доступа к веб-консоли через браузер.
```

```
Пожалуйста, сохраните этот IP-адрес, так как это окно будет  
перезагружено. Хотите продолжить? [Y/n] y
```

```
Installation completed successfully
```

Если IP-адрес не получен (например, в сегменте сети отсутствует DHCP-сервер), будет предложено ввести IP-адрес с маской подсети вручную в формате `ip-address/mask` (например, `192.168.0.1/24`).

После успешного завершения первичной инсталляции вы можете продолжить настройку устройства в интерфейсе командной строки или подключиться к веб-консоли управления для продолжения настройки устройства.

КОМАНДЫ ДИАГНОСТИКИ И МОНИТОРИНГА

Команды диагностики и мониторинга (Описание)

С помощью команд режима диагностики CLI вы можете просматривать информацию о системе, выполнять базовые команды управления системой, получать информацию о доступности сетевого окружения, выполнять мониторинг трафика по заданным параметрам.

Базовые команды управления

Для перезагрузки узла:

```
Admin@nodename> reboot
```

Для выключения узла:

```
Admin@nodename> shutdown
```

Для перехода в режим конфигурации CLI:

```
Admin@nodename> configure
```

Для выхода из интерфейса CLI:

```
Admin@nodename> exit
```

Команды просмотра системной информации

Для просмотра версии ПО системы:

```
Admin@nodename> show system version
```

Для просмотра количества активных сессий TCP/UDP/ICMP:

```
Admin@nodename> show system sessions
```

Для просмотра количества активных сессий по отдельным протоколам или временным интервалам:

```
Admin@nodename> show system sessions counters [ parameters ]
```

Для очистки статистики:


```
Admin@nodename> clear system sessions
```

Для просмотра текущих даты и времени на узле:

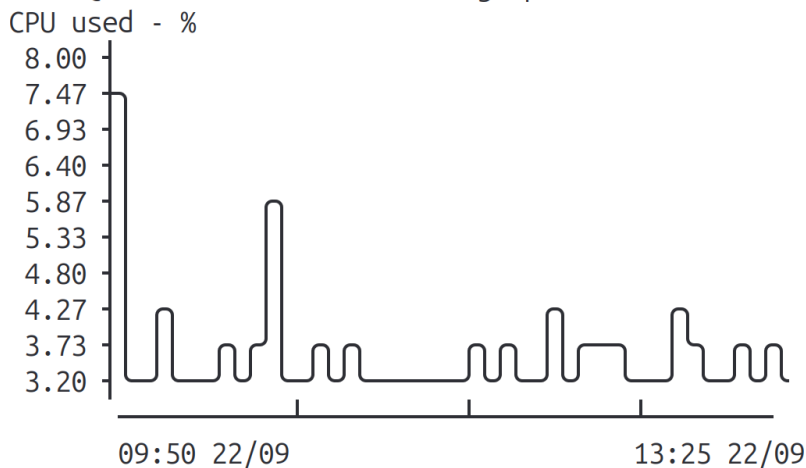
```
Admin@nodename> date
```

Команды мониторинга состояния системы

Команды мониторинга позволяют отображать состояние компонентов системы в виде временных диаграмм (доступны в версии 7.5.0 и выше).

С помощью команды `show monitoring <parameters>` вы можете получить информацию о состоянии процессора, дисковой подсистемы, интерфейсов, оперативной памяти, RAID-массива, просматривать статистику по рабочей температуре устройства и по DNS- и HTTP-запросам. Например:

```
Admin@nodename> show monitoring cpu
```



```
Admin@nodename>
```

При использовании команды без аргументов будет последовательно выведено состояние всех системных объектов мониторинга:

```
Admin@nodename> show monitoring
```

С помощью аргументов команды вы можете выводить информацию о каждом объекте мониторинга по отдельности.

Для мониторинга загрузки процессора:

```
Admin@nodename> show monitoring cpu
```

Для мониторинга состояния файловой системы:

```
Admin@nodename> show monitoring disk-info
```

Для мониторинга состояния RAID-массива:

```
Admin@nodename> show monitoring raid
```

Для мониторинга загрузки дисковой подсистемы операциями ввода/вывода:

```
Admin@nodename> show monitoring disk-io
```

Для мониторинга загрузки swap-раздела:

```
Admin@nodename> show monitoring swap
```

Для мониторинга загрузки интерфейсов:

```
Admin@nodename> show monitoring interface <port-name>
```

Для мониторинга загрузки оперативной памяти:

```
Admin@nodename> show monitoring memory
```

Для мониторинга рабочей температуры устройства:

```
Admin@nodename> show monitoring temperature
```

Для мониторинга состояния источников питания:

```
Admin@nodename> show monitoring power-supply
```

Для мониторинга статистики DNS-запросов:

```
Admin@nodename> show monitoring dns-requests
```

Для мониторинга статистики HTTP-запросов:

```
Admin@nodename> show monitoring http-requests
```

Команды просмотра информации об интерфейсах

Для просмотра информации обо всех имеющихся в системе интерфейсах используйте команду:

```
Admin@nodename> show network interface
```

Вы можете просмотреть статистику и подробную информацию об определенном интерфейсе. Для этого необходимо указать в команде его название:

```
Admin@nodename> show network interface <interface-name>
```

Также вы можете вывести отдельно информацию об интерфейсе либо статистику интерфейса:

```
Admin@nodename> show network interface <interface-name> type info  
Admin@nodename> show network interface <interface-name> type statistics
```

Для просмотра списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов используйте команду:

```
Admin@nodename> show network interface-mapping
```

i Примечание

Под физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. При использовании этой команды не отображаются изменения MAC-адресов в параметрах UserGate NGFW. Измененные MAC-адреса можно посмотреть с помощью команды `show network interface <interface-name>`.

Сортировка интерфейсов выполняется по номеру порта PCI-шины.

Для удаления списка используйте команду:

```
Admin@nodename> clear network interface-mapping
```

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов на настроенном устройстве UserGate.

Команды проверки доступности сетевых ресурсов

Для проверки доступности узла с помощью утилиты `ping` используйте команду:

```
Admin@nodename> ping <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
<code>host</code>	IP-адрес или доменное имя узла
<code>count</code>	Количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет продолжаться, пока соединение не будет прервано пользователем. Чтобы прервать отставку запросов, используйте комбинацию клавиш <code>Ctrl + C</code>
<code>interface</code>	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для отправки echo-запросов
<code>interval</code>	Интервал времени, определяющий частоту отправки пакетов. Указывается в секундах

Параметр	Описание
mtu	Размер MTU отправляемых пакетов
numeric	Не определять имя узла
ttl	Время жизни пакета
timestamp	Отображение временных меток
virtual-router	Имя виртуального маршрутизатора

Для трассировки соединения до определенного узла используйте команду:

```
Admin@nodename> traceroute <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
host	IP-адрес или доменное имя узла, для которого выполняется трассировка
interface	Интерфейс, с которого будут отправляться пакеты
min-interval	Минимальный интервал между отправкой пакетов
not-map-ip	Не искать имя узла для IP-адреса при отображении
port	Указать порт вместо порта по умолчанию (1–65535)
use-icmp-echo	Использовать ICMP-echo

Для проверки доступности удаленного HTTP/HTTPS-сервера используйте команду:

```
Admin@nodename> netcheck <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
address	

Параметр	Описание
	Адрес или имя узла для проверки доступности: • доменное имя узла для проверки доступности по TCP; • URL для проверки доступности по HTTP; • IP-адрес с портом для проверки по TCP (в этом случае в параметре type необходимо указать tcp)
type	Протокол для проверки доступности узла: • http; • tcp (если порт не указан, используется порт 80)
check-cert	Проверка SSL-сертификата
dns-ip	IP-адрес DNS-сервера
dns-tcp	Использование TCP вместо UDP для DNS-запроса
data	Запрос содержимого сайта. По умолчанию запрашиваются только заголовки
timeout	Максимальный тайм-аут ожидания ответа от веб-сервера
user-agent	Параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только через определенные браузеры. Значение параметра указывается в двойных кавычках

Для проверки записи DNS-домена используйте команду:

```
Admin@nodename> dig <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
host	Доменное имя узла или IP-адрес для реверсивного поиска
dns	Указание IP-адреса DNS-сервера
reverse-lookup	Получение имени узла по IP-адресу
tcp	Использование протокола TCP вместо UDP

Для проверки принадлежности IP-адреса по текущей базе GeoIP используйте команду:

```
Admin@nodename> check-geoip ip <IP-address>
```

Команды управления ARP-записями

Для просмотра информации об ARP-записях используйте команду:

```
Admin@nodename> show network arp
```

При просмотре записей вы можете использовать дополнительные фильтры.

Параметр	Описание
node - name	Название узла кластера, ARP-записи которого необходимо отобразить. Далее необходимо указать интерфейс или IP-адрес узла: <pre>Admin@nodename> show network arp node-name <node-name> interface <iface-name></pre> <pre>Admin@nodename> show network arp node-name <node-name> host <ip></pre>
interface	Название интерфейса UserGate NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

```
Admin@nodename> show network arp host <IP-address>
Admin@nodename> show network arp interface <interface-name>
Admin@nodename> show network arp mac <MAC-address>
```

ARP-записи также можно просматривать в режиме конфигурации CLI. Команды просмотра в режиме конфигурации идентичны командам режима диагностики.

i Примечание

В режиме диагностики действия выполняются с системными ARP-записями; в режиме конфигурации — со статическими.

Вы можете добавлять статические ARP-записи в режиме конфигурации с помощью команды:

```
Admin@nodename# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node - name	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP- и MAC-адреса устройства
interface	Название интерфейса UserGate NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

Команды удаления системных и статических ARP-записей имеют аналогичную структуру, отличается действие, которое необходимо выполнить:

- **clear** — удаление системных записей в режиме диагностики;
- **delete** — удаление статических записей в режиме конфигурации.

Для удаления системной ARP-записи используйте команду:

```
Admin@nodename> clear network arp interface <iface-name> host <ip>
```

Чтобы удалить запись на другом узле кластера:

```
Admin@nodename> clear network arp interface <iface-name> node-name <node-name> host <ip>
```


Чтобы удалить все системные записи на заданном интерфейсе:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> ... ]
```

Для удаления всех системных записей интерфейса другого узла:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> ... ] node-name <node-name>
```

Команды отслеживания пакетов

В режиме диагностики CLI вы можете отслеживать сетевые пакеты с помощью команды:

```
Admin@nodename> show network trace
```

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации CLI на уровне **network**. Подробнее — в разделе «[Настройка устройства](#)».

В выводе команды отслеживания пакетов будет отображаться следующая информация:

- IP-адреса источника и назначения;
- сетевой протокол;
- названия портов источника и назначения;
- номера TCP/UDP-портов источника и назначения.

Команда отслеживания пакетов также доступна в режиме конфигурации.

Для выхода из режима отслеживания пакетов используйте комбинацию клавиш **Ctrl + C**.

Команды мониторинга трафика

Для мониторинга трафика используйте команду:

```
Admin@nodename> show traffic
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Вы можете установить фильтрацию по параметрам: • source-ip — IP-адрес источника; • source-port — порт источника; • dest-ip — IP-адрес назначения; • dest-port — порт назначения; • vlan-tag — тег VLAN; • interface-name — название интерфейса; • node-name — название узла; • protocol — протокол
connections	Отображение информации о соединениях. Вы можете установить фильтрацию по параметрам: • protocol — протокол; • source-ip — IP-адрес источника; • dest-ip — IP-адрес назначения; • node-name — название узла; • expect — отображение неустановленных соединений

Параметр	Описание
capture	Отображение захвата пакетов. Вы можете установить фильтрацию по параметрам: • count — количество захватываемых пакетов. Значение по умолчанию — 1000. Для захвата без ограничения количества пакетов явно укажите: count unlimited. Опция доступна в версии ПО 7.3.0 и выше. • destination — IP-адрес назначения. • destination-port — порт назначения. • ipv4-protocol — номер протокола IPv4 (0–255). • interfaces — название интерфейса. • protocol — выбор протокола. • rule — выбор имеющегося правила для захвата пакетов. • source — IP-адрес источника. • source-port — порт источника

Пример команды мониторинга трафика:

```
Admin@nodename> show traffic connections node-name utmcore@dineanoulwer
dest-ip 192.168.0.100 expect on
```

Команды просмотра LLDP

Вы можете просматривать информацию о сетевом окружении, полученную по LLDP (Link Layer Discovery Protocol) с помощью команды:

```
Admin@nodename> show lldp <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
neighbors	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • Chassis ID — идентификатор шасси. • SysName — имя системы.

Параметр	Описание
	• SysDescr — описание системы, содержит информацию об оборудовании и операционной системе устройства. • Management — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • Capability — функции устройства (например, маршрутизатор, коммутатор и т. п.). • Port ID — идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • PortDescr — описание порта. • TTL — время жизни передаваемых пакетов LLDP
statistics	Статистика интерфейсов, в параметрах которых был указан профиль LLDP: • Interface — название интерфейса. • Transmitted — общее количество кадров LLDP, переданных через интерфейс. • Received — общее количество кадров LLDP, полученных на интерфейсе. • Discarded — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • Unrecognized — количество кадров LLDP с неподтвержденным содержимым, полученных на этом интерфейсе. • Ageout — в каждом кадре LLDP содержится информация о том, насколько долго является актуальной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется. • Inserted — количество добавлений записей с информацией о соседях LLDP. • Deleted — количество удалений записей о соседях LLDP

Примечание

Для просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на UserGate NGFW: профили LLDP должны быть настроены [в библиотеке элементов](#) и активированы [в настройках интерфейсов](#).

Мониторинг работы протоколов маршрутизации

С помощью команд этого раздела вы можете выполнять мониторинг работы протоколов маршрутизации, настроенных на UserGate NGFW.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используйте команду:

```
Admin@nodename> show network route
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
<code>ip</code>	IP-адрес, маршрут до которого необходимо отобразить
<code>node - name</code>	Выбор узла кластера
<code>connected</code>	Маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate NGFW. Такие маршруты помечены символом «C» в списке маршрутов
<code>kernel</code>	Маршруты, добавленные администратором. Маршруты помечены символом «K» в списке маршрутов
<code>summary</code>	Количество активных подключений и записей FIB (Forwarding Information Base)
<code>ospf</code>	Маршруты, полученные с помощью протокола динамической маршрутизации OSPF. Такие маршруты помечены символом «O» в списке маршрутов
<code>bgp</code>	Маршруты, полученные с помощью протокола динамической маршрутизации BGP. Такие маршруты помечены символом «B» в списке маршрутов
<code>rip</code>	Маршруты, полученные с помощью протокола динамической маршрутизации RIP. Маршруты помечены символом «R» в списке маршрутов
<code>virtual - router</code>	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf - name> all)

Мониторинг OSPF

С помощью команд этого раздела вы можете выполнять диагностику протокола OSPF.

Для просмотра информации протокола OSPF используйте команду:

```
Admin@nodename> show network ospf
...
Admin@nodename> show network ospf <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера
virtual-router	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF (<vrf-name> all)
route	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF
database	Отображение информации: • Router Link States — пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны. Используются для передачи информации о собственных интерфейсах и своих соседях соседним маршрутизаторам, находящимся в той же зоне. • Network Link States — пакеты LSA Type 2 (Network LSA) генерируются выделенным маршрутизатором (Designated Router, DR) для описания всех маршрутизаторов, подключенных к его сегменту напрямую. • Summary Link States — пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • ASBR-Summary Link States — пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора

Параметр	Описание
	(Autonomous System Border Router, ASBR) в других областях
neighbor	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора). • Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором (Designated Router, DR). Если приоритеты маршрутизаторов равны, будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например Full/DR, Full/BDR, Full/Drother. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Дополнительные параметры: • interface-name — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • all — отображение таблицы со всеми соседями. • detail — отображение подробной информации о соседях
interface	Отображение информации об интерфейсах OSPF. Дополнительные параметры: • interface-name — отображение информации об указанном интерфейсе. • traffic — статистика переданных и принятых пакетов OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment)
border-routers	Отображение информации о пограничных маршрутизаторах

Для перезапуска процесса OSPF используйте команду:

```
Admin@nodename> clear network ospf <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
<code>interface-name</code>	Название интерфейса
<code>node-name</code>	Выбор узла кластера
<code>virtual-router</code>	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<code><vrf-name></code> <code>all</code>)
<code>interface</code>	Интерфейс, на котором необходимо перезапустить процесс OSPF (<code><interface-name></code>)
<code>neighbor</code>	Выбор соседей, в отношении которых будет перезапущен процесс

Мониторинг BGP

С помощью команд этого раздела вы можете выполнять диагностику протокола BGP.

Для просмотра таблиц BGP-маршрутизатора используйте команду:

```
Admin@nodename> show network bgp
...
Admin@nodename> show network bgp <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
<code>node-name</code>	Выбор узла кластера
<code>virtual-router</code>	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<code><vrf-name></code> <code>all</code>)
<code>ip</code>	IP-адрес, маршрут до которого необходимо отобразить
<code>statistics</code>	Отображение статистики BGP
<code>neighbors</code>	

Параметр	Описание
	Отображение информации о BGP-соседях. Для отображения информации об определенном соседе укажите его IP-адреса Дополнительные параметры, доступные при указании соседа: • received-routes — принятые маршруты до применения к ним входящей политики (Route map и фильтры). • advertised-routes — маршруты, которые анонсируются указанному соседу
summary	Просмотр краткой информации о соседях

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии) используйте команду:

```
Admin@nodename> clear network bgp
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
ip	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации
node-name	Выбор узла кластера
virtual-router	Название виртуального маршрутизатора, которому принадлежит BGP-сосед

Если на соседних устройствах поддерживается метод Route Refresh, вы можете избежать полной реинициализации сессии с соседом. Для этого необходимо отправить специальное сообщения **ROUTE REFRESH**, позволяющее обновить информацию без прерывания работы маршрутизации.

Для обновления информации без обрыва сессии с соседом используйте команду:

```
Admin@nodename> clear network bgp ip <neighbor-ip> soft in | out
Admin@nodename> clear network bgp virtual-router <vrf-name> ip
<neighbor-ip> soft in | out
```

Мониторинг RIP

С помощью команд этого раздела вы можете выполнять диагностику протокола RIP.

Для просмотра информации протокола RIP из таблицы маршрутизатора по умолчанию используйте команду:

```
Admin@nodename> show network rip
...
Admin@nodename> show network rip <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера
status	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т. п.
virtual-router	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить (<vrf-name> all)

Мониторинг мультикаст-трафика

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию используйте команду:

```
Admin@nodename> show network mroute
...
Admin@nodename> show network mroute <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера
count	Отображение статистики о группе и источнике
virtual-router	Выбор виртуального маршрутизатора (<vrf-name> all)
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации
fill	Таблица маршрутизации мультикаст-трафика
ip	Отображение записи для определенного IP-адреса

Мониторинг IGMP

Для мониторинга работы протокола IGMP (Internet Group Management Protocol) используйте команду:

```
Admin@nodename> show network igmp <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера
virtual-router	Выбор виртуального маршрутизатора
statistics	Статистика по сообщениям: • IGMP Membership Query — сообщение от сервера к клиенту с директивой обновить подписку на получаемые клиентом группы. Без обновления сервер перестанет вещать группы в данном сегменте сети. • IGMP Leave — сообщение от клиента к серверу с запросом убрать мультикаст-группу из списка получаемых. • IGMP Membership Report — сообщение от клиента к серверу с запросом получать трафик этой группы
join	Отображение информации о группах IGMP

Параметр	Описание
sources	Отображение информации об источниках мультикаст-трафика
groups	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: • общее количество групп; • интерфейс, через который группа доступна; • адрес группы; • режим INCLUDE или EXCLUDE; • таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report; • время, в течение которого группа известна
interface	Отображение информации об интерфейсе, связанном с мультикаст-маршрутизацией: • название интерфейса, его статус и адрес; • версия IGMP; • опрашиватель (IGMP querier) и его адрес; • таймер, который обнуляется каждый раз, когда приходит сообщение Query с меньшим IP-адресом. Дополнительные параметры: • interface-name — название интерфейса; • detail — подробная информация об интерфейсе

Мониторинг PIM

Для мониторинга работы протокола PIM (Protocol-Independent Multicast) используйте команду:

```
Admin@ndename> show network pim <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
<code>node - name</code>	Выбор узла кластера, для которого необходимо отобразить информацию
<code>virtual - router</code>	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию
<code>vxlan - groups</code>	Информация о группах VXLAN, использующихся в мультивещании
<code>statistics</code>	Статистика протокола
<code>join</code>	Отображение информации о группах протокола PIM
<code>neighbor</code>	Информация о соседях: • интерфейс, через который была получена информация о соседе; • адрес соседа; • время, прошедшее с последнего начала работы PIM; • время, в течение которого сосед доступен; • приоритет DR
<code>next - hop</code>	Записи об адресах next-hop
<code>state</code>	Информация об известных S, G маршрутах, Incoming Interface (IIF), Outgoing Interface List (OIL)
<code>rp - info</code>	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP
<code>interface</code>	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т. п. Дополнительные параметры: • <code>interface - name</code> — название интерфейса; • <code>traffic</code> — Статистика отправленных и полученных сообщений; • <code>detail</code> — подробная информация об интерфейсе
<code>group - type</code>	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
<code>secondary</code>	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Команды мониторинга состояния кластера

Команды мониторинга состояния кластера могут быть запущены на любом из узлов, входящих в кластер. Вы можете получить информацию о текущем состоянии кластера, его узлов, режиме работы кластера и истории переключения состояний.

Для мониторинга состояния кластера используйте команду:

```
Admin@nodename> show ha-cluster state
```

Для мониторинга состояния узлов кластера используйте команду:

```
Admin@nodename> show ha-cluster tablestat
```

Для просмотра информации об истории переключения состояния кластера используйте команду:

```
Admin@nodename> show ha-cluster failover
```

Команды управления заблокированными COB IP-адресами

Для просмотра таблицы с заблокированными системой COB IP-адресами используйте команду:

```
Admin@nodename> show blocked-ip
```

Для разблокирования отдельных IP-адресов используйте команду:

```
Admin@nodename> clear blocked-ip ips [ ip-address ip-address ... ]
```

Команды просмотра журналов диагностики

С помощью команд этого раздела вы можете просматривать события, содержащиеся в журналах диагностики системы, в статическом и динамическом режиме.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log core static | grep ldap
```

Подробнее о функции фильтрации вывода — в разделе «[Общие положения](#)».

Просмотр системного журнала диагностики

Для вывода всего системного журнала диагностики в консоль используйте команду:

```
Admin@nodename> show logs log core static
```

Для вывода событий системного журнала диагностики в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log core dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш **Ctrl + C**.

Просмотр журналов диагностики протоколов маршрутизации

С помощью команд этого раздела вы можете просматривать события журналов диагностики протоколов маршрутизации. Включение в журналы событий выбранного протокола выполняется командой **debug** в режиме конфигурации (подробнее — в разделе «[Режим конфигурации](#)»).

Для вывода событий журнала диагностики в консоль используется команда вида:

```
Admin@nodename> show logs log routing <parameters> <static|dynamic>
```

В команде необходимо указать протоколы, для которых будут выводиться события диагностики.

Параметр	Описание
all-routers	Все протоколы
rip	Протокол RIP
bgp	Протокол BGP
igmp	Протокол IGMP
pim	Протокол PIM
ospf	Протокол OSPF
bfd	Протокол BFD
msdp	Протокол MSDP
mroute	Таблица мультикаст-маршрутизации mroute
ssmpingd	Инструмент тестирования мультикаст-вещания ssmpingd

Для вывода всего журнала диагностики в консоль используйте команду:

```
Admin@nodename> show logs log routing <parameters> static
```

Для вывода событий журнала диагностики в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log routing <parameters> dynamic
```

Параметры команд аналогичны параметрам, указанным ранее.

Для отключения вывода событий журнала используйте комбинацию клавиш **Ctrl + C**.

Просмотр журналов диагностики VPN-сервера

С помощью команд этого раздела вы можете просматривать события журналов диагностики VPN-сервера и VPN-клиента (когда UserGate NGFW выступает в роли узла-инициатора соединения в сценарии Site-to-site VPN).

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

```
Admin@nodename> show logs log vpn-server static
```

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-server dynamic
```

Для вывода всего журнала диагностики VPN-сервера, работающего в режиме инициатора соединения в сценарии Site-to-site VPN, используйте команду:

```
Admin@nodename> show logs log vpn-client static
```

Для вывода событий журнала диагностики VPN-сервера, работающего в режиме инициатора соединения в сценарии Site-to-site VPN, в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-client dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш Ctrl + C.

Просмотр информации об авторизованных пользователях

Для просмотра информации обо всех авторизованных пользователях используйте команду:

```
Admin@nodename> show user-auth
```

Для просмотра деталей сессии определенного пользователя используйте команду:

```
Admin@nodename> show user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (**login**), так и его IP-адрес (**ip-address**).

Для удаления сессии определенного пользователя используйте команду:

```
Admin@nodename> clear user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (**login**), так и его IP-адрес (**ip-address**).

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации интерфейса командной строки используется команда:

```
Admin@nodename> configure
```

В режиме конфигурации приглашение командной строки будет выглядеть следующим образом:

```
Admin@nodename#
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

Где:

<action> — действие, которое необходимо выполнить;

<level> — уровень контекста конфигурации, который соответствует одному из разделов структуры конфигурации в веб-интерфейсе NGFW;

<filter> — идентификатор объекта, к которому происходит обращение;

<configuration_info> — значение параметров, которые необходимо применить к объекту.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • execute — выполнение команд, которые не относятся к текущей конфигурации устройства (ping, date, traceroute и т. п.) Команда доступна независимо от уровня конфигурации. Подробнее — в разделе «Команды execute». • create — создание новых объектов. • set — изменение параметров объектов, включение различных параметров. • show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено все, что находится глубже текущего уровня. • delete — удаление объекта или параметра из списка параметров. • edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображен под командной строкой. • end — переход на один уровень конфигурации выше. • top — возврат на самый верхний уровень конфигурации. • export — экспорт сертификатов. Подробнее — в разделе «Команды export». • import — импорт конфигурации. Подробнее — в разделе «Команды import». • debug — включение журналирования событий протоколов динамической маршрутизации в режиме отладки. Подробнее — в разделе «Команды debug». • exit — выход из режима конфигурации.

Наименование	Описание
	Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображен под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show adapter: port0 interface-name : port0 node-name : utmcore@dineanoulwer zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp</pre> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end два раза:

Наименование	Описание
	<pre data-bbox="608 253 1015 524">Admin@nodename# Level: network interface Admin@nodename# end Level: network Admin@nodename# end Admin@nodename#</pre> Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду top: <pre data-bbox="608 763 1015 938">Admin@nodename# Level: network interface Admin@nodename# top Admin@nodename#</pre>
<level>	Уровни контекста конфигурации в командной строке повторяют разделы конфигурации в веб-интерфейсе UserGate NGFW: • settings — соответствует разделу веб-интерфейса «UserGate»; • users — соответствует разделу веб-интерфейса «Пользователи и устройства»; • network — соответствует разделу веб-интерфейса «Сеть»; • network-policy — соответствует разделу веб-интерфейса «Политики сети»; • security-policy — соответствует разделу веб-интерфейса «Политики безопасности»; • vpn — соответствует разделу веб-интерфейса «VPN»; • global-portal — соответствует разделу веб-интерфейса «Глобальный портал»; • libraries — соответствует разделу веб-интерфейса «Библиотеки»; • monitoring — соответствует разделу веб-интерфейса «Диагностика и мониторинг»
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее

Наименование	Описание
	идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать параметры(<configuration_info>). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках. Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду: <pre>Admin@nodename# show network interface adapter port0</pre> Будет отображена информация об интерфейсе port0 текущего узла NGFW. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла: <pre>Admin@nodename# show network interface adapter (node-name another_nodename interface port0)</pre>  Важно! Круглые скобки должны быть отделены пробелами с обеих сторон
<configuration_info>	Указание параметра с аргументом. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать группу с именем VPN users: <pre>Admin@nodename# create users group "VPN users"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра. Параметры записываются в квадратных скобках и разделяются пробелами. Например, необходимо в группу VPN users добавить пользователей user1 и user2. Параметру users необходимо задать аргумент [user1 user2]:

Наименование	Описание
	<pre>Admin@nodename# set users group "VPN users" users [user1 user2]</pre>  Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон

Команды execute

Команды имеют следующую структуру:

```
Admin@nodename# execute <command-name>
```

Список команд раздела **execute**.

Команда	Описание
cache	Очистка кэша LDAP-записей: <pre>Admin@nodename# execute cache ldap-clear</pre>
check-geoip	Проверка географической принадлежности IP-адреса по текущей базе GeoIP: <pre>Admin@nodename# execute check-geoip ip <ip-address></pre>
clear-cli-history	Удаление истории команд интерфейса CLI (доступно в версии 7.5.0 и выше). Можно удалить историю всех введенных команд интерфейса CLI или только команд в одном из режимов работы интерфейса (в режиме конфигурации или в режиме диагностики):

Команда	Описание
	<pre>Admin@nodename# execute clear-cli-history Admin@nodename# execute clear-cli-history modes [<configure diagnostic>]</pre>
configure-cluster	Генерация секретного кода, необходимого для добавления нового узла в кластер конфигурации: <pre>Admin@nodename# execute configure-cluster generate-secret-key <parameter></pre> Где: • secret — ключ для генерации секретного кода в формате [0–9a–zA–Z]+#[0–9a–zA–Z]+ (например, example#key); • expiration-time — срок действия кода в секундах; • request-limit — срок действия запроса на генерацию кода.  Важно! Для использования этой команды необходимо наличие лицензии на модуль Cluster
date	Просмотр текущих значений даты и времени на узле: <pre>Admin@nodename# execute date</pre>
dig	Проверка записи DNS домена: <pre>Admin@nodename# execute dig host <hostname> <parameters> Admin@nodename# execute dig host <IP-address> <parameters></pre> В команде можно использовать следующие параметры: • reverse-lookup — получение имени устройства по IP-адресу;

Команда	Описание
	• dns — указание IP-адреса DNS-сервера; • tcp — использование протокола TCP вместо UDP.
factory-reset	Возврат устройства в первоначальное состояние (доступно в версии 7.5.0 и выше): <pre>Admin@nodename# execute factory-reset</pre> Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
firewall	Применение всех правил межсетевого экрана с обрывом текущих сессий: <pre>Admin@nodename# execute firewall force-changes</pre>
license	Команда регистрации продукта имеет следующую структуру: <pre>Admin@nodename# execute license activate <pin-code></pre> В качестве <pin-code> укажите код активации продукта
logs	Команда разовой отправки журналов по имеющемуся правилу экспорта журналов: <pre>Admin@nodename# execute logs send-once <export-log-name></pre>
mc-force-disconnect	Команда аварийного отключения узла от MC, с которым он был интегрирован. В зависимости от выбранного аргумента импортированные из MC объекты сохраняются локально или удаляются: • keep — отключение от MC с сохранением всех импортированных из MC объектов (библиотеки, правила и т. д.). Импортированные из MC объекты конвертируются в локальные. • delete — отключение от MC с удалением всех импортированных из MC объектов (библиотеки, правила и т. д.). Импортированные объекты, которые в

Команда	Описание
	настоящий момент используются, конвертируются в локальные. <pre>Admin@nodename# execute mc-force-disconnect keep Admin@nodename# execute mc-force-disconnect delete</pre>
netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя узла для проверки доступности по TCP или URL — для HTTP; • dns-ip — IP-адрес сервера DNS; • dns-tcp — использование TCP вместо UDP для DNS-запроса; • check-cert — проверка SSL-сертификата; • type — проверка доступности по: ◦ http; ◦ tcp (если порт не указан, то используется порт 80); • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; • timeout — максимальный тайм-аут ожидания ответа от веб-сервера; • user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. <pre>Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name></pre>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: • host — IP-адрес или доменное имя узла.

Команда	Описание
	• count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). • numeric — не определять имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — максимальный размер блока данных отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. <pre>Admin@nodename# execute ping host <hostname> count <number></pre>
reboot	Перезагрузка устройства: <pre>Admin@nodename# execute reboot</pre>
restore-mac	Восстановление mac-адреса интерфейса: <pre>Admin@nodename# execute restore-mac interface <interface-name></pre>
shutdown	Выключение устройства: <pre>Admin@nodename# execute shutdown</pre>
termination	Закрытие сессий администраторов или пользователей: <pre>Admin@nodename# execute termination <admin- sessions user-sessions></pre>

Команда	Описание
	Подробнее — в разделе «Настройка сессий администраторов»
traceroute	Трассировка соединения до определенного узла. Параметры команды: • host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; • interface <iface-name> — интерфейс, с которого будут отправляться пакеты; • not-map-ip — не искать hostname для IP-адреса при отображении; • use-icmp-echo — использовать ICMP echo; • port — указать порт вместо порта по умолчанию (1 — 65535); • min-interval — минимальный интервал между пакетами. <pre>Admin@nodename# execute traceroute host <hostname></pre>
update	Обновление: • software-updates — обновление программного обеспечения. • libraries-updates — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.

Часть представленных выше команд, кроме команд обновления, регистрации продукта, управления сессиями администраторов и очистки кэша, также доступны в режиме [диагностики и мониторинга](#). Для их выполнения используется команда:

```
Admin@nodename> <command-name>
```

Команды import

Импорт доступен в разделах «Настройки», «Пользователи», «Сеть», «Политики сети», «Политики безопасности», «Глобальный портал», «VPN».

В разделе «Настройки» (**settings**) можно импортировать сертификаты. Подробнее — в разделе «[Настройка сертификатов](#)».

В разделах «Пользователи» (**users**), «Сеть» (**network**), «Политики сети» (**network-policy**), «Политики безопасности» (**security-policy**), «Глобальный портал» (**global-portal**), «VPN» (**vpn-server**, **vpn-client**) можно импортировать правила, написанные на UPL. При использовании импорта, все существующие правила будут заменены на указанные.

В разделе «Пользователи» (**users**) можно импортировать правила captive-портала. Подробнее о правилах — в разделе «[Captive-портал](#)».

В разделе «Сеть» (**network**) можно импортировать правила DNS. Подробнее — в разделе «[Настройка правил DNS](#)».

В разделе «Политики сети» (**network-policy**) можно импортировать правила межсетевого экрана, NAT и маршрутизации, пропускной способности, балансировки нагрузки. Подробнее о правилах читайте в соответствующих разделах: «[Настройка правил межсетевого экрана](#)», «[Настройка правил NAT и маршрутизации](#)», «[Настройка правил пропускной способности](#)». «[Настройка балансировки нагрузки](#)».

В разделе «Политики безопасности» (**security-policy**) можно импортировать правила контентной фильтрации, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, сценариев, защиты почтового трафика, ICAP-правил и правил защиты DoS. О добавлении правил читайте в соответствующих разделах: «[Настройка фильтрации контента](#)», «[Настройка веб-безопасности](#)», «[Настройка правил инспектирования туннелей](#)», «[Настройка инспектирования SSL](#)», «[Настройка инспектирования SSH](#)», «[Настройка сценариев](#)», «[Настройка правил защиты почтового трафика](#)», «[Настройка правил ICAP](#)», «[Настройка правил защиты DoS](#)».

В разделе «Глобальный портал» (**global-portal**) можно импортировать правила веб-портала и reverse-прокси. Подробнее о создании правил — в разделах: «[Настройка веб-портала](#)» и «[Настройка правил reverse-прокси](#)».

В разделе «VPN» (**vpn-server**, **vpn-client**) можно импортировать серверные и клиентские правила, о добавлении которых читайте в разделах: «[Настройка серверных правил](#)» и «[Настройка клиентских правил](#)».

Команды export

Команда для экспорта сертификатов.

Вы можете экспортировать сертификаты, всю цепочку сертификатов и CSR:

```
Admin@nodename# export settings certificates <certificate-name>  
Admin@nodename# export settings certificates <certificate-name> with-  
chain on
```

Подробнее об управлении сертификатами — в разделе «[Настройка сертификатов](#)».

Команда debug

Команда debug позволяет включить журналирование событий протоколов маршрутизации в режиме отладки. События записываются в debug-лог. Их просмотр также возможен в режиме мониторинга в консоли CLI (подробнее — в разделе «[Диагностика и мониторинг](#)»).

Для включения журналирования конкретного протокола маршрутизации используется команда:

```
Admin@nodename# debug <protocol> <parameters>
```

Поддерживаются следующие протоколы:

- rip;
- ospf
- bgp;
- igmp;
- pim;
- bfd;
- msdp;
- mroute — таблица мультикаст-маршрутизации;
- ssm pingd — инструмент тестирования мультикаст-вещания.

НАСТРОЙКА УСТРОЙСТВА

Настройка устройства (Описание)

Настройка параметров работы CLI

На уровне `settings cli` настраиваются параметры работы интерфейса командной строки.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@nodename# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида `Admin@nodename#`) на удобное вам. Например, чтобы поменять вид системного приглашения на `NodeAABBCC`, выполните следующую команду:

```
Admin@nodename# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@nodename# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@nodename#
```

Чтобы задать уровень детализации диагностики используется команда:

```
Admin@nodename# set settings cli log-level
```

Вы можете установить следующие уровни детализации:

- **off** — отключить журналирование;
- **error** — только ошибки;
- **warning** — ошибки и предупреждения;
- **info** — ошибки, предупреждения и дополнительная информация;
- **debug** — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:

```
Admin@nodename# show settings cli
```

Настройка базовых параметров устройства

На уровне `settings general` настраиваются базовые параметры UserGate NGFW.

Структура команд для настройки базовых параметров устройства:

```
Admin@nodename# set settings general <settings-module> <parameters>
```

Базовые параметры устройства сгруппированы в разделы.

Раздел	Описание
admin-console	Параметры консоли управления: • timezone — часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т. п. • language — язык интерфейса: ◦ ru — русский; ◦ en — английский.

Раздел	Описание
	• webaccess — режим аутентификации веб-консоли: ◦ password — аутентификация по имени и паролю; ◦ cert — аутентификация по X.509-сертификату. • uc-profile — выбор профиля пользовательских сертификатов. • web-ssl-profile — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». • response-pages-ssl-profile — выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации captive-портала. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». • api-session-lifetime — время ожидания сеанса администратора в минутах. По истечении этого времени при вводе команды CLI, использующей API-вызовы (команды создания объектов, изменения параметров, просмотра параметров, удаления объектов или параметров), сессия администратора будет завершена сообщением Authentication session expired. Restart CLI
server-time	Параметры установки точного времени: • ntp-enabled — включение и отключение использования NTP-серверов. • primary-ntp-server — адрес основного NTP-сервера. • second-ntp-server — адрес запасного NTP-сервера. • time — установка времени на устройстве. Время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
modules	Настройка работы модулей устройства: • proxy-port — указание нестандартного номера порта, который будет использоваться для подключения к встроенному прокси-серверу. • auth-captive — указание служебного домена, который будет использоваться UserGate NGFW при авторизации пользователей через captive-портал.

Раздел	Описание
	• logout-captive — указание служебного домена, который будет использоваться пользователями UserGate NGFW для окончания сессии. • cert-captive — указание служебного домена, который будет использоваться UserGate NGFW при авторизации пользователей через captive-портал с помощью сертификатов. • block-page-domain — указание служебного домена, который будет использоваться для отображения страницы блокировки. • ftp-enabled — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. • ftp-domain — указание служебного домена, который будет использоваться для предоставления пользователям сервиса FTP поверх HTTP. • tunnel-inspection-zone — выбор зоны для инспектируемых туннелей: ◦ name — название зоны; ◦ enabled — включение или отключение зоны. • snmp-engine-id — настройка идентификатора SNMP устройства: ◦ length <fixed dynamic> — длина идентификатора. Фиксированная (не более 8 байт), только для типа text или динамическая (не более 27 байт). ◦ type <ip4 ip6 mac text octets> — формат идентификатора SNMP (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ value — значение идентификатора. • terminal-sever-agent — настройка пароля для подключения агентов авторизации терминального сервера. • lldp — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: ◦ transmit-delay — задержка передачи. Указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например после изменения

Раздел	Описание
	имени узла или адреса управления. Может принимать значения от 1 до 3600. Указывается в секундах. ◦ transmit-hold — значение мультипликатора удержания. Произведение значений transmit-delay и transmit-hold определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100
cache	Параметры кэширования прокси-сервера: • caching-mode — включение или отключение режима кэширования. • exclusions — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду: <pre>Admin@nodename# delete settings general cache exclusions [<URL>]</pre> • max-cacheable-size — максимальный размер объектов, которые будут кэшироваться (МБ). • ram-size: размер оперативной памяти, отведенный под кэширование (МБ)
log-analyzer	Параметры модуля сбора статистики: • use-local-stat-server — использование локальной службы журналирования
proxy-portal	Параметры предоставления доступа к внутренним ресурсам компании с помощью веб-портала: • enabled — включение или отключение использования веб-портала. • hostname — имя узла, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. • port — порт TCP, который будет использоваться сервисом веб-портала. • auth-profile — указание профиля аутентификации, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей аутентификации».

Раздел	Описание
	• auth-template — выбор шаблона страницы аутентификации. • portal-template — выбор шаблона веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. • enable-ldap — выбор домена AD или LDAP на странице аутентификации: ◦ on — показывать; ◦ off — не показывать. • use-captcha — показывать на странице аутентификации веб-портала код для ввода пользователем: ◦ on — показывать; ◦ off — не показывать. • ssl-profile — выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей SSL». • certificate — выбор сертификата, который будет использоваться для создания HTTPS-соединения. • auth-mode — выбор метода аутентификации: ◦ aaa — аутентификация через логин и пароль локальных пользователей или аутентификация пользователей на AAA-сервере; ◦ pki — аутентификация посредством X.509-сертификатов. • user-cert-profile — выбор профиля пользовательских сертификатов при аутентификации посредством сертификатов
pcap	Настройка захвата пакетов. Команда для настройки: <pre>Admin@nodename# set settings general pcap packet-capture-mode <parameters></pre> Параметры: • no-capture — без захвата; • one-packet — один пакет; • previous — предшествующие пакеты;

Раздел	Описание
	• previous-and-following — предшествующие и последующие пакеты: ◦ previous-packets — количество предшествующих пакетов (от 4 до 30 пакетов); ◦ following-packets — количество последующих пакетов (от 2 до 15 пакетов)
change-tracker	Настройка учета изменений параметров устройства: • enabled — включение или отключение учета изменений параметров. • event-tracker-types — типы изменений (например, приказ, регламентные работы и т. д.). Для удаления типа изменения используется команда: <pre>Admin@nodename# delete settings general change-tracker event-tracker-types [type1 ...]</pre>
management-center	Настройка агента UserGate Management Center. Команда для настройки: <pre>Admin@nodename# set settings general management-center <parameters></pre> Параметры: • enabled — включение или отключение агента UserGate Management Center; • mc-address — адрес сервера UserGate Management Center; • device-code — уникальный код устройства для подключения устройства к UserGate Management Center
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек. Расписание для обновления программного обеспечения задается командой: <pre>Admin@nodename# set settings general updates- schedule software schedule <schedule disabled></pre>

Раздел	Описание
	Единое расписание для скачивания обновлений библиотек задается командой: <pre>Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule disabled></pre> Расписание для скачивания обновлений отдельных библиотек задается командой: <pre>Admin@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule/disabled></pre> Время задается в crontab-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями. Команда для просмотра расписания обновлений: <pre>Admin@nodename# show settings general updates-schedule</pre>
upstream-proxy	Настройка перенаправления HTTP-трафика на вышестоящий прокси-сервер (для версий ПО 7.1.x–7.3.x): • enabled — включение или выключение перенаправления трафика на вышестоящий прокси-сервер (on/off); • mode — тип вышестоящего прокси-сервера (HTTP(S)/SOCKS5); • ip — IP-адрес вышестоящего прокси-сервера; • port — порт вышестоящего прокси-сервера;

Раздел	Описание
	• auth — аутентификация на вышестоящем прокси-сервере (on/off); • name — логин на вышестоящем прокси-сервере; • password — пароль на вышестоящем прокси-сервере
metrics-collection	Настройка параметров передачи метрик телеметрии. Доступна в версии 7.5.0 и выше. • enabled — включение или выключение отправки метрик телеметрии. По умолчанию отправка метрик телеметрии включена. • masking-sensitive-data — маскирование чувствительных данных в отправляемых метриках. К чувствительным данным относятся IP-адреса, MAC-адреса, URL, адреса эл. почты и т. д. По умолчанию маскирование чувствительных данных отключено.

Настройка управления устройством

Настройка диагностики

В этом разделе вы можете управлять параметрами диагностики устройства, необходимыми службе технической поддержки для решения возможных проблем.

Параметры диагностики задаются на уровне `settings loglevel`.

С помощью следующей команды вы можете установить необходимый уровень детализации журналирования событий:

```
Admin@nodename# set settings loglevel value <off | error | warning | info | debug>
```

- **off** — ведение журналов диагностики отключено;
- **error** — журналировать только ошибки;
- **warning** — журналировать только ошибки и предупреждения;
- **info** — журналировать только ошибки, предупреждения и дополнительную информацию;

- **debug** — журналировать все возможные события.

При журналировании на уровнях **warning**, **info** и **debug** может снижаться производительность UserGate NGFW, поэтому рекомендуется устанавливать уровни **error** или **off**, если технической поддержкой UserGate не было предложено иное.

Для просмотра состояния уровня детализации диагностики используется команда:

```
Admin@nodename# show settings loglevel
```

Для включения или отключения удаленного помощника (radmin) используется команда:

```
Admin@nodename# set settings radmin enabled <on | off>
```

Для просмотра состояния удаленного помощника используется команда:

```
Admin@nodename# show settings radmin
```

Режим emergency

Если произошел сбой в работе ядра UserGate NGFW, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации UserGate NGFW. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Команда входа в режим emergency CLI выглядит следующим образом:

```
ssh Admin@emergency@<NGFW_IP> -p 2200
```

Команда включения и отключения удаленного доступа к серверу для технической поддержки в режиме emergency:


```
Admin@emergency@NGFW# set radmin-emergency enabled <on | off>
<parameters>
```

В команде указываются следующие сетевые параметры:

- interface — название интерфейса;
- ip-addr — IP-адрес интерфейса;
- gateway-address — IP-адрес шлюза.

В версии 7.5.0 и выше в режиме emergency доступна команда возврата устройства в первоначальное состояние:

```
Admin@emergency@NGFW# execute factory-reset
```

Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды.

Настройка получения обновлений

В этом разделе вы можете установить канал получения обновлений для устройства (стабильные версии или бета-версии).

Канал обновлений устанавливается с помощью команды:

```
Admin@nodename# set settings device-mgmt updates-channel <stable |
beta>
```

Для просмотра наличия обновлений и выбранного канала обновления используется команда:

```
Admin@nodename# show settings device-mgmt updates-channel
```

Управление резервным копированием

На уровне `settings device-mgmt` вы можете создавать правила резервного копирования.

Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

```
Admin@nodename# create settings device-mgmt settings-backup
<parameters>
```

Параметры правил резервного копирования.

Параметр	Описание
enabled	Включение или отключение правила создания резервной копии устройства
name	Название правила резервного копирования
description	Описание правила резервного копирования
type	Выбор типа удаленного сервера для экспорта файлов: • ssh; • ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи
path	Путь на сервере, куда будут выгружены файлы

Параметр	Описание
schedule	Расписание экспорта файлов резервных копий. Время задается в crontab-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Для изменения существующего правила резервного копирования используется команда:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения, аналогичен списку параметров, доступных при создании правила.

Для удаления правила резервного копирования используется команда:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Для просмотра параметров правила резервного копирования используется команда:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в правиле параметры (см. список параметров [в таблице выше](#)).

Экспорт параметров

Создание и настройка правил экспорта параметров устройства происходит на уровне `settings device-mgmt settings-export`.

Для создания правила экспорта параметров используется команда:

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Параметры правила экспорта.

Параметр	Описание
<code>enabled</code>	Включение или отключение правила экспорта параметров устройства
<code>name</code>	Название правила экспорта
<code>description</code>	Описание правила экспорта
<code>type</code>	Тип удаленного сервера для экспорта параметров: • <code>ssh</code>; • <code>ftp</code>
<code>address</code>	IP-адрес удаленного сервера
<code>port</code>	Порт сервера
<code>login</code>	Учетная запись на удаленном сервере
<code>password</code>	Пароль учетной записи на удаленном сервере
<code>path</code>	Путь на сервере, куда будут выгружены параметры
<code>schedule</code>	Расписание экспорта параметров. Время задается в <code>crontab</code>-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.

Параметр	Описание
	• Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Для изменения существующего правила экспорта параметров устройства используется команда:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения, аналогичен [списку параметров](#), доступных при создании правила.

Для удаления правила экспорта параметров используется команда:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Для просмотра параметров правила экспорта используется команда:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в существующем правиле параметры (см. список параметров в [таблице выше](#)).

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используйте следующую команду:

```
Admin@nodename# set settings change-control config <off | log | block>
```

Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate NGFW.

- **log** — активация режима отслеживания изменений конфигурации. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- **off** — отключение режима отслеживания изменений конфигурации. Необходимо указать пароль, который был задан при активации режима отслеживания конфигурации.
- **block** — активация режима отслеживания изменений конфигурации. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик.

Перед активацией защиты конфигурации администратор производит настройку устройства в соответствии с требованиями организации, после чего защищает параметры от изменений (режим **log** или **block**). Любое изменение параметров через веб-интерфейс, CLI или другими способами будет приводить к журналированию и блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений используется команда:

```
Admin@nodename# show settings change-control config
```

Настройка защиты исполняемых файлов от изменения

Для настройки защиты исполняемого кода устройства от потенциального несанкционированного изменения используется команда:

```
Admin@nodename# set settings change-control code <off | log | block>
```

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate NGFW.

- **log** — активация режима отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- **off** — отключение режима отслеживания несанкционированных изменений исполняемого кода. Необходимо указать пароль, который был задан при активации режима отслеживания исполняемого кода.
- **block** — активация режима отслеживания несанкционированных изменений исполняемого кода. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик. Чтобы отключить созданное правило межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов используется команда:

```
Admin@nodename# show settings change-control code
```

Настройка режима ускоренной обработки сетевого трафика

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@nodename# set settings fastpath enabled <on/off>
```

Для просмотра параметров режима ускоренной обработки трафика используется команда:

```
Admin@nodename# show settings fastpath
```

Настройка кластеров

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда для изменения параметров существующего узла кластера:

```
Admin@nodename# set settings device-mgmt configuration-cluster <node-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменение имени узла кластера.
description	Изменение описание узла кластера.
ip	Установка IP-адреса интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения параметров узла кластера:

```
Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-name>
```

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

```
Admin@nodename# execute configure-cluster generate-secret-key
```


Настройка кластера отказоустойчивости

Настройка кластеров отказоустойчивости производится на уровне **settings device-mgmt ha-clusters**.

Для создания кластера отказоустойчивости:

```
Admin@nodename# create settings device-mgmt ha-clusters
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • on, • off.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • active-passive: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных); • active-active: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
session-sync	Настройка синхронизации пользовательских сессий в кластере: • off — отключение синхронизации пользовательских сессий; • on — включение синхронизации пользовательских сессий; • ha-cluster-id: ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер,

Параметр	Описание
	например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: <pre>Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info></pre> Доступные параметры для <virtual-ips-filter>: • new: создать виртуальный IP-адрес для заданного кластера; • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • ip: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask); • ha-interfaces: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка session-sync активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Пример команды создания кластера:

```
Admin@nodename# create settings device-mgmt ha-clusters nodes
[ node_1 ] name "Test HA cluster" description "Test HA cluster
description" mode active-passive enabled on virtual-ips new ha-
interfaces [ node_1/port3 ] ip 192.168.1.5/24
```

Для редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-cluster <cluster-name>
```

Параметры для редактирования:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • on, • off.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • active-passive: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных); • active-active: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
master-node	Назначение мастер-узла кластера отказоустойчивости.
session-sync	Настройка синхронизации сессий в кластере: • off — отключение синхронизации пользовательских сессий; • on — включение синхронизации пользовательских сессий; • ha-cluster-id: ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий

Параметр	Описание
	(кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: <pre>Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info></pre> Доступные параметры для <virtual-ips-filter>: • new: создать виртуальный IP-адрес для заданного кластера; • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • ip: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask); • ha-interfaces: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка session-sync активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Примеры редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster"
nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces
[ node_1/port3 node_2/port3 ]
...
Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster"
master-node utmcore@iononsteswer
```

Для удаления кластера:

```
Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- **nodes**,
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>
```

Настройка кластеров (версия 7.5.0 и выше)

Настройка кластера конфигурации

Кластер конфигурации настраивается на уровне `settings device-mgmt configuration-cluster`.

Для изменения параметров существующего узла кластера используется команда:

```
Admin@nodename# set settings device-mgmt configuration-cluster <node-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменение имени узла кластера
description	Изменение описание узла кластера
ip	Установка IP-адреса интерфейса, входящего в зону, выделенную для кластера

Команды для удаления и отображения параметров узла кластера:

```
Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-name>
```

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

```
Admin@nodename# execute configurate-cluster generate-secret-key
```

Настройка кластера отказоустойчивости

Кластер отказоустойчивости настраивается на уровне `settings device-mgmt ha-clusters`.

Для создания кластера отказоустойчивости используется команда:

```
Admin@nodename# create settings device-mgmt ha-clusters
```

Далее необходимо задать следующие параметры:

Параметр	Описание
<code>enabled</code>	Включение/отключение кластера отказоустойчивости: • <code>on</code>, • <code>off</code>
<code>name</code>	Название кластера отказоустойчивости
<code>description</code>	Описание кластера отказоустойчивости
<code>nodes</code>	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
<code>delivery-mode</code>	Выбор режима отправки служебного трафика: • Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. • Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>virtual-ips</code>	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • <code>ip</code> — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask) ; • <code>ha-interfaces</code> — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)
<code>mode</code>	Выбор режима работы кластера: • active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен); • active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)

Параметр	Описание
<code>advertise-time</code>	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
<code>master-down-timer</code>	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
<code>preemption-delay</code>	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
<code>allow-non-vip-traffic</code>	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный»
<code>use-vmac</code>	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
<code>no-preempt</code>	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
<code>heartbeat</code>	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
<code>ha-cluster-multicast-id</code>	<code><num></code> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически
<code>sync-session</code>	

Параметр	Описание
	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
<code>sync-udp-icmp</code>	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
<code>vrid</code>	Идентификатор виртуального маршрутизатора (VRID)
<code>node-sync</code>	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
<code>excluded-sync-ips</code>	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
<code>unicast-sync-ip</code>	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-sync-port</code>	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-vrrp-ip</code>	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-vrrp-port</code>	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>track-interfaces-enabled</code>	Включение/отключение проверки интерфейсов
<code>track-interfaces</code>	

Параметр	Описание
	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • change-priority — понизить приоритет узла кластера. • fault — считать узел недоступным

Пример команды создания кластера отказоустойчивости:

```
Admin@nodename# create settings device-mgmt ha-clusters name ExampleCluster
nodes [ node_1 node_2 ] mode active-passive delivery-mode multicast heartbeat
[ node_1/port0 node_2/port0 ] node-sync [ node_1/port1 node_2/port1 ]
```

Команда для редактирования параметров кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters <cluster-name>
```

Команда для настройки кластера отказоустойчивости в облачной среде Yandex Cloud

```
Admin@nodename#
```

```
set settings device-mgmt ha-clusters ExampleCluster cloud service-
provider yandex-cloud yandex-cloud-settings routes new
```

Параметры для редактирования:

Параметр	Описание
heartbeat	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
mode	Выбор режима работы кластера: • active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-

Параметр	Описание
	узлом и переводится на резервный узел в случае, если основной недоступен). • active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
name	Название кластера отказоустойчивости
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
delivery-mode	Выбор режима отправки служебного трафика: • Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. • Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
enabled	Включение/отключение кластера отказоустойчивости: • on, • off
description	Описание кластера отказоустойчивости
virtual-ips	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • ip — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask) ; • ha-interfaces — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)
advertise-time	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120

Параметр	Описание
<code>master-down-timer</code>	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
<code>preemption-delay</code>	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
<code>allow-non-vip-traffic</code>	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный»
<code>use-vmac</code>	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
<code>no-preempt</code>	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
<code>master-node</code>	Назначение мастер-узла кластера отказоустойчивости
<code>ha-cluster-multicast-id</code>	<code><num></code> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически
<code>sync-session</code>	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
<code>sync-udp-icmp</code>	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
<code>vrid</code>	Идентификатор виртуального маршрутизатора (VRID)
<code>node-sync</code>	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные

Параметр	Описание
	интерфейсы, необходимо разрешить синхронизацию сессий.
<code>excluded-sync-ips</code>	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
<code>unicast-sync-ip</code>	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-sync-port</code>	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-vrrp-ip</code>	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>unicast-vrrp-port</code>	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
<code>track-interfaces-enabled</code>	Включение/отключение проверки интерфейсов
<code>track-interfaces</code>	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • change-priority — понизить приоритет узла кластера. • fault — считать узел недоступным
<code>checkers</code>	Настройка диагностики узлов кластера. Проверка доступности шлюзов • gateway-availability — проверка доступности шлюзов: ◦ enabled — включение/включение/отключение проверки доступности шлюзов. Чтобы помимо проверки самих шлюзов также выполнялась

Параметр	Описание
	проверка доступа в интернет, необходимо включить проверку сети. ◦ action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). ◦ fall-count — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ interval-time — регулярная проверка шлюзов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ rise-count — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. • resource-availability — проверка доступности ресурсов: ◦ enabled — включение/включение/отключение проверки доступности ресурсов. ◦ action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). ◦ fall-count — количество последовательных неудовлетворительных результатов проверки, после которых узел признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ interval-time — регулярная проверка ресурсов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ rise-count — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. ◦ resources — указание IP-адресов или FQDN тех ресурсов, доступ к которым будет проверяться
cloud	

Параметр	Описание
	Параметры кластера: • destination-prefix — укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud. • next-hops — IP-адреса интерфейсов узлов кластера. • route-table-id — идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud

Примеры редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster
nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces
[ node_1/port3 node_2/port3 ]
...
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster
master-node utmcore@iononsteswer
```

Для удаления кластера:

```
Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- **nodes**,
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>
```

Настройка управления доступом к консоли

UserGate NGFW

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

```
Admin@nodename# set settings administrators general
```

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: • on. • off.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).

Параметр	Описание
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

```
Admin@nodename# set settings administrators general block-time 400
```

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

```
Admin@nodename# show settings administrators general

strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

```
Admin@nodename# create settings administrators administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. • password: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора в формате domain\user. Структура команды при указании данного параметра: • connector: название сконфигурированного ранее LDAP-коннектора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. <pre>Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on</pre>

Параметр	Описание
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора • connector: название используемого LDAP-коннектора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. <pre>Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on</pre>
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • enabled: включение/отключение учётной записи администратора: ◦ on. ◦ off. • login: логин администратора. • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. • auth-profile: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type>
<admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-
type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user
testd.local\user1
```

```
login           : testd.local\user1
enabled         : on
type            : ldap_user
locked          : off
admin-profile    : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-
type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user
testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
api-permissions	Права доступа к API: • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: <pre>Admin@nodename# create settings administrators profiles ... api-permissions <permission> all</pre> или <pre>Admin@nodename# create settings administrators profiles ... api-permissions <permission> [object ...]</pre>
webui-permissions	Права доступа к веб-интерфейсу UserGate: • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты:

Параметр	Описание
	<pre>Admin@nodename# create settings administrators profiles ... webui-permissions <permission> all</pre> или <pre>Admin@nodename# create settings administrators profiles ... webui-permissions <permission> [object ...]</pre>
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: <pre>Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all</pre> или <pre>Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [object ...]</pre>

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name>
<parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

```
Admin@nodename# show settings administrators admin-sessions ( node
<node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

```
Admin@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Пример выполнения команд:

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : utmcore@dineanoulwer
```

```
admin-login      : Admin
source           : web
session_start_date : 2023-08-10T11:33:10Z
ip               : 10.0.2.2
node             : utmcore@dineanoulwer
```

```
Admin@nodename# execute termination admin-sessions 10.0.2.2/web
```

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : utmcore@dineanoulwer
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

```
Admin@nodename# execute termination admin-sessions ( node <node-name>
ip <session-ip> source <cli | web | ssh> admin-login <administrator-
login> )
```


Настройка сертификатов

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, которое будет отображено в списке.
description	Описание сертификата.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.
private-key	Приватный ключ в формате PEM.
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение).
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP сервера.
role	Тип сертификата: • web-cert-chain: цепочка сертификатов веб-консоли. • ssl-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • ssl-root: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • user: пользовательский сертификат, который может быть использован для авторизации пользователей при

Параметр	Описание
	их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • ssl-cert: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • captive-portal: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • saml: сертификат, который будет использован в SAML-клиенте. • none.

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.

Параметр	Описание
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: • web-cert-chain: цепочка сертификатов веб-консоли. • ssl-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • ssl-root: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • user: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • ssl-cert: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • captive-portal: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-

Параметр	Описание
	портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • saml: сертификат, который будет использован в SAML-клиенте. • none.
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP сервера.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

```
Admin@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Чтобы удалить сертификат из кэша используется команда:

```
Admin@nodename# delete settings certificates-cache <common-name>
```

Настройка параметров устройства

Изменение параметров устройства в CLI производится на уровне **settings device**. Для изменения используется следующая команда (где <setting-name> — название параметра):

```
Admin@nodename# set settings device <setting-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
l7	Включение или отключение загрузки модуля L7: • on; • off. По умолчанию модуль загружен. Важно! После изменения этого параметра требуется перезагрузка устройства UserGate
sip	Включение или отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: <pre>Admin@nodename# set settings device sip enabled</pre> • on; • off. По умолчанию модуль выгружен. Для разрешения передачи медиа-трафика напрямую между конечными участниками разговора: <pre>Admin@nodename# set settings device sip direct-media</pre> • on;

Параметр	Описание
	• off. Важно! После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (нажать «Принудительно применить» в разделе «Политики сети» → «Межсетевой экран»)
h323	Включение или отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • on; • off. По умолчанию модуль выгружен
idps	Включение или отключение загрузки модуля IDPS: • on; • off. По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка устройства UserGate
sunrpc	Включение или отключение загрузки модуля SunRPC: • on; • off. По умолчанию модуль выгружен
ftp-alg	Включение или отключение загрузки модуля FTP; модуль необходимо включать для сопоставления

Параметр	Описание
	сигнального соединения и соединения передачи данных в случае использования NAT: • on; • off.  Важно! Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен
auth-type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • ah — включение подписи; • pass — отключение проверки
fw-drop-invalid	Включение или отключение блокировки пакетов с некорректным набором параметров в полях заголовка: • on; • off. По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной
fw-established	Включение или отключение создания одного общего правила межсетевого экрана для обратных пакетов: • on; • off. По умолчанию настройка выключена
bypass-optimization	Включение или отключение оптимизации инспектирования SSL: • on; • off. При включённом параметре bypass-optimization для снижения нагрузки на прокси-сервер инспекция SSL не будет происходить, если на узле нет запрещающих правил инспектирования SSL. При этом в журнале веб-доступа при

Параметр	Описание
	включённой опции журналирования будет присутствовать только информация уровней L3/L4. По умолчанию настройка выключена

Для просмотра текущих настроек используйте команду:

```
Admin@nodename# show settings device
```

Настройка прокси-сервера

Набор команд для просмотра и настройки параметров прокси-сервера доступны на уровне **settings proxy**. Позволяет настроить такие параметры, как добавление заголовков HTTP — `via` и `forwarded`, а также настройки таймаутов на подключение к сайтам и на загрузку контента. Для изменения параметров прокси-сервера используется команда (где `<setting-name>` — название параметра):

```
Admin@nodename# set settings proxy <setting-name>
```

Для изменения доступны следующие параметры:

Параметр	Описание
via	Добавление HTTP заголовков Via: • on. • off. По умолчанию отключено.
forwarded	Добавление HTTP заголовков Forwarded: • on. • off. По умолчанию отключено.
xforwarded	Добавление HTTP заголовков X-Forwarded-For: • on. • off.

Параметр	Описание
	По умолчанию отключено.
connection-timeout	Время ожидания, выделяемое на подключение HTTP. По умолчанию — 20 секунд.
loading-timeout	Время ожидания, выделяемое на загрузку контента HTTP. По умолчанию — 60 секунд.
smode	Режим SYN Proxy: • on. • off. По умолчанию режим включен.
icap-wait-timeout	Время, которое сервер UserGate ждет ответа от ICAP-сервера; указывается в секундах. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила Переслать и игнорировать , UserGate отправит данные пользователю без модификации, если же действие правила Переслать , UserGate не отдаст данные пользователю. Значение по умолчанию — 10 секунд.
proxy_host_rfc	Доступно: • relaxed — использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • strict — соблюдать RFC. Данный режим используется по умолчанию.

Для просмотра текущих настроек используйте команду:

```
Admin@nodename# show settings proxy
```

Настройка работы с вышестоящими прокси-серверами

Настройка работы с вышестоящими прокси-серверами в версии 7.4.0 и выше

В интерфейсе командной строки настройка сценария перенаправления трафика доступна на уровне `upstream-proxy`.

Настройка состоит из следующих основных шагов:

1. Настройка подключения к вышестоящему прокси-серверу.
2. Создание профиля подключения.
3. Создание правила вышестоящего прокси.

Настройка подключения к вышестоящему прокси-серверу

Создание подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

```
Admin@nodename# create upstream-proxy servers <parameters>
```

Параметры для настройки подключения:

Параметр	Описание
enabled	Подключение к вышестоящему прокси-серверу: • on — включено; • off — отключено.
name	Название подключения к вышестоящему прокси-серверу
description	Описание подключения.
mode	Тип вышестоящего прокси-сервера: • https; • socks5.
ip	IP-адрес вышестоящего прокси-сервера.

Параметр	Описание
port	Порт вышестоящего прокси-сервера.
auth	Аутентификация на вышестоящем прокси-сервере: • on — требуется; • off — не требуется.
user	Логин для подключения к вышестоящему прокси-серверу.
password	Пароль для подключения к вышестоящему прокси-серверу.

Редактирование параметров ранее созданного подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

```
Admin@nodename# set upstream-proxy servers <server-name> <parameters>
```

В команде редактирования можно использовать те же параметры, которые используются в команде создания подключения.

Посмотреть настройки ранее созданного подключения можно с помощью команды:

```
Admin@nodename# show upstream-proxy servers <server-name>
```

Удалить ранее созданное подключение к вышестоящему прокси-серверу можно с помощью команды:

```
Admin@nodename# delete upstream-proxy servers <server-name>
```

Создание профиля подключения

Создать профиль подключения к вышестоящему прокси-серверу можно с помощью команды:

```
Admin@nodename# create upstream-proxy profiles <parameters>
```

Параметры для настройки профиля:

Параметр	Описание
enabled	Включение/отключение профиля: • on — включен; • off — отключен.
name	Название профиля.
description	Описание профиля.
used-servers	Указание вышестоящих прокси-серверов из списка ранее настроенных в системе.
http-method	Выбор метода HTTP-запроса для проверки состояния подключения с помощью контрольного обращения к указанному URL-ресурсу: GET, HEAD, OPTIONS .
url-host	Указание URL-ресурса для проверки состояния подключения через вышестоящий прокси-сервер.
check-interval	Интервал проверки подключения в секундах.
check-timeout	Время ожидания ответа проверки подключения в секундах.

Редактирование параметров ранее созданного профиля подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

```
Admin@nodename# set upstream-proxy profiles <profile-name>
```

В команде редактирования можно использовать те же параметры, которые используются в команде создания профиля.

Посмотреть настройки ранее созданного профиля можно с помощью команды:

```
Admin@nodename# show upstream-proxy profiles <profile-name>
```

Удалить ранее созданный профиль можно с помощью команды:

```
Admin@nodename# delete upstream-proxy profiles <profile-name>
```

Создание правила вышестоящего прокси

Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе [UserGate Policy Language](#).

Создать правило подключения к вышестоящему прокси-серверу можно с помощью команды:

```
Admin@nodename# create upstream-proxy rules <position> upl-rule
<parameters>
```

Редактировать ранее созданные правила можно с помощью команды:

```
Admin@nodename# set upstream-proxy rules <position> upl-rule
<parameters>
```

Посмотреть ранее созданные правила можно с помощью команды:

```
Admin@nodename# show upstream-proxy rules <position>
```

Удалить ранее созданные правила можно с помощью команды:

```
Admin@nodename# delete upstream-proxy rules <position>
```

Параметры для настройки правил:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true) — включение правила; • enabled(no) или enabled(false) — отключение правила.
name	Название правила. Например, name("Rule 1") .

Параметр	Описание
desc	Описание правила. Например, <code>desc("Rule example set via CLI")</code> .
proxy_profile	Профиль подключения к вышестоящему прокси-серверу. Например, <code>proxy_profile(Profile1)</code> .
fallback_action	Резервное действие при недоступности вышестоящего прокси-сервера: • прямое подключение — <code>fallback_action(direct);</code> • страница блокировки — <code>fallback_action(blockpage)</code>.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии.
src.zone	Зона источника трафика. Например, для указания зоны Trusted: <code>src.zone = Trusted</code> . Подробнее о настройке зон с использованием интерфейса командной строки — в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: <code>src.ip = lib.network();</code> в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе Настройка IP-адресов . Для указания списка доменов источника: <code>src.ip = lib.url();</code> в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, <code>src.geoip = RU</code>). Коды названий стран доступны по ссылке ISO 3166-1 .

Параметр	Описание
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе Настройка LDAP-коннектора. Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2").</code>
time	Настройка расписания работы правила. Для установки расписания: <code>time = lib.time();</code> в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка активации лицензии и обновления ПО

Для настройки активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/отключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • on — включен; • off — отключен.
ip	IP-адрес внешнего прокси-сервера.

Параметр	Описание
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: • on — требуется; • off — не требуется.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

Подробнее о функциональности Upstream Proxy, сценариях использования и настройках в веб-консоли администратора — в разделе [Upstream Proxy](#).

Настройка функциональности Upstream Proxy в версиях 7.1.x – 7.3.x

Для перенаправления HTTP-трафика на вышестоящий прокси-сервер используется команда:

```
Admin@nodename# set settings general upstream-proxy <parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/отключение перенаправления трафика на вышестоящий прокси-сервер: • on — включено; • off — отключено.
mode	Тип вышестоящего прокси-сервера: • https;

Параметр	Описание
	• socks5.
ip	IP-адрес вышестоящего прокси-сервера.
port	Порт вышестоящего прокси-сервера.
auth	Аутентификация на вышестоящем прокси-сервере: • on — требуется; • off — не требуется.
name	Логин на вышестоящем прокси-сервере.
password	Пароль на вышестоящем прокси-сервере.

Для просмотра созданных настроек перенаправления HTTP-трафика на вышестоящий прокси-сервер используется команда:

```
Admin@nodename# show settings general upstream-proxy
```

Настройка активации лицензии и обновления ПО производится на уровне `settings device-mgmt`. Для настройки активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/отключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • on — включен; • off — отключен.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.

Параметр	Описание
auth	Аутентификация на внешнем прокси-сервере: • on — требуется; • off — не требуется.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

Настройка параметров мониторинга устройства

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе [Оповещения](#).

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring snmp-parameter**:

```
Admin@nodename# edit monitoring snmp-parameter <parameters>
```

Для редактирования доступны следующие параметры:

Наименование	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.

Наименование	Описание
location	Информация о физическом расположении SNMP-агента.
description	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (length), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text. Engine ID может быть сформирован в формате: • ip4 — IPv4. • ipv6 — IPv6. • mac — MAC-адрес. • text — Текст. • octets — Октеты.

Подробнее о параметрах SNMP устройства UserGate читайте в разделе [SNMP](#).

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring snmp**:

```
Admin@nodename# edit monitoring snmp <parameters>
```

Для редактирования доступны следующие параметры:

Наименование	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.

Наименование	Описание
	На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
events	Выбор типов параметров, доступных для мониторинга по правилу.

Для работы SNMP-менеджера с UserGate NGFW необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе [Настройки сети](#).

Настройка профилей безопасности SNMP

Для настройки профилей безопасности для аутентификации SNMP-менеджеров используются команды на уровне **monitoring snmp-security-profile**:

```
Admin@nodename# edit monitoring snmp-security-profile <parameters>
```

Для редактирования доступны следующие параметры:

Наименование	Описание
name	Название профиля безопасности SNMP
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • none — без аутентификации, без шифрования. • no-encrypt — с аутентификацией, без шифрования. • encrypt — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • sha; • md5; • sha224; • sha256; • sha384; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.

Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

```
Admin@nodename# edit monitoring alert-rules <parameters>
```

Для редактирования доступны следующие параметры:

Наименование	Описание
enabled	Включает/отключает данное правило.
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

Настройка захвата пакетов

Захват пакетов позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, Wireshark. Это бывает необходимо при диагностировании сетевых проблем.

Рсар-фильтры определяют условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол IPv4.

Для настройки рсар-фильтров используются команды на уровне **monitoring pcap-filter**:

```
Admin@nodename# edit monitoring pcap-filter <parameters>
```

В pcap-правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.

Для настройки pcap-правил используются команды на уровне **monitoring pcap-rule**:

```
Admin@nodename# edit monitoring pcap-rule <parameters>
```

Настройка профилей клиентских сертификатов

Раздел **Профили клиентских сертификатов** находится на уровне **settings certificate-profiles**.

Для создания профиля клиентского сертификата предназначена команда:

```
Admin@nodename# create settings certificate-profiles <parameters>
```

Далее могут использоваться следующие параметры:

Параметр	Описание
name	Название профиля клиентского сертификата.
description	Описание профиля.
username-field	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • common — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • email — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • principal — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN.

Параметр	Описание
	Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, берется первый, указанный в сертификате.
certificates	Сертификаты УЦ, назначаемые профилю.
crl	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты, срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: • off — не проверять ни один сертификат. • on — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • peer — проверять только сертификат клиента. • best-effort — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных).
receive-timeout	Интервал времени, по истечении которого UserGetе NGFW перестает ожидать ответа от службы отзыва сертификатов.

Для просмотра ранее созданных профилей клиентских сертификатов используются команды:

```
Admin@nodename# show settings certificate-profiles
Admin@nodename# show settings certificate-profiles <certificate-profile-name>
```

Для редактирования ранее созданного профиля используется команда:

```
Admin@nodename# set settings certificate-profiles <certificate-profile-name> <parameters>
```

Параметры, доступные для редактирования профиля, аналогичны параметрам создания профиля, рассмотренным ранее.

Для удаления ранее созданного профиля используется команда:

```
Admin@nodename# delete settings certificate-profiles <certificate-profile-name>
```

Настройка параметров управления телеметрией

Настройка параметров управления телеметрией устройства в интерфейсе командной строки производится на уровне `settings telemetry`.

Для редактирования параметров используется следующая команда:

```
Admin@nodename# set settings telemetry <parameters>
```

Возможна настройка следующих параметров:

Параметр	Описание
enabled	Включение/отключение сбора телеметрии на устройстве: • on, • off. По умолчанию сбор телеметрии включен.
hide-sensitive-data	Включение/отключение функции сокрытия персональных данных в телеметрии (доступно в версии ПО 7.4.0 и выше): • on, • off. По умолчанию функция отключена.

Посмотреть текущие настройки можно с помощью команды:

```
Admin@nodename# show settings telemetry
```

Функция экспорта и импорта конфигурации

В версии 7.5.0 и выше UserGate NGFW поддерживает функцию экспорта и импорта конфигурации устройства в текстовом формате. С помощью этой функции вы можете:

- разворачивать новые устройства посредством клонирования конфигураций;
- добавлять однотипные параметры на устройства;
- быстро восстанавливать устройства после сбоев;
- проводить анализ, аудит или документирование изменений параметров устройств.

Экспорт и импорт конфигурации выполняется с помощью утилиты **scp** (Secure Copy Protocol) в приложении терминала на компьютере пользователя.

Экспорт конфигурации

Команда экспорта имеет следующий вид:

```
USER_KEY="<value>" scp -P 2200 -o 'SendEnv=USER_KEY' <user-name>@<IP-address>:sys_config <file-name>
```

Укажите имя пользователя, IP-адрес UserGate NGFW, название экспортируемого файла. Для шифрования чувствительных данных (паролей, ключей, сертификатов) при экспорте конфигурации задайте переменную окружения с собственной кодовой строкой (**USER_KEY**). Для импорта этого файла конфигурации необходимо будет использовать ту же кодовую строку.

Пример команды экспорта конфигурации:

```
USER_KEY="123123" scp -P 2200 -o 'SendEnv=USER_KEY'
Admin@192.168.1.100:sys_config configfile1
```

i Примечание

Если при выполнении команды экспорта или импорта конфигурации с помощью команды `scp` будет получено сообщение об ошибке вида `subsystem request failed on channel 0`, добавьте в указанную команду параметр `-0`.

Полученный файл содержит полную структурированную конфигурацию устройства в текстовом виде. В начале файла конфигурации находится блок метаданных:

```
-----
# Comment
author: ''
product: NGFW
version: 7.X.X. YYYY
created: August 12, 2025, 08:04
secret: bamy2jBfI6jcVTXWT6RkNbDl0AA=
factory-reset: off
-----
```

Назначение параметров в блоке метаданных:

- **author** — параметр, в котором вы можете указать имя автора подготовленной конфигурации.
- **product** — название продукта. Значение параметра устанавливается системой при экспорте данных.
- **version** — версия UGOS устройства. Значение параметра устанавливается системой при экспорте данных.
- **created** — время создания файла конфигурации. Значение параметра устанавливается системой при экспорте данных. Этот параметр не должен меняться пользователем.
- **secret** — ключ шифрования чувствительных данных. Значение параметра устанавливается системой при экспорте данных.

- **factory - reset** — параметр, определяющий порядок импорта данных из файла конфигурации:
 - **off** — параметры конфигурации из файла будут добавлены к существующей конфигурации на устройстве;
 - **on** — параметры конфигурации из файла заменят собой параметры существующей конфигурации.
- **#** — символ, с помощью которого вы можете добавлять произвольные комментарии в блоке метаданных.

Импорт конфигурации

Для импорта конфигурации на устройство используйте команду вида:

```
USER_KEY="<value>" scp -P 2200 -o 'SendEnv=USER_KEY' <file-name> <user-name>@<IP-address>:sys_config
```

Укажите имя пользователя, IP-адрес UserGate NGFW, название импортируемого файла, переменную окружения с той же кодовой строкой, которая была использована при экспорте конфигурации.

Пример команды импорта конфигурации:

```
USER_KEY="123123" scp -P 2200 -o 'SendEnv=USER_KEY' configfile1  
Admin@192.168.1.100:sys_config
```

В зависимости от значения параметра **factory - reset** [в блоке метаданных](#) импортируемого файла параметры конфигурации будут добавлены к имеющейся конфигурации устройства или заменят ее.

Импортированные данные сразу же применяются на устройстве после импорта файла. Записи об изменениях параметров конфигурации отображаются в системном журнале событий (event log).

Просмотр журнала ошибок операций импорта и экспорта

Ошибки операций импорта и экспорта конфигурации можно просмотреть с помощью команды:

```
Admin@nodename> show logs transfer-logs <parameters>
```

Дополнительные параметры команды:

- **direction** — порядок отображения записей:
 - **new-first** — сначала новые записи;
 - **old-first** — сначала старые записи.
- **raw** — отображение полного списка записей журнала.

НАСТРОЙКИ СЕТИ

Зоны

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

```
Admin@nodename# create network zone
```

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны.

Параметр	Описание
	◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса.

Параметр	Описание
	• alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • response-pages: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • rpc: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • ha: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • VRRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "Admin Console": доступ к веб-консоли управления (TCP 8001). • DNS: доступ к сервису DNS-прокси (TCP 53, UDP 53). • "HTTP Proxy": доступ к сервису HTTP(S)-прокси (TCP 8090). • "Authorization agent": доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • "SMTP Proxy": сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "POP3 Proxy": сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика.

Параметр	Описание
	• "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • "PROXY PORTAL": сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • L7 DNS: детектирование трафика DNS на уровне приложений. • L7 NTP: детектирование трафика NTP на уровне приложений. • "SAML SERVER": выбор SAML-сервера в списке сервисов зоны и общих настройках UserGate. • "Log Analyzer": сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713). • "Dynamic routing OSPF": сервис динамической маршрутизации OSPF. • "Dynamic routing BGP": сервис динамической маршрутизации BGP. • "SNMP Proxy": сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • "SSH Proxy": сервис, использующийся для инициирования трафика SSH. • Multicast: сервис мультикастинга. • NTP: доступ к сервису точного времени, запущенному на сервере UserGate. • "Dynamic routing RIP": сервис динамической маршрутизации RIP. • UserID agent: сервис для осуществления прозрачной аутентификации. В качестве источника данных аутентификации используются журналы ActiveDirectory и Syslog. • BFD: сервис Bidirectional Forwarding Detection для быстрого обнаружения сетевых ошибок. • "HTTPS RPC": доступ к API поверх HTTPS (TCP 4443). Доступен в версии 7.3.3 и выше.
service-addresses	Указание разрешённых IP-адресов для сервисов: • service: выбор сервисов (список соответствует enable d-services).

Параметр	Описание
	• allowed-addresses: разрешённые IP-адреса: ◦ geoip — код GeoIP. ◦ ip-list — заранее созданный в библиотеке элементов список IP-адресов.
antispoof-enabled	Включение/отключение защиты от IP-спуфинга: • on. • off.
antispoof-negate	Возможные значения: • on. • off. При antispoof-negate on адреса источников, указанные в значении ip-spoofing-networks, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • on. • off.
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled
on
```

Команда удаления зоны или её параметров:

```
Admin@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Следующая команда отобразит настройки зоны:

```
Admin@nodename# show network zone <zone-name>
```

Интерфейсы

В интерфейсе командной строки можно отобразить список упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов. Команда просмотра доступна как в режиме диагностики и мониторинга, так и в режиме конфигурации.

```
Admin@nodename> show network interface-mapping
```

```
Admin@nodename# show network interface-mapping
```

Упорядочение интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующую команду (в режиме диагностики и мониторинга и в режиме конфигурации соответственно):

```
Admin@nodename> clear network interface-mapping
```

```
Admin@nodename# delete network interface-mapping
```

После добавления сетевых портов в настроенный UserGate NGFW его необходимо перезагрузить — список обновится и станет доступным для отображения.

На уровне `network interface` доступна настройка параметров различных типов интерфейсов UserGate NGFW.

Настройка физических сетевых интерфейсов

Физические сетевые интерфейсы (адаптеры) настраиваются на уровне `network interface adapter`.

Для отображения информации обо всех сетевых адаптерах используйте команду:

```
Admin@nodename# show network interface adapter
```

Для отображения информации об определенном сетевом адаптере:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Для изменения параметров сетевого адаптера используйте команду вида:

```
Admin@nodename# set network interface adapter <adapter-name>
<parameters>
```

В команде необходимо указать параметры сетевого адаптера.

Параметр	Описание
enabled	Включение или отключение сетевого интерфейса: • on; • off
description	Описание сетевого интерфейса
alias	Псевдоним («алиас») интерфейса
iface-type	Тип интерфейса: • l3 — интерфейс, работающий в режиме Layer 3. Вы можете назначить IP-адрес для интерфейса и использовать его в правилах межсетевого экрана, контентной фильтрации и других. Это стандартный режим работы интерфейса. • mirror — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP; • manual — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса

Параметр	Описание
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a–z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе « Настройка профилей LLDP »

Параметр	Описание
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде  Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
rx-ring	Размер буфера RX ring интерфейса типа adapter
tx-ring	Размер буфера TX ring интерфейса типа adapter
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение или отключение ретранслятора (on/off). • utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP - адрес/none). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов
user-speed	Выбор скорости интерфейса. Параметр доступен только для ПАК UserGate FG в версии 7.5.0 и выше. Для портов 10–17 вы можете переключить скорость работы интерфейса с 10 Гбит/с на 25 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например:

Параметр	Описание
	Admin@nodename# set network interface adapter port10 user-speed 25000 Для портов 18–19 вы можете переключить скорость работы интерфейса со 100 Гбит/с на 40 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например: Admin@nodename# set network interface adapter port18 user-speed 100000  Примечание При просмотре параметров интерфейса с помощью команды <code>show network interface adapter <adapter-name></code> параметр <code>speed</code> отображает фактическую скорость интерфейса, полученную из системы; параметр <code>user-speed</code> — указанную администратором скорость или значение <code>auto</code> для портов 0–9.

Для удаления значений параметров сетевого адаптера используйте команду:

```
Admin@nodename# delete network interface adapter <adapter-name>
<parameters>
```

Параметры, доступные для удаления:

- `ip-address` — заданный IP-адрес;
- `dhcp-relay server-address` — IP-адрес DHCP-сервера.

Настройка VLAN-интерфейса

VLAN-интерфейсы создаются и настраиваются на уровне `network interface vlan`.

Для добавления нового VLAN-интерфейса используйте команду вида:

```
Admin@nodename# create network interface vlan <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
<code>enabled</code>	Включение или отключение VLAN-интерфейса: • <code>on</code>; • <code>off</code>
<code>description</code>	Описание интерфейса
<code>alias</code>	Псевдоним («алиас») интерфейса
<code>iface-type</code>	Тип интерфейса: • <code>l3</code> — Layer 3. Вы можете назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. • <code>mirror</code> — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
<code>iface-mode</code>	Режим назначения IP-адреса: • <code>dhcp</code> — получение динамического IP-адреса по DHCP; • <code>manual</code> — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
<code>tag</code>	Тег VLAN. Допускается создание до 4094 интерфейсов
<code>node-name</code>	Имя узла кластера, на котором создается VLAN
<code>interface</code>	Физический интерфейс, на котором создается VLAN
<code>zone</code>	Зона, которой будет принадлежать интерфейс
<code>link-info</code>	Настройка параметров сетевого интерфейса: • <code>bc_forwarding</code> — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • <code>proxy_arp</code>, <code>proxy_arp_pvlan</code> — механизмы Proxy ARP. При указании параметра <code>proxy_arp</code> UserGate

Параметр	Описание
	NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра <code>proxy_arp_pvlan</code> UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — <code>proxy_arp/1</code>; для отключения — <code>proxy_arp/0</code>. Поле <code>link-info</code> будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров <code>link-info</code> недоступно.
<code>netflow-profile</code>	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow»
<code>ip-addresses</code>	Назначение IP-адреса для интерфейса. Адрес задается в виде [<code><ip_address/mask></code>] или [<code><ip_address/mask> <ip_address/mask></code>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.

Параметр	Описание
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле $MTU - 40$
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение или отключение ретранслятора (on/off). • utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP - адрес/none). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего VLAN-интерфейса используйте команду:

```
Admin@nodename# set network interface vlan <vlan-name> <parameters>
```

Параметры, доступные для изменения, аналогичны параметрам создания VLAN-интерфейса, кроме параметров **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

- **ip-address** — заданный IP-адрес;
- **dhcp-relay server-address** — IP-адрес DHCP-сервера.

Для отображения информации обо всех VLAN-интерфейсах используйте команду:

```
Admin@nodename# show network interface vlan
```

Для отображения информации об определенном интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Bond-интерфейсы создаются и настраиваются на уровне `network interface bond`.

Для создания bond-интерфейса используйте команду вида:

```
Admin@nodename# create network interface bond <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
<code>enabled</code>	Включение или отключение интерфейса: • <code>on</code>; • <code>off</code>
<code>interface-name</code>	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет <code>bond1</code>
<code>description</code>	Описание интерфейса
<code>alias</code>	Псевдоним («алиас») интерфейса
<code>node-name</code>	Узел кластера, на котором будет создан bond-интерфейс
<code>zone</code>	Зона, которой будет принадлежать bond-интерфейс
<code>link-info</code>	Настройка параметров сетевого интерфейса: • <code>bc_forwarding</code> — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • <code>proxy_arp</code>, <code>proxy_arp_pvlan</code> — механизмы Proxy ARP. При указании параметра <code>proxy_arp</code> UserGate

Параметр	Описание
	NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow»
bonding	Дополнительные параметры bond-интерфейса: • aggr-mode — режим работы bond-интерфейса: ◦ round-robin — режим round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. ◦ active-backup — режим active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, если станет недоступным текущий активный интерфейс. При использовании этого режима MAC-адрес bond-

Параметр	Описание
	интерфейса виден вовне только через один сетевой порт. Такая политика применяется для обеспечения отказоустойчивости. ◦ xor — режим XOR. Передача распределяется между сетевыми картами с применением формулы: «<MAC-адрес источника> XOR <MAC-адрес назначения>» по модулю «число интерфейсов». Одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике xmit_hash. Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости. ◦ broadcast — передача на все сетевые интерфейсы. Эта политика применяется для обеспечения отказоустойчивости. ◦ 802.3ad — режим IEEE 802.3ad. Режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Интерфейс, через который будет отправляться пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать политику xmit_hash. ◦ transmit — режим adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, другая сетевая карта получает MAC-адрес вышедшей из строя карты. ◦ load — режим adaptive load balancing. Включает в себя предыдущую политику, а также осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт вовне, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-

Параметр	Описание
	адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. • mii-monitoring — периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • down-delay — время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. • up-delay — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. • lacp-rate — интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: ◦ slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. ◦ fast — запрос партнера на передачу LACPDU-пакетов каждую секунду. • failover-mac — определение способа назначения MAC-адресов на объединенные интерфейсы в режиме active backup при переключении интерфейсов. Возможные значения: ◦ disabled — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. ◦ active — MAC-адрес на bond-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на bond-интерфейсе меняется во время обработки отказа. ◦ follow — MAC-адрес на bond-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. Пока второй и последующий интерфейсы находятся в резервном режиме, этот MAC-адрес на них не устанавливается. MAC-адрес присваивается во время обработки отказа. Когда резервный интерфейс становится активным, он принимает новый MAC-адрес (тот же, что присвоен bond-интерфейсу), а старому активному интерфейсу присваивается MAC-адрес, который принадлежал текущему активному интерфейсу.

Параметр	Описание
	• xmit-hash — определение хеш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ l2 — использует только MAC-адреса для генерации хеш-суммы. При использовании этого алгоритма трафик для конкретного сетевого узла будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. ◦ l2-3 — использует как MAC-адреса, так и IP-адреса для генерации хеш-суммы. Алгоритм совместим с IEEE 802.3ad. ◦ l3-4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хеш-суммы. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, в котором были отправлены, так как отправляются через разные интерфейсы. • interface — интерфейсы, которые будут объединены в bond-интерфейс
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP. • manual — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
iface-type	Тип интерфейса: • l3 — Layer 3. Вы можете назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. • mirror — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
ip-addresses	Назначение IP-адреса для интерфейса.

Параметр	Описание
	Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде  Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение или отключение ретранслятора (on/off). • utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP - адрес/none). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bond-интерфейса используйте команду:

```
Admin@nodename# set network interface bond <bond-name> <parameters>
```


Параметры, доступные для изменения, аналогичны параметрам создания bond-интерфейса, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления bond-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

- **ip-address** — заданный IP-адрес;
- **dhcp-relay server-address** — IP-адрес DHCP-сервера.
- **bonding interface** — интерфейсы, объединенные в bond-интерфейс.

Для отображения информации обо всех bond-интерфейсах используйте команду:

```
Admin@nodename# show network interface bond
```

Для отображения информации об определенном интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Настройка bridge-интерфейса

Bridge-интерфейсы создаются и настраиваются на уровне **network interface bridge**.

Для добавления нового bridge-интерфейса используйте команду:

```
Admin@nodename# create network interface bridge <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: • on;

Параметр	Описание
	• off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет bridge1
description	Описание bridge-интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Имя узла кластера, на котором создается интерфейс
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров

Параметр	Описание
	 Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
bridging	Дополнительные параметры bridge-интерфейса: • iface-type — режим работы интерфейса: ◦ l2 — Layer 2, создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В этом режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security и правила контентной фильтрации. ◦ l3 — Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. • interface — интерфейсы, которые будут использованы для создания моста. • stp — включение или отключение использования Spanning Tree Protocol (STP) для защиты от петель (on/off). • forward-delay — задержка перед переключением моста в активный режим (forwarding), в случае если включен STP (указывается в секундах). • max-age — время, по истечении которого STP-соединение считается потерянным (указывается в секундах). • bypass-pair — пара интерфейсов, которая будет использована для построения байпас-моста. Требуется поддержка оборудования ПАК UserGate
iface-mode	Режим назначения IP-адреса: • dhcp — получение динамического IP-адреса по DHCP. • manual — без адреса.

Параметр	Описание
	Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде i Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение или отключение ретранслятора (on/off). • utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP - адрес/none). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bridge-интерфейса используйте команду:

```
Admin@nodename# set network interface bridge <bridge-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Для удаления bridge-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления:

- **ip-address** — заданный IP-адрес;
- **dhcp-relay server-address** — IP-адрес DHCP-сервера.

Для отображения информации обо всех bridge-интерфейсах используйте команду:

```
Admin@nodename# show network interface bridge
```

Для отображения информации об определенном bridge-интерфейсе используйте команду:

```
Admin@nodename# show network interface bridge <bridge-name>
```

Настройка PPPoE-интерфейса

PPPoE-интерфейсы создаются и настраиваются на уровне **network interface PPPoE**.

Для создания PPPoE-интерфейса используйте команду вида:

```
Admin@nodename# create network interface pppoe <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: • on; • off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет rpp1
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Имя узла кластера, на котором создается интерфейс
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров

Параметр	Описание
	 Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
config	Дополнительные параметры PPPoE-интерфейса: • interface — интерфейс, на котором будет создаваться PPPoE-интерфейс. • login — имя пользователя для соединения PPPoE. • password — пароль пользователя для соединения PPPoE. • persist-connection — автоматическое переподключение при обрыве связи. • auth-type — тип авторизации: ◦ CHAP; ◦ PAP. • holdoff — интервал времени в секундах после разрыва соединения перед повторным запуском. • default-route — PPPoE-интерфейс, который будет использоваться как маршрут по умолчанию. • echo-interval — интервал проверки соединения. • echo-failure — количество неуспешных проверок соединения, по достижении которого UserGate NGFW будет считать, что соединение отсутствует, и разорвет его. • providers-dns — использование DNS-серверов, выданных провайдером. • connection-attempts — количество неуспешных попыток подключения, по достижении которого попытки автосоединения будут прекращены. • service-name — имя сервиса, которое необходимо указать в случае его предоставления провайдером
mtu	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet

Параметр	Описание
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40

Для изменения параметров существующего PPPoE-интерфейса используйте команду:

```
Admin@nodename# set network interface pppoe <pppoe-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Для удаления PPPoE-интерфейса используйте команду:

```
Admin@nodename# delete network interface pppoe <pppoe-name>
```

Для отображения информации обо всех PPPoE-интерфейсах используйте команду:

```
Admin@nodename# show network interface pppoe
```

Для отображения информации об определенном PPPoE-интерфейсе используйте команду:

```
Admin@nodename# show network interface pppoe <pppoe-name>
```

Настройка VPN-интерфейса

VPN-интерфейсы создаются и настраиваются на уровне **network interface vpn**.

Для создания VPN-интерфейса используйте команду вида:

```
Admin@nodename# create network interface vpn <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: • on; • off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет tunnel1
description	Описание VPN-интерфейса
alias	Псевдоним («алиас») интерфейса
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров

Параметр	Описание
	 Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
iface-mode	Режим назначения IP-адреса: • <code>dhcp</code> — получение динамического IP-адреса по DHCP. • <code>manual</code> — без адреса. Если предполагается, что интерфейс будет принимать VPN-подключения (site-to-site VPN или remote access VPN), необходимо использовать статический IP-адрес. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. Для использования интерфейса в роли клиента необходимо выбрать динамический режим
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<code><ip_address/mask></code>] или [<code><ip_address/mask> <ip_address/mask></code>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде  Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mtu	Размер MTU для выбранного интерфейса
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40

Для изменения параметров существующего VPN-интерфейса используйте команду:

```
Admin@nodename# set network interface vpn <vpn-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Для удаления VPN-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface vpn <vpn-name>
```

Параметр, доступный для удаления: **ip-addresses**.

Для отображения информации обо всех VPN-интерфейсах используйте команду:

```
Admin@nodename# show network interface vpn
```

Для отображения информации об определенном VPN-интерфейсе используйте команду:

```
Admin@nodename# show network interface vpn <vpn-name>
```

Настройка туннельного интерфейса

Туннельные интерфейсы создаются и настраиваются на уровне **network interface tunnel**.

Для создания туннельного интерфейса используйте команду вида:

```
Admin@nodename# create network interface tunnel <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: • on; • off
interface-number	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет gre1
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Узел кластера, на котором будет создан туннельный интерфейс
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров

Параметр	Описание
	 Важно! Удаление заданных параметров link-info недоступно.
mtu	Размер MTU для выбранного интерфейса
mss	Размер MSS (доступно в версии 7.3.0 и выше). Корректные значения: • 0; • для VXLAN — число в диапазоне от 4 до числа, получаемого по формуле $MTU - 40$; • для IPsec — число в диапазоне от 4 до числа, получаемого по формуле $MTU - 60$; • для GRE — число в диапазоне от 4 до числа, получаемого по формуле $MTU - 64$
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде  Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
local-ip	Локальный адрес интерфейса point-to-point
remote-ip	Удаленный адрес интерфейса point-to-point
mode	Режим работы туннельного интерфейса: • gre — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер IP-протокола — 47.

Параметр	Описание
	• ipip — протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP-пакета в другой — это добавление внешнего заголовка, в котором IP-адресом источника является адрес точки входа в туннель, а IP-адресом назначения — адрес точки выхода из туннеля. • vxlan — протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789
vxlan-id	Идентификатор VXLAN. Только для типа туннельного интерфейса VXLAN

Для изменения параметров существующего туннельного интерфейса используйте команду:

```
Admin@nodename# set network interface tunnel <tunnel-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-number**, **node-name** (изменение значений этих параметров недоступно).

Для удаления туннельного интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface tunnel <tunnel-name>
<parameters>
```

Параметры, доступные для удаления: **ip-addresses**.

Для отображения информации обо всех туннельных интерфейсах используйте команду:

```
Admin@nodename# show network interface tunnel
```

Для отображения информации об определенном туннельном интерфейсе:

```
Admin@nodename# show network interface tunnel <tunnel-name>
```

Настройка loopback-интерфейса

Loopback-интерфейсы создаются и настраиваются на уровне `network interface loopback`.

Для создания интерфейса используется команда вида:

```
Admin@nodename# create network interface loopback <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
<code>enabled</code>	Включение или отключение интерфейса: • <code>on</code>; • <code>off</code>
<code>interface-name</code>	Название интерфейса
<code>description</code>	Описание интерфейса
<code>alias</code>	Псевдоним («алиас») интерфейса
<code>ip-addresses</code>	Назначение IP-адреса для интерфейса. Адрес задается в виде [<code><ip_address/mask></code>] или [<code><ip_address/mask></code> <code><ip_address/mask></code>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
<code>iface-mode</code>	Режим назначения IP-адреса: • <code>dhcp</code> — получение динамического IP-адреса по DHCP. • <code>manual</code> — без адреса.

Параметр	Описание
	Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе « Настройка профилей LLDP »
zone	Зона, которой будет принадлежать интерфейс
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	

Параметр	Описание
	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
node-name	Узел кластера, на котором будет создан интерфейс
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • enabled — включение или отключение ретранслятора (on/off). • utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP-адрес/none). • server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего loopback-интерфейса используйте команду вида:

```
Admin@nodename# set network interface loopback <interface-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания loopback-интерфейса, кроме **node-name**, **interface** (изменение значений этих параметров недоступно).

Для удаления loopback-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления:

- **ip-address** — заданный IP-адрес;

- `dhcp-relay server-address` — IP-адрес DHCP-сервера.

Для отображения информации обо всех loopback-интерфейсах используйте команду:

```
Admin@nodename# show network interface loopback
```

Для отображения информации об определенном loopback-интерфейсе используйте команду:

```
Admin@nodename# show network interface loopback <interface-name>
```

Шлюзы

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

```
Admin@nodename# create network gateway
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • on. • off.
name	Название шлюза.
description	Описание шлюза.

Параметр	Описание
interface	Интерфейс, использующийся для выхода в Интернет: • Выбор конкретного порта (port0, port1, port2 итд.); • auto — после выбора этого параметра порт определится автоматически. Данная опция доступна для узлов, прошедших инициализацию. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0.
virtual-router	Выбор виртуального маршрутизатора, для которого настраивается шлюз.
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • on. • off.
default	Использование данного шлюза в качестве шлюза по умолчанию: • on. • off.

Обновление параметров шлюза:

```
Admin@nodename# set network gateway <gateway-name>
```

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

```
Admin@nodename# delete network gateway <gateway-name>
```

Чтобы отобразить информацию о всех шлюзах:

```
Admin@nodename# show network gateway
```

или об определённом шлюзе:

```
Admin@nodename# show network gateway <gateway-name>
```

DHCP

Раздел находится на уровне **network dhcp**.

Для создания подсети DHCP, используется команда:

```
Admin@nodename# create network dhcp
```

Далее необходимо указание параметров:

Параметр	Описание
enabled	Включение/отключение использования данного диапазона IP-адресов: • on. • off.
name	Название подсети.
description	Описание подсети.
interface	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
ip-range	Диапазон IP-адресов, выдаваемый клиентам DHCP. Диапазон задаётся в формате: <IP_start-IP_end>.
mask	Маска подсети, выдаваемая клиентам DHCP.
expiration-time	Время в секундах, на которое выдаются IP-адреса.

Параметр	Описание
domain	Название домена, выдаваемое клиентам DHCP.
gateway	IP-адрес шлюза, выдаваемый клиентам DHCP.
dns-servers	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
reserved-hosts	MAC-адреса и сопоставленные с ними IP-адреса: • mac: MAC-адрес. • ip: IP-адрес, сопоставленный MAC-адресу. • hostname: имя хоста.
ignored-mac	Список MAC-адресов, игнорируемых DHCP-сервером.
pxe-boot-ip	Адрес сервера PXE.
pxe-boot-filename	Название файла для загрузки с PXE-сервера.
options	Номер опции и ее значение: • code: номер опции DHCP. • values: значение опции.

Обновление существующей DHCP-подсети:

```
Admin@nodename# set network dhcp <dhcp-name>
```

Параметры, информацию о которых можно обновить, аналогичны параметрам, доступным при создании.

Для удаления подсети:

```
Admin@nodename# delete network dhcp <dhcp-name>
```

Также доступно удаление отдельных параметров подсети DHCP:

- **dns-servers**.
- **ignored-mac**.
- **reserved-hosts** (необходимо указать все три значения: **mac**, **ip**, **hostname**).

- **options** (необходимо указать оба значения: **code**, **values**).

Чтобы отобразить информацию о всех созданных подсетях:

```
Admin@nodename# show network dhcp
```

или об определённой подсети DHCP:

```
Admin@nodename# show network dhcp <dhcp-name>
```

DNS-настройки

Раздел находится на уровне **network dns**.

Настройка системных DNS-серверов

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

```
Admin@nodename# set network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin@nodename# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin@nodename# show network dns system-dns-servers
```

Настройка DNS-прокси

DNS-прокси настраивается на уровне **network dns proxy-settings**.

Для редактирования настроек DNS-прокси используется следующая команда:

```
Admin@nodename# set network dns proxy-settings
```

Далее необходимо указать параметры, значения которых необходимо изменить:

Параметр	Описание
filtering	Фильтрация DNS-запросов: • on. • off.
caching	Кэширование ответов DNS: • on. • off.
limit	Ограничение количества DNS-запросов в секунду для каждого пользователя (значение по умолчанию: 100).
max-ttl	Максимально возможное время жизни для записей DNS.
recursive	Осуществление рекурсивных DNS-запросов: • on. • off.
dns-timeout	Время до следующей попытки отправления запроса на DNS-сервера (указывается в миллисекундах).
a-aaaa-unknown	Ответы только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS: • on. • off.

Параметр	Описание
retries	Количество попыток DNS-запроса.
factory-defaults	Сброс до заводских настроек значения выбранного параметра (параметры представлены в данной таблице) или всех параметров (all).

Пример команды редактирования параметров DNS-proxy:

```
Admin@nodename# set network dns proxy-settings limit 10 dns-timeout 10
```

Чтобы просмотреть настройки DNS-прокси:

```
Admin@nodename# show network dns proxy-settings
```

Настройка правил DNS

Внимание!

NGFW не может работать в роли DNS сервера. Предусмотрена только роль DNS проху. При указании в правилах DNS адреса самого NGFW, возможно образование DNS петли, со всеми вытекающими последствиями.

Правила DNS настраиваются на уровне **network dns rules** с использованием UPL. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Параметры правил DNS:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение использования правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила. Например: name("DNS rule example") .

Параметр	Описание
desc	Описание правила DNS-прокси. Например: desc("DNS rule example set via CLI") .
url.domain	Список доменов, на которые необходимо перенаправлять. Допускается использование звёздочки (*) для указания шаблона доменов. Чтобы указать список доменов: url.domain = "*.example.com" .
dns_server	Список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены. Для указания сервера: dns_server(1.2.3.4) .

Пример создания правила DNS с использованием UPL:

```
Admin@nodename# create network dns rules 1 upl-rule OK \
...url.domain = "*.example.com" \
...dns_server(1.2.3.4) \
...name("DNS rule example") \
...desc("DNS rule example description over CLI") \
...enabled(true) \
...
Admin@nodename#
Admin@nodename# show network dns rules

% ----- 1 -----
OK \
  url.domain = "*.example.com" \
  dns_server(1.2.3.4) \
  desc("DNS rule example description over CLI") \
  enabled(true) \
  id("0f83e1bb-0aa5-4f42-8eeb-9c4ffa30c04a") \
  name("DNS rule example")
```

Настройка статических записей DNS-прокси

Раздел находится на уровне **network dns static-records**.

Для добавления статической DNS-записи предназначена команда:

```
Admin@nodename# create network dns static-records
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статической записи: • on. • off.
name	Название записи.
description	Описание DNS-записи.
domain	FQDN (Fully Qualified Name) статической записи, например, www.example.com .
ips	Список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN.

Команда

```
Admin@nodename# show network dns static-records
```

отобразит информацию о всех существующих статических DNS-записях. Для отображения информации об определённой записи:

```
Admin@nodename# show network dns static-records <static-record-name>
```

Пример создания статической записи DNS:

```
Admin@nodename# create network dns static-records name "Test DNS static
record" description "Test DNS static record description" enabled on
domain example.com ips [ 10.10.0.100 ]
Admin@nodename#
Admin@nodename# show network dns static-records

Test DNS static record
      name           : Test DNS static record
```

```

description      : Test DNS static record description
domain           : example.com
ips              : 10.10.0.100
enabled          : on

```

Для редактирования информации о статических записях DNS:

```
Admin@nodename# set network dns static-records <static-record-name>
```

Список параметров, доступных для изменения, аналогичен списку команды **create**.

Пример редактирования ранее созданной статической записи DNS:

```

Admin@nodename# set network dns static-records "Test DNS static record"
ips [ 10.10.0.101 ]
Admin@nodename# show network dns static-records "Test DNS static
record"

name           : Test DNS static record
description    : Test DNS static record description
domain         : example.com
ips            : 10.10.0.100; 10.10.0.101
enabled        : on

```

Для удаления статической записи:

```
Admin@nodename# delete network dns static-records <static-record-name>
```

Также возможно удаление из статической записи только значений параметра **ips**.

Пример удаления значения параметра **ips** в ранее созданной записи и удаления всей статической записи DNS.

```

Admin@nodename# delete network dns static-records "Test DNS static
record" ips [ 10.10.0.101 ]
Admin@nodename# show network dns static-records "Test DNS static

```

```
record"

name          : Test DNS static record
description    : Test DNS static record description
domain        : example.com
ips           : 10.10.0.100
enabled       : on

Admin@nodename# delete network dns static-records "Test DNS static
record"
Admin@nodename# show network dns static-records

Admin@nodename#
```

Настройка виртуальных маршрутизаторов

В данном разделе описана настройка статических маршрутов, протоколов динамической маршрутизации OSPF, BGP, RIP и мультикаст-маршрутизации с использованием интерфейса командной строки (настройка рассмотрена в соответствующих разделах). Настройка производится на уровне **network virtual-router**.

Далее представлены команды, использующиеся для общей настройки виртуальных маршрутизаторов.

Команда для добавления нового виртуального маршрутизатора:

```
Admin@nodename# create network virtual-router <parameters>
```

Далее указываются параметры:

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора.
description	Описание виртуального маршрутизатора

Параметр	Описание
node-name	Выбор узла UserGate, на котором будет создан виртуальный маршрутизатор (при наличии кластера).
interfaces	Интерфейсы, которые будут использованы в данном виртуальном маршрутизаторе. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, добавлены быть не могут; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие.

Команда для отображения информации о виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name>
```

Пример создания виртуального маршрутизатора:

```
Admin@nodename# create network virtual-router name test_router
description "Test virtual router" interfaces [ port2 ]
Admin@nodename# show network virtual-router test_router

name           : test_router
description    : Test virtual router
node-name      : node_1
interfaces     : port2
...
```

Команда для редактирования параметров виртуального маршрутизатора:

```
Admin@nodename# set network virtual-router <virtual-router-name>
```

Параметры, доступные для обновления, аналогичны параметрам команды **create**, кроме:

- **name**.
- **node-name**.

Пример редактирования параметров виртуального маршрутизатора:

```
Admin@nodename# set network virtual-router test_router interfaces
[ port3 ]
Admin@nodename# show network virtual-router test_router

name          : test_router
description    : Test virtual router
node-name     : node_1
interfaces     : port2; port3
...
```

Чтобы удалить виртуальный маршрутизатор используется команда:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
```

Настройка статических маршрутов

Для добавления нового статического маршрута используется команда:

```
Admin@nodename# set network virtual-router <virtual-router-name> routes
new
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • on. • off.
name	Имя маршрута.
description	Описание маршрута.
type	

Параметр	Описание
	Тип маршрута: • unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • unreachable — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • prohibit — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.
gateway	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с сервера UserGate.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем приоритетней маршрут

Пример добавления статического маршрута:

```

Admin@nodename# set network virtual-router test_router routes new name
"Test static route" description "Test static route description"
destination-ip 192.168.200.0/24 gateway 192.168.100.100 interface port3
type unicast metric 1 enabled on
Admin@nodename#
Admin@nodename# show network virtual-router test_router

name                : test_router
description         : Test virtual router
node-name           : node_1
interfaces           : port2; port3
routes              :
    Test static route

```

```

name          : Test static route
enabled       : on
description   : Test static route description
destination-ip : 192.168.200.0/24
gateway       : 192.168.100.100
interface     : port3
metric        : 1
...

```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@nodename# set network virtual-router <virtual-router-name> routes
<static-route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Пример редактирования статического маршрута:

```

Admin@nodename# set network virtual-router test_router routes "Test
static route" metric 10
Admin@nodename# show network virtual-router test_router

name          : test_router
description    : Test virtual router
node-name     : node_1
interfaces    : port2; port3
routes        :
    Test static route
        name          : Test static route
        enabled       : on
        description   : Test static route description
        destination-ip : 192.168.200.0/24
        gateway       : 192.168.100.100
        interface     : port3
        metric        : 10
...

```


Используйте следующую команду для удаления статического маршрута:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
routes <static-route-name>
```

Пример удаления статического маршрута:

```
Admin@nodename# delete network virtual-router test_router routes "Test
static route"
Admin@nodename# show network virtual-router test_router

name                : test_router
description          : Test virtual router
node-name            : node_1
interfaces           : port2; port3
routes               : []
...
```

Для отображения статических маршрутов:

```
Admin@nodename# show network virtual-router <virtual-router-name>
routes
```

Настройка OSPF

Для настройки OSPF с использованием CLI используйте следующую команду:

```
Admin@nodename# set network virtual-router <virtual-router-name> ospf
```

Далее необходимо указать параметры OSPF-маршрутизатора:

Параметр	Описание
enabled	Включение/отключение OSPF-маршрутизатора: • on. • off.

Параметр	Описание
router-id	IP-адрес маршрутизатора. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору). При выключении OSPF (enabled off) значение router-id может быть удалено (none).
metric	Метрика распространяемых маршрутов.
default-originate	Оповещение других маршрутизаторов о том, что у данного роутера настроен маршрут по умолчанию: • on. • off.
interfaces	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор. Для добавления интерфейса или изменения параметров добавленного ранее интерфейса используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> ospf interfaces new Admin@nodename# set network virtual-router <virtual-router-name> ospf interfaces <interface-name></pre> Далее указываются следующие параметры: • enabled <on off>: включение/отключение использования интерфейса. • interface: название интерфейса, входящего в данный виртуальный маршрутизатор. • description: описание интерфейса. • bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. • cost: стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним

Параметр	Описание
	маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1. • priority: целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1. • network-type: выбор типа сети для оптимизации процесса установления соседства. Доступны: ◦ none — не установлен. ◦ bc — broadcast. ◦ ptm — point to multipoint. ◦ ptp — point to point. • passive-mode <on off>: включение/отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается слать пакеты обновления протокола маршрутизации. • hello-interval: время, через которое маршрутизатор посылает hello-пакеты; указывается в секундах. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд. • dead-interval: время, по истечению которого маршрутизатор считается неработающим; указывается в секундах. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд. • retransmit-interval: временный интервал перед повторной отсылкой пакета LSA; указывается в секундах. Значение по умолчанию 5 секунд. • transmit-delay: примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state); задаётся в секундах. Значение по умолчанию 1 секунда. • authentication: тип аутентификации. Доступны: ◦ enabled <on off> — включение/отключение требования аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов. ◦ auth-type — выбор типа аутентификации: plain (передача ключа в открытом виде для аутентификации роутеров) или digest

Параметр	Описание
	(использование MD5-хеши для ключа для аутентификации OSPF-пакетов). ◦ md5 — идентификатор ключа. ◦ key — ключ. Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.
areas	Настройка области OSPF. Для добавления новой области или изменения параметров созданной ранее области используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> ospf areas new Admin@nodename# set network virtual-router <virtual-router-name> ospf areas <area-name></pre> Далее указываются следующие параметры: • enabled <on off>: включение/отключение использования данной области. • name: название области. • description: описание области. • cost: стоимость LSA, анонсируемых в stub-области. • area-id: идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Идентификатор области должен совпадать для установления соседства OSPF. • auth-type: тип аутентификации. Доступны следующие значения: ◦ none — не требовать аутентификацию OSPF-пакетов. ◦ plain — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. ◦ digest — использование MD5-хеши для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне зоны.

Параметр	Описание
	• area-type: тип области OSPF. Доступны следующие типы: ◦ normal — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. ◦ nssa — Not-So-Stubby Area определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR). ◦ stub — тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. • no-summary: разрешение/запрет инъекции суммированных маршрутов в тупиковые типы областей: ◦ on. ◦ off. • interfaces: выбор интерфейсов OSPF, на которых будет доступна данная зона. • virtual-links: Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений. Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону.
redistribute	Распространение OSPF маршрутов: • connected — распространение маршрутов в непосредственно подключённые к UserGate сети. • kernel — распространение маршрутов, которые были добавлены администратором.

Для отображения конфигурации OSPF в виртуальном маршрутизаторе используется команда:

```
Admin@nodename# show network virtual-router <virtual-router-name> ospf
```

Пример конфигурирования OSPF в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router ospf router-id
192.168.100.3 areas new area-id 1 area-type normal name "New OSPF area"
enabled on interfaces [ ]
...
Admin@nodename# show network virtual-router test_router

name                : test_router
description          : Test virtual router
node-name            : node_1
interfaces           : port2; port3
routes               : []
ospf                  :
    router-id         : 192.168.100.3
    enabled            : off
    default-originate : off
    metric             : None
    areas              :
        New OSPF area
            name        : New OSPF area
            enabled      : on
            cost         : 1
            area-id      : 1
            area-type    : normal
            no-summary   : off

    interfaces        : []
...

```

Для удаления настроек OSPF используется команда:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
ospf <parameter>
```

Параметры, доступные для удаления:

- **interface.**
- **area.**

Настройка BGP

Настройка протокола динамической маршрутизации BGP (Border Gateway Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> bgp
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение OSPF-маршрутизатора: • on. • off.
router-id	IP-адрес маршрутизатора. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору. При выключении BGP (enabled off) значение router-id может быть удалено (none).
asn	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
multiple-path	Включение/отключение балансировки трафика на маршруты с одинаковой стоимостью: • on. • off.

Параметр	Описание
redistribute	Распространение BGP маршрутов: • connected — распространение маршрутов в непосредственно подключённые к UserGate сети. • kernel — распространение маршрутов, которые были добавлены администратором. • ospf — распространение маршрутов, полученных по протоколу OSPF.
networks	Список сетей, относящихся к данной автономной системе. Необходимо указать в формате <ip/mask>.
routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами. Для создания routemap или изменения параметров созданного ранее routemap используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp routemaps new Admin@nodename# set network virtual-router <virtual-router-name> bgp routemaps <routemap- name></pre> Параметры routemap: • name — название routemap. • description — описание routemap. • action — действие: ◦ allow — разрешить прохождение данных, попадающих под условия routemap. ◦ block — запретить прохождение данных, попадающих под условия routemap. • next-hop — установка для отфильтрованных маршрутов значения next hop в указанный IP-адрес. • weight — установка для отфильтрованных маршрутов веса в указанное значение. • metric — установка для отфильтрованных маршрутов метрики в указанное значение. • position — порядковый номер routemap в общем списке.

Параметр	Описание
	• preference — установка для отфильтрованных маршрутов предпочтения в указанное значение. • as-prepend — установка значения AS-prepend — список автономных систем, добавляемых для данного маршрута. • community — установка значения для BGP community для отфильтрованных маршрутов. • append-community — Добавлять community. • ip-match — необходимо добавить все необходимые IP-адреса при выборе сравнения по IP-адресу. • as-path-match — необходимо добавить все необходимые номера автономных сетей при выборе сравнения по AS-пути. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (<u> </u>), который интерпретируется как: ◦ Пробел. ◦ Запятая. ◦ Начало строки. ◦ Конец строки. ◦ AS set delimiter { and }. ◦ AS confederation delimiter (and). • community-match — необходимо добавить строки всех необходимых BGP community при выборе сравнения по Community.
filters	Фильтр позволяет фильтровать маршруты при перераспределении. Для создания фильтра или изменения параметров созданного ранее фильтра используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp filters new Admin@nodename# set network virtual-router <virtual-router-name> bgp filters <filter- name></pre> Параметры: • name — название фильтра. • description — описание фильтра.

Параметр	Описание
	• action — действие: ◦ allow — разрешить прохождение данных, попадающих под условия routemap. ◦ block — запретить прохождение данных, попадающих под условия routemap. • ip-filter — необходимо добавить все необходимые IP-адреса при выборе фильтрации по IP-адресу. Адреса могут быть указаны в следующих форматах: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0./8:11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. • as-path-filter — необходимо добавить все необходимые номера автономных сетей при выборе фильтрации по AS пути. • position — порядковый номер фильтра в общем списке.
neighbors	BGP-соседи. Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp neighbors new Admin@nodename# set network virtual-router <virtual-router-name> bgp neighbors <host-ip></pre> Параметры: • enabled — включение/отключение использования соседа: ◦ on. ◦ off. • description — описание BGP-соседа. • host — IP-адрес соседа. • remote-asn — номер автономной системы, к которой относится сосед. • weight — вес маршрутов, получаемых от данного соседа.

Параметр	Описание
	• ttl — максимальное количество хопов, разрешенное до этого соседа. • allowas-in — эта функция позволяет получать и обрабатывать маршруты, даже если маршрутизатор обнаруживает собственный номер автономной системы в AS Path в маршруте агрегации. ◦ on. ◦ off. • allowas-in-number — количество раз, которое в AS Path может содержаться номер автономной системы BGP-соседа. Возможны значения от 0 до 10 (0 — origin) • bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. • next-hop-self — замена значения next-hop-self на собственный IP-адрес, если сосед является BGP: ◦ on. ◦ off. • ebgp-multihop — до этого BGP-соседа не прямое соединение (более одного хопа): ◦ on. ◦ off. • route-reflector-client — определение, является ли BGP-сосед клиентом Route reflector: ◦ on. ◦ off. • soft-reconfiguration — использование soft reconfiguration (без разрыва соединений) для обновления конфигурации: ◦ on. ◦ off. • default-originate — анонс соседу маршрут по умолчанию: ◦ on. ◦ off. • send-community — пересылать community BGP-соседам: ◦ on. ◦ off.

Параметр	Описание
	• enable-auth — включение/отключение аутентификации для соседа: ◦ on. ◦ off. • password — пароль для аутентификации соседа. • filter-in — ограничение информации о маршрутах, получаемых от соседей. • filter-out — ограничение информации о маршрутах, анонсируемых соседям. • route-map-in — ограничение маршрутизирующей информации, которую BGP получает от соседей. • route-map-out — ограничение маршрутизирующей информации, которую BGP отдаёт соседям.

Команда для отображения конфигурации BGP в виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name> bgp
```

Пример команды конфигурирования BGP в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router bgp router-id
192.168.95.224 asn 1 networks [ 192.168.100.0/24 ] redistribute
[ connected kernel ]
Admin@nodename# show network virtual-router test_router

name                : test_router
description          : Test virtual router
node-name            : node_1
interfaces           : port2; port3
...
bgp                  :
  enabled             : off
  asn                 : 1
  router-id           : 192.168.95.224
  redistribute        : connected; kernel
  multiple-path       : off
  networks            : 192.168.100.0/24
  routemaps           : []
```

```
neighbors      : []
filters        : []
...
```

Команда для удаления параметров BGP-маршрутизатора:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
bgp <parameter>
```

Для удаления доступны следующие параметры:

- Адреса сетей, относящихся к данной автономной системе: **networks**.
- Условия применения routemap: **routemaps <routemap-name> ip-match | community-match | as-path-match**.
- Условия применения фильтра: **filters <filter-name> ip-filter | as-path-filter**.
- Фильтры BGP-соседей и routemaps: **neighbors <host-ip> filter-in | filter-out | routemap-in | routemap-out**.
- опции распространения BGP маршрутов: **redistribute [connected | kernel]**.

Настройка RIP

Настройка протокола маршрутизации RIP (Routing Information Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> rip
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: • on. • off.
version	Версия протокола RIP: • 1.

Параметр	Описание
	• 2. Как правило, используется 2-я версия протокола.
metric	Метрика RIP. По умолчанию метрика равна 1; максимальное значение — 15. Значение 16 считается бесконечным.
distance	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
originate	Отправлять себя в качестве маршрута по умолчанию.
networks-cidr	Указание сети в виде CIDR. Указывается в формате <ip/mask>.
networks-interface	Указание сетевого интерфейса, с которого будут отправлять обновления маршрутной информации; указываются интерфейсы, принадлежащие виртуальному маршрутизатору.
redistribute	Распространение маршрутов: • connected — распространение другим роутерам RIP маршрутов в непосредственно подключённые к UserGate сети: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • static — распространение другим маршрутизаторам статических маршрутов: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • kernel — распространение другим роутерам RIP маршрутов, которые были добавлены администратором: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • ospf — распространение другим RIP-роутерам маршрутов, полученных по OSPF: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off.

Параметр	Описание
	• bgp — распространение другим RIP-роутерам маршрутов, полученных по BGP: ◦ <code><metric></code> — значение метрики; может принимать значения от 0 до 16. ◦ off.
interfaces	Настройка интерфейсов, на которых поддерживается протокол RIP; интерфейсы должны быть добавлены в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: <pre>Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces new Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces <interface-name></pre> Параметры: • interface — выбор интерфейса. • send-version — версия протокола RIP, которую маршрутизатор будет отправлять. Доступны: ◦ 0. ◦ 1. ◦ 2. ◦ 3. • receive-version — версия протокола RIP, которую маршрутизатор будет принимать. Доступны: ◦ 0. ◦ 1. ◦ 2. ◦ 3. • password — строка для авторизации, которая будет отправляться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информацией по протоколу RIP, должны иметь одинаковый пароль. • split-horizone — метод предотвращения петель маршрутизации, при котором маршрутизатор не

Параметр	Описание
	распространяет информацию о сети через интерфейс, на который прибыло обновление. ◦ on. ◦ off. • poisoned-reverse — метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отправляет его соседу, от которого его получил. ◦ on. ◦ off. • passive-mode — режим работы интерфейса, при котором он принимает обновления RIP, но не отправляет их. ◦ on. ◦ off.

Команда для отображения конфигурации RIP в виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name> rip
```

Пример команды конфигурирования RIP в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router rip version 2
originate on
Admin@nodename# show network virtual-router test_router

name                : test_router
description          : Test virtual router
node-name            : node_1
interfaces           : port2; port3
...
rip                  :
  enabled             : off
  distance             : 120
  metric              : 1
  originate            : on
  interfaces           : []
  redistribute         : {}
```



```

version                : 2
...
Admin@nodename# set network virtual-router test_router rip interfaces
new interface port2
Admin@nodename# show network virtual-router test_router

name                   : test_router
description            : Test virtual router
node-name             : node_1
interfaces            : port2; port3
...
rip                   :
    enabled            : off
    distance           : 120
    metric             : 1
    originate         : on
    interfaces        :
        port2
            interface   : port2
            passive-mode : off
            poisoned-reverse : off
            receive-version : 0
            send-version  : 0
            split-horizone : off

    redistribute      : {}
    version           : 2
...

```

Команда для удаления параметров RIP-маршрутизатора:

```

Admin@nodename# delete network virtual-router <virtual-router-name>
rip <parameter>

```

Для удаления доступны следующие параметры:

- Интерфейсы RIP: **interfaces**.
- Сети RIP: **networks-cidr**.

- Сетевого интерфейса, с которого будут отправлять обновления
- маршрутной информации: **networks-interface**.

Настройка мультикаст-маршрутизации

Настройка мультикаст-маршрутизации в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name>
multicast-router
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: • on. • off.
ecmp	Разрешение распределения трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP): • on. • off. Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если данная опция отключена, то весь трафик на определенный хост назначения будет пересылаться только через один из роутеров (next hop).
ecmp-rebalance	Использование ECMP rebalance: • on — если один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). • off — если один из интерфейсов, через который отсылался трафик, отключился, то перераспределяются только те потоки, которые передавались через отключенный интерфейс.
join-prune	Интервал отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.

Параметр	Описание
register-suppress	Интервал, после которого маршрутизатор отправляет сообщение register suppress.
keep-alive	Интервал, через который маршрутизатор будет посылать сообщения keeralive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.
interfaces	Интерфейс, который будет использоваться для работы мультикаста; для указания доступны только интерфейсы, добавленные в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> multicast-router interfaces new Admin@nodename# set network virtual-router <virtual-router-name> multicast-router interfaces <interface-name></pre> Далее необходимо указать параметры: • interface — выбор интерфейса для работы мультикаста. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор. • hello-timeout — интервал отправки PIM HELLO сообщений в секундах. PIM Hello сообщения отправляются периодически со всех интерфейсов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг. • dr-priority — приоритет при выборе Designated router (DR), с помощью которого администратор может управлять процессом выбора DR для локальной сети. • bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. • enable-igmp — приём сообщений IGMP report и IGMP query на данном интерфейсе.

Параметр	Описание
	• use-igmpv2 — использование версии IGMP v2, по умолчанию используется IGMP v3.
rendevouz-points	При настройке Rendezvous points можно указать следующие параметры: • enabled — включение/отключение данного RP: ◦ on. ◦ off. • name — название RP. • ip — Unicast IP-адрес RP. • asm-allowed-groups — список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Если ничего не задано, то ограничений нет.
ssm-allowed-groups	Настройка мультикаст роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть указаны любые сети из диапазона 232.0.0.0/8; если ничего не задано, то ограничений нет.
spt-exclusions	Настройка мультикаст роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

Для отображения конфигурации мультикастинга в виртуальном маршрутизаторе используйте следующую команду:

```
Admin@nodename# show network virtual-router <virtual-router-name>
multicast-router
```

Пример команды конфигурирования мультикаст-маршрутизации в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router multicast-router
interfaces new interface port2 use-igmpv2 on
Admin@nodename# show network virtual-router test_router

name                : test_router
description          : Test virtual router
```

```

node-name      : node_1
interfaces     : port2; port3
...
multicast-router :
    enabled      : off
    ecmp-rebalance : off
    ecmp         : off
    join-prune   : 60
    keep-alive   : 31
    register-suppress : 5
    interfaces   :
        port2
            interface : port2
            enabled   : off
            enable-igmp : off
            use-igmpv2 : on
            bfd       : Not set

    rendezvous-points : []
...

```

Команда для удаления параметров мультикаст-маршрутизатора:

```

Admin@nodename# delete network virtual-router <virtual-router-name>
multicast-router

```

Для удаления доступны следующие параметры:

- Интерфейсы, используемые для работы мультикаста: **interfaces**.
- Rendezvous points: **rendevouz-points <rp-name>**, а также список разрешенных групповых адресов для any source multicast с данного RP: **rendevouz-points <rp-name> asm-allowed groups**.
- Список разрешенных групповых адресов для source specific multicast: **ssm-allowed-groups**.
- Список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree: **spt-exclusions**.

Настройка WCCP

Настройка WCCP (Web Cache Communication Protocol) производится на уровне **network wccp**. Для создания сервисной группы WCCP используется следующая команда:

```
Admin@nodename# create network wccp <parameter>
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение сервисной группы: • on. • off.
name	Название сервисной группы WCCP.
description	Описание сервисной группы.
password	Пароль, необходимый для аутентификации UserGate в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
fwd-type	Способ перенаправления трафика с серверов WCCP на UserGate: • l2 — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес UserGate. • gre — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
ret-type	Способ перенаправления трафика с UserGate на серверы WCCP: • l2 — используя перенаправление L2. В этом случае UserGate (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер).

Параметр	Описание
	• gre — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
service-group	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
priority	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
ports	Порты для перенаправления (порты назначения трафика). При необходимости указываются несколько портов в формате: ports-to-redirect + [80 442]. Важно! UserGate может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate с другими портами, будет отправляться в интернет без фильтрации.
ports-source	Перенаправление трафика на основании значений портов источника: • on. • off.
protocol	Выбор протокола: • tcp — Transmission Control Protocol (TCP). • udp — User Datagram Protocol (UDP).
routers-lists	Список IP-адресов серверов WCCP. Подробнее о создании списков IP-адресов с помощью CLI читайте в разделе Настройка IP-адресов.
routers-ips	IP-адреса серверов WCCP.
assignment-type	

Параметр	Описание
	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. • hash — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета: ◦ source-ip — вычисление хэша по IP-адресу источника. ◦ source-port — вычисление хэша по порту источника. ◦ dest-ip — вычисление хэша по IP-адресу назначения. ◦ dest-port — вычисление хэша по порту назначения. ◦ alt-source-ip — вычисление альтернативного хэша по IP-адресу источника. ◦ alt-source-port — вычисление альтернативного хэша по порту источника. ◦ alt-dest-ip — вычисление альтернативного хэша по IP-адресу назначения. ◦ alt-dest-port — вычисление альтернативного хэша по порту назначения. • mask — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP. ◦ source-ip — схема маскирования по IP-адресу источника. ◦ source-port — схема маскирования по порту источника. ◦ dest-ip — схема маскирования по IP-адресу назначения. ◦ dest-port — схема маскирования по порту назначения. ◦ mask-value — значение маски схемы маскирования. Для схемы маскирования по порту — 16 бит; по IP-адресу — 32 бита; указываются в шестнадцатеричном формате.

Для задания значений сервисной группы WCCP или обновления информации о ней:


```
Admin@nodename# set network wccp <service-group-name> <parameter>
```

Далее указываются параметры, значения которых необходимо обновить; параметры представлены в таблице выше.

Для просмотра информации о сервисной группе WCCP:

```
Admin@nodename# show network wccp <service-group-name>
```

Примеры команд создания и редактирования WCCP:

```
Admin@nodename# create network wccp name "Test service group" protocol
tcp service-group 1 routers-ips [ 192.168.100.120 ] fwd-type l2 ret-
type l2 ports [ 80 ] priority 1 password 12345
Admin@nodename# show network wccp "Test service group"

name                : Test service group
enabled             : off
fwd-type            : l2
ret-type            : l2
service-group       : 1
priority            : 1
protocol            : tcp
ports               : 80
assignment-type     : hash
source-ip           : off
source-port         : off
dest-ip             : off
dest-port           : off
alt-source-ip       : off
alt-source-port     : off
alt-dest-ip         : off
alt-dest-port       : off
routers-ips         : 192.168.100.120
Admin@nodename# set network wccp "Test service group" description "Test
service group description" service-group 100
Admin@nodename# show network wccp "Test service group"
```

```

name           : Test service group
description    : Test service group description
enabled        : off
fwd-type       : l2
ret-type       : l2
service-group  : 100
priority       : 1
protocol       : tcp
ports          : 80
assignment-type : hash
source-ip      : off
source-port    : off
dest-ip        : off
dest-port      : off
alt-source-ip  : off
alt-source-port : off
alt-dest-ip    : off
alt-dest-port  : off
routers-ips    : 192.168.100.120

```

Удаление сервисной группы полностью или некоторых её параметров:

```
Admin@nodename# delete network wccp <service-group-name>
```

Параметры, доступные для удаления:

- routers-lists.
- routers-ips.
- ports.

НАСТРОЙКА РАЗДЕЛА ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Настройка групп пользователей

Настройка групп пользователей производится на уровне **users group**.

Для добавления новой группы пользователей используется команда:

```
Admin@nodename# create users group <parameter>
```

Возможно указать следующие параметры:

Параметр	Описание
name	Название группы пользователей.
description	Описание группы пользователей.
transient	Указать: • on — группа для гостевых пользователей. • off — не является группой для гостевых пользователей.
users	Добавление пользователей в группу.
ldap-users	Добавление пользователей LDAP. При добавлении пользователей LDAP необходимо указать LDAP-коннектор (ldap-users connector <ldap-server-name> users + [<domain\user1> <domain\user2> ...]).

Для редактирования информации о группе пользователей необходимо воспользоваться следующей командой (параметры, доступные для обновления, аналогичны с параметрами, доступными при создании группы):

```
Admin@nodename# set users group <group-name> <parameter>
```

Для отображения настроек группы используется следующая команда:

```
Admin@nodename# show users group <group-name>
```

Примеры команд создания и редактирования группы пользователей:

```
Admin@nodename# create users group name "Test user group" ldap-users
connector "LDAP connector" users [ testd.local\user1 ]
Admin@nodename# show users group "Test user group"
```

```
name          : Test user group
is-ldap       : off
is-transient  : off
users         : user1 user1 (testd.local\user1)
```

```
Admin@nodename# set users group "Test user group" users [ user2 ]
Admin@nodename# show users group "Test user group"
```

```
name          : Test user group
is-ldap       : off
is-transient  : off
users         : user2; user1 user1 (testd.local\user1)
```

С использованием следующих команд можно удалить группу пользователей или отдельных пользователей группы:

```
Admin@nodename# delete users group <group-name>
```

Для удаления локальных пользователей:

```
Admin@nodename# delete users group <group-name> users [ <user1>
<user2> ... ]
```

Для удаления пользователей LDAP:

```
Admin@nodename# delete users group <group-name> ldap-users connector
<ldap-server-name> users [ <domain\user1> <domain\user2> ... ]
```

Пример удаления из группы пользователя LDAP:

```
Admin@nodename# delete users group "Test user group" ldap-users
connector "LDAP connector" users [ testd.local\user1 ]
```

Настройки пользователей

Настройка пользователей производится на уровне **users user**.

Команда для добавления пользователей:

```
Admin@nodename# create users user <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение пользователя.
name	Имя пользователя.
login	Логин пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
password	Пароль пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
expiration-date	Срок действия учётной записи пользователя. Указывается в формате YYYY-MM-DD.
groups	Группы, в которые будет добавлен пользователь.
ip	IP-адреса для идентификации пользователя; пользователь всегда должен получать доступ в сеть с указанных адресов.
mac	MAC-адреса для идентификации пользователей; пользователь всегда должен получать доступ в сеть с указанных адресов.
ip-range	Диапазон IP-адресов для идентификации пользователя; пользователь всегда должен получать доступ в сеть с адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>.
ip-mac	

Параметр	Описание
	Идентификация пользователя с помощью комбинации MAC и IP-адресов; пользователь всегда должен получать доступ в сеть с указанных адресов. Указывается в формате <ip-mac>.
vlan-tag	Тег VLAN для идентификации пользователя.
emails	Почтовые адреса пользователя.
phones	Номера телефонов пользователя.

Для обновления параметров учётной записи пользователя:

```
Admin@nodename# set users user <user-name> <parameter>
```

Список доступных параметров аналогичен списку параметров, доступному при создании учётной записи пользователя.

Команда для просмотра учётной записи пользователя:

```
Admin@nodename# show users user <user-name>
```

Пример команд создания и редактирования учётной записи пользователя:

```
Admin@nodename# create users user name user_2 login user2 password
12345 expiration-date 2023-12-31 ip [ 192.168.100.112 ] enabled on
Admin@nodename# show users user user_2

name           : user_2
login          : user2
enabled        : on
expiration-date : December 31, 2023, 00:00
ip             : 192.168.100.112
Admin@nodename# set users user user_2 emails [ example@example.org ]
Admin@nodename# show users user user_2

name           : user_2
login          : user2
enabled        : on
```

```
emails           : example@example.org
expiration-date  : December 31, 2023, 00:00
ip              : 192.168.100.112
```

Для удаления учётной записи пользователя используется следующая команда:

```
Admin@nodename# delete users user <user-login>
```

Также имеется возможность удаления определённой информации из учётной записи. Для удаления доступны (при удалении требуется ввод значения параметра):

- **groups.**
- **static-addresses.**
- **emails.**
- **phones.**

Настройка серверов аутентификации

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

```
Admin@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.

Параметр	Описание
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • on — использование SSL-соединения для подключения к LDAP-серверу. • off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
cache-ttl	Время жизни записей LDAP-кэша. (Опция доступна начиная с релиза UGOS 7.1.3).
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

```
Admin@nodename# set users auth-server ldap <ldap-server-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:


```
Admin@nodename# show users auth-server ldap <ldap-server-name>
```

Примеры команд создания и редактирования LDAP-коннектора:

```
Admin@nodename# create users auth-server ldap name "New LDAP connector"
ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains
[ testd.local ] search-roots [ dc=testd,dc=local ] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"
```

```
name           : New LDAP connector
enabled        : on
ssl            : on
address        : 10.10.0.10
bind-dn        : ug@testd.local
domains        : testd.local
search-roots   : dc=testd,dc=local
keytab_exists   : off
```

```
Admin@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"
```

```
name           : New LDAP connector
description     : New LDAP connector description
enabled        : on
ssl            : on
address        : 10.10.0.10
bind-dn        : ug@testd.local
domains        : testd.local
search-roots   : dc=testd,dc=local
keytab_exists   : off
```

Для удаления LDAP-коннектора используется команда:

```
Admin@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains.**
- **search-roots.**

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
Admin@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin@nodename# set users auth-server radius <radius-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS
server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name          : New RADIUS server
enabled       : on
addresses     :
  host        : 10.10.0.9
  port        : 1812
```

```
Admin@nodename# set users auth-server radius "New RADIUS server"
description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name          : New RADIUS server
description    : New RADIUS server description
enabled       : on
addresses     :
  host        : 10.10.0.9
  port        : 1812
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server radius <radius-server-name>
<parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses.**

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name
"New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name                : New TACACS+ server
enabled             : on
address             : 10.10.0.11
port                : 1812
single-connection   : off
timeout             : 4
```

```
Admin@nodename# set users auth-server tacacs "New TACACS+ server"
description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name                : New TACACS+ server
description          : New TACACS+ server description
enabled             : on
address             : 10.10.0.11
port                : 1812
single-connection   : off
timeout             : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка сервера NTLM

Настройка сервера NTLM производится на уровне **users auth-server ntlm**.

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

```
Admin@nodename# create users auth-server ntlm <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
domain	IP-адрес или доменное имя сервера NLM.

Команда для обновления информации о NTLM-сервере:

```
Admin@nodename# set users auth-server ntlm <ntlm-server-name>
<parameter>
```

Команда для отображения информации о сервере NTLM:

```
Admin@nodename# show users auth-server ntlm <ntlm-server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Примеры команд для создания и редактирования сервера NTLM:

```
Admin@nodename# create users auth-server ntlm name "New NTLM server"
domain 10.10.0.12 enabled on
Admin@nodename# show users auth-server ntlm "New NTLM server"

name           : New NTLM server
enabled        : on
domain         : 10.10.0.12

Admin@nodename# set users auth-server ntlm "New NTLM server"
description "New NTLM server description"
Admin@nodename# show users auth-server ntlm "New NTLM server"

name           : New NTLM server
description    : New NTLM server description
```

```
enabled      : on
domain       : 10.10.0.12
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers ntlm <ntlm-server-name>
```

Настройка сервера SAML IDP

Настройка сервера SAML IDP производится на уровне **users auth-server saml-idp**.

Для создания сервера аутентификации SAML IDP используется следующая команда:

```
Admin@nodename# create users auth-server saml-idp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
metadata-url	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML.
certificate	Сертификат, который будет использован в SAML-клиенте.
sso-url	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
sso-binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-url	

Параметр	Описание
	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Команда для обновления информации о сервере SAML IDP:

```
Admin@nodename# set users auth-server saml-idp <saml-idp-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Команда для отображения информации о сервере SAML IDP:

```
Admin@nodename# show users auth-server saml-idp <saml-idp-server-name>
```

Примеры команд для создания и редактирования сервера SAML IDP:

```
Admin@nodename# create users auth-server saml-idp name "New SAML IDP
server" slo-url http://logout.example.org sso-url http://
login.example.o
rg enabled on
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"

name          : New SAML IDP server
enabled       : on
certificate    : Unused
sso-url       : http://login.example.org
sso-binding    : post
slo-url       : http://logout.example.org
slo-binding    : post
Admin@nodename# set users auth-server saml-idp "New SAML IDP server"
description "New SAML IDP server description"
```



```
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"
```

```
name           : New SAML IDP server
description    : New SAML IDP server description
enabled       : on
certificate    : Unused
sso-url       : http://login.example.org
sso-binding    : post
slo-url       : http://logout.example.org
slo-binding    : post
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers saml-idp <saml-idp-server-
name>
```

Настройка профилей аутентификации

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
Admin@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
mfa	Указание профиля мультифакторной аутентификации (если её необходимо использовать). Для указания профиль MFA должен быть создан заранее. Подробнее о создании профилей MFA с использованием интерфейса командной строки читайте в разделе Настройка профилей MFA (мультифакторной аутентификации) .

Параметр	Описание
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная авторизация пользователя на Captive-портале.
max-attempts	Число неудачных попыток авторизации через Captive-портал до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации; указывается в секундах.
auth-methods	Метод аутентификации: • local-user-auth: аутентификация по базе данных локально заведенных пользователей. • policy-accept: не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети; применяется совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • http-basic: аутентификация с помощью метода HTTP Basic. • ldap: аутентификация с использованием LDAP-коннектора. • radius: аутентификация с использованием RADIUS-сервера. • tacacs: аутентификация с использованием сервера TACACS+. • ntlm: аутентификация с использованием NTLM-сервера. • saml-idp: аутентификация с использованием сервера SAML IDP.

Команда для редактирования настроек профилей аутентификации:

```
Admin@nodename# set users auth-profile <auth-profile-name> <parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
Admin@nodename# create users auth-profile name "New LDAP auth profile"
auth-methods ldap [ "New LDAP connector" ]
Admin@nodename# show users auth-profile "New LDAP auth profile"
```

```
name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic       : off
    local-user-auth  : off
    policy-accept    : off
    ldap             : New LDAP connector
```

```
Admin@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"
```

```
name                : New LDAP auth profile
description          : New LDAP auth profile description
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic       : off
    local-user-auth  : off
    policy-accept    : off
    ldap             : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
Admin@nodename# delete users auth-profile <auth-profile-name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-metod>
```

Настройка Captive-профилей

Настройка Captive-профилей производится на уровне **users captive-profiles**.

Для создания Captive-профиля необходимо использовать следующую команду:

```
Admin@nodename# create users captive-profiles <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название captive-профиля.
description	Описание captive-профиля.
auth-template	Шаблон страницы авторизации.
auth-mode	Метод идентификации, с помощью которого UserGate запомнит пользователя: ip — Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут

Параметр	Описание
	относятся к данному пользователю; устанавливается по умолчанию. • cookie — Запоминать cookie. После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя.
auth-profile	Профиль аутентификации, определяющий методы аутентификации. Подробнее о настройке профилей авторизации с использованием CLI смотрите в разделе Настройка профилей аутентификации.
custom-redirect	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
use-cookie	Возможность сохранения авторизации в браузере на указанное время. Для сохранения информации используются cookie. • on. • off.
cookie-exptime	Время, на которое будет сохранена аутентификация; задаётся в часах.
enable-ldap	Возможность выбора домена AD/LDAP на странице авторизации: • on. • off.
use-captcha	Использование CAPTCHA: пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала: • on. • off.
use-https	Использование HTTPS при отображении страницы авторизации Captive-портала. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. • on.

Параметр	Описание
	• off.
notification-profile	Профиль оповещения, который будет использоваться для отсылки гостевым пользователям информации о созданном пользователе и его пароле. Подробнее о настройке профилей оповещений с использованием CLI смотрите в разделе Настройка профилей оповещений .
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль. Текст оповещения обособляется кавычками ("").
exp-time	Дата и время, когда учетная запись временного пользователя будет отключена. Указывается в формате: уууу-mm-ddThh:mm:ssZ.
session-ttl	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена; задаётся в часах.
password-len	Длина пароля 1 — 15 символов.
password-complexity	Сложность пароля: • num: использование только цифр. • alpha_num: использование букв и цифр. • alpha_num_special: использование букв, цифр и специальных символов.
ta-groups	Группа для временных пользователей, в которую будут помещены создаваемые пользователи.
captive-auth-mode	Выбор метода аутентификации Captive-профиля: • aaa – аутентификация посредством логина/пароля локального пользователя или через AAA-сервер. • rki – аутентификация посредством X.509 сертификатов.

Параметр	Описание
uc-profile	Выбор профиля пользовательского сертификата при аутентификации методом rki.

Для редактирования профиля необходимо использовать следующую команду:

```
Admin@nodename# set users captive-profiles <captive-profile-name>
<parameter>
```

При обновлении настроек captive-профиля доступны параметры, аналогичные параметрам, доступным при создании профиля.

Команда для отображения настроек captive-профиля:

```
Admin@nodename# show users captive-profiles <captive-profile-name>
```

Пример создания и редактирования captive-профиля:

```
Admin@nodename# create users captive-profiles name "New captive
profile" auth-profile "LDAP auth profile" captive-auth-mode aaa enable-
ldap on
Admin@nodename# set users captive-profiles "New captive profile" use-
https on
```

Для удаления профиля используется команда:

```
Admin@nodename# delete users captive-profiles <captive-profile-name>
```

Также, с использованием следующей команды, доступно удаление групп для временных пользователей (всегда должна быть указана хотя бы одна группа для временных пользователей):

```
Admin@nodename# delete users captive-profiles <captive-profile-name>
ta-groups
```

Captive-портал

В данном разделе описана настройка правил Captive-портала; настройка производится на уровне **users captive-portal**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Параметры правил captive-портала:

Параметр	Описание
OK PASS	Действия правила Captive-портала: • OK – использовать аутентификацию. • PASS – не использовать аутентификацию.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила captive-портала. Например: name("Captive rule example") .
desc	Описание правила captive-портала. Чтобы задать описание правила: desc("Captive portal rule example set via CLI") .
profile	Captive-профиль указывается при использовании аутентификации на captive-портале. Например, profile("Example Captive profile") . Подробнее о создании и настройке captive-профилей читайте в разделе Настройка Captive-профилей .
rule_log	Включение/отключение записи срабатывания в журнал правил: • rule_log(yes) или rule_log(true). • rule_log(no) или rule_log(false). Если параметр не указан, то функция журналирования отключена.
src.zone	Зона источника. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.

Параметр	Описание
	Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url(); в скобках необходимо указать название списка URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Пример создания и редактирования правила captive-портала с использованием UPL:

```
Admin@nodename# create users captive-portal 1 upl-rule OK \
...profile("New captive profile") \
...rule_log(true) \
...name("Captive portal rule new") \
...
Admin@nodename# show users captive-portal 1
% ----- 1 -----
OK \
  rule_log(yes) \
  profile("New captive profile") \
  enabled(false) \
  id("676df2b1-03e9-42b2-8375-0b8f78c4c47c") \
  name("Captive portal rule new")

Admin@nodename# set users captive-portal 1 upl-rule OK \
...src.zone = Trusted \
...dst.zone = Untrusted
...
```

```
Admin@nodename# show users captive-portal 1
% ----- 1 -----
OK \
  src.zone = Trusted \
  dst.zone = Untrusted \
  rule_log(yes) \
  profile("New captive profile") \
  enabled(false) \
  id("676df2b1-03e9-42b2-8375-0b8f78c4c47c") \
  name("Captive portal rule new")
```

Настройка терминальных серверов

В данном разделе описана настройка терминальных серверов с использованием интерфейса командной строки. Настройка производится на уровне **users terminal-servers**.

Для создания терминального сервера необходимо ввести следующую команду:

```
Admin@nodename# create users terminal-servers <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение терминального сервера: • on. • off.
name	Название терминального сервера.
description	Описание терминального сервера.
hosts	IP-адрес хоста. Для добавления нескольких адресов укажите их через пробел.

Команда для редактирования параметров (параметры приведены выше в таблице) терминального сервера:

```
Admin@nodename# set users terminal-servers <terminal-server-name>
<parameter>
```

Команда для отображения информации о терминальном сервере:

```
Admin@nodename# show users terminal-servers <terminal-server-name>
```

Пример создания и редактирования терминального сервера:

```
Admin@nodename# create users terminal-servers name "Test terminal
server" hosts [ 10.10.0.20 ] enabled on
Admin@nodename# show users terminal-servers "Test terminal server"

name          : Test terminal server
enabled       : on
hosts         : 10.10.0.20

Admin@nodename# set users terminal-servers "Test terminal server"
description "Test terminal server description"
Admin@nodename# show users terminal-servers "Test terminal server"

name          : Test terminal server
description   : Test terminal server description
enabled       : on
hosts         : 10.10.0.20
```

Команда удаления терминального сервера:

```
Admin@nodename# delete users terminal-servers <terminal-server-name>
```

Также возможно удаление отдельных хостов. Для удаления необходимо уточнить их адреса:

```
Admin@nodename# delete users terminal-servers <terminal-server-name>
hosts
```

Настройка профилей MFA (мультифакторной аутентификации)

Данный раздел описывает настройку профилей мультифакторной аутентификации с использованием CLI. Настройка профилей MFA производится на уровне **users mfa-profiles**. Можно создать несколько типов профилей:

- **MFA через TOTP:** использование токена TOTP (Time-based One Time Password) в качестве второго фактора аутентификации.
- **MFA через email:** использование одноразового пароля, полученного по email, в качестве второго фактора аутентификации.
- **MFA через SMS:** использование одноразового пароля, полученного по SMS, в качестве второго фактора аутентификации.

Для создания профиля мультифакторной аутентификации используется команда:

```
Admin@nodename# create users mfa-profiles <parameter>
```

Команда для удаления профиля мультифакторной аутентификации:

```
Admin@nodename# delete users mfa-profiles <mfa-name>
```

Для отображения информации о всех профилях или об определённом профиле MFA используются следующие команды:

```
Admin@nodename# show users mfa-profiles
Admin@nodename# show users mfa-profiles <mfa-name>
```

Настройка MFA через TOTP

Команда для добавления нового профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
show-qr-code	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.
notification-profile	Выбор профиля оповещения.
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").

Команда для редактирования параметров профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# set users mfa-profiles totp <mfa-totp-name> <parameter>
```

Параметры, доступные для редактирования, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp name "Test TOTP MFA
profile" notification-profile pass show-qr-code on
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"

name                : Test TOTP MFA profile
show-qr-code        : on
notification-profile : pass
notification-body    : Your authentication code is {2fa_auth_code}!
```

Do not share it with anybody!

```
Admin@nodename# set users mfa-profiles totp "Test TOTP MFA profile"
description "Test TOTP MFA profile description"
```

```
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"
```

```

name                : Test TOTP MFA profile
description          : Test TOTP MFA profile description
show-qr-code        : on
notification-profile  : pass
notification-body    : Your authentication code is {2fa_auth_code}!
Do not share it with anybody!
```

Настройка MFA через email

Команда для добавления нового профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-profile	Выбор профиля оповещения.
notification-sender	Email отправителя сообщения.
notification-subject	Тема оповещения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через email:

```
Admin@nodename# set users mfa-profiles smtp <mfa-email-profile>
<parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp name "Test SMTP MFA
profile" notification-profile "Example SMTP profile" notification-
sender sender@example.org notification-subject "Test notification subj"
notification-body "Test notification text"
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"
```

```
name                : Test SMTP MFA profile
notification-profile : Example SMTP profile
notification-sender  : sender@example.org
notification-subject : Test notification subj
notification-body    : Test notification text
code-lifetime       : 60
```

```
Admin@nodename# set users mfa-profiles smtp "Test SMTP MFA profile"
code-lifetime 70
```

```
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"
```

```
name                : Test SMTP MFA profile
notification-profile : Example SMTP profile
notification-sender  : sender@example.org
notification-subject : Test notification subj
notification-body    : Test notification text
code-lifetime       : 70
```

Настройка MFA через SMS

Команда для добавления нового профиля мультифакторной аутентификации через SMS:


```
Admin@nodename# create users mfa-profiles smpp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-sender	Имя отправителя сообщения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# set users mfa-profiles smpp <mfa-sms-profile>
<parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp name "Test SMPP MFA
profile" notification-profile "Example SMPP profile" notification-
sender Tes_sender notification-body "Test notification text"
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"
```

```
name                : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender  : Tes_sender
notification-body    : Test notification text
```

```
code-lifetime      : 60
Admin@nodename# set users mfa-profiles smpp "Test SMPP MFA profile"
code-lifetime 80
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"

name                : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender  : Tes_sender
notification-body    : Test notification text
code-lifetime       : 80
```

Просмотр информации об авторизованных пользователях

Для просмотра информации об авторизованных пользователях используется следующая команда интерфейса командной строки в режиме мониторинга:

```
Admin@nodename> show user-auth
```

Для просмотра деталей аутентификационной сессии определенного пользователя используется команда:

```
Admin@nodename> show user-auth <user name>
```

Для удаления сессии определенного пользователя используется команда:

```
Admin@nodename> clear user-auth <parameter>
```

где в качестве параметра может использоваться как имя пользователя, так и его IP-адрес.

Настройка применения политик к пользователям

Для локальных пользователей UserGate политики применяются автоматически.

Если пользователи проходят аутентификацию через LDAP-коннектор, NTLM или Kerberos, то для применения политик к пользователям (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) необходимо сбросить сессии всех пользователей и произвести очистку кэша LDAP-записей на UserGate.

С помощью интерфейса командной строки CLI можно сбросить сессии отдельных пользователей. Команда выполняется в режиме конфигурации (configure), для выполнения команды необходимо знать IP-адрес пользователя:

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

Для очистки кэша используется команда:

```
Admin@nodename# execute cache ldap-clear
```

Настройка UserID-агента

UserID-агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI), Syslog (посредством стандартизированного протокола syslog [RFC 3164](#), [RFC 5424](#), [RFC 6587](#)) и RADIUS (начиная с релиза ПО 7.2.0). Подробнее о схеме работы UserID-агента читайте в разделе [Пользователи и устройства](#) Руководства администратора NGFW.

Настройка UserID в CLI производится на уровне **users userid-agent**.

Настройка параметров UserID-агента

Общие параметры UserID-агента настраиваются с помощью команды:

```
Admin@nodename# set users userid-agent configurate-agent <parameters>
```

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию – 120 секунд.
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
radius-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей по RADIUS-логу. (Доступно в версии ПО 7.2.0 и выше.)
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале Агент UserID . Список может быть создан в разделе библиотек (IP-адреса). Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID. Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.
tcp-enabled	Протокол TCP для приёма журналов по протоколу syslog: • on; • off.
udp-enabled	Протокол UDP для приёма журналов по протоколу syslog: • on; • off.

Настройка источника событий

Microsoft Active Directory

Для добавления Microsoft Active Directory в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent active-directory <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий Active Directory предназначена команда:

```
Admin@nodename# set users userid-agent active-directory <source-name>
<parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа Microsoft Active Directory в таблице выше.

Для просмотра параметров ранее созданных источников событий Active Directory предназначена команда:

```
Admin@nodename# show users userid-agent active-directory
Admin@nodename# show users userid-agent active-directory <source-name>
```

Для удаления ранее созданного источника событий Active Directory предназначена команда:

```
Admin@nodename# delete users userid-agent active-directory <source-name>
```

Syslog-sender

Для добавления отправителя syslog в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent syslog-sender <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе Библиотеки → Syslog фильтры UserID-агента . Подробнее читайте в разделе Syslog фильтры UserID-агента .
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах syslog.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий отправителя syslog предназначена команда:

```
Admin@nodename# set users userid-agent syslog-sender <source-name>
<parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа syslog-sender в таблице выше.

Для просмотра параметров ранее созданных источников событий syslog предназначена команда:

```
Admin@nodename# show users userid-agent syslog-sender
Admin@nodename# show users userid-agent syslog-sender <source-name>
```

Для удаления ранее созданного источника событий syslog предназначена команда:

```
Admin@nodename# delete users userid-agent syslog-sender <source-name>
```

RADIUS-server

Данная опция доступна начиная с релиза ПО 7.2.0.

Для добавления RADIUS-сервера в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent radius-server <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.

Параметр	Описание
address	Адреса хостов, с которых UserGate будет получать события по протоколу RADIUS.
server-secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
default-domain	Имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
attribute-for-group	Номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
attribute-for-name	Номер radius attribute type, в котором находится имя пользователя, по умолчанию 1.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах RADIUS.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий RADIUS предназначена команда:

```
Admin@nodename# set users userid-agent radius-server <source-name>
<parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа RADIUS в таблице выше.

Для просмотра параметров ранее созданных источников событий RADIUS предназначена команда:

```
Admin@nodename# show users userid-agent radius-server
Admin@nodename# show users userid-agent radius-server <source-name>
```

Для удаления ранее созданного источника событий RADIUS предназначена команда:


```
Admin@nodename# delete users userid-agent radius-server <source-name>
```

НАСТРОЙКА РАЗДЕЛА ПОЛИТИКИ СЕТИ

Настройка правил межсетевого экрана

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

```
Admin@nodename# create network-policy firewall
```

Параметры правил межсетевого экрана:

Параметр	Описание
PASS DENY	Действие правила межсетевого экрана: • PASS — разрешить трафик. • DENY — запретить трафик.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила межсетевого экрана. Например: name("Rule example") .
desc	Описание правила. Например: desc("Firewall rule example configured in CLI") .
ips_profile	Профиль COB. Подробнее о создании и настройке профилей COB с использованием интерфейса командной строки читайте в разделе Настройка профилей COB . Например: ips_profile("Test ips profile") .
l7_profile	Профиль приложений. Подробнее о создании и настройке профилей приложений с использованием интерфейса

Параметр	Описание
	командной строки читайте в разделе Настройка профилей приложений. Например: <code>l7_profile("Test application-profile")</code>.
reject_with	Настройка доступна для правил с действием Запретить: • reject_with(no). • reject_with("host_unreach") — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • reject_with("tcp_rst") — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указание сервиса, использующего протокол TCP. • reject_with("tcp_reset-both") — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario". Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • rule_log(session) — журналировать начало сессии.

Параметр	Описание
fragmented	Указание пакетов, к которым применяется правило межсетевого экрана: • fragmented(yes) или fragmented(true) — применить правило к только фрагментированным пакетам. • fragmented(no) или fragmented(false) — применить правило к только нефрагментированным пакетам. • fragmented(all) — применить правило ко всем пакетам. Если не указать fragmented при создании правила, то правило межсетевого экрана применяется ко всем пакетам.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило межсетевого экрана (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило:

Параметр	Описание
	<pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Пример создания правила межсетевого экрана с использованием UPL:

```
Admin@nodename# create network-policy firewall 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = known \
...service = HTTP \
...rule_log(session) \
...name("Test firewall rule") \
...enabled(true)
...
Admin@nodename# show network-policy firewall 1
% ----- 1 -----
PASS \
    user = known \
    src.zone = Trusted \
    dst.zone = Untrusted \
    service = HTTP \
    rule_log(session) \
    enabled(true) \
    id("1505d309-621b-4f88-a2e4-98667c477535") \
    name("Test firewall rule")
```

Настройка правил NAT и маршрутизации

Правила NAT и маршрутизации настраиваются на уровне **network-policy nat-routing**. Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе [UserGate Policy Language](#).

Для создания правила используется команда:

```
Admin@nodename# create network-policy nat-routing <position> upl-rule
<parameters>
```

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set network-policy nat-routing <position> upl-rule <parameters>
```

Команда для просмотра ранее созданных правил:

```
Admin@nodename# show network-policy nat-routing <position>
```

Команда для удаления ранее созданных правил:

```
Admin@nodename# delete network-policy nat-routing <position>
```

Подробнее о применении правил NAT — в разделе «[NAT и маршрутизация](#)».

Настройка правил NAT

При настройке правил NAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила NAT. Например, <code>name("NAT rule example")</code>
desc	Описание правила. Например, <code>desc("NAT rule example set via CLI")</code>
nat	Тип правила
snat_target_ip	IP-адрес, на который будет заменен адрес источника. Адрес указывается в кавычках. Например, <code>snat_target_ip ("1.1.1.1")</code>

Параметр	Описание
<code>rule_log</code>	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
<code>src.zone</code>	Зона источника трафика. Например, для указания зоны Trusted: <code>src.zone = Trusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>src.ip</code>	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: <code>src.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
<code>user</code>	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>

Параметр	Описание
<code>dst.zone</code>	Зона назначения трафика. Для указания зоны назначения трафика, например <code>Untrusted: dst.zone = Untrusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>dst.ip</code>	Добавление списков IP-адресов, доменов назначения, или MAC-адресов. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов назначения используйте: <code>dst.ip = 02:00:00:00:00:00</code>
<code>service</code>	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках укажите название группы сервисов

Пример создания правила NAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...nat \
...rule_log(session) \
...name("Test NAT rule") \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 1
```



```
% ----- 1 -----
OK \
  src.zone = Trusted \
  dst.zone = Untrusted \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("0344640b-b392-4920-9853-77d85ec1338c") \
  name("Test NAT rule")\
  nat
```

Настройка правил NoNAT

При настройке правил NoNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила NAT. Например, <code>name("NAT rule example")</code>
desc	Описание правила. Например, <code>desc("NAT rule example set via CLI")</code>
nonat	Тип правила
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
src.zone	Зона источника трафика.

Параметр	Описание
	Например, указание зоны <code>Trusted</code>: <code>src.zone = Trusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>src.ip</code>	Добавление адресов источника трафика в виде списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: <code>src.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте строку вида: <code>src.ip = 02:00:00:00:00:00</code>
<code>user</code>	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа <code>Any</code>, <code>Unknown</code>, <code>Known</code>. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known</code>; • <code>user = user1</code>; • <code>user = "testd.local\\user2"</code>; • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.zone</code>	Зона назначения трафика. Например, указание зоны <code>Untrusted</code>: <code>dst.zone = Untrusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>dst.ip</code>	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее

Параметр	Описание
	о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов. Подробнее о создании сервисов или групп сервисов — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках укажите название группы сервисов

Пример создания правила NoNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 6 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = "testd.local\\user3" \
...rule_log(session) \
...name("NoNAT rule 1") \
...nonat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 6
% ----- 6 -----
OK \
  user = "testd.local\\user3" \
  src.zone = Trusted \
  dst.zone = Untrusted \
  rule_log(session) \
  enabled(true) \
  name("NoNAT rule 1")\
  nonat
```

Настройка правил DNAT

При настройке правил DNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила DNAT. Например, <code>name("DNAT rule example")</code>
desc	Описание правила. Для описание правила используйте: <code>desc("DNAT rule example created via CLI")</code>
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, <code>snat_target_ip ("1.1.1.1")</code>
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
src.zone	Зона источника трафика. Например, чтобы указать зону Trusted: <code>src.zone = Trusted</code> . Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов.

Параметр	Описание
	Для указания списка IP-адресов: <code>src.ip = lib.network();</code> в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url();</code> в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
<code>src.geoip</code>	Указание Geo IP источника; необходимо указать код страны. Например, <code>src.geoip = RU</code>. Коды названий стран доступны по ссылке
<code>user</code>	Список пользователей или групп, для которых применяется данное правило. Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.zone</code>	Зона назначения трафика. Например, для указания зоны Untrusted: <code>dst.zone = Untrusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>dst.ip</code>	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network();</code> в скобках необходимо указать название списка. Подробнее

Параметр	Описание
	о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
<code>target_ip</code>	Адрес назначения DNAT. Для указания адреса назначения: <code>target_ip("1.1.1.1")</code>
<code>target_snat</code>	Изменение IP-адреса источника на адрес UserGate: • <code>target_snat(yes)</code> или <code>target_snat(true)</code>; • <code>target_snat(no)</code> или <code>target_snat(false)</code>
<code>service</code>	Тип сервиса. Можно указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Untrusted \
...target_ip("10.10.0.15") \
...dnat \
...rule_log(session) \
...name("Test DNAT") \
...enabled(yes)
...
Admin@nodename# show network-policy nat-routing 1
% ----- 1 -----
OK \
    src.zone = Untrusted \
```

```
target_ip("10.10.0.15") \  
direction(input) \  
rule_log(session) \  
enabled(true) \  
id("00e60d4e-9b93-454b-a424-58e2102f84c2") \  
name("Test DNAT")\  
dnat
```

Настройка правил NoDNAT

При настройке правил NoDNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила DNAT. Например, <code>name("DNAT rule example")</code>
desc	Описание правила. Например, <code>desc("DNAT rule example created via CLI")</code>
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, <code>snat_target_ip ("1.1.1.1")</code>

Параметр	Описание
<code>rule_log</code>	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
<code>src.zone</code>	Зона источника трафика. Например, чтобы указать зону Trusted: <code>src.zone = Trusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>src.ip</code>	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: <code>src.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
<code>src.geoip</code>	Указание GeoIP источника; необходимо указать код страны. Например, <code>src.geoip = RU</code>. Коды названий стран доступны по ссылке
<code>user</code>	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора».

Параметр	Описание
	Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.zone</code>	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: <code>dst.zone = Untrusted.</code> Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>dst.ip</code>	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network();</code> в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url();</code> в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
<code>target_ip</code>	Адрес назначения DNAT. Для указания адреса назначения: <code>target_ip("1.1.1.1")</code>
<code>target_snat</code>	Изменение IP-адреса источника на адрес UserGate: • <code>target_snat(yes)</code> или <code>target_snat(true);</code> • <code>target_snat(no)</code> или <code>target_snat(false)</code>
<code>service</code>	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name";</code> для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...).</code> Чтобы указать группу сервисов: <code>service = lib.service();</code> в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...user = known \
...rule_log(session) \
...name("NoDNAT rule") \
...nodnat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 7
% ----- 7 -----
OK \
    user = known \
    src.zone = Untrusted \
    dst.zone = Trusted \
    rule_log(session) \
    enabled(true) \
    name("NoDNAT rule")\
    nodnat
```

Настройка правил трансляции портов

При настройке правил трансляции портов укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила трансляции портов. Например, <code>name("Port forwarding rule example")</code>

Параметр	Описание
desc	Описание правила. Для создания описание правила используйте: <code>desc ("Port forwarding rule example created via CLI")</code>
port_mapping	Тип правила.
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, <code>snat_target_ip ("1.1.1.1")</code>
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: <code>src.zone = Trusted</code> . Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: <code>src.ip = lib.network()</code> ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: <code>src.ip = lib.url()</code> ; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, <code>src.geoip = RU</code> . Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило.

Параметр	Описание
	Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.ip</code>	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
<code>port_map</code>	Переназначение портов публикуемых сервисов. Для переназначения портов необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, <code>port_map(tcp, 2000, 2100)</code>. Следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100
<code>target_ip</code>	Адрес назначения DNAT. Например, <code>target_ip("1.1.1.1")</code>
<code>target_snat</code>	Изменение IP-адреса источника на адрес узла UserGate: • <code>target_snat(yes)</code> или <code>target_snat(true)</code>; • <code>target_snat(no)</code> или <code>target_snat(false)</code>

Пример создания правила трансляции портов с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = Untrusted \
... dst.ip = lib.network(UG_IP) \
... target_ip("10.10.0.16") \
... port_map(tcp, 2222, 23) \
... rule_log(session) \
... name(port_fw1) \
... port_mapping \
...
Admin@nodename# show network-policy nat-routing 8
% ----- 8 -----
OK \
    src.zone = Untrusted \
    dst.ip = lib.network(UG_IP) \
    target_ip("10.10.0.16") \
    port_map(tcp, 2222, 23) \
    direction(input) \
    rule_log(session) \
    enabled(true) \
    id("laf47c3f-96a3-4e65-90e3-debf169bb745") \
    name(port_fw1)\
    port_mapping
```

Настройка правил маршрутизации на основе политик

Для настройки правил маршрутизации на основе политик (policy-based routing, PBR) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила;

Параметр	Описание
	• <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
<code>name</code>	Название правила. Например, <code>name("Policy-based routing rule example")</code>
<code>desc</code>	Описание правила. Для создания описание правила используйте: <code>desc("Policy-based routing rule example set via CLI")</code>
<code>route</code>	Тип правила.
<code>gateway</code>	Выбор одного из существующих шлюзов. Например, <code>gateway("1.1.1.1")</code>. О добавлении шлюзов с использованием интерфейса командной строки — в разделе «Настройка шлюзов»
<code>scenario</code>	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария используйте: <code>scenario = "Example of a scenario"</code>. Подробнее о настройке сценариев с использованием интерфейса командной строки — в разделе «Настройка сценариев»
<code>rule_log</code>	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
<code>src.zone</code>	Зона источника трафика. Для указания зоны источника: <code>src.zone = Trusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
<code>src.ip</code>	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: <code>src.ip = lib.network();</code> в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов».

Параметр	Описание
	Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: <code>src.ip = 02:00:00:00:00:00</code>
<code>src.geoip</code>	Указание GeoIP источника; необходимо указать код страны (например, <code>src.geoip = RU</code>). Коды названий стран доступны по ссылке
<code>user</code>	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.ip</code>	Добавление списков IP-адресов, доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»

Параметр	Описание
<code>dst.geoip</code>	Указание GeoIP назначения; необходимо указать код страны. Например, <code>dst.geoip = RU</code>. Коды названий стран доступны по ссылке
<code>service</code>	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках необходимо указать название группы сервисов

Пример создания и редактирования правила PBR с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule OK \
... route \
... gateway("def") \
... name("testpbr1") \
... enabled(true) \
... rule_log(session) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... service = (HTTPS, HTTP) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... user = "CN=Users1,DC=LOCAL"
Admin@nodename# show network-policy nat-routing 7
% ----- 7 -----
OK \
  user = "CN=Users1,DC=LOCAL" \
  service = (HTTPS, HTTP) \
  gateway(def) \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("0585a95f-4707-4c11-840d-44643bc2c799") \
```



```
name(testpbr1)\
route
```

Настройка правил трансляции адресов сетей

При настройке правил трансляции адресов сетей (network mapping) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code> — включение правила; • <code>enabled(no)</code> или <code>enabled(false)</code> — отключение правила
name	Название правила. Например, <code>name("Network mapping rule example")</code> .
desc	Описание правила. Для создания описание правила используйте: <code>desc("Network mapping rule example set via CLI")</code>
netmap	Тип правила.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • <code>rule_log(no)</code> или <code>rule_log(false)</code> — отключить журналирование. Если при создании правила <code>rule_log</code> не указано, функция журналирования отключена; • <code>rule_log(session)</code> — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: <code>src.zone = Trusted</code> . Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов.

Параметр	Описание
	Для указания списка IP-адресов: <code>src.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
<code>src.geoip</code>	Указание GeoIP источника; необходимо указать код страны. Например, <code>src.geoip = RU</code>. Коды названий стран доступны по ссылке
<code>user</code>	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known;</code> • <code>user = user1;</code> • <code>user = "testd.local\\user2";</code> • <code>user = (user1, "testd.local\\user2")</code>
<code>dst.ip</code>	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»

Параметр	Описание
<code>dst.geoip</code>	Указание GeoIP назначения; необходимо указать код страны. Например, <code>dst.geoip = RU</code> . Коды названий стран доступны по ссылке
<code>target_ip</code>	Параметр подмены сетей; адрес сети, на которую будет производится замена. Например, <code>target_ip("1.1.1.0")</code>
<code>direction</code>	Параметр подмены сетей. Направление: • <code>direction(input)</code> — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>. • <code>direction(output)</code> — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>
<code>service</code>	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »).
	Чтобы указать сервис: <code>service = "service name"</code> ; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code> .
	Чтобы указать группу сервисов: <code>service = lib.service()</code> ; в скобках необходимо указать название группы сервисов

Пример создания правила трансляции адресов сетей с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = External \
... target_ip("192.168.222.0/24") \
... direction(output) \
... netmap \
... rule_log(session) \
... name(netmap1) \
...
Admin@nodename# show network-policy nat-routing 8
% ----- 8 -----
```

```
OK \
  src.zone = External \
  target_ip("192.168.222.0/24") \
  direction(output) \
  rule_log(session) \
  enabled(true) \
  id("26cbd3e8-0210-494c-9fd4-57300b47a9fe") \
  name(netmap1)\
  netmap
```

Настройка балансировки нагрузки

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing** с использованием языка описания политик UPL. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Настройка балансировщиков нагрузки TCP/UDP и reverse-прокси рассмотрена далее.

Для отображения информации о всех балансировщиках используется команда:

```
Admin@nodename# show network-policy load-balancing
```

Настройка балансировщика TCP/UDP

Настройка данного раздела производится на уровне **network-policy load-balancing tcp-udp**.

Структура команды создания балансировщика нагрузки TCP/UDP следующая:

```
Admin@nodename# create network-policy load-balancing tcp-udp <position>
upl-rule
```

Параметры правил балансировки нагрузки TCP/UDP:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.

Параметр	Описание
name	Название правила балансировки. Например: name("TCP_UDP balancer") .
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
desc	Описание правила. Например: desc("TCP_UDP balancing rule") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL . Например: src.ip = lib.network("Test ip-list") .
src.geoip	Указание Geo IP в качестве источника. Например: src.geoip = RU .
url.address	IP-адрес виртуального сервера. Например: url.address = 10.10.0.20 .
url.port	Порт, для которого необходимо производить балансировку нагрузки. Например: url.port = 1812 .
service	Протокол — TCP или UDP, для которого необходимо производить балансировку нагрузки. Например: service = udp .

Параметр	Описание
scheduler	Методы распределения нагрузки на реальные серверы: • rr — round robin — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • wrr — weighted round robin — работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • lc — least connections — новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. • wlc — weighted least connections — работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. Например: scheduler(rr).
real_server	Реальные сервера, на которые будет перенаправляться трафик. Для сервера необходимо указать: • ip — IP-адрес сервера. • port — порт сервера, на который будут перенаправлять запросы пользователей. • weight — коэффициент, использующийся для неравномерного распределения нагрузки на реальные серверы. • mode — режим: ◦ gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: real_server(masq, 10.10.0.9:1812, 50).
ipvs_fallback	Настройка аварийного режима: • ip — IP-адрес сервера.

Параметр	Описание
	• port — порт сервера, на который будут пересылаться запросы пользователей. • mode — режим: ◦ gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: <code>ipvs_fallback(masq, 10.10.100.100:1812).</code>
monitor	Настройка мониторинга реальных серверов: • kind — тип проверки: ◦ ping: проверка доступности узла с использованием утилиты ping. ◦ connect: проверка работоспособности узла путём установления TCP-соединения на определённый порт. ◦ negotiate: проверка работоспособности узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. • service — необходимо указать (HTTP или DNS) при использовании проверки типа negotiate. • request — запрос необходимо указать при использовании проверки типа negotiate. • response — ожидаемый ответ; необходимо указать при использовании проверки типа negotiate. • interval — интервал времени, через который должна выполняться проверка. • timeout — интервал времени ожидания ответа на проверку. • max-failures — количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки. Например:

Параметр	Описание
	<pre>monitor_kind(ping) \ monitor_interval(60) \ monitor_timeout(60) \ monitor_failurecount(10) \</pre>

Для редактирования существующего правила балансировки нагрузки используется следующая команда:

```
Admin@nodename# set network-policy load-balancing tcp-udp <position>
upl-rule
```

Команды для отображения информации о всех правилах балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp
```

Для отображения информации об определённом правиле балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp <position>
```

Пример создания правила балансировщика нагрузки с использованием UPL:

```
Admin@nodename# create network-policy load-balancing tcp-udp 1 upl-rule
OK \
...src.zone = Trusted \
...url.address = 10.10.0.20 \
...url.port = 1812 \
...service = udp \
...scheduler(rr) \
...real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \
...name(tcpudp_balancer1) \
...enabled(true)
...
```



```
Admin@nodename# show network-policy load-balancing tcp-udp

% ----- 1 -----
OK \
  src.zone = Trusted \
  url.address = 10.10.0.20 \
  url.port = 1812 \
  service = udp \
  scheduler(rr) \
  real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \
  monitor_kind(ping) \
  monitor_interval(60) \
  monitor_timeout(60) \
  monitor_failurecount(10) \
  enabled(true) \
  id(cbed6ed7-901e-4641-83a1-a05f82dae177) \
  name(tcpudp_balancer1)
```

Для удаления существующего балансировщика нагрузки используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing tcp-udp <position>
```

Настройка балансировщика reverse-прокси

Настройка правил балансировки reverse-прокси производится на уровне **network-policy load-balancing reverse-proxy**.

Для создания правила балансировки reverse-прокси:

```
Admin@nodename# create network-policy load-balancing reverse-
proxy <position> upl-rule
```

Параметры правил балансировки нагрузки reverse-proxy:

Параметр	Описание
PASS	Действие для создания правила с помощью UPL.

Параметр	Описание
OK	
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила балансировки. Например: name("RP balancer") .
desc	Описание правила. Например: desc("Test reverse-proxy balancing rule") .
profile	Указание профилей серверов reverse-proxy, на которые будет распределяться нагрузка. Подробнее о создании и настройке серверов reverse-proxy с использованием CLI в разделе Настройка серверов reverse-прокси . Например, profile("Reverse proxy server1", "Reverse proxy server2") .

Команда для редактирования параметров правила балансировки reverse-прокси:

```
Admin@nodename# set network-policy load-balancing reverse-proxy <position> upl-rule
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании правила балансировки серверов reverse-прокси.

Команды для отображения информации о всех правилах балансировки reverse-proxy:

```
Admin@nodename# show network-policy load-balancing reverse-proxy
```

Для отображения информации об определённом правиле балансировки reverse-proxy:

```
Admin@nodename# show network-policy load-balancing reverse-proxy <position>
```

Пример создания правила балансировщика нагрузки reverse-proxy с использованием UPL:

```
Admin@nodename# create network-policy load-balancing reverse-proxy 1
upl-rule OK \
...profile("Reverse proxy server1", "Reverse proxy server2") \
...desc("Test reverse proxy balancing rule") \
...name(test_reversep1) \
...enabled(true)
...
Admin@nodename# show network-policy load-balancing reverse-proxy

% ----- 1 -----
OK \
  profile("Reverse proxy server1", "Reverse proxy server2") \
  desc("Test reverse proxy balancing rule") \
  enabled(true) \
  id("1ed892bb-26ee-4ab1-8a55-2f412ce8b55a") \
  name(test_reversep1)
```

Для удаления существующего правила балансировки нагрузки reverse-proxy используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing reverse-
proxy <position>
```

Настройка правил управления пропускной способностью

Настройка правил управления пропускной способностью производится на уровне **network-policy traffic-shaping** с использованием синтаксиса языка UPL. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Для создания правила управления пропускной способностью используется следующая команда:

```
Admin@nodename# create network-policy traffic-shaping <position> upl-  
rule
```

Параметры правил управления пропускной способностью:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила пропускной способности. Например: name("Traffic shaping rule example") .
desc	Описание правила. Для задания описания правила: desc("The example of traffic shaping rule configured in CLI") .
bandwidth_pool	Полоса пропускания, например, bandwidth_pool("1 Mbps") . Подробнее о создании и настройке полос пропускания читайте в разделе Настройка полос пропускания .
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час;

Параметр	Описание
	максимальное количество пакетов, журналируемых на событие равно 5. • rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило пропускной способности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило управления пропускной способностью: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>

Параметр	Описание
dst.zone	Зона назначения трафика. Для задания зоны назначения используется: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка а списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
application	Список приложений, для которых применяется данное правило. Доступно указание: • всех групп приложений: application = lib.category(All). • групп приложений: application = lib.applicationgroup(); в скобках необходимо указать название группы приложений. • категорий приложений: application = lib.category(); в скобках необходимо указать название категорий приложений.
time	Настройка расписания работы правила.

Параметр	Описание
	Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правила управления пропускной способностью используется команда:

```
Admin@nodename# set network-policy traffic-shaping <position> upl-rule
```

Для просмотра всех созданных правил управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping
```

Для просмотра определенного правила управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping <position>
```

Пример создания правила управления пропускной способностью с использованием UPL:

```
Admin@nodename# create network-policy traffic-shaping 1 upl-rule OK \
...user = known \
...src.zone = Trusted \
...dst.zone = Untrusted \
...service = (HTTP, HTTPS) \
...time = lib.time("Working hours") \
...rule_log(session) \
...bandwidth_pool("1 Mbps") \
...name("Test traffic shaping rule") \
...desc("Test traffic shaping rule description") \
...enabled(true)
...
Admin@nodename# show network-policy traffic-shaping 1
```

```
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  dst.zone = Untrusted \
  service = (HTTP, HTTPS) \
  time = lib.time("Working hours") \
  desc("Test traffic shaping rule description") \
  rule_log(session) \
  bandwidth_pool("1 Mbps") \
  enabled(true) \
  id(e63c34e6-af7f-4a4d-a29d-b51d4070655c) \
  name("Test traffic shaping rule")
```

Для удаления правила управления пропускной способностью используется команда:

```
Admin@nodename# delete network-policy traffic-shaping <position>
```

НАСТРОЙКА РАЗДЕЛА ПОЛИТИКИ БЕЗОПАСНОСТИ

Настройка фильтрации контента

Настройка правил контентной фильтрации производится на уровне **security-policy content-filtering**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила контентной фильтрации используется команда:

```
Admin@nodename# create security-policy content-filtering <position>
upl-rule
```

Параметры правил контентной фильтрации:

Параметр	Описание
PASS DENY WARNING	Действие правила контентной фильтрации: • PASS — разрешить посещение веб-страницы. • DENY — заблокировать веб-страницу. • WARNING — предупредить пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила контентной фильтрации. Для указания названия правила: name("Content filtering rule example").
desc	Описание правила. Например: desc("Content filtering rule example set via CLI").
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario". Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.

Параметр	Описание
virus_usergate	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием Запретить; возможны значения: • virus_usergate = yes или virus_usergate = true — использовать проверку потоковым антивирусом UserGate. • virus_usergate = no или virus_usergate = false — не использовать проверку потоковым антивирусом UserGate.
Страница блокировки	Выбор страницы блокировки; если страница не указана, то используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например, DENY("Blockpage (RU)"). Подробнее о настройке страниц блокировки читайте в разделе Настройка шаблонов страниц. Можно использовать внешнюю страницу, задав внешний URL: redirect(302, "http://www.example.com").
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило контентной фильтрации (локальные или LDAP).

Параметр	Описание
	Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.

Параметр	Описание
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка типов контента: response.header.Content-Type = lib.mime(); в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.
morphology	Список баз словарей морфологии, по которым будут проверяться веб-страницы. Для задания списка баз словарей морфологии: morphology = lib.morphology(); в скобках необходимо указать название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка морфологии`_и.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent(); в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.

Параметр	Описание
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET .
request.header.Referer	Список URL, в котором указаны рефереры для текущей страницы, или категория URL, к которой относится реферер. Чтобы указать список или категорию URL: request.header.Referer = lib.url() (в скобках необходимо указать название списка) или request.header.Referer = "URL category" Подробнее о настройке списков URL через CLI читайте в разделе Настройка списков URL ; о категориях URL — Настройка категорий URL .
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правил контентной фильтрации используется команда:

```
Admin@nodename# set security-policy content-filtering <position> upl-rule
```

Для просмотра всех созданных правил контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering
```

Для просмотра определенного правила контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering <position>
```

Пример создания правила контентной фильтрации с использованием UPL:

```
Admin@nodename# create security-policy content-filtering 1 upl-rule  
PASS \
```

```

...src.zone = Trusted \
...url = lib.url("Test URL list") \
...user = known \
...rule_log(yes) \
...name("Test content-filtering rule") \
...desc("Test content-filtering rule description") \
...enabled(true)

...
Admin@nodename# show security-policy content-filtering 1
% ----- 1 --- "Content Rules" -----
PASS \
    user = known \
    url = lib.url("Test URL list") \
    src.zone = Trusted \
    desc("Test content-filtering rule description") \
    rule_log(yes) \
    enabled(true) \
    id("96b2ee34-528a-4b06-8726-69711ba639ba") \
    name("Test content-filtering rule")

```

Для удаления существующего правила контентной фильтрации используется команда:

```
Admin@nodename# delete security-policy content-filtering <position>
```

Настройка веб-безопасности

Настройка веб-безопасности производится на уровне **security-policy safe-browsing**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила веб-безопасности используется команда:

```
Admin@nodename# create security-policy safe-browsing <position> upl-
rule
```

Параметры правил веб-безопасности:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила веб-безопасности. Например: name("Safe browsing rule example").
desc	Описание правила, например, desc("Safe browsing rule example set via CLI").
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) - отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) - включить журналирование
enable_adblock	Блокировка рекламы • enable_adblock(yes) или enable_adblock(true). • enable_adblock(no) или enable_adblock(false).
url_list_exclusions	Список сайтов, для которых блокировать рекламу не требуется: url_list_exclusions("URL list name"). О создании и настройке списков URL с использованием CLI читайте в разделе Настройка списков URL.
enable_injector	Инжектирование кода в веб страницы: • enable_injector(yes) или enable_injector(true). • enable_injector(no) или enable_injector(false).
custom_injector	Код инжектора.
safe_search	Использование функции безопасного поиска: • safe_search(yes) или safe_search(true). • safe_search(no) или safe_search(false).

Параметр	Описание
search_history_logging	Журналирование поисковых запросов пользователей: • search_history_logging(no) или search_history_logging(false) - отключить журналирование поисковых запросов пользователей. Если при создании правила search_history_logging не указано, функция журналирования отключена. • search_history_logging(yes) или search_history_logging(true) - включить журналирование поисковых запросов пользователей.
social_sites_block	Блокировка приложений социальных сетей: • social_sites_block(yes) или social_sites_block(true). • social_sites_block(no) или social_sites_block(false).
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.
user	Пользователи и группы пользователей, для которых применяется правило веб-безопасности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило:

Параметр	Описание
	<pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Для редактирования правил веб-безопасности используется команда:

```
Admin@nodename# set security-policy safe-browsing <position> upl-rule
```

Для просмотра всех созданных правил веб-безопасности используется команда:

```
Admin@nodename# show security-policy safe-browsing
```

Для просмотра определенного правила веб-безопасности используется команда:

```
Admin@nodename# show security-policy safe-browsing <position>
```

Пример создания правила веб-безопасности с помощью UPL:

```

Admin@nodename# create security-policy safe-browsing 1 upl-rule PASS \
...user = known \
...src.zone = Trusted \
...enable_adblock(yes) \
...safe_search(yes) \
...rule_log(yes) \
...name("Test safe browsing rule") \

```

```
...desc("Test safe browsing rule description") \
...enabled(true)
...
Admin@nodename# show security-policy safe-browsing 1
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  rule_log(yes) \
  enable_adblock(yes) \
  safe_search(yes) \
  desc("Test safe browsing rule description") \
  enabled(true) \
  id("406a2753-750e-4830-82a8-583043e72359") \
  name("Test safe browsing rule")
```

Для удаления правила веб-безопасности используется команда:

```
Admin@nodename# delete security-policy safe-browsing <position>
```

Настройка правил инспектирования туннелей

Настройка правил инспектирования туннелей производится на уровне **security-policy tunnel-inspection**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила инспектирования туннелей используется команда:

```
Admin@nodename# create security-policy tunnel-inspection <position>
upl-rule
```

Параметры правил инспектирования туннелей:

Параметр	Описание
OK PASS	Действие правила инспектирования туннелей: • OK — Инспектировать.

Параметр	Описание
	• PASS — Не расшифровывать
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования туннелей. Например: name("Tunnel inspection rule example").
desc	Описание правила. Например: desc("Tunnel inspection rule example configured via CLI").
service	Тип туннеля: • service = gre: инспектирование туннелей GRE. • service = gtpu: инспектирование туннелей GTP-U. • service = ipsec_null: инспектирование нешифрованных IPsec-туннелей
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
dst.zone	Зона назначения трафика, например, dst.zone = "Tunnel inspection zone". Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Для редактирования правил инспектирования туннелей используется команда:

```
Admin@nodename# set security-policy tunnel-inspection <position> upl-rule
```

Для просмотра всех созданных правил инспектирования туннелей используется команда:

```
Admin@nodename# show security-policy tunnel-inspection
```

Для просмотра определенного правила инспектирования туннелей используется команда:

```
Admin@nodename# show security-policy tunnel-inspection <position>
```

Пример создания правила инспектирования туннелей:

```

Admin@nodename# create security-policy tunnel-inspection 1 upl-rule
PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...service = ipsec_null \
...name("Test tunnel-inspection rule") \
...desc("Test tunnel-inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy tunnel-inspection 1
% ----- 1 -----
PASS \
    src.zone = Untrusted \
    dst.zone = Trusted \
    service = ipsec_null \
    desc("Test tunnel-inspection rule description") \
    enabled(true) \
    id("051cf677-3d36-4d5c-968f-73c3421c2b28") \
    name("Test tunnel-inspection rule")

```

Для удаления правила инспектирования туннелей используется команда:

```
Admin@nodename# delete security-policy tunnel-inspection <position>
```

Настройка инспектирования SSL

Настройка правил инспектирования SSL производится на уровне **security-policy ssl-inspection**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила инспектирования SSL используется команда:

```
Admin@nodename# create security-policy ssl-inspection <position> upl-rule
```

Параметры правил инспектирования SSL:

Параметр	Описание
OK PASS	Действие правила инспектирования SSL: • OK — Расшифровать. • PASS — Не расшифровывать • OK ... forward — Расшифровать и переслать; forward указывается среди свойств правила. При настройке правила с действием Расшифровать и переслать необходимо указать профиль пересылки SSL. Подробнее о создании и настройке с использованием CLI профилей пересылки читайте в разделе Настройк а профилей пересылки SSL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования SSL. Для указания названия правила: name("SSL inspection rule example").
desc	Описание правила. Например: desc("SSL inspection rule example configured in CLI").
ssl_forward_profile	Профиль пересылки SSL; профиль необходимо указать при настройке правила инспектирования SSL с действием Расшифровать и переслать. Указывается в формате: ssl_forw ard_profile("SSL forward profile example").
ssl_profile	Профиль SSL; указывается: ssl_profile("Default SSL profile"). Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
block_invalid_cert	Блокирование доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат отозван, выписан на другое доменное имя или

Параметр	Описание
	недоверенным центром сертификации, срок действия сертификата истёк. Доступно в правилах с действием Расшифровать: • block_invalid_cert(yes) или block_invalid_cert(true) — включение блокировки. • block_invalid_cert(no) или block_invalid_cert(false) — отключение блокировки.
check_revoc_cert	Проверка сертификата сайта в списке отозванных сертификатов (CRL) и блокирование доступа, если он там найден. Доступно в правилах с действием Расшифровать: • check_revoc_cert(yes) или check_revoc_cert(true) — включение проверки сертификата. • check_revoc_cert(no) или check_revoc_cert(false) — отключение проверки сертификата.
block_expired_cert	Блокирование сертификатов с истёкшим сроком действия. Доступно в правилах с действием Расшифровать: • block_expired_cert(yes) или block_expired_cert(true) — включить блокировку сертификатов с истёкшим сроком действия. • block_expired_cert(no) или block_expired_cert(false) — отключить блокировку сертификатов с истёкшим сроком действия.
block_self_signed_cert	Блокирование самоподписанных сертификатов. Доступно в правилах с действием Расшифровать: • block_self_signed_cert(yes) или block_self_signed_cert(true) — включить блокировку самоподписанных сертификатов. • block_self_signed_cert(no) или block_self_signed_cert(false) — отключить блокировку самоподписанных сертификатов.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSL (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило:

Параметр	Описание
	<pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1.

Параметр	Описание
service	Тип сервиса: HTTPS, SMTPS или POP3S. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки доменных имён, для которых применяется правило инспектирования SSL. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена типа www.example.com, а не http://www.example.com/home/. Для указания списка доменов: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки читайте в разделе Настройка списков URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Для редактирования правил инспектирования SSL используется команда:

```
Admin@nodename# set security-policy ssl-inspection <position> upl-rule
```

Для просмотра параметров всех созданных правил инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection
```

Для просмотра параметров определенного правила инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection <position>
```

Пример создания правила инспектирования SSL:

```
Admin@nodename# create security-policy ssl-inspection 1 upl-rule OK \
...user = unknown \
...ssl_profile("Default SSL profile") \
...rule_log(yes) \
...name("Decrypt all test rule") \
...desc("Description for decrypt all rest rule") \
...enabled(true)
...
Admin@nodename# show security-policy ssl-inspection 1
% ----- 1 -----
OK \
    user = unknown \
    desc("Description for decrypt all rest rule") \
    rule_log(yes) \
    ssl_profile("Default SSL profile") \
    enabled(true) \
    id("134b7274-01ee-47db-9fc1-a2f06b340b94") \
    name("Decrypt all test rule")
```

Для удаления правила инспектирования SSL используется команда:

```
Admin@nodename# delete security-policy ssl-inspection <position>
```

Настройка инспектирования SSH

Настройка правил SSH-инспектирования производится на уровне **security-policy ssh-inspection**. О структуре команд читайте подробнее в разделе [UserGate Policy Language](#).

Для создания правила инспектирования SSH используется команда:

```
Admin@nodename# create security-policy ssh-inspection <position> upl-  
rule
```

Параметры правил инспектирования SSH:

Параметр	Описание
OK PASS	Действие правила инспектирования SSH: • OK — Расшифровать. • PASS — Не расшифровывать
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила инспектирования SSH. Для указания названия правила: name("SSH inspection rule example") .
desc	Описание правила. Например: desc("SSH inspection rule example configured in CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
block_ssh_shell	Блокирование удалённого запуска shell (интерпретатора командной строки, оболочки). Доступно в правилах с действием Расшифровать : • block_ssh_shell(yes) или block_ssh_shell(true) — включить блокировку. • block_ssh_shell(no) или block_ssh_shell(false) - отключить блокировку.

Параметр	Описание
block_ssh_exec	Блокирование удалённого выполнения по SSH. Доступно в правилах с действием Расшифровать: • block_ssh_exec(yes) или block_ssh_exec(true) — включить блокировку. • block_ssh_exec(no) или block_ssh_exec(false) — отключить блокировку.
ssh_command	Команда linux, которую требуется передать, в формате <code>ssh user@host 'command'</code> Например: ssh_command("ssh root@192.168.1.1 reboot"). Редактирование команды SSH доступно в правилах с действием Расшифровать.
block_sftp	Блокирование соединения SFTP (Secure File Transfer Protocol). Доступно в правилах с действием Расшифровать: • block_sftp(yes) или block_sftp(true) — включить блокировку соединения. • block_sftp(no) или block_sftp(false) — отключить блокировку соединения.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSH (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила.

Параметр	Описание
	Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей.

Для редактирования правил инспектирования SSH используется команда:

```
Admin@nodename# set security-policy ssh-inspection <position> upl-rule
```

Для просмотра всех созданных правил инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection
```

Для просмотра определенного правила инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection <position>
```

Пример создания правила инспектирования SSH с использованием UPL:

```
Admin@nodename# create security-policy ssh-inspection 1 upl-rule OK \
...service = ("Any TCP") \
...block_ssh_shell(yes) \
...block_sftp(yes) \
...rule_log(yes) \
...name("Test SSH inspection rule") \
...desc("Test SSH inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy ssh-inspection 1
% ----- 1 -----
OK \
    service = "Any TCP" \
    block_ssh_shell(yes) \
    block_sftp(yes) \
    desc("Test SSH inspection rule description") \
    rule_log(yes) \
```

```
enabled(true) \
id(d703f390-896f-47c2-91bd-69c6d37aa6d2) \
name("Test SSH inspection rule")
```

Для удаления правила инспектирования SSH используется правило:

```
Admin@nodename# delete security-policy ssh-inspection <position>
```

Настройка COB

Настройка параметров [управления загрузкой](#) системы обнаружения и предотвращения вторжений производится на уровне security-policy intrusion-prevention.

```
Admin@nodename# set security-policy intrusion-prevention <parameter>
```

Доступны параметры:

Параметр	Описание
flow-control	Включение/отключение функции flow control (доступно в версии 7.4.0 и выше): • on — функция включена; • off — функция отключена.
mode	Включение/отключение режима умного сканирования (сканируется часть проходящих пакетов сессии в пределах установленного лимита): • on — режим включен; • off — режим отключен.
limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Посмотреть установленные настройки можно с помощью команды:

```
Admin@nodename# show security-policy intrusion-prevention
```

По умолчанию функция flow control и режим умного сканирования включены; проверяются первые 200 КБ каждой сессии.

[Профили COB](#) создаются в библиотеке элементов и добавляются в [правила межсетевого экрана](#) для активации системы обнаружения и предотвращения вторжений.

Настройка защиты почтового трафика

Настройка правил защиты почтового трафика

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила защиты почтового трафика используется следующая команда:

```
Admin@nodename# create security-policy mail-security <position> upl-rule
```

Параметры правил защиты почтового трафика:

Параметр	Описание
PASS WARNING DENY("with error") DENY	Действие правила защиты почтового трафика: • PASS — Пропустить — пропустить трафик без изменения. • WARNING — Маркировать — маркировать почтовые сообщения специальным тэгом в теме письма или дополнительном поле. • DENY("with error") — Блокировать с ошибкой — блокировать письмо и сообщать об ошибке доставки письма серверу SMTP (для SMTP(S)-трафика) или клиенту (для POP3(S)-трафика). • DENY — Блокировать без ошибки — блокировать письмо без уведомления о блокировке.

Параметр	Описание
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила защиты почтового трафика. Например: name("Mail security rule example").
desc	Описание правила. Например: desc("Mail security rule example configured in CLI").
rule_log	Запись в журнал информации о срабатывании правила защиты почтового трафика. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — включить журналирование.
antispam_usergate	Проверка почтового трафика антиспамом UserGate (задаётся для правил с действием Маркировать, Блокировать с ошибкой или Блокировать без ошибки): • antispam_usergate(yes) или antispam_usergate(true) — включить проверку. • antispam_usergate(no) или antispam_usergate(false) — отключить проверку.
dnsbl	Антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику в правилах с действием Маркировать, Блокировать с ошибкой или Блокировать без ошибки: • dnsbl(yes) или dnsbl(true) — использовать антиспам-проверку. • dnsbl(no) или dnsbl(false) — отключить использование антиспам-проверки. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам и вирусы.

Параметр	Описание
mark_hdr	Заголовок. Поле куда помещать тег маркировки; задаётся для правил с действием Маркировать : mark_hdr(Subject) .
mark	Текст тега, который маркирует письмо; задаётся для правил с действием Маркировать , например, mark("Text for marking emails") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты почтового трафика (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" </pre>

Параметр	Описание
	<pre>user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
envelope_from	Почтовый адрес отправителя письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_from = "Sender email group". Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.
envelop_to	Почтовый адрес адресата письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_to = "Receiver email group". Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.

Для редактирования правила защиты почтового трафика используется команда:

```
Admin@nodename# set security-policy mail-security <position> upl-rule
```

Для просмотра параметров всех созданных правил защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security
```

Для просмотра параметров определенного правила защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security <position>
```

Пример создания правила защиты почтового трафика:

```
Admin@nodename# create security-policy mail-security 1 upl-rule WARNING \
\
...src.zone = Untrusted \
...service = (SMTP, POP3, SMTPS, POP3S) \
...mark_hdr(Subject) \
...mark("[SPAM]") \
...antispam_usergate(yes) \
...rule_log(yes) \
...name("Test SMTP and POP3 filtering") \
...desc("Test SMTP and POP3 filtering description") \
...enabled(true)
...
Admin@nodename# show security-policy mail-security 1
% ----- 1 -----
WARNING \
    src.zone = Untrusted \
    service = (SMTP, POP3, SMTPS, POP3S) \
    rule_log(yes) \
    desc("Test SMTP and POP3 filtering description") \
    mark_hdr(Subject) \
    mark("[SPAM]") \
    antispam_usergate(yes) \
    enabled(true) \
```

```
id("7d86d348-9619-4097-94d1-bad4f3e85554") \
name("Test SMTP and POP3 filtering")
```

Для удаления правила защиты почтового трафика используется команда:

```
Admin@nodename# delete security-policy mail-security <position>
```

Настройка антиспама

Параметры антиспама настраиваются на уровне **security-policy mail-security-antispam**.

Для настройки параметров антиспама используется следующая команда:

```
Admin@nodename# set security-policy mail-security-antispam <parameters>
```

Параметры настройки антиспама:

Параметр	Описание
batv-enabled	on/off . Включение/выключение защиты BATV (Bounce Address Tag Validation), предотвращающей рассылку спам-сообщений в виде возвратных сообщений.
dnsbl-servers	Указание списка DNSBL-серверов для проверки SMTP-трафика.
dnsbl-black-list	Список запрещенных серверов в дополнение к тем, что есть в списках DNSBL. Возможно добавление списка по GeoIP, или списка IP-адресов.
dnsbl-white-list	Список серверов, исключенных из DNSBL проверки. Возможно добавление списка по GeoIP, или списка IP-адресов.

Для просмотра параметров антиспама используется следующая команда:

```
Admin@nodename# show security-policy mail-security-antispam
<parameters>
```

Возможен просмотр всех настроек антиспама целиком (по нажатию Enter), или отдельно белого/черного списков DNSBL при указании параметров **dnsbl-white-list** или **dnsbl-black-list**.

Для удаления параметров антиспама используется следующая команда:

```
Admin@nodename# delete security-policy mail-security-antispam
<parameters>
```

Возможно удаление серверов DNSBL, белого/черного списков DNSBL.

Настройка правил ICAP

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила ICAP используется команда:

```
Admin@nodename# create security-policy icap-rules <position> upl-rule
```

Параметры правил ICAP:

Параметр	Описание
PASS OK	Действие правила ICAP: • PASS — Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • OK — Переслать — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера (стандартный режим работы большинства ICAP-серверов). • OK ... ignore — Переслать и игнорировать — переслать данные ICAP-сервер и игнорировать ответ от ICAP-сервера (вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика); ignore указывается среди свойств правила.

Параметр	Описание
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила ICAP. Для указания названия правила: name("ICAP rule example").
desc	Описание правила. Например: desc("ICAP rule example set via CLI").
profile	ICAP-серверы, куда UserGate будет пересылать запросы; указывается в формате: profile("Example ICAP server"). О настройке серверов ICAP через CLI читайте в разделе Настройка ICAP-серверов.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило ICAP (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке

Параметр	Описание
	LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора. Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка а списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка: response.header.Content-Type = lib.mime(); в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.
category	Список категорий или категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category(); в скобках необходимо указать название списка категорий URL.

Параметр	Описание
	Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: category = "URL category name".
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url(); в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET.
service	Тип сервиса: HTTP, SMTP или POP3. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).

Для редактирования правила ICAP используется команда:

```
Admin@nodename# set security-policy icap-rules <position> upl-rule
```

Для просмотра параметров всех созданных ICAP правил используется команда:

```
Admin@nodename# show security-policy icap-rules
```

Для просмотра параметров определенного правила ICAP:

```
Admin@nodename# show security-policy icap-rules <position>
```

Пример создания правила ICAP:

```
Admin@nodename# create security-policy icap-rules 1 upl-rule PASS \
...src.zone = Trusted \
...http.method = (GET, POST) \
...profile("ICAP server1") \
```

```
...name("Test ICAP rule") \
...desc("Test ICAP rule description") \
...enabled(true)
...
Admin@nodename# show security-policy icap-rules 1
% ----- 1 -----
PASS \
    src.zone = Trusted \
    http.method = (GET, POST) \
    desc("Test ICAP rule description") \
    profile("ICAP server1") \
    enabled(true) \
    id("80a7dca6-96f7-42c8-baad-8716be8d3b93") \
    name("Test ICAP rule")
```

Для удаления правила ICAP используется команда:

```
Admin@nodename# delete security-policy icap-rules <position>
```

Настройка ICAP-серверов

Настройка ICAP-серверов производится на уровне **security-policy icap-server**.

Структура команды для создания ICAP-сервера:

```
Admin@nodename# create security-policy icap-server <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя ICAP-сервера.
description	Задать описание ICAP-сервера.
ip	Задать IP-адрес ICAP-сервера.

Параметр	Описание
port	Задать TCP-порт ICAP-сервера; значение по умолчанию: 1344.
max-msg-size	Определить максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу.
check-icap	Задать период проверки доступности сервера ICAP.
bypass	Если эта опция включена, то UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен.
reqmod-path	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Reqmod.
respmod-path	Использовать режим Respmode: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Respmode.
user-header	Установить отсылку имени пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. • off — не отсылать имя пользователя на ICAP-сервер.
user-encode	Установить кодировку имени пользователя в Base64: • on. • off.
ip-header	Установить отсылку IP-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. • off — не отсылать IP-адрес пользователя на ICAP-сервер.
mac-header	

Параметр	Описание
	Установить отсылку MAC-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. • off — не отсылать MAC-адрес пользователя на ICAP-сервер.

Структура команды для обновления существующего ICAP-сервера:

```
Admin@nodename# set security-policy icap-server <server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового ICAP-сервера.

Структура команды для отображения информации об ICAP-сервере:

```
Admin@nodename# show security-policy icap-server <server-name>
```

Структура команды для удаления ICAP-сервера:

```
Admin@nodename# delete security-policy icap-server <server-name>
```

Настройка профилей DoS

Настройка профилей DoS производится на уровне **security-policy dos-profile**.

Структура команды для создания профиля DoS:

```
Admin@nodename# create security-policy dos-profile <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя профиля.
description	Задать описание профиля.
aggregate	Установить суммирование количества пакетов, проходящих в секунду для всех IP адресов или подсчёт индивидуально для каждого IP-адреса.
syn	Настройка защиты от сетевого флуда для протокола TCP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
udp	Настройка защиты от сетевого флуда для протокола UDP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
icmp	Настройка защиты от сетевого флуда для протокола ICMP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
max-sessions	Установить ограничение количества сессий: • <num> — задать число сессий. • off — отключить ограничение числа сессий.

Структура команды для редактирования существующих профилей DoS:

```
Admin@nodename# set security-policy dos-profile <profile-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды добавления нового профиля DoS.

Структура команды для удаления профиля:

```
Admin@nodename# delete security-policy dos-profile <profile-name>
```

Структура команды для отображения информации о профиле DoS:

```
Admin@nodename# show security-policy dos-profile <profile-name>
```

Настройка правил защиты DoS

Настройка правил защиты от DoS атак производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Структура команды для создания правила защиты от DoS атак:

```
Admin@nodename# create security-policy dos-rules <position> upl-rule <parameters>
```

Параметры правил защиты от DoS атак:

Параметр	Описание
PASS WARNING DENY	Действие правила защиты DoS: • PASS — разрешить трафик; защита от DoS атак не применяется. • WARNING — применить профиль защиты от DoS атак. • DENY — безусловно блокировать трафик.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила защиты DoS. Например: name("DoS rule example") .
desc	Описание правила.

Параметр	Описание
	Например: desc("DoS rule example configured in CLI") .
profile	Профиль защиты DoS. Выбор профиля доступен только для правил с действием Защитить (WARNING). Для указания профиля: profile("DoS profile example"). О создании и настройке профилей защиты читайте в разделе Настройка профилей DoS.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario". Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были

Параметр	Описание
	добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты DoS (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: src.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка а списков URL.
dst.geoip	

Параметр	Описание
	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Структура команды для редактирования правила защиты от DoS атак:

```
Admin@nodename# set security-policy dos-rules <position> upl-rule
<parameters>
```

Структура команды для просмотра правил защиты от DoS атак:

```
Admin@nodename# show security-policy dos-rules
Admin@nodename# show security-policy dos-rules <position>
```

Пример создания правила защиты от DoS атак с помощью UPL:

```
Admin@nodename# create security-policy dos-rules 1 upl-rule WARNING \
...src.zone = Untrusted \
...dst.zone = DMZ \
...service = (HTTP, HTTPS) \
...profile("Test DoS profile") \
...rule_log(session) \
```

```

...name("Test DoS rule") \
...desc("Test DoS rule description") \
...enabled(true)
...
Admin@nodename# show security-policy dos-rules 1
% ----- 1 -----
WARNING \
    src.zone = Untrusted \
    dst.zone = DMZ \
    service = (HTTP, HTTPS) \
    desc("Test DoS rule description") \
    rule_log(session) \
    profile("Test DoS profile") \
    enabled(true) \
    id("68da2f83-59ae-4a7d-b595-f6ff31bf34c6") \
    name("Test DoS rule")

```

Структура команды для удаления правила защиты от DoS атак:

```
Admin@nodename# delete security-policy dos-rules <position>
```

НАСТРОЙКА ГЛОБАЛЬНОГО ПОРТАЛА

Настройка веб-портала

Настройка веб-портала производится на уровне **global-portal web-portal**. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Структура команды создания страницы веб-портала:

```
Admin@nodename# create global-portal web-portal <position> upl-rule
<parameters>
```

Параметры настройки закладок веб-портала:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название закладки. Например: name("Example of bookmark publishing") .
desc	Описание закладки. Например: desc("Example of bookmark publishing configured in CLI") .
url	URL ресурса, который необходимо опубликовать через веб-портал. Необходимо указывать полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. URL указывается как url = "http://www.example.com" .
url.domain	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Для указания домена прямого доступа: url.domain = "example.com" .
rdp_check_session_alive	Разрыв сессии RDP по завершению авторизации на веб-портале: • rdp_check_session_alive(yes) или rdp_check_session_alive(true) — разрывать сессию. • rdp_check_session_alive(no) или rdp_check_session_alive(false) — не разрывать сессию.
ssl_profile	Профиль SSL для построения защищенного канала для отображения веб-портала; указывается: ssl_profile("SSL profile example") .
certificate	Сертификат, который будет использоваться для создания HTTPS-соединения. Чтобы задать сертификат: certificate("Certificate example") .
icon	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из predefined иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку.

Параметр	Описание
	Можно указать: • icon("Default icon name") — использовать штатную иконку (в скобках указывается название штатной иконки). • icon("Icon encoded with Base64") — использовать свою иконку. Необходимо указать содержимое файла, кодированное с использованием Base64. • icon("http://www.icon-url-example.com") — указать URL для использования сторонней иконки.
additional_url	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Для указания: additional_url("http://additional-url-example.com").
user	Пользователи и группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>

Для редактирования правила веб-портала используется команда:

```
Admin@nodename# set global-portal web-portal <position> upl-rule
<parameters>
```

Для просмотра параметров правил веб-портала используется команда:

```
Admin@nodename# show global-portal web-portal <position>
```

Пример создания правила веб-портала с использованием UPL:

```
Admin@nodename# create global-portal web-portal 1 upl-rule OK \
...user = "CN=Default Group,DC=LOCAL" \
...url = "http://www.intranet.loc" \
...name("Test web portal") \
...desc("Test web portal description") \
...enabled(true)
...
Admin@nodename# show global-portal web-portal 1
% ----- 1 -----
OK \
  user = "CN=Default Group,DC=LOCAL" \
  url = "http://www.intranet.loc" \
  icon("default.svg") \
  desc("Test web portal description") \
  enabled(true) \
  id("2fead5a1-29c3-4835-bbdb-1d0e07f84c28") \
  name("Test web portal")
```

Для удаления правила веб-портала используется команда:

```
Admin@nodename# delete global-portal web-portal <position>
```

Настройка правил reverse-прокси

Правила reverse-прокси настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Структура команды для создания правила reverse-прокси:

```
Admin@nodename# create global-portal reverse-proxy-rules <position>
upl-rule <parameters>
```

Параметры настройки правил reverse-прокси:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила reverse-прокси. Например: name("Reverse proxy rule example") .
desc	Описание правила. Например: desc("Reverse proxy rule example set via CLI") .
profile	Сервер reverse-прокси, куда NGFW будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example") .
url.port	Порт, на котором NGFW будет слушать входящие запросы, например, url.port = 80 .
is_https	Поддержка HTTPS: • is_https(yes) или is_https(true) — использовать HTTPS. • is_https(no) или is_https(false) — не использовать HTTPS.
ssl_profile	Профиль SSL; указывается при использовании HTTPS: ssl_profile("Default SSL profile") . Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL .
certificate	Сертификат, используемый для поддержки HTTPS-соединения. Указывается при использовании HTTPS: certificate("Certificate example") .
cert_auth_enabled	Аутентификация по сертификату: • cert_auth_enabled(yes) или cert_auth_enabled(true) — включить авторизацию по сертификату. • cert_auth_enabled(no) или cert_auth_enabled(false) — отключить авторизацию по сертификату.
src.zone	Зона источника трафика.

Параметр	Описание
	Для указания зоны источника, например, Untrusted: src.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	

Параметр	Описание
	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent(); в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.
rewrite_path	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на <code>http://www.example.com/path1</code> в <code>http://www.example.loc/path2</code>. Для этого необходимо указать: rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2").

Для редактирования правила reverse-прокси используется команда:

```
Admin@nodename# set global-portal reverse-proxy-rules <position> upl-
rule <parameters>
```

Для просмотра параметров правила reverse-прокси используется команда:

```
Admin@nodename# show global-portal reverse-proxy-rules <position>
```


Пример создания правила reverse-прокси:

```
Admin@nodename# create global-portal reverse-proxy-rules 1 upl-rule OK
\
...url.port = 80 \
...src.zone = Untrusted \
...profile("Reverse proxy server1") \
...rewrite_path("example.com/path1", "example.local/path2") \
...name("Test reverse proxy rule") \
...desc("Test reverse proxy rule description") \
...enabled(true)
...
Admin@nodename# show global-portal reverse-proxy-rules 1
% ----- 1 -----
OK \
    url.port = 80 \
    src.zone = Untrusted \
    desc("Test reverse proxy rule description") \
    profile("Reverse proxy server1") \
    rewrite_path("example.com/path1", "example.local/path2") \
    enabled(true) \
    id("7dc7041a-6538-400b-8f1e-9b18287218ac") \
    name("Test reverse proxy rule")
```

Для удаления правила reverse-прокси используется команда:

```
Admin@nodename# delete global-portal reverse-proxy-rules <position>
```

Настройка серверов reverse-прокси

Настройка серверов reverse-прокси производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера reverse-прокси используется следующая команда:

```
Admin@nodename# create global-portal reverse-proxy-servers <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера reverse-прокси.
description	Описание сервера reverse-прокси.
address	Адрес или домен сервера reverse-прокси.
port	TCP-порт сервера reverse-прокси.
https	Использование протокола HTTPS до публикуемого сервера: • on: использовать. • off: не использовать.
keep-source-ip	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: • on: оставить оригинальный IP-адрес источника. • off: заменить IP-адрес источника на IP-адрес UserGate. i Важно! Если в пакетах сохраняется оригинальный IP-адрес источника, для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UG NGFW, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UG NGFW или можно настроить статические маршруты через UG NGFW для «белых» IP-адресов источников.

Команда для редактирования параметров сервера reverse-прокси:

```
Admin@nodename# set global-portal reverse-proxy-servers <server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для отображения информации о сервере reverse-прокси:

```
Admin@nodename# show global-portal reverse-proxy-servers <server-name>
```

Структура команды для удаления сервера:

```
Admin@nodename# delete global-portal reverse-proxy-servers <server-name>
```

НАСТРОЙКА VPN В CLI

Настройка серверных правил

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе [UserGate Policy Language](#).

Для создания серверного правила VPN используется команда:

```
Admin@nodename# create vpn server-rules <position> upl-rule <parameters>
```

При настройке необходимо указать:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания.

Параметр	Описание
name	Название серверного правила VPN. Например: name("VPN server rule example") .
desc	Описание правила. Например: desc("VPN server rule example configured in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
vpn_network	Сеть VPN. Для указания сети: vpn_network("VPN network example") . О настройках сети VPN с использованием интерфейса командной строки читайте в разделе Настройка сетей VPN .
auth_profile	Профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль аутентификации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Чтобы указать профиль аутентификации: auth_profile("Example user auth profile") . Подробнее о создании и настройке профилей аутентификации с использованием интерфейса командной строки читайте в разделе Настройка профилей аутентификации .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel1) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
ep_only	Опция (доступна начиная с релиза ПО 7.1.2) позволяет ограничить возможность подключения по данному правилу только для VPN-клиентов UserGate Client (true, false).
src.zone	Зона, с которой разрешено принимать подключения к VPN. Для указания зоны источника, например, Untrusted: src.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов, с которых разрешено принимать подключения к VPN. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов интерфейса, на который будет происходить подключение клиентов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов.

Пример создания серверного правила VPN:

```
Admin@nodename# create vpn server-rules 3 upl-rule OK\
...name("Test server VPN rule") \
```

```
...desc("Test server VPN rule description") \
...profile("New server VPN profile") \
...vpn_network("Test VPN network") \
...auth_profile(Local) \
...interface(tunnel3) \
...src.zone = Untrusted \
...dst.ip = lib.network("UG address") \
...user = ("CN=VPN servers,DC=LOCAL") \
...enabled(true) \
```

Для редактирования серверного правила VPN:

```
Admin@nodename# set vpn server-rules <position> upl-rule <parameters>
```

Для удаления серверных правил VPN:

```
Admin@nodename# delete vpn server-rules <position>
```

Для просмотра сконфигурированных серверных правил VPN:

```
Admin@nodename# show vpn server-rules <position>
```

Настройка клиентских правил

Клиентские правила настраиваются на уровне **vpn client-rules**. Подробнее о структурах команд настройки клиентских правил читайте в разделе [UserGate Policy Language](#).

Команда для создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules <position> upl-rule
<parameters>
```

При настройке правил необходимо указать:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название клиентского правила VPN. Например, name("VPN client rule example") .
desc	Описание клиентского правила VPN. Указывается, как desc("VPN client rule example set in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel3) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
server_address	IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на NGFW, выполняющего роль VPN-сервера. Задаётся в формате: server_address("1.2.3.4") .

При отображении правил, помимо заданных условий и свойств, будут показаны последняя ошибка VPN и статус подключения.

Пример создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules 2 upl-rule OK\
...name("Test VPN client rule") \
...desc("Test VPN client rule description") \
...profile("Client VPN profile") \
...interface(tunnel3) \
```

```
...server_address("10.10.0.1") \
...enabled(true) \
```

Для редактирования клиентского правила VPN:

```
Admin@nodename# set vpn client-rules <position> upl-rule <parameters>
```

Для удаления клиентского правила VPN:

```
Admin@nodename# delete vpn client-rules <position>
```

Для просмотра параметров созданных клиентских правил VPN:

```
Admin@nodename# show vpn client-rules <position>
```

Настройка сетей VPN

Настройка VPN-сетей производится на уровне **vpn networks**.

Для создания сети VPN необходимо использовать следующую команду:

```
Admin@nodename# create vpn networks <parameters>
```

Настраиваемые параметры сети VPN:

Параметр	Описание
name	Название сети VPN.
description	Описание сети VPN.
ip-range	Диапазон IP-адресов, которые будут использованы клиентами и сервером; указывается в формате: <IP_start-IP_end>. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.

Параметр	Описание
mask	Маска сети, например, 255.255.255.0.
use-system-dns	Назначение клиенту DNS-серверов, которые использует UserGate: • on: использовать системных DNS-серверов. • off: не использовать системных DNS-серверов.
dns-servers	DNS-серверы, которые будут переданы клиенту.
routes-ip	Маршрут VPN. Необходимо указать IP-адрес в формате "A.B.C.D" или "A.B.C.D/m".
routes-ip-list	Маршрут VPN. Необходимо указать группу IP-адресов. Подробнее о создании групп IP-адресов через CLI читайте в разделе Настройка IP-адресов .
all-routes	Отсутствие ограничений на маршрутизацию по VPN соединению при использовании UserGate VPN клиента.
include-routes-ip	IP-адреса, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
include-routes-ip-list	Список IP-адресов, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip	IP-адреса, доступ к которым закрыт через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip-list	Список IP-адресов, доступ к которым закрыт через VPN соединение при использовании UserGate VPN клиента.
restrict-lan-access	Запрет доступа к локальной сети при использовании UserGate VPN клиента.

Пример команды создания сети VPN:

```
Admin@nodename# create vpn networks name "Test VPN network" description
"This is a new test VPN network" ip-range 10.10.3.2-10.10.2.200 mask
255.255.255.0
```

Редактирование параметров сети:

```
Admin@nodename# set vpn networks <network-name> <parameters>
```

Удаление сети VPN или отдельных параметров сети VPN:

```
Admin@nodename# delete vpn networks <network-name>
```

Просмотр информации о сети VPN:

```
Admin@nodename# show vpn networks <network-name>
```

Настройка профилей безопасности VPN

Начиная с версии nodename 7.1.0 определены два типа профилей безопасности VPN — серверные и клиентские.

Профили безопасности VPN настраиваются на уровне **vpn server-security-profiles** и **vpn client-security-profiles**.

Создание серверного профиля безопасности VPN

Для создания серверного профиля безопасности VPN предназначена следующая команда:

```
Admin@nodename# create vpn server-security-profiles <parameters>
```

Настраиваемые параметры серверного профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Версия протокола, используемого для создания защищённого канала связи между двумя сетями. Возможны следующие варианты: ipsec — IPsec(IKEv1). ipsec-l2tp — IPsec(IKEv1)/L2TP.

Параметр	Описание
	• ikev2 — IPsec(IKEv2).
ike-mode	Режим IKE: • main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. • aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
local-id-type	Тип параметра IKE local ID. Необходим для валидации peer-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: • none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. • IPv4 — IP-адрес узла. • FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). • CIDR — Адрес узла в формате бесклассовой адресации (CIDR).
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.

Параметр	Описание
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
authentication-mode	Метод аутентификации. Возможна аутентификация с помощью логина и пароля посредством метода EAP (AAA) или посредством сертификатов (PKI).
user-certificate-profile	При выборе метода аутентификации с PKI необходимо указать сконфигурированный ранее профиль клиентских сертификатов.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: • off — Механизм отключен. DPD запросы не отсылаются. • always — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. • idle — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд.

Параметр	Описание
	Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа ДН для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Group 1 Prime 768 bit. • Group 2 Prime 1024 bit. • Group 5 Prime 1536 bit. • Group 14 Prime 2048 bit. • Group 15 Prime 3072 bit. • Group 16 Prime 4096 bit. • Group 17 Prime 6144 bit. • Group 18 Prime 8192 bit.
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn server-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES.

Параметр	Описание
	◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifeseize-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifeseize	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifeseize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off .
nat-keepalive	Период отправки пакетов NAT keealive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keealive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keealive в сторону peer-узла для поддержания сессии NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn server-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256.

Параметр	Описание
	◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.

Создание клиентского профиля безопасности VPN

Для создания клиентского профиля безопасности VPN предназначена следующая команда:

```
Admin@nodename# create vpn client-security-profiles <parameter>
```

Настраиваемые параметры клиентского профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Протокол установления VPN канала. Возможны следующие варианты выбора поля: • ipsec-l2tp — IPsec(IKEv1)/L2TP VPN. • ipsec — IPsec(IKEv1) VPN с оборудованием сторонних производителей. • ikev2 — IPsec(IKEv2) VPN.
ike-mode	Режим IKE: • main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет

Параметр	Описание
	использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. • aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
local-id-type	Тип параметра IKE local ID. Необходим для валидации реер-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: • none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. • IPv4 — IP-адрес узла. • FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). • CIDR — Адрес узла в формате бесклассовой адресации (CIDR).
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
authentication-login	Логин, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.
authentication-password	Пароль, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.

Параметр	Описание
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
vpn-local-network	IP-адрес разрешенной локальной подсети для организации VPN с узлом Cisco.
vpn-remote-network	IP-адрес разрешенной подсети со стороны удаленного VPN-сервера для организации VPN с узлом Cisco.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: • off — Механизм отключен. DPD запросы не отсылаются. • always — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. • idle — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить

Параметр	Описание
	до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Group 1 Prime 768 bit. • Group 2 Prime 1024 bit. • Group 5 Prime 1536 bit. • Group 14 Prime 2048 bit. • Group 15 Prime 3072 bit. • Group 16 Prime 4096 bit. • Group 17 Prime 6144 bit. • Group 18 Prime 8192 bit.
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn client-security- profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.

Параметр	Описание
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifeseize-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifeseize	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifeseize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off .
nat-keepalive	Период отправки пакетов NAT keealive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keealive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keealive в сторону peer-узла для поддержания сессии NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn client-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES.

Параметр	Описание
	◦ AES128. ◦ AES192. ◦ AES256.

Примеры создания и редактирования профилей безопасности VPN

Создание нового профиля безопасности VPN:

```
Admin@nodename# create vpn server-security-profiles <profile-name>
<parameters>
Admin@nodename# create vpn client-security-profiles <profile-name>
<parameters>
...

Admin@nodename# create vpn server-security-profiles name "New server
VPN profile"
```

Редактирование параметров профиля безопасности VPN:

```
Admin@nodename# set vpn server-security-profiles <profile-name>
<parameters>
Admin@nodename# set vpn client-security-profiles <profile-name>
<parameters>
...

Admin@nodename# set vpn server-security-profiles "New server VPN
profile" phase1-security [ SHA1/AES128 SHA1/3DES ] phase2-security
[ SHA1/AES128 SHA1/3DES ]
Admin@nodename# set vpn server-security-profiles "New server VPN
profile" dh-groups [ "Group 16 Prime 4096 bit" ]
Admin@nodename# set vpn server-security-profiles "New server VPN
profile" nat-keepalive 20
```

Удаление параметров профиля безопасности VPN:

```

Admin@nodename# delete vpn server-security-profiles <profile-name>
<parameters>
Admin@nodename# delete vpn client-security-profiles <profile-name>
<parameters>
...
Admin@nodename# delete vpn server-security-profiles "New server VPN
profile" phase1-security [ MD5/AES128 ]
Admin@nodename# delete vpn server-security-profiles "New server VPN
profile" phase2-security [ MD5/AES128 ]
Admin@nodename# delete vpn server-security-profiles "New server VPN
profile" dh-groups [ "Group 16 Prime 4096 bit" ]

```

Просмотр информации о сконфигурированных профилях безопасности VPN:

```

Admin@nodename# show vpn server-security-profiles <profile-name>
Admin@nodename# show vpn client-security-profiles <profile-name>
...
Admin@nodename# show vpn client-security-profiles "New client VPN
profile"

```

НАСТРОЙКА VPN В CLI (В ВЕРСИИ 7.5.0 И ВЫШЕ)

Настройка серверных правил VPN

В UserGate NGFW версии 7.5.0 и выше серверные правила VPN реализованы в виде модульной структуры, состоящей из трех отдельно настраиваемых объектов:

- [правил подключения](#);
- [правил аутентификации](#);
- [политик VPN](#).

Подробнее о структуре серверных правил — в разделе [«Общие понятия»](#).

Серверные правила создаются для двух сценариев:

- Защищенное соединение офисов (site-to-site VPN). Подробнее о создании site-to-site VPN — в разделе [«Настройка VPN для защищенного соединения офисов»](#).
- Удаленный доступ конечных устройств в сеть офиса (remote access VPN). Подробнее о создании remote access VPN — в разделе [«Настройка VPN для удаленного доступа в сеть»](#).

В интерфейсе командной строки серверные правила VPN настраиваются на уровне `vpn-server`.

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом (узлом-инициатором) и завершается ответом VPN-сервера (узла-ответчика) — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Команда для создания правила подключения:

```
Admin@nodename# create vpn-server connection-rules [ike|dtls]
<parameters>
```

Дополнительные параметры команды.

Параметр	Описание
ike	Протокол подключения. Может использоваться в сценариях site-to-site и remote access VPN
dtls	Протокол подключения. Используется только при подключении конечных устройств с помощью UserGate Client в сценарии remote access VPN
name	Название правила подключения
description	Описание правила подключения

Параметр	Описание
<code>protocol</code>	Версия протокола IKE: • <code>ikev1</code>; • <code>ikev2</code>
<code>ike-mode</code>	Режим работы протокола IKEv1: • <code>main</code>; • <code>aggressive</code>
<code>psk</code>	Значение общего ключа (pre-shared key)
<code>src-zones</code>	Зона источника трафика
<code>src-ips</code>	Адрес источника трафика (инициатора соединения): • <code>ip</code> — список IP-адресов; • <code>url</code> — список доменов; • <code>geoip</code> — GeoIP
<code>dst-ips</code>	Адрес назначения трафика (интерфейса, на который будут приходить подключения): • <code>ip</code> — список IP-адресов; • <code>url</code> — список доменов
<code>key-lifetime</code>	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1: • <code>num+s m h</code>, например <code>1s</code>, <code>2m</code>, <code>3h</code>
<code>dpd-state</code>	Режимы работы механизма Dead peer detection (DPD): • <code>off</code> — механизм отключен. DPD-запросы не отсылаются. • <code>always</code> — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в параметре <code>dpd-max-failures</code>. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается. • <code>idle</code> — DPD-запросы не отсылаются, пока есть ESP-трафик через созданный канал. Если в течение

Параметр	Описание
	двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures . Если нет ни одного ответа, соединение завершается
dpd-interval	Интервал отправки дополнительных запросов DPD. Указывается в секундах
dpd-max-failures	Количество повторов отправки DPD-запросов
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами
security	Алгоритмы аутентификации и шифрования
dtls-security	Алгоритмы аутентификации и шифрования для использования с протоколом DTLS.

Пример создания правила подключения с протоколом IKE:

```
Admin@nodename# create vpn-server connection-rules ike name Test1
description "Test connection rule #1" protocol ikev1 psk 123321 ike-
mode main src-zones [ Untrusted ] dh-groups [ "Group 2 Prime 1024 bit"
"Group 14 Prime 2048 bit" ] security [ SHA1/AES256 SHA256/AES256 ] key-
lifetime 1h dpd-state always dpd-interval 65 dpd-max-failures 5
Repeat preshared key:
Admin@nodename# show vpn-server connection-rules ike Test1
```

```
name                : Test1
description          : Test connection rule #1
type                 : ike
protocol             : ikev1
ike-mode             : main
src-zones            : Untrusted
dh-groups            : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
security             :
  authentication     : SHA1
```



```

encryption      : AES256

authentication  : SHA256
encryption      : AES256

key-lifetime    : 1 h
dpd-state       : always
dpd-interval    : 65
dpd-max-failures : 5

Admin@nodename#

```

Для изменения параметров правила подключения используется команда:

```

Admin@nodename# set vpn-server connection-rules [ike|dtls] [rule-name]
<parameters>

```

Для просмотра созданных ранее правил подключения используется команда:

```

Admin@nodename# show vpn-server connection-rules [ike|dtls] <rule-name>

```

Для удаления правил подключения используется команда:

```

Admin@nodename# delete vpn-server connection-rules [ike|dtls] [rule-
name]

```

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа узла-инициатора на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

Команда для создания правила аутентификации:

```
Admin@nodename# create vpn-server authentication-rules [site-to-site|
remote-access] <parameters>
```

Дополнительные параметры команды.

Параметр	Описание
ikev2	Протокол установления защищенного соединения IPsec IKEv2
ipsec	Протокол установления защищенного соединения IPsec IKEv1. Используется только в сценарии site-to-site
l2tp-ipsec	Протокол установления защищенного соединения L2TP/IPsec IKEv1
dtls	Протокол установления защищенного соединения DTLS. Используется только в сценарии remote access
name	Название правила аутентификации
description	Описание правила аутентификации
auth-ptofile	Профиль аутентификации для пользователей VPN
connection-rules	Выбор созданного ранее правила подключения
initiator-type	Выбор параметра идентификации узла-инициатора соединения: • ipv4; • fqdn
initiator-value	Значение параметра идентификации узла-инициатора: • <ip> — например, 192.168.0.1; • <domain> — например, example.com
responder-type	Выбор параметра идентификации узла-ответчика: • ipv4; • fqdn
responder-value	Значение параметра идентификации узла-ответчика: • <ip> — например, 192.168.0.1;

Параметр	Описание
	• <code><domain></code> — например, <code>example.com</code>
<code>auth-mode</code>	Выбор режима аутентификации: • <code>psk</code> — аутентификации с помощью общего ключа (pre-shared key). • <code>pki</code> — аутентификации с помощью x.509 сертификатов. • <code>aaa</code> — аутентификации с помощью сервера AAA (логин и пароль). Только для сценария <code>remote access</code>
<code>psk</code>	Значение общего ключа (pre-shared key) для сценария <code>site-to-site</code> с IKEv2
<code>certificate</code>	Сертификат сервера. Сертификат используется для аутентификации сервера при установлении VPN-соединения.
<code>client-certificate-profile</code>	Профиль сертификата VPN-клиента. Профиль клиентского сертификата предназначен для получения имени пользователя из соответствующего атрибута в сертификате клиента, проверки иерархии доверия и подлинности сертификата по спискам отозванных сертификатов. Подробнее о создании профиля клиентского сертификата — в разделе «Настройка профилей клиентских сертификатов»
<code>key-lifetime</code>	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 2: • <code>num+s m h</code>, например <code>1s</code>, <code>2m</code>, <code>3h</code>
<code>key-lifeseize-enabled</code>	Включение параметра указания максимального размера данных, шифруемых одним ключом: • <code>on</code>; • <code>off</code>
<code>key-lifeseize</code>	Максимальный размер данных, шифруемых одним ключом: • <code>num+KB MB GB</code>, например <code>1KB</code>, <code>2MB</code>, <code>3GB</code>
<code>nat-keepalive</code>	NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот

Параметр	Описание
	промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону VPN-клиентов для поддержания сессии NAT активной. Необходимо указать интервал отправки пакетов keepalive
local-networks remote-networks	Адреса локальных и удаленных подсетей. Используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Адреса указываются в формате [<ip/mask> <ip/mask> ...]
dont-check-initiator-announce	При активации этого параметра VPN-сервер не будет проверять подсети инициатора соединения в селекторе трафика при организации защищенного канала передачи данных. Функция удобна для подключения множества клиентов (инициаторов) по одному правилу
dynamic-routing	Разрешить для протокола IKEv2 работу протоколов динамической маршрутизации через туннель
security	Указание алгоритмов аутентификации и шифрования канала передачи данных

Пример создания правила аутентификации с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-server authentication-rules site-to-site
l2tp-ipsec name Test2 description "Test authentication rule #2"
initiator-type ipv4 initiator-value 172.16.1.10 responder-type ipv4
responder-value 172.16.1.1 auth-profile "Local auth profile" key-
lifetime 1h key-lifetime-enabled on key-lifetime 100MB security [ SHA1/
AES256 SHA256/AES256 ] connection-rules [ CR1 ]
Admin@nodename# show vpn-server authentication-rules site-to-site l2tp-
ipsec Test2

name                               : Test2
```

```

description      : Test authentication rule #2
connection-rules : CR1
initiator-type   : ipv4
initiator-value  : 172.16.1.10
responder-type   : ipv4
responder-value  : 172.16.1.1
auth-profile     : Local auth profile
key-lifetime     : 1 h
key-lifetime-enabled : on
key-lifetime-size : 100.0 MB
nat-keepalive    : 0
security         :
    authentication : SHA1
    encryption     : AES256

    authentication : SHA256
    encryption     : AES256

```

```
Admin@nodename#
```

Для изменения параметров правила аутентификации используется команда:

```
Admin@nodename# set vpn-server authentication-rules [site-to-site|
remote-access] [rule-name] <parameters>
```

Для просмотра созданных правил аутентификации используется команда:

```
Admin@nodename# show vpn-server authentication-rules [site-to-site|
remote-access] [ikev2|ipsec|l2tp-ipsec] <rule-name>
```

Для удаления правил аутентификации используется команда:

```
Admin@nodename# delete vpn-server authentication-rules [site-to-site|
remote-access] [ikev2|ipsec|l2tp-ipsec] [rule-name]
```

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации узла-инициатора и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Политики VPN создаются с помощью синтаксиса языка [UPL](#).

Команда для создания политик VPN:

```
Admin@nodename# create vpn-server vpn-policy [position] upl-rule
```

Дополнительные параметры команды.

Параметр	Описание
OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code>. • <code>enabled(no)</code> или <code>enabled(false)</code>. Если при создании правила не указывать, то правило будет включено после создания
name	Название правила. Например: <code>name("VPN rule example")</code>
desc	Описание правила. Например: <code>desc("VPN rule example configured in CLI")</code>
auth_rules	Выбор созданного ранее правила аутентификации. Например: <code>auth_rules("Authentication rule 1")</code>
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Например, чтобы указать интерфейс tunnel1: <code>interface(tunnel1)</code> .
ip_range	Диапазон IP-адресов туннеля, которые будут использованы VPN-клиентами. Например: <code>ip_range("172.30.255.2-172.30.255.5")</code>

Параметр	Описание
mask	Маска сети VPN-туннеля. Например: <code>mask(255.255.255.0)</code>
vpn_routes	Маршруты, передаваемые узлу-инициатору при установлении VPN-туннеля. Например: <code>vpn_routes(10.10.0.0/24)</code>
use_system_dns	Использование системных DNS-серверов для VPN-клиентов. Например: <code>use_system_dns(true)</code> или <code>use_system_dns(false)</code>
dns_server	Адрес DNS-сервера. Например: <code>dns_server(10.10.0.100)</code>
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор. Подробнее о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора». Пример добавления локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
type	Сценарий установления VPN-соединения. Возможные значения: • <code>type(s2s_l2tp)</code> — сценарий site-to-site, протокол L2TP/IPsec; • <code>type(s2s_ipsec)</code> — сценарий site-to-site, протокол IPsec; • <code>type(ra_ep)</code> — сценарий remote access, конечное устройство с установленным UserGate Client; • <code>type(ra_native)</code> — сценарий remote access, конечное устройство со встроенным VPN-клиентом операционной системы

Параметр	Описание
<code>include_routes</code>	Для каждого включенного адреса в таблице маршрутизации конечного устройства добавляется маршрут вида <code>n.n.n.n/c</code> → VPN-шлюз с гарантированно минимальной метрикой 2. Например: <code>include_routes(10.10.10.10/32)</code>
<code>exclude_routes</code>	При добавлении IP-адресов в список исключаемых, в таблице маршрутизации конечного устройства будет добавлен маршрут по умолчанию вида <code>0.0.0.0/0</code> → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN. Например: <code>exclude_routes(10.10.10.10/32)</code>
<code>disable_lan</code>	Если включен этот параметр (<code>disable_lan(true)</code>), то для каждой подсети локального интерфейса создается копия маршрута через VPN-шлюз с гарантированно минимальной метрикой 2. Такие же копии маршрутов создаются для всех адресов, которые имеют тип <code>local interface</code>
<code>tunnel_all</code>	Если включен этот параметр (<code>tunnel_all(true)</code>), в таблицу маршрутизации конечного устройства будет добавлен маршрут по умолчанию (default route) вида <code>0.0.0.0/0</code> → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы маршрутизации конечного устройства

Пример политики VPN для сценария site-to-site с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-server vpn-policy 6 upl-rule \
...OK
...auth_rules(AR1) \
...vpn_routes(10.10.0.0/24) \
...ip_range("172.30.255.2-172.30.255.5") \
...desc("Серверная политика VPN 1") \
...mask(255.255.255.0) \
...use_system_dns(false) \
...user = "CN=VPN users,DC=LOCAL" \
...dns_server(8.8.8.8) \
...enabled(false) \
...type(s2s_l2tp) \
```



```
...interface(tunnel2) \
...name(VR1)
```

Для изменения параметров политики VPN используется команда:

```
Admin@nodename# set vpn-server vpn-policy [position] upl-rule
```

Для просмотра созданных политик VPN используется команда:

```
Admin@nodename# show vpn-server vpn-policy <position>
```

Для удаления политик VPN используется команда:

```
Admin@nodename# delete vpn-server vpn-policy [position]
```

Просмотр журналов диагностики VPN-сервера

В режиме диагностики интерфейса командной строки вы можете просматривать события журналов диагностики VPN-сервера в статическом и динамическом режиме.

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

```
Admin@nodename> show logs log vpn-server static
```

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-server dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш **Ctrl + C**.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log vpn-server static | grep l2tp
```

Подробнее о функции фильтрации вывода — в разделе «[Общие положения](#)».

Настройка клиентских правил VPN

Клиентские правила используются VPN-сервером, который инициирует подключение в сценарии site-to-site VPN. Подробнее о создании site-to-site VPN — в разделе «[Настройка VPN для защищенного соединения офисов](#)».

В интерфейсе командной строки клиентские правила VPN настраиваются на уровне `vpn-client`.

Настройка параметров подключения клиента

При настройке VPN-подключения указываются используемые протоколы для установления соединения, выбираются методы аутентификации, а также определяются параметры обеих фаз формирования защищенного канала.

Команда для создания подключения клиента:

```
Admin@nodename# create vpn-client connections [ikev2|ipsec|l2tp-ipsec]
<parameters>
```

Дополнительные параметры команды.

Параметр	Описание
<code>name</code>	Название подключения
<code>description</code>	Описание подключения
<code>ike-mode</code>	Режим работы IKEv1: • <code>main</code>; • <code>aggressive</code>
<code>psk</code>	Значение общего ключа (pre-shared key)
<code>initiator-type</code>	Параметр идентификации узла-инициатора: • <code>ipv4</code>;

Параметр	Описание
	• fqdn
initiator-value	Значение параметра идентификации узла-инициатора: • <ip> — например, 192.168.0.1; • <domain> — например, example.com
responder-type	Параметр идентификации узла-ответчика: • ipv4; • fqdn
responder-value	Значение параметра идентификации узла-ответчика: • <ip> — например, 192.168.0.1; • <domain> — например, example.com
authentication-login	Логин для аутентификации узла-инициатора на узле-ответчике в сценарии с протоколом IPsec/L2TP
authentication-password	Пароль для аутентификации узла-инициатора на узле-ответчике в сценарии с протоколом IPsec/L2TP
check-ip	Параметр <code>check_ip</code> определяет, будет ли узел-инициатор соединения запрашивать проверку IP-адреса у VPN-сервера. VPN-сервер может принять предложенный IP-адрес или назначить другой. Если параметр разрешен, узел-инициатор соединения добавляет параметр Payload Configuration в сообщение IKE_AUTH и передает в поле INTERNAL_IP4_ADDRESS значение, зависящее от типа туннельного интерфейса: • Для туннельного интерфейса с динамическим назначением IP-адреса в поле INTERNAL_IP4_ADDRESS передается значение 0.0.0.0/0, что является запросом на динамическое выделение IP-адреса. VPN-сервер, получив значение 0.0.0.0/0, выделяет IP-адрес из собственного пула, заданного в параметрах соединения на сервере. • Для туннельного интерфейса со статическим IP-адресом в поле INTERNAL_IP4_ADDRESS передается его IP-адрес. VPN-сервер использует это значение для проверки соответствия политике подключения. Если параметр не разрешен, механизм согласования сетевых параметров для проверки IP-адреса туннельного интерфейса на VPN-сервере не применяется. Значение IP-

Параметр	Описание
	адреса определяется настройками туннельного интерфейса на узле-инициаторе.
auth-mode	Режим аутентификации: • pki — режим аутентификации с помощью сертификата; • psk — режим аутентификации с помощью общего ключа
certificate	Сертификат узла-инициатора (клиента)
phase1-key-lifetime	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1: • num+s m h, например 1s, 2m, 3h
dpd-state	Режимы работы механизма Dead peer detection (DPD): • off — механизм отключен. DPD-запросы не отсылаются. • always — DPD-запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается. • idle — DPD-запросы не отсылаются, пока есть ESP-трафик через созданный канал. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается
dpd-interval	Интервал отсылки дополнительных запросов DPD. Указывается в секундах
dpd-max-failures	Количество повторов отправки DPD-запросов

Параметр	Описание
<code>dh-groups</code>	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами
<code>phase1-security</code>	Алгоритмы аутентификации и шифрования для фазы 1
<code>phase2-key-lifetime</code>	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 2: • <code>num+s m h</code>, например <code>1s</code>, <code>2m</code>, <code>3h</code>
<code>key-lifeseize-enabled</code>	Включение параметра указания максимального размера данных, шифруемых одним ключом: • <code>on</code>; • <code>off</code>
<code>key-lifeseize</code>	Максимальный размер данных, шифруемых одним ключом: • <code>num+KB MB GB</code>, например <code>1KB</code>, <code>2MB</code>, <code>3GB</code>
<code>dynamic-routing</code>	Разрешить работу протоколов динамической маршрутизации через туннель (для протокола IKEv2)
<code>local-networks</code> <code>remote-networks</code>	Адреса локальных и удаленных подсетей. Используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Адреса указываются в формате [<code><ip/mask></code> <code><ip/mask></code> ...]
<code>phase2-security</code>	Алгоритмы аутентификации и шифрования канала передачи данных (для фазы 2)

Пример настройки клиентского подключения с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-client connections l2tp-ipsec name
Connection1 description "Test connection" ike-mode main authentication-
login vpn_client1 authentication-password password111 psk 123321
```

```

initiator-type ipv4 initiator-value 172.16.1.10 responder-type ipv4
responder-value 172.16.1.1 phase1-key-lifetime 1h dpd-state off dh-
groups [ "Group 2 Prime 1024 bit" "Group 14 Prime 2048 bit" ] phase1-
security [ SHA1/AES256 SHA256/AES256 ] phase2-key-lifetime 1h key-
lifesize 100MB key-lifesize-enabled on phase2-security [ SHA1/AES256
SHA256/AES256 ]

```

Repeat preshared key:

```
Admin@nodename# show vpn-client connections l2tp-ipsec Connection1
```

```

name                               : Connection1
description                         : Test connection
ike-mode                           : main
authentication-login               : vpn_client1
phase1-key-lifetime                : 1 h
phase2-key-lifetime                : 1 h
key-lifesize-enabled               : on
key-lifesize                       : 100.0 MB
initiator-type                     : ipv4
initiator-value                    : 172.16.1.10
responder-type                     : ipv4
responder-value                    : 172.16.1.1
dpd-state                          : off
dpd-interval                       : 60
dpd-max-failures                   : 5
dh-groups                          : Group 2 Prime 1024 bit; Group 14 Prime 2048
bit
phase1-security                    :
    authentication                  : SHA1
    encryption                      : AES256

    authentication                  : SHA256
    encryption                      : AES256

phase2-security                    :
    authentication                  : SHA1
    encryption                      : AES256

    authentication                  : SHA256

```

```
encryption      : AES256
```

```
Admin@nodename#
```

Для изменения параметров клиентского подключения используется команда:

```
Admin@nodename# set vpn-client connections [ikev2|ipsec|l2tp-ipsec]
<connection-name>
```

Для просмотра параметров клиентских подключений используется команда:

```
Admin@nodename# show vpn-client connections [ikev2|ipsec|l2tp-ipsec]
<connection-name>
```

Для удаления клиентского подключения используется команда:

```
Admin@nodename# delete vpn-client connections [ikev2|ipsec|l2tp-ipsec]
<connection-name>
```

Настройка клиентских правил

Клиентское правило в сценарии site-to-site VPN используется для инициирования подключения к VPN-серверу (узлу-ответчику).

Клиентские правила VPN создаются с помощью синтаксиса языка [UPL](#).

Команда для создания клиентских правил:

```
Admin@nodename# create vpn-client rules [position] upl-rule
```

Дополнительные параметры команды.

Параметр	Описание
OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: • <code>enabled(yes)</code> или <code>enabled(true)</code>. • <code>enabled(no)</code> или <code>enabled(false)</code>.

Параметр	Описание
	Если при создании правила не указывать, то правило будет включено после создания
name	Название правила. Например: <code>name("VPN rule example")</code>
desc	Описание правила. Например: <code>desc("VPN rule example configured in CLI")</code>
connection	Название ранее созданного клиентского подключения. Например: <code>connection(Connection1)</code>
interface	VPN-интерфейс, который будет использоваться для подключения. Например, чтобы указать интерфейс tunnel3: <code>interface(tunnel3)</code>
server_address	Адрес VPN-сервера (IP-адрес или доменное имя). Например: <code>server_address("172.16.1.1")</code>

Пример клиентского правила с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-client rules 5 upl-rule \
...OK
...server_address(172.16.1.1)
...connection(Connection1)
...interface(tunnel3)
...enabled(false)
...name(Rule1)
```

Для изменения параметров правила используется команда:

```
Admin@nodename# set vpn-client rules [position] upl-rule
```

Для просмотра созданных правил используется команда:

```
Admin@nodename# show vpn-client rules <position>
```

Для удаления правил используется команда:

```
Admin@nodename# delete vpn-client rules [position]
```


Просмотр журналов диагностики VPN-сервера, работающего в режиме инициатора соединения

В режиме диагностики интерфейса командной строки вы можете просматривать события журналов диагностики VPN-сервера (когда UserGate NGFW выступает в роли узла-инициатора соединения в сценарии site-to-site VPN), в статическом и динамическом режиме.

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

```
Admin@nodename> show logs log vpn-client static
```

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-client dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш **Ctrl + C**.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log vpn-client static | grep l2tp
```

Подробнее о функции фильтрации вывода — в разделе «[Общие положения](#)».

НАСТРОЙКА БИБЛИОТЕК

Настройка библиотек (Описание)

Настройка морфологии

Для создания списка морфологии используется следующая команда:

```
Admin@nodename# create libraries morphology <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название морфологического списка.
description	Описание списка.
threat-lvl	Уровень угрозы: • very-low — очень низкий уровень угрозы. • low — низкий уровень угрозы. • medium — средний уровень угрозы. • high — высокий уровень угрозы. • very-high — высокий уровень угрозы.
threshold	Вес морфологической категории, при превышении которого сработает правило.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Параметр	Описание
words	Слова и фразы, которые необходимо добавить в список. • word — слова и фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. • weight — вес слова или фразы. Если вес не задан, то автоматический устанавливается значение 100. Для добавления слов и фраз: <pre>Admin@nodename# create libraries morphology ... words new word "word or phrase" weight <weight></pre>

Чтобы редактировать список, необходимо использовать следующую команду:

```
Admin@nodename# set libraries morphology <morphology-list-name>
<parameter>
```

Далее указываются параметры, значения которых необходимо обновить (список параметров представлен в таблице выше). Для добавления в список новых слов или фраз необходимо использовать команду:

```
Admin@nodename# set libraries morphology <morphology-list-name> words
new word "word or phrase" weight <weight>
```

Чтобы заменить слово в списке:

```
Admin@nodename# set libraries morphology <morphology-list-name> words
( word "old word or phrase" weight <weight> ) word "new word or phrase"
weight <weight>
```

Следующие команды используются для удаления всего морфологического списка или отдельных слов, содержащихся в нём:

```
Admin@nodename# delete libraries morphology <morphology-list-name>
Admin@nodename# delete libraries morphology <morphology-list-name>
words ( word "word or phrase" weight <weight> )
```

Команды отображения информации о всех имеющихся морфологических списках:

```
Admin@nodename# show libraries morphology
```

Чтобы отобразить информацию об определённом списке, далее необходимо указать название интересующего морфологического списка. Чтобы просмотреть содержание определённого морфологического списка:

```
Admin@nodename# show libraries morphology <morphology-list-name> words
```

Настройка сервисов

Данный раздел настраивается на уровне **libraries services**.

Для добавления нового сервиса используется следующая команда:

```
Admin@nodename# create libraries services <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название сервиса.
description	Описание сервиса.
protocols	Указание сетевого протокола и портов источника/назначения: • protocol — сетевой протокол. • alg — L7 шлюз, только для TCP или UDP (поддерживается SIP, H323, FTP, TFTP — для протокола UDP).

Параметр	Описание
	• dest-ports — порт(ы) назначения (указывается номер порта или диапазон портов). • source-ports — порт(ы) источника (указывается номер порта или диапазон портов).

Для редактирования существующего сервиса:

```
Admin@nodename# set libraries services <service-name> <parameter>
```

Для обновления сетевого протокола и портов источника/назначения сервиса:

```
Admin@nodename# set libraries services <service-name> protocols
( <protocol-filter> )
```

<protocol-filter> — фильтр, настроенный с использованием значений параметра protocols.

Далее указываются новые значения параметра **protocols**.

Для добавления сетевого протокола и портов источника/назначения в существующий сервис:

```
Admin@nodename# set libraries services <service-name> protocols new
<parameter>
```

Далее необходимо указать **protocol, dest-ports, source-ports**.

Чтобы удалить сервис используется следующая команда:

```
Admin@nodename# delete libraries services <service-name>
```

Также возможно удаления из сервиса заданных сетевых протоколов:

```
Admin@nodename# delete libraries services <service-name> protocols
( <protocol-filter> )
```

Следующие команды предназначены для отображения информации о всех сервисах или об определённом сервисе:

```
Admin@nodename# show libraries services
Admin@nodename# show libraries services <service-name>
```

Настройка групп сервисов

Данный раздел находится на уровне **libraries service-groups**. Для создания группы сервисов предназначена следующая команда:

```
Admin@nodename# create libraries service-groups <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы сервисов.
description	Описание группы.
services	Сервисы, которые необходимо добавить в группу.

Для редактирования группы сервисов (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы):

```
Admin@nodename# set libraries service-groups <service-group-name>
<parameter>
```

Чтобы добавить в группу сервисы:

```
Admin@nodename# set libraries service-groups <service-group-name>
[ <service1> < service2> ... ]
```

Следующие команды используются для удаления группы сервисов или отдельных сервисов, содержащихся в ней:

```
Admin@nodename# delete libraries service-groups <service-group-name>
Admin@nodename# delete libraries service-groups <service-group-name>
services [ <service> ... ]
```

Команды отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries service-groups
```

об определённом списке:

```
Admin@nodename# show libraries service-groups <service-group-name>
```

или списка сервисов, добавленных в группу:

```
Admin@nodename# show libraries service-groups <service-group-name>
services
```

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • very-low — очень низкий уровень угрозы. • low — низкий уровень угрозы. • medium — средний уровень угрозы. • high — высокий уровень угрозы.

Параметр	Описание
	• very-high — высокий уровень угрозы.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> ips [ <ip1>
<ip2> ... ]
```


Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1>
<ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка Useragent браузеров

Раздел настраивается на уровне **libraries useragents**.

Следующая команда используется для добавления нового списка Useragent браузеров:

```
Admin@nodename# create libraries useragents <parameter>
```

Далее указываются следующие данные:

Параметр	Описание
name	Название списка Useragent.
description	Описание списка.

Параметр	Описание
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
patterns	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php.

Для редактирования существующего списка:

```
Admin@nodename# set libraries useragents <useragent-list-name>
<parameter>
```

Далее указываются параметры, которые необходимо обновить. Параметры представлены в таблице выше. Чтобы добавить новые Useragent браузеров:

```
Admin@nodename# set libraries useragents <useragent-list-name>
[ <useragent1> <useragent2> ... ]
```

Следующие команды используются для удаления всего списка или отдельных Useragent браузеров, содержащихся в нём:

```
Admin@nodename# delete libraries useragents <useragent-list-name>
Admin@nodename# delete libraries useragents <useragent-list-name>
patterns [ <useragent> ... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries useragents
```

Чтобы отобразить информацию об определённом списке, необходимо указать название списка Useragent браузеров. Чтобы просмотреть содержание списка Useragent браузеров:

```
Admin@nodename# show libraries useragents <useragent-list-name>
patterns
```

Настройка типов контента

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

```
Admin@nodename# create libraries content-types <parameter>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.
description	Описание списка.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab.

Параметр	Описание
	Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
mime	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml.

Для редактирования списка используется следующая команда:

```
Admin@nodename# set libraries content-types <content-types-list-name>
<parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

```
Admin@nodename# delete libraries content-types <content-types-list-
name>
```

Также доступно удаление отдельных типов контента из списка:

```
Admin@nodename# delete libraries content-types <content-types-list-
name> mime [ <mime-type> ... ]
```

Следующие команды используются для отображения информации о списках типов контента:

```
Admin@nodename# show libraries content-types
Admin@nodename# show libraries content-types <content-types-list-name>
```

Для отображения типов контента, содержащихся в списке, используется команда:

```
Admin@nodename# show libraries content-types <content-types-list-name>
mime
```

Настройка списков URL

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

```
Admin@nodename# create libraries url-list <parameter>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка URL.
description	Описание списка URL.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 – вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7.

Параметр	Описание
	- Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
urls	URL, которые необходимо добавить в список.
case-sensitivity	Чувствительность к регистру в написании адреса URL: - sensitive — чувствительно к регистру букв в адресе. - insensitive — нечувствительно к регистру букв в адресе. - domain — список адресов доменов.

Для редактирования списка URL:

```
Admin@nodename# set libraries url-list <url-list-name> <parameter>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

```
Admin@nodename# delete libraries url-list <url-list-name>
Admin@nodename# delete libraries url-list <url-list-name> urls
[ <url> ... ]
```

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

```
Admin@nodename# show libraries url-list
Admin@nodename# show libraries url-list <url-list-name>
Admin@nodename# show libraries url-list <url-list-name> urls
```

Настройка календарей

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

```
Admin@nodename# create libraries time-sets <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.
time-set	• interval-name — название интервала повторения. • type — тип интервала повторения: ◦ daily — ежедневно: ■ time-from — время начала (указывается в формате HH:MM). ■ time-to — время окончания (указывается в формате HH:MM). ■ all-day on — весь день. ◦ weekly — каждую неделю: ■ time-from — время начала (указывается в формате HH:MM). ■ time-to — время окончания (указывается в формате HH:MM). ■ all-day on — весь день. ■ days [Mon Tue Wed Thu Fri Sat Sun] — дни недели. ◦ monthly — каждый месяц: ■ time-from — время начала (указывается в формате HH:MM). ■ time-to — время окончания (указывается в формате HH:MM). ■ all-day on — весь день. ■ days — числа месяца (от 1 до 31). ◦ fixed — единовременно: ■ time-from — время начала (указывается в формате HH:MM).

Параметр	Описание
	■ time-to — время окончания (указывается в формате HH:MM). ■ all-day on — весь день. ■ fixed-date — нужная дата (указывается в формате YYYY-MM-DD). ◦ span — повторяющиеся события: ■ time-from — время начала (указывается в формате HH:MM). ■ time-to — время окончания (указывается в формате HH:MM). ■ all-day on — весь день. ■ fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). ■ fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). ◦ range — диапазон дат: ■ time-from-enabled <on off> — включение/отключение указания даты начала интервала. ■ fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). ■ time-from — время начала (указывается в формате HH:MM). ■ time-to-enabled <on off> — включение/отключение указания даты окончания интервала. ■ fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). ■ time-to — время окончания (указывается в формате HH:MM).

Для редактирования календаря:

```
Admin@nodename# set libraries time-sets <time-sets-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для редактирования интервала, заданного в календаре:


```
Admin@nodename# set libraries time-sets <time-sets-name> ... time-set
<time-set-type> ( <time-set-filter> )
```

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

```
Admin@nodename# create libraries time-sets <time-sets-name> ... time-
set <time-set-type> new
```

Команда для удаления группы элементов:

```
Admin@nodename# delete libraries time-sets <time-sets-name>
```

Для удаления элемента календаря:

```
Admin@nodename# delete libraries time-sets <time-sets-name> <time-set-
type> ( <time-set-filter> )
```

Для отображения информации о всех календарях:

```
Admin@nodename# show libraries time-sets
```

Для отображения информации об определённом календаре:

```
Admin@nodename# show libraries time-sets <time-sets-name>
```

Для отображения информации об элементах группы с одинаковым типом повторения:

```
Admin@nodename# show libraries time-sets <time-sets-name> <time-set-
type>
```

Настройка полос пропускания

Раздел находится на уровне **libraries bandwidth-pools**.

Для добавления новой полосы пропускания используется следующая команда:

```
Admin@nodename# create libraries bandwidth-pools <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название полосы пропускания.
description	Описание полосы пропускания.
rate	Скорость передачи данных; указывается в Кбит/с.
dscp	Значение DSCP QoS (при указании будет прописываться в каждый IP-пакет: принимает значения от 0 до 63).

Для редактирования параметров полосы пропускания:

```
Admin@nodename# set libraries bandwidth-pools <bandwidth-name>
<parameter>
```

Параметры, доступные для изменения такие же, как и для команды создания полосы пропускания.

Чтобы удалить полосу пропускания:

```
Admin@nodename# delete libraries bandwidth-pools <bandwidth-name>
```

С использованием **show** можно отобразить информацию о всех полосах пропускания:

```
Admin@nodename# show libraries bandwidth-pools
```

или об определённой полосе:

```
Admin@nodename# show libraries bandwidth-pools <bandwidth-name>
```

Настройка шаблонов страниц

Раздел находится на уровне **libraries response-pages**. Доступно создание следующих типов шаблонов страниц (<response-page-type>):

- **blockpage** — шаблоны страниц блокировки;
- **captiveportal-user-auth** — шаблоны страниц авторизации captive-портала;
- **captiveportal-user-session** — шаблоны страниц captive-портала, сессия пользователя;
- **content-warning** — шаблоны страниц предупреждения;
- **ftp-client** — шаблоны страниц отображения FTP поверх HTTP;
- **proxy-portal** — шаблоны страниц веб-портала;
- **pp-login-ssh** — шаблоны страниц SSH-логина веб-портала;
- **pp-login-rdp** — шаблоны страниц RDP-логина веб-портала;
- **totp-init-page** — шаблоны страниц инициализации TOTP;
- **network-error-page** — шаблоны страниц сетевых ошибок от прокси-сервера (доступно в версии ПО 7.4.0 и выше).

Команда, используемая для создания шаблона страницы:

```
Admin@nodename# create libraries response-pages <response-page-type>
<parameter>
```

Необходимо указать параметры:

Параметр	Описание
name	Название шаблона страницы.

Параметр	Описание
description	Описание шаблона.
original-template	Выбор базового шаблона. Базовые шаблоны для страницы блокировки (blockpage): • blockpage-en — шаблон страницы блокировки на английском языке; • blockpage-ru — шаблон страницы блокировки на русском языке. Базовые шаблоны для страницы авторизации captive-портала (captiveportal-user-auth): • captiveportal_user_auth-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке; • captiveportal_user_auth-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке; • captiveportal-user-auth-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; • captiveportal-user-auth-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; • captiveportal-user-auth-email-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; • captiveportal-user-auth-email-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; • captiveportal-user-auth-sms-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; • captiveportal-user-auth-sms-ru — шаблон страницы авторизации пользователя с помощью captive-

Параметр	Описание
	портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; • captiveportal-user-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации; • captiveportal-user-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации. Базовые шаблоны для страницы captive-портал, сессия пользователя (captiveportal-user-session): • captiveportal-user-session-en — шаблон на английском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps; • captiveportal-user-session-ru — шаблон на русском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps. Базовые шаблоны для страницы предупреждения (content-warning): • content-warning-en — шаблон страницы предупреждения на английском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить; • content-warning-ru — шаблон страницы предупреждения на русском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить.

Параметр	Описание
	Базовые шаблоны для страницы отображения FTP поверх HTTP (ftp-client): • ftp-client-en — шаблон на английском языке для отображения контента FTP-серверов поверх HTTP; • ftp-client-ru — шаблон на русском языке для отображения контента FTP-серверов поверх HTTP. Базовые шаблоны для страницы веб-портала (proxy-portal): • proxy-portal-en — шаблон на английском языке для отображения страницы веб-портала; • proxy-portal-ru — шаблон на русском языке для отображения страницы веб-портала. Базовые шаблоны для страницы SSH-логина веб-портала (pp-login-ssh): • pp-login-ssh-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал; • pp-login-ssh-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. Базовые шаблоны для страницы RDP-логина веб-портала (pp-login-rdp): • pp-login-rdp-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал; • pp-login-rdp-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. Базовые шаблоны для страницы инициализации TOTP (totp-init-page): • totp-init-page-en — шаблон на английском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей; • totp-init-page-ru — шаблон на русском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей.

Параметр	Описание
	Базовые шаблоны для страницы сетевых ошибок от прокси-сервера (network-error-page). Доступно в версии ПО 7.4.0 и выше: • network-error-page-en — шаблон на английском языке для отображения страницы сетевых ошибок от прокси-сервера; • network-error-page-ru — шаблон на русском языке для отображения страницы сетевых ошибок от прокси-сервера.
default	Использовать шаблон по умолчанию: • on; • off.

Для редактирования значений шаблона:

```
Admin@nodename# set libraries response-pages <response-page-type>
<response-page-name> <parameters>
```

Далее необходимо указать значения параметров; параметры представлены в таблице выше.

Чтобы удалить шаблон страницы, используется следующая команда:

```
Admin@nodename# delete libraries response-pages <response-page-type>
<response-page-name>
```

Для просмотра информации о всех имеющихся шаблонах страниц:

```
Admin@nodename# show libraries response-pages
```

Для просмотра информации об отдельном типе шаблонов страниц:

```
Admin@nodename# show libraries response-pages <response-page-type>
```

Для просмотра информации об отдельном шаблоне страницы:

```
Admin@nodename# show libraries response-pages type <response-page-type> <response-page-name>
```

Настройка категорий URL

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

```
Admin@nodename# create libraries url-categories <parameter>
```

Параметры, которые необходимо указать:

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для редактирования параметров группы:

```
Admin@nodename# set libraries url-categories <list-name> <parameter>
```

Для добавления категорий URL в существующую группу:

```
Admin@nodename# set libraries url-categories <list-name> categories  
[ <url-category> ... ]
```

Команды для удаления группы URL-категорий:

```
Admin@nodename# delete libraries url-categories <list-name>
```

или отдельных категорий из группы:


```
Admin@nodename# delete libraries url-categories <list-name> categories
[ <url-category> ... ]
```

Команды для просмотра информации о всех группах URL-категорий:

```
Admin@nodename# show libraries url-categories
```

об определённой группе:

```
Admin@nodename# show libraries url-categories <list-name>
```

Чтобы отобразить список категорий URL, входящих в группу:

```
Admin@nodename# show libraries url-categories <list-name> categories
```

Настройка изменённых категорий URL

Настройка раздела **Изменённые категории URL** производится на уровне **overridden-url-categories**.

Для добавления новой изменённой категории URL:

```
Admin@nodename# create libraries overridden-url-categories <parameter>
```

Далее необходимо указать параметры:

Параметр	Описание
domain	Доменное имя проверяемого ресурса.
description	Описание изменяемого домена.
categories	Новые категории сайта (можно указать не более 2-х категорий).

Для редактирования параметров:

```
Admin@nodename# set libraries overridden-url-categories <domain>
<parameter>
```

Для удаления сайта с изменёнными категориями:

```
Admin@nodename# delete libraries overridden-url-categories <domain>
```

Для отображения всего списка сайтов с изменёнными категориями:

```
Admin@nodename# show libraries overridden-url-categories
```

Для отображения информации об определённом сайте с изменёнными категориями URL:

```
Admin@nodename# show libraries overridden-url-categories <domain>
```

Настройка групп приложений

Данный раздел настраивается на уровне **libraries application-groups**.

Для создания группы приложений используется команда:

```
Admin@nodename# create libraries application-groups
```

Далее указываются параметры:

Параметр	Описание
name	Название группы приложений.
description	Описание группы приложений.
apps	Приложения, которые необходимо добавить в группу.

Для редактирования параметров:

```
Admin@nodename# set libraries application-groups <app-group-name>
```

Чтобы добавить новые приложения в существующую группу, используется команда:

```
Admin@nodename# set libraries application-groups <app-group-name> apps
[ <application> ... ]
```

Для удаления группы приложений полностью или отдельных приложений в ней используются команды:

```
Admin@nodename# delete libraries application-groups <app-group-name>
Admin@nodename# delete libraries application-groups <app-group-name>
apps [ <application> ... ]
```

Следующие команды предназначены для отображения информации о всех созданных группах приложений:

```
Admin@nodename# show libraries application-groups
```

или об определённой группе:

```
Admin@nodename# show libraries application-groups <app-group-name>
```

Также доступно отображение приложений, входящих в определённый список:

```
Admin@nodename# show libraries application-groups <app-group-name>
apps
```

Настройка профилей приложений

Настройка профилей приложений производится на уровне **libraries application-profile**.

Для создания профиля приложений используется команда:

```
Admin@nodename# create libraries application-profile <parameter>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля приложений.
description	Описание профиля приложений.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур приложений.
unknown-application-settings	Параметры сигнатуры для неизвестных приложений.

Представленная ниже команда предназначена для редактирования существующего профиля приложений:

```
Admin@nodename# set libraries application-profile <application-profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании профиля.

С использованием следующих команда возможен просмотр информации о всех профилях приложений:

```
Admin@nodename# show libraries application-profile
```

или об одном профиле:

```
Admin@nodename# show libraries application-profile <application-profile-name>
```

Пример создания профиля приложений:

```
Admin@nodename# create libraries application-profile name "Test app
profile 1" description "Test app profile 1 description" filters new
action drop value "category = Games" enabled on
Admin@nodename# show libraries application-profile "Test app profile 1"
```

```
name          : Test app profile 1
description    : Test app profile 1 description
filters       :
  enabled      : on
  value        : category = Games
  enable-setting : on
  action       : drop
  pcap         : off
  track-by     : src
  duration     : 0 days 0 hours 5 minutes
```

Для удаления профиля приложений используется команда:

```
Admin@nodename# delete libraries application-profile <application-
profile-name>
```

Подробнее о профилях приложений читайте в статье [Профили приложений](#) Руководства администратора.

Настройка сигнатур приложений

На уровне **libraries application-signature** возможно создание и настройка пользовательских кастомизированных сигнатур приложений.

Для создания пользовательской сигнатуры приложений используется команда:

```
Admin@nodename# create libraries application-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.

Параметр	Описание
description	Описание сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. • on — включить. • off — отключить.
categories	Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен. • Media streaming • Email • Coin Miners • TunnelingGames • Remote access • Conferencing • Trojan Horses • Business • Mobile • Proxies and anonymizers • Standard networks • VOIP • Web posting • Software update • File storage and backup • Web browsing • File sharing P2P • Instant messaging • Social networking
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • very-low — очень низкий. • low — низкий. • medium — средний.

Параметр	Описание
	• high — высокий. • very-high — очень высокий.
technology	Технология приложения. • browser-based — браузерное веб-приложение. • client-server — клиент-серверное приложение. • network-protocol — сетевой протокол. • peer-to-peer — приложение точка-точка.
type	Тип сигнатуры: • app — сигнатура приложения. • proto — сигнатура протокола. • support — вспомогательная сигнатура.
uasl	Описание сигнатуры приложений с помощью синтаксиса UASL.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры приложений:

```
Admin@nodename# set libraries application-signature <application-signature-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команда возможен просмотр информации о всех сигнатурах приложений:

```
Admin@nodename# show libraries application-signature
```

или об одной сигнатуре:

```
Admin@nodename# show libraries application-signature <application-signature-name>
```

Пример создания сигнатуры приложений:

```
Admin@nodename# create libraries application-signature name "Test app
signature 2" description "Test app signature 2 description" categories
[ "Web browsing" ] signature-id 2 technology browser-based threat low
type app uasl "UASL(.dst_addr=192.168.10.1;)"
Admin@nodename# show libraries application-signature "Test app
signature 2"

signature-id      : 2
name              : Test app signature 2
threat            : low
technology        : browser-based
categories        : Web browsing
uasl              : UASL(.dst_addr=192.168.10.1;)
owner             : You
type              : custom
description       : Test app signature 2 description
```

Для удаления созданной ранее сигнатуры приложений используется команда:

```
Admin@nodename# delete libraries application-signature <application-
signature-name>
```

Подробнее о сигнатурах приложений читайте в статье [Приложения](#) Руководства администратора.

Настройка пользовательских тайм-аутов

Значение пользовательского тайм-аута настраивается в интерфейсе командной строки (CLI) на уровне `libraries application-signature`.

Для проприетарных сигнатур приложений (сигнатур, созданных UserGate) значение тайм-аута бездействия устанавливается с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name">
idle-timeout <num>
```


Значение тайм-аута указывается в секундах в диапазоне от 60 до 604800 секунд.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```
Admin@nodename# show libraries application-signature <"signature-name">
```

Пример:

```
Admin@nodename# set libraries application-signature "1C" idle-timeout
400
Admin@nodename# show libraries application-signature "1C"

signature-id      : 188
name              : 1C
type              : app
description       : 1C is a Russian company specializing in the
                   distribution, support and development of computer programs
                   and databases for business and home use.
threat            : very-low
technology        : Client-server
categories        : Business
idle-timeout      : 400
```

Вернуть значение тайм-аута по умолчанию можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name">
idle-timeout default
```

Пример:

```
Admin@oulimetioeth# set libraries application-signature "1C" idle-
timeout default
Admin@oulimetioeth# show libraries application-signature "1C"

signature-id      : 188
name              : 1C
```

```

type           : app
description    : 1C is a Russian company specializing in the
distribution, support and development of computer programs
                  and databases for business and home use.
threat         : very-low
technology     : Client-server
categories     : Business
idle-timeout   : default

```

В пользовательских сигнатурах (сигнатурах, созданных самими пользователями) значение тайм-аута бездействия можно указать при создании сигнатуры:

```

Admin@nodename# create libraries application-signature name <signature-
name> uasl <"uasl-code"> idle-timeout <num>

```

Значение тайм-аута указывается в секундах.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```

Admin@nodename# show libraries application-signature <"signature-name">

```

Пример создания пользовательской сигнатуры с указанием тайм-аута бездействия:

```

Admin@nodename# create libraries application-signature name test_sig1
uasl "UASL(.name=\"EXAMPLE2\");" idle-timeout 500
Admin@nodename# show libraries application-signature "test_sig1"

signature-id   : 1050002
name           : test_sig1
type           : app
threat         : very-low
idle-timeout   : 500
uasl           : UASL(.name="EXAMPLE2";)

```

В ранее созданных пользовательских сигнатурах можно менять значение тайм-аута с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name">
idle-timeout <num>
```

Пример:

```
Admin@oulimetioeth# set libraries application-signature "test_sig1"
idle-timeout 700
Admin@oulimetioeth# show libraries application-signature "test_sig1"

signature-id      : 1050002
name              : test_sig1
type              : app
threat            : very-low
idle-timeout      : 700
uasl              : UASL(.name="EXAMPLE2";)
```

Установить значение тайм-аута по умолчанию (в зависимости от протокола транспортного уровня) можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name">
idle-timeout default
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@nodename# create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.

Параметр	Описание
description	Описание группы почтовых адресов.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails
[ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab.

Параметр	Описание
	Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones
[ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка сигнатур COB

На уровне **libraries ips-signature** возможно создание и настройка пользовательских кастомизированных сигнатур системы обнаружения вторжения (COB).

Для создания пользовательской сигнатуры COB используется команда:

```
Admin@nodename# create libraries ips-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. • on — включить. • off — отключить.
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • very-low — очень низкий. • low — низкий. • medium — средний. • high — высокий. • very-high — очень высокий.

Параметр	Описание
	Не может быть изменен для сигнатур, созданных UserGate.
action	Действие на срабатывание сигнатуры. Определены следующие значения: • none — действие не определено. • pass — пропустить пакет. • drop — отбросить пакет. • rst — отбросить пакет с разрывом TCP соединения (отправка TCP reset). • block — блокировать IP-адрес источника и/или назначения.
log	Журналирование: • on — включить запись в журнал. • off — отключить запись в журнал.
os	Тип операционной системы, для которой определена сигнатура: • windows • linux • bsd • macos • solaris • cisco • ios • android • other Не может быть изменено для сигнатур, созданных UserGate.
pcap	Трассировка срабатывания сигнатуры с записью в файл формата pcap. • on — включить. • off — отключить.
track-by	Применимость действий типа block или rst на срабатывание сигнатуры: • src — действия block или rst применяются к адресу источника отправления пакетов.

Параметр	Описание
	• dst — действия block или rst применяются к адресу назначения отправления пакетов. • both — действия block или rst применяются и к источнику, и к назначению.
duration	Длительность блокировки для действия block .
uasl	Описание сигнатуры с помощью синтаксиса UASL. Не может быть изменено для сигнатур, созданных UserGate.
cve	Идентификатор уязвимостей по реестру CVE.
bdu	Идентификатор уязвимостей по реестру BDU.
url	Опциональная ссылка на ресурс с описанием уязвимости.
category	Категория сигнатуры — группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup. • attack_response — сигнатуры, определяющие ответы на известные сетевые атаки. • coinminer — скачивание, установка, деятельность известных майнеров. • dns — известные уязвимости DNS. • dos — сигнатуры известных Denial of services атак. • exploit — сигнатуры известных эксплоитов. • ftp — известные FTP-уязвимости. • imap — известные IMAP-уязвимости. • info — потенциальная утечка информации. • ldap — известные LDAP-уязвимости. • malware — скачивание, установка, деятельность известных malware. • misc — другие известные сигнатуры. • netbios — известные уязвимости протокола NETBIOS. • phishing — сигнатуры известных phishing атак. • pop3 — известные уязвимости протокола POP3. • rpc — известные уязвимости протокола RPC. • scada — известные уязвимости протокола SCADA. • scan — сигнатуры, определяющие попытки сканирования сети на известные приложения.

Параметр	Описание
	• <code>shellcode</code> — сигнатуры, определяющие известные попытки запуска программных оболочек. • <code>smtp</code> — известные уязвимости протокола SMTP. • <code>snmp</code> — известные уязвимости протокола SNMP. • <code>sql</code> — известные уязвимости SQL. • <code>telnet</code> — известные попытки взлома по протоколу telnet. • <code>tftp</code> — известные уязвимости протокола TFTP. • <code>user_agents</code> — сигнатуры подозрительных Useragent. • <code>voip</code> — известные уязвимости протокола VoIP. • <code>web_client</code> — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • <code>web_server</code> — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • <code>web_specific_apps</code> — сигнатуры, определяющие известные попытки взлома различных веб приложений. • <code>worm</code> — сигнатуры, определяющие сетевую активность известных сетевых червей. Не может быть изменена для сигнатур, созданных UserGate.
classtype	Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Список классов может быть пополнен. • <code>arbitrary-code-execution</code> — попытка запуска произвольного кода. • <code>attempted-admin</code> — попытка получения административных привилегий. • <code>attempted-dos</code> — попытка совершения атаки Denial of Service. • <code>attempted-recon</code> — попытка атаки, направленной на утечку данных. • <code>attempted-user</code> — попытка получения пользовательских привилегий. • <code>bad-unknown</code> — потенциально плохой трафик. • <code>command-and-control</code> — попытка общения с C&C центром • <code>default-login-attempt</code> — попытка логина с именем/паролем по умолчанию.

Параметр	Описание
	• denial-of-service — обнаружена атака Denial of Service. • exploit-kit — обнаружен exploit kit • misc-activity — прочая активность. • misc-attack — обнаружена атака. • shellcode-detect — обнаружен исполняемый код. • string-detect — обнаружена подозрительная строка. • suspicious-login — попытка логина с использованием подозрительного имени пользователя. • trojan-activity — обнаружен сетевой троян. • web-application-attack — обнаружена атака на веб-приложение. Не может быть изменен для сигнатур, созданных UserGate.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры COB:

```
Admin@nodename# set libraries ips-signature <ips-signature-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команд возможен просмотр информации о сигнатурах COB:

```
Admin@nodename# show libraries ips-signature
```

или об определенной сигнатуре:

```
Admin@nodename# show libraries ips-signature <ips-signature-name>
```

Пример создания сигнатуры COB:

```
Admin@nodename# create libraries ips-signature name "Test signature"
action none threat low description "Test signature description" log on
pcap on url example.org uasl "UASL(.name=\"EXAMPLE\";)" enabled off
```

```
Admin@nodename# show libraries ips-signature "Test signature"
```

```
signature-id      : 5
name              : Test signature
enabled          : off
description       : Test signature description
threat           : low
action           : none
log              : on
pcap             : on
track-by         : src
duration         : 0 days 0 hours 5 minutes
uasl             : UASL(.name="EXAMPLE";)
url              : example.org
owner            : You
type             : custom
```

Для удаления созданной ранее сигнатуры COB используется команда:

```
Admin@nodename# delete libraries ips-signature <ips-signature-name>
```

Подробнее о сигнатурах COB читайте в статье [Сигнатуры COB](#) Руководства администратора.

Настройка профилей COB

Настройка профилей COB производится на уровне **libraries ips-profile**.

Для создания профиля системы обнаружения вторжения используется команда:

```
Admin@nodename# create libraries ips-profile <parameter>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля COB.
description	Описание профиля COB.

Параметр	Описание
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур COB. • new — создание нового фильтра в профиле; • value — SQL-подобное выражение для выбора сигнатур из библиотеки; • enabled — активация фильтра в профиле; • settings — задание свойств отображенных фильтром сигнатур: ◦ action — предпринимаемое действие, если сигнатура сработала, т.е. была найдена в трафике. Действия могут быть следующие: пропустить пакет (pass), отбросить пакет (drop), сбросить пакет с разрывом TCP соединения (reset), заблокировать IP-адрес источника и/или назначения (block-ip). Значение default (по умолчанию) оставляет для всех сигнатур то действие, которое было определено в самих сигнатурах по умолчанию. ◦ enabled — возможность включить/отключить сигнатуры. ◦ log — включение/отключение журналирования срабатывания сигнатуры. ◦ pcap-file — включение/отключение записи в PCAP-файл, если сигнатура сработала.

Пример создания профиля COB:

```
Admin@nodename# create libraries ips-profile name 222 filters new value
"protocol = 'http' AND (category = 'exploit') AND (os = 'Linux')"
```

```
settings action drop log on pcap-file on enabled on
```

Команда для редактирования существующего профиля COB:

```
Admin@nodename# set libraries ips-profile <ips-profile-name>
<parameter>
```

Список настраиваемых параметров аналогичен списку параметров, используемых при создании профиля (таблица выше).

Пример редактирования созданного ранее профиля COB:

```
Admin@nodename# set libraries ips-profile 222 filters 1 settings action
reset
```

С помощью следующей команды можно перенастроить параметры системных сигнатур COB, входящих в правило:

```
Admin@nodename# set libraries ips-profile <ips-profile-name> override
signature <signature-name> <parameters>
```

Следующая команда позволяет вернуть перенастроенные ранее параметры системной сигнатуры COB в первоначальное значение:

```
Admin@nodename# set libraries ips-profile <ips-profile-name> override
signature <signature-name> restore-default
```

С использованием следующих команд возможен просмотр информации о профилях COB:

```
Admin@nodename# show libraries ips-profile
```

или об определенном профиле:

```
Admin@nodename# show libraries ips-profile <ips-profile-name>
```

Пример просмотра определенного фильтра в ранее созданном профиле COB:

```
Admin@nodename# show libraries ips-profile 222 filters 1

enabled      : on
value        : protocol = 'http' AND (category = 'exploit') AND (os = 'L
linux')
settings     :
  enabled     : on
  action      : reset
  pcap-file   : on
  duration    : 5
```

```
track-by      : both
log           : on
```

Для удаления профиля COB используется команда:

```
Admin@nodename# delete libraries ips-profile <ips-profile-name>
```

Для удаления определенного фильтра в ранее созданном профиле COB используется команда:

```
Admin@nodename# delete libraries ips-profile <ips-profile-name> filters
<filter-number>
```

Подробнее о профилях COB читайте в статье [Профили COB](#) Руководства администратора.

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.

Параметр	Описание
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

```
Admin@nodename# create libraries notification-profiles smpp
<parameter>
```

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.

Параметр	Описание
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: <pre>Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7 8]</pre>
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan.

Параметр	Описание
	• 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp>
<profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp>
<profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-
name> phone-translation-rules [ phone1!phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
<profile-name>
```

Настройка профилей Netflow

Раздел находится на уровне **libraries netflow-profiles**.

Команда для создания профиля NetFlow:

```
Admin@nodename# create libraries netflow-profiles <parameter>
```

Далее необходимо указать параметры профиля:

Параметр	Описание
name	Название профиля NetFlow.
description	Описание профиля.
ip	IP-адрес NetFlow коллектора, куда сенсор будет отправлять статистику.
port	UDP порт, на котором NetFlow коллектор будет принимать статистику.
protocol	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): • 5 — Netflow версии 5. • 9 — Netflow версии 9.

Параметр	Описание
	• 10 — Netflow версии 10.
active-timeout	Время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока (например, передача большого файла через сеть). Задаётся в секундах; значение по умолчанию: 1800 секунд, максимальное значение — 3600 секунд.
inactive-timeout	Время, резервируемое на завершение неактивного потока; указывается в секундах. Значение по умолчанию — 15 секунд; максимальное значение — 3600 секунд.
max-flows	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. После достижения указанного количества все последующие потоки не будут учитываться (ограничение необходимо для защиты от DoS-атак); значение по умолчанию — 2000000; для снятия ограничения установить 0.
nat-events	Включить/отключить отправку информации о NAT преобразованиях в статистику NetFlow: • on. • off.
refresh-rate	Количество пакетов, после которого шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
timeout-rate	Время, через которое старый шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Чтобы редактировать существующий профиль:

```
Admin@nodename# set libraries netflow-profiles <profile-name>
```

Параметры, значения которых можно изменить, представлены в таблице выше.

Следующая команда предназначена для удаления профиля NetFlow:

```
Admin@nodename# delete libraries netflow-profiles <profile-name>
```

Для отображения информации о всех профилях NetFlow или об отдельном профиле используются следующие команды:

```
Admin@nodename# show libraries netflow-profiles
Admin@nodename# show libraries netflow-profiles <profile-name>
```

Настройка профилей LLDP

Создание и настройка профилей LLDP (Link Layer Discovery Protocol) производятся на уровне **libraries lldp-profiles**.

Команда для создания профиля LLDP:

```
Admin@nodename# create libraries lldp-profiles <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля LLDP.
description	Описание профиля.
port-status	Режимы: • rx — только приём данных LLDP — UserGate не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • tx — только передача данных LLDP — UserGate будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей. • rx-tx — приём и передача данных LLDP — UserGate будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.

Следующая команда предназначена для редактирования информации о профиле:

```
Admin@nodename# set libraries lldp-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль LLDP, используя следующую команду:

```
Admin@nodename# delete libraries lldp-profiles <profile-name>
```

Чтобы отобразить информацию о профилях:

```
Admin@nodename# show libraries lldp-profiles
Admin@nodename# show libraries lldp-profiles <profile-name>
```

Настройка профилей SSL

Создание и настройка профилей SSL производятся на уровне **libraries ssl-profiles**.

Команда для создания профиля SSL:

```
Admin@nodename# create libraries ssl-profiles <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля SSL.
description	Описание профиля.

Параметр	Описание
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: • tls1. • tls1.1. • tls1.2.
max-tls-version	Максимальная версия TLS, которая может быть использована в данном профиле: • tls1. • tls1.1. • tls1.2. • tls1.3.
ssl-ciphers	Выбор необходимых алгоритмов шифрования и цифровой подписи.
ssl-ciphers-suite	Установка алгоритмов шифрования для стандартных протоколов. Параметр предназначен для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS; необходимо указать версию: • tls1. • tls1.1. • tls1.2. • tls1.3.

Следующая команда предназначена для редактирования информации о профиле:

```
Admin@nodename# set libraries ssl-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль SSL полностью или удалить отдельные алгоритмы шифрования и цифровой подписи, заданные в нём:

```
Admin@nodename# delete libraries ssl-profiles <profile-name>
Admin@nodename# delete libraries ssl-profiles <profile-name> ssl-
ciphers [ cipher ... ]
```

Чтобы отобразить информацию о профилях SSL:

```
Admin@nodename# show libraries ssl-profiles
Admin@nodename# show libraries ssl-profiles <profile-name>
```

Настройка профилей пересылки SSL

Данный раздел находится на уровне **libraries ssl-forwarding-profiles**.

Для создания профиля пересылки используется команда:

```
Admin@nodename# create libraries ssl-forwarding-profiles <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля пересылки SSL.
description	Описание профиля пересылки.
type	Тип пересылки: • I2. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • I3. Копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.
mac	MAC-адрес назначения (указывается при использовании типа пересылки L2).
iface	Интерфейс UserGate, с которого будет производиться пересылка (указывается при использовании типа пересылки L2).

Параметр	Описание
source-ip	GRE IP-адрес источника (указывается при использовании типа пересылки L3).
dest-ip	GRE IP-адрес назначения (указывается при использовании типа пересылки L3).

Следующая команда предназначена для обновления параметров профилей пересылки:

```
Admin@nodename# set libraries ssl-forwarding-profiles <profile-name>
<parameter>
```

Для удаления профиля:

```
Admin@nodename# delete libraries ssl-forwarding-profiles <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом профиле пересылки, используются следующие команды:

```
Admin@nodename# show libraries ssl-forwarding-profiles
Admin@nodename# show libraries ssl-forwarding-profiles <profile-name>
```

Настройка объектов HIP

Данный раздел находится на уровне **libraries hip-object**

Для создания объекта HIP используется команда:

```
Admin@nodename# create libraries hip-object <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название объекта HIP.

Параметр	Описание
description	Описание объекта HIP.
process	Проверка процессов, запущенных на конечном устройстве.
running-services	Проверка служб, запущенных на конечном устройстве.
installed-updates	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.
os-version	Версия операционной системы устройства пользователя.
products	Проверка на соответствие статуса: • antimalware — антивирусное ПО на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • firewall — межсетевой экран на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • backup — ПО для резервного копирования ◦ products — название продукта. ◦ vendor — производитель продукта. • disk-encryption — ПО шифрования диска на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • dlp — система предотвращения утечек информации на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • patch-management — ПО для установки обновлений на конечном устройстве. ◦ products — название продукта ◦ vendor — производитель продукта.
registry-keys	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце.

Параметр	Описание
	• REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft.
security	Проверка активных компонентов: • firewall — межсетевой экран (да, нет, не проверять). • virus-protection — антивирусное ПО (да, нет, не проверять). • automatic-update — автоматическая установка обновлений (да, нет, не проверять). • bitlocker — шифрование дисков (да, нет, не проверять).
ug-client-version	Версия ПО UserGate Client.

Команда для редактирования параметров объектов HIP:

```
Admin@nodename# set libraries hip-object <hip-object-name> <parameters>
```

Для удаления объекта:

```
Admin@nodename# delete libraries hip-object <hip-object-name>
```

Чтобы отобразить информацию о всех имеющихся объектах или об определённом объекте, используются следующие команды:

```
Admin@nodename# show libraries hip-object
Admin@nodename# show libraries hip-object <hip-object-name>
```

Настройка профилей HIP

Данный раздел находится на уровне **libraries hip-profile**

Для создания профиля HIP используется команда:

```
Admin@nodename# create libraries hip-profile <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля HIP.
description	Описание профиля HIP.
enabled	Включение/отключение использования профиля..
hip-objects	Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP. Подробнее о создании объектов HIP читайте в разделе Настройка объектов HIP .

Следующая команда предназначена для обновления параметров HIPprofiles:

```
Admin@nodename# set libraries hip-profile <hip-profile-name>  
<parameters>
```

Для удаления профиля:

```
Admin@nodename# delete libraries hip-profile <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом HIP profiles, используются следующие команды:

```
Admin@nodename# show libraries hip-profile  
Admin@nodename# show libraries hip-profile <hip-profile-name>
```

Настройка профилей BFD

Данный раздел находится на уровне **libraries bfd-profile**

Для создания профиля BFD используется команда:

```
Admin@nodename# create libraries bfd-profile
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля BFD.
description	Описание профиля.
detect-multiplier	Множитель времени обнаружения; влияет на время обнаружения неисправностей соединения.
receive-interval	Интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами); указывается в миллисекундах.
transmit-interval	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами; указывается в миллисекундах.
echo-receive-interval	Минимальный интервал, через который данная система способна принимать echo-пакеты; указывается в миллисекундах.
echo-transmit-interval	Минимальный интервал, через который система будет способна отправлять echo-пакеты BFD; указывается в миллисекундах.
echo-mode	Включить или выключить режим передачи Echo mode .
passive-mode	Включить или выключить режим Passive .
ttl	Минимальное ожидаемое TTL для входящего управляющего пакета BFD. Может принимать значения от 1 до 254.

Следующая команда предназначена для обновления параметров BFD profiles:

```
Admin@nodename# set libraries bfd-profile <profile-name> <parameter>
```

Для удаления профиля:

```
Admin@nodename# delete libraries bfd-profile <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом BFD profiles, используются следующие команды:

```
Admin@nodename# show libraries bfd-profile
Admin@nodename# show libraries bfd-profile <profile-name>
```

Настройка Syslog фильтров UserID агента

Создание и настройка syslog-фильтров производятся на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

```
Admin@nodename# create libraries syslog-filters <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка сценариев

Общие правила создания сценариев

Настройка сценариев происходит на уровне **libraries scenarios** с использованием UPL (подробнее о написании правил с помощью UserGate Policy Language читайте в разделе [Типы правил](#)).

Для задания условий сценариев и их объединения используются определения (definitions). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слэша (как при использовании многострочного ввода).

Для создания/изменения условий сценариев используется функция **def scenario_cond**, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
<scenario_conditions>
end
```

Параметры, использующиеся для задания разных типов условий, будут рассмотрены в следующих разделах.

Далее, после указания условий, указываются общие свойства сценария, представленные в таблице ниже:

Наименование	Описание
OK	Действие для создания сценария.
scenario_cond	Пользовательское имя определения, содержащего список условий сценария: scenario_cond = condition_example .
enabled	Включить/отключить использование сценария: • enabled(true); • enabled(false).
name	Задать имя сценария: name("Example scenario name") .
desc	Задать описание сценария: desc("Description for scenario created as an example") .
trigger	Применение: • trigger(one_user) — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; • trigger(all_users) — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила.
duration	Задать период активности сценария; указывается в минутах.
operation_mode	Задать режим активации сценария: • operation_mode(all) — сценарий сработает, если выполнятся все условия; • operation_mode(any) — сценарий сработает, если выполнится хотя бы одно из условий.

Примечание При обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием **Объём трафика**. Сценарий будет применён ко всем пользователям в течение минуты; ограничение объёма трафика: 1 ГБ/день:


```
Admin@nodename# create libraries scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(1GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
...
```

Для изменения, например, объёма трафика:

```
Admin@nodename# set libraries scenarios 3 upl-rule \
...def scenario_cond scenario_cond_test
...traffic_limit(2GB) \
...period(day) \
...scond_type(traffic)
...end
...OK \
...scenario_cond = scenario_cond_test
```

Типы условий, используемых при создании сценариев

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
scond_type	Тип условия: scond_type(url_category) .
category	Категории или группы категорий сайтов: category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME).

Наименование	Описание
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: scond_type(virus_detection) .

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
scond_type	Тип условия: scond_type(app) .
application	Категории приложений или группы приложений: • application = lib.applicationgroup(APP_GROUP) или application = lib.applicationgroup(all); • application = lib.category(APPS_CATEGORY_NAME).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Условие типа COB

Параметры условия типа **COB**:

Наименование	Описание
scond_type	Тип условия: scond_type(ips) .
ips_tl	

Наименование	Описание
	Уровень угрозы: • ips_tl(very_low) – очень низкий; • ips_tl(low) – низкий; • ips_tl(medium) – средний; • ips_tl(high) – высокий; • ips_tl(very_high) – очень высокий.

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
scond_type	Тип условия: scond_type(mime_type) .
response.header.Content-Type	Тип контента: response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST) .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(traffic) .
traffic_limit	Ограничение объёма трафика: • traffic_limit(1) – 1 байт трафика; • traffic_limit(1KB) – 1 Кбайт трафика; • traffic_limit(1MB) – 1 Мбайт трафика; • traffic_limit(1GB) – 1 Гбайт трафика.
period	Период времени: • period(minute) – минута;

Наименование	Описание
	• period(hour) – час; • period(day) – день; • period(week) – неделя; • period(month) – месяц.

Условие типа Проверка состояния

Для настройки условия типа **Проверка состояния** предназначены параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(health_check) .
health_check_method	Метод проверки: • health_check_method(ping) – ping; • health_check_method(dns) – DNS-запрос; • health_check_method(get) – HTTP-метод GET.
url.address	Адрес, на который будут выполняться ping и DNS-запрос: url.address = "1.1.1.1" .
url.domain	FQDN для проверки состояния путём выполнения DNS-запроса или URL для метода HTTP GET: url.domain = "example.ru" .
gateway	Название используемого шлюза: gateway() . Важно! Шлюз должен быть предварительно создан.
health_result	Результат выполнения проверки: • health_result(positive) – положительный; • health_result(negative) – отрицательный.
health_request_timeout	Тайм-аут подключения (в секундах): health_request_timeout() .
health_answer_timeout	Время ожидания ответа на запрос HTTP GET (в секундах): health_answer_timeout() .
health_type_request	Тип DNS-запроса: • health_type_request(a). • health_type_request(aaaa).

Наименование	Описание
	• <code>health_type_request(cname)</code>. • <code>health_type_request(ns)</code>. • <code>health_type_request(ptr)</code>.
<code>count_interval</code>	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
<code>max_event_count</code>	Количество срабатываний: <code>max_event_count()</code> .

Настройка тегов

Использование тегов доступно в версии ПО 7.3.0 и выше.

Создание и настройка тегов производятся на уровне **libraries tags**.

Команда для создания тегов:

```
Admin@nodename# create libraries tags <parameters>
```

Далее необходимо указать:

Параметр	Описание
<code>name</code>	Название тега.
<code>description</code>	Описание тега.
<code>color</code>	Выбор цветовой маркировки тега для отображения в веб-интерфейсе: • <code>no-color</code> (Значение по умолчанию); • <code>red</code>; • <code>orange</code>; • <code>yellow</code>; • <code>green</code>; • <code>aqua</code>; • <code>blue</code>; • <code>violet</code>; • <code>pink</code>; • <code>purple</code>;

Параметр	Описание
	• light-gray; • light-green; • light-blue; • black; • rose; • magenta; • wood;

Команда для редактирования информации о теге:

```
Admin@nodename# set libraries tags <tag-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании тега.

Чтобы отобразить информацию о тэгах:

```
Admin@nodename# show libraries tags <tag-name>
```

Пользователь может удалить тег, используя следующую команду:

```
Admin@nodename# delete libraries tags <tag-name>
```

Примеры работы с тэгами в библиотеке:

```
Admin@nodename# create libraries tags name "Test tag 6" description
"Tag made with CLI" color magenta
Admin@nodename# show libraries tags
```

Test tag 6

```
name          : Test tag 6
description    : Tag made with CLI
color         : magenta
```

Tag 5

```
name          : Tag 5
```

```
description : Test tag #5
color       : green
```

Tag 1

```
name         : Tag 1
description   : Test tag #1
color        : no-color
```

```
Admin@nodename# show libraries tags "Test tag 6"
```

```
name         : Test tag 6
description   : Tag made with CLI
color        : magenta
```

```
Admin@nodename# set libraries tags "Test tag 6" description "Update tag
from cli"
```

```
Admin@nodename# show libraries tags "Test tag 6"
```

```
name         : Test tag 6
description   : Update tag from cli
color        : magenta
```

```
Admin@nodename# delete libraries tags "Test tag 6"
```

НАСТРОЙКА РАЗДЕЛА ЖУРНАЛЫ И ОТЧЕТЫ

Настройка экспорта журналов

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM.

Для создания нового правила экспорта журналов используется команда:

```
Admin@nodename# create logs logs-export <parameters>
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение правила: • on. • off.
name	Название правила.
description	Описание правила.
server-type	Тип сервера: • ssh; • ftp; • syslog. При выборе типа сервера доступны следующие дополнительные настройки: • port — Порт сервера, на который следует отправлять данные. • login — Имя учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • password — Пароль учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • path — Каталог на сервере для копирования файлов журналов (не применяется к методу отправки syslog). • passive — Пассивный режим ftp. • transport — Только для типа серверов syslog. TCP или UDP. • protocol — Только для типа серверов syslog. RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. • severity — Только для типа серверов syslog. Критичность. Возможны следующие значения: alert, critical, error, warning, notice, info.

Параметр	Описание
	• facility — Только для типа серверов syslog. Объект. Возможны следующие значения: user-level, system-daemons, security-auth, log-audit, log-alert, local (0-7). • hostname — Только для типа серверов syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN). • app-name — Только для типа серверов syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
target	IP-адрес или доменное имя сервера.
logs	Журналы для экспорта: • dns — Журнал DNS. • events — Журнал событий. • webaccess — Журнал веб-доступа. • idps — Журнал COB. • mailsecurity — Журнал почтового трафика. • ssh — Журнал инспектирования SSH. • traffic — Журнал трафика. • userid — Журнал UserID. Для каждого журнала можно выбрать синтаксис выгрузки: • cef; • cef-compact; • json; • cee-json; • off.
schedule	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. rontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего).

Параметр	Описание
	- Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Для редактирования ранее созданных правил используется команда:

```
Admin@nodename# set logs logs-export <log-export-rule-name>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил экспорта.

Для просмотра параметров созданных ранее правил экспорта используется команда:

```
Admin@nodename# show logs logs-export
Admin@nodename# show logs logs-export <log-export-rule-name>
```

Для удаления созданных ранее правил экспорта используется команда:

```
Admin@nodename# delete logs logs-export <log-export-rule-name>
```

Для настройки параметров разового экспорта журналов используется команда:

```
Admin@nodename# execute logs send-once <log-export-rule-name>
<parameters>
```

Параметр	Описание
fresh	Экспортировать свежие логи.
range	

Параметр	Описание
	Указать диапазон экспорта: • start-export-range — начало диапазона в формате: 2022-12-31T23:59:59 • end-export-range — конец диапазона в формате: 2022-12-31T23:59:59

Настройка отчетов

Настройка отчетов в интерфейсе командной строки CLI (доступно в версии 7.4.0 и выше) происходит в режиме конфигурации на уровне `reports`. С помощью команд этого раздела можно просматривать имеющиеся на устройстве шаблоны отчетов, создавать и редактировать правила отчетов, просматривать ранее созданные отчеты.

Шаблоны отчетов

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией UserGate.

Для просмотра имеющихся шаблонов отчетов используется команда:

```
Admin@nodename# show reports report-templates
```

Правила отчетов

Правила отчетов задают параметры создаваемого отчета, а также расписание запуска отчетов и способы их доставки пользователям.

Для создания нового правила отчетов используется команда:

```
Admin@nodename# create reports report-rules <parameters>
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение правила: • on; • off.
name	Название правила.
description	Описание правила.
language	Выбор языка создания отчета: • ru; • en.
time-range	Диапазон времени в секундах, за который необходимо подготовить отчет.
format	Выбор формата, в котором будет создан отчет: • pdf; • html.
query-limit	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
query-limit-by	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчётов, которые содержат группирование.
templates	Список шаблонов, которые будут использоваться для построения отчёта. Обязательно необходимо добавить хотя бы один шаблон.
email-sender	Отправитель письма с созданным отчётом.
email-recipients	Список получателей письма с отчётом. Получатели должны быть добавлены в списки библиотеки «Почтовые адреса» (email-list).
email-subject	Тема письма с отчетом.

Параметр	Описание
email-body	Содержимое письма с отчетом.
smtp-profile	Профиль SMTP, который будет использован для отправки отчетов.
schedule	Выбор расписания для отправки отчетов. Crontab-подобный формат, при котором строка выглядит как шесть полей, разделённых пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0 — воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звёздочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, 5-7 будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделённые запятыми. Например, 1,5,10,11 или 1-11,19-23. • Звёздочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, выражение «2-10/2» будет значить: «2,4,6,8,10», а выражение: «*/2» в поле «часы» будет означать каждые два часа.

Для редактирования ранее созданных правил используется команда:

```
Admin@nodename# set reports report-rules <report-rule-name>
<parameters>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил отчетов.

Для просмотра параметров созданных ранее правил отчетов используется команда:

```
Admin@nodename# show reports report-rules
Admin@nodename# show reports report-rules <report-rule-name>
```

Для удаления созданных ранее правил отчетов используется команда:

```
Admin@nodename# delete reports report-rules <report-rule-name>
```

Созданные отчеты

Для просмотра информации о созданных отчетах используется команда:

```
Admin@nodename# show reports generated-reports
Admin@nodename# show reports generated-reports <generated-report-name>
```

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ PMC

Общие сведения

Для программно-аппаратных комплексов (ПАК) UserGate, оснащенных модулем управления PMC (Platform Management Controller), доступен интерфейс командной строки PMC CLI. С помощью команд интерфейса можно просматривать состояние элементов аппаратной платформы, осуществлять мониторинг работы платформы, управлять ее настройками и доступом к ней.

О наличии модуля PMC в устройстве и типах имеющихся портов для подключения — в документации на аппаратные платформы в разделе «[Аппаратные платформы](#)».

О командах интерфейса и правилах их использования — в разделе «[Интерфейс командной строки PMC](#)».

USERGATE APPLICATION AND SECURITY LANGUAGE (UASL)

UserGate Application and Security Language (UASL)

Общие положения

UserGate Application and Security Language (UASL) – язык, разработанный для возможности написания пользовательских сигнатур и приложений.

После создания пользовательские сигнатуры и приложения можно добавлять в профили COB и приложений для дальнейшего использования в правилах межсетевого экранирования.

Структура сигнатуры выглядит следующим образом:

```
UASL (.parameter1=<value1>; .parameter2=<value2>; ...)
```

Параметры сигнатуры записываются в круглых скобках; для разделения параметров используется точка с запятой (;).

Также допускается использование многострочного ввода:

```
UASL (.parameter1=<value1>;  
      .parameter2=<value2>;  
      ...  
      )
```

Примечание

Максимальная длина пользовательской сигнатуры составляет 1024 байта.

Все условия одной сигнатуры без исключений будут объединены логическим оператором **И**.

Создание, редактирование или удаление сигнатур можно отслеживать по записям журнала событий.

Подробнее о семантике, конструкциях и правилах языка UASL читайте в следующих статьях данного раздела.

Метаинформация

Поле **.rev** предназначено для указания дополнительной информации: пользователь, который создал сигнатуру, дата создания, тип и версия сигнатуры. Поле является опциональным и не влияет на работу COB; может быть использовано для отслеживания изменений.

Формат поля следующий:

```
.rev = <date>,<version>,<status>,<author>;
```

где параметры имеют следующий тип данных:

- <date>: целочисленный;
- <version>: целочисленный;
- <status>: строковый;
- <author>: строковый.

Идентификатор

Для задания идентификатора сигнатуры или приложения используется поле **.id**:

```
.id=<id_value>
```

Указание данного поля является опциональным. Идентификатор также может быть задан в свойствах сигнатуры/приложения.

Примечание

Значение, заданное в свойствах сигнатуры на вкладке *Общие*, имеет приоритет над значением, заданным с использованием UASL.

Идентификатор сигнатуры может принимать значения от 1000000 до 1049999 ; идентификатор приложения — от 1050000 до 1099999.

При задании идентификатора вручную его значение не является уникальным и может повторяться.

Если идентификатор не был задан администратором, то UserGate назначит его автоматически; при назначении в автоматическом режиме значения идентификатора не повторяются. При исчерпании пула идентификаторов будет отображена ошибка.

Фильтрация по IP-адресам

Данные параметры позволяют настроить проверку заданных IP-адресов:

```
.src_addr[!]=<IP_address/subnet>;  
.dst_addr[!]=<IP_address/subnet>;
```

Допустимы следующие форматы указания IP-адресов:

- A.B.C.D;
- A.B.C.D/E;
- A.B.C.D:E.

При задании IP-адреса указание маски подсети необязательно; чтобы задать несколько IP-адресов используйте квадратные скобки, например:

```
.src_addr=[<IP_address1>, <IP_address2>];
```

Примеры:

```
.src_addr!=10.10.10.1;  
.src_addr=10.10.10.0/24;  
.src_addr=[10.10.10.0/24, 10.10.20.0/24, 10.10.30.0/24];
```

Фильтрация по портам

Для задания проверки TCP/UDP-портов используйте параметры:

- **.src_port** — для проверки портов источника:
- **.dst_port** — для проверки портов назначения:

Доступно использование следующих выражений:

Наименование	Описание
.src_port=<port_number>; .dst_port=<port_number>;	Указание конкретного порта источника и/или назначения.
.src_port!=<port_number>; .dst_port!=<port_number>;	Проверка всех портов кроме указанного.
.src_port=<port_number>; .dst_port=<port_number>;	Проверка всех портов, номер которых меньше или равен номеру указанного порта.
.src_port!=<port_number>; .dst_port!=<port_number>;	Проверка всех портов, номер которых больше указанного.
.src_port=<port_number>; .dst_port=<port_number>;	Проверка всех портов, номер которых больше или равен номеру указанного порта.
.src_port!=<port_number>; .dst_port!=<port_number>;	Проверка всех портов, номер которых меньше указанного.
.src_port=<port_number1>:<port_number2>; .dst_port=<port_number1>:<port_number2>;	Проверка портов, находящихся в указанном диапазоне (port_number1 и port_number2 включительно).
.src_port!=<port_number1>:<port_number2>; .dst_port!=<port_number1>:<port_number2>;	Проверка всех портов, не входящих в указанный диапазон (т.е. проверяются порты с номерами менее port_number1 и более port_number2).

Примеры:

```
.src_port=1000;; # '>= 1000'
.dst_port=5060;
.dst_port=1000;;
.dst_port=2000:8000; # '>= 2000 and <= 8000'
.dst_port!=2000:8000; # '< 2000 and > 8000'
```

Сканирование пакетов без полезной нагрузки

Поле **.nopayload** предназначено для возможности сканирования пакетов, в которых отсутствует полезная нагрузка.

Примечание

Поле неприменимо для сигнатур с поиском шаблонов и проверкой метки.

Например, данное поле может быть использовано для обнаружения сканирования портов пакетами без полезной нагрузки. Далее представлена сигнатура для обнаружения SYN-сканирования:

```
UASL(.protocol=tcp; .tcp.flags=S; .rate=1000,2; .track=src_ip; .nopayload;)
```

Примечание

Указание поля **.nopayload** не исключает сканирования пакетов с нагрузкой.

Поиск шаблонов

Следующий параметр позволяет задать шаблон, на наличие которого система обнаружения и предотвращения вторжений будет проверять содержимое пакетов (packet payload):

```
.pattern[!]="string";
```

i Примечание

Следует помнить, что при поиске учитывается регистр символов.

Данные, представленные в шестнадцатеричной системе счисления (HEX), должны быть указаны с использованием символа вертикальной черты (|), например, |05 00 27|.

Для указания специальных символов используйте соответствия, представленные в таблице:

Символ	Запись в шестнадцатеричном формате
"	22 .
;	3B или 3b .
\	5C или 5c .
	7C или 7c .
:	3A или 3a .

Помимо оператора =, может быть использован и оператор !=. Тогда будет производится поиск пакетов, не содержащих заданный шаблон.

Общий формат задания параметра:

```
.pattern[!]="string"; [.where=<MODE>;] [.no_case;;] [.distance=<RANGE>[,<MODE>;] [.within=<RANGE>[,<MODE>;] [.service=<MODE>;]
```

Модификаторы области поиска (**.where**, **.no_case**, **.distance**, **.within**, **.service**) будут рассмотрены далее.

При написании сигнатуры доступно использование нескольких параметров **.pattern** с целью снижения уровня ложных срабатываний.

i **Примечание**

Использование параметра `.host` в кастомизированной пользовательской сигнатуре делает эту сигнатуру диссекторной. В этом случае параметр поиска шаблонов `.pattern` обязательно нужно использовать вместе с параметром области поиска `.where`.

Модификаторы области поиска

.no_case

Модификатор `no_case` позволяет осуществлять поиск, заданный параметром `.pattern`, без учета регистра символов.

Пример:

```
UASL(.id=XXX; .name="XXX"; .pattern="Host: "; .pattern="google.com";)
```

.where

Модификатор `.where` используется для указания области поиска сигнатуры:

```
.where=<MODE>;
```

где `<MODE>` может принимать следующие значения:

Наименование	Описание
packet_origin	Областью поиска является весь пакет без протокольного декодера.
uri	Область поиска — поле URI заголовка HTTP.
host	Областью поиска для HTTP-сессии является поле Host (до переноса строки).
header	Областью поиска для HTTP-сессии являются http заголовки, smtp и pop3 команды, заголовки протоколов tls и ssh.

Наименование	Описание
body	Областью поиска является содержимое пакетов HTTP.
file	Областью поиска являются: декодированное http содержимое, вложения в eml, ftp-data сессии.

Примечание

При создании сигнатуры с модификатором `.where` поле диссектора автоматически считается, как поле с модификатором `.service=any`, то есть применяются все диссекторы, подходящие под значение модификатора `.where`.

.service

Данный модификатор области поиска предназначен для выбора диссектора:

```
.service=<MODE>;
```

где <MODE> может принимать следующие значения:

Наименование	Описание
http	Диссектор HTTP
dns	Диссектор DNS

Пример:

```
UASL(.name="block.google"; .protocol=tcp; .service=http; .host="google.com"; )
```

.distance, .within, .at, .startin

Данные модификаторы позволяют:

Наименование	Описание
.distance	Пропустить заданное количество байтов (RANGE) от начала или последнего найденного блока. Задаётся в формате:

Наименование	Описание
	<pre>.distance=<RANGE> [,<MODE>];</pre> где <RANGE> — это целое число, начиная с 0. Опциональные параметры (<MODE>) будут рассмотрены далее. Например, следующая запись задаёт пропуск 10 байтов с начала для первого шаблона или от последнего найденного для второго и последующего шаблонов: <pre>.distance=10;</pre> Пример использования опциональных параметров: • пропустить 10 байтов от начала: <pre>.distance=10, start;</pre> • пропустить 10 байтов от последнего найденного шаблона: <pre>.distance=10, match;</pre>
.within	Сканировать в заданном интервале (RANGE) от начала или последнего найденного блока (шаблон полностью попадает в заданный интервал). Задаётся в формате: <pre>.within=<RANGE> [,<MODE>];</pre> где <RANGE> — это целое число, начиная с 1. Опциональные параметры (<MODE>) будут рассмотрены далее. Например, следующая запись задаёт поиск с 1-го по 10-й байт с начала для первого шаблон или от последнего найденного для второго и последующего шаблона: <pre>.within=10;</pre> Пример использования опциональных параметров: • поиск с 1-го (с начала) по 10-й байт: <pre>.within=10, start;</pre>

Наименование	Описание
	поиск в диапазоне 10 байтов после последнего найденного шаблона: <pre>.within=10, match;</pre>
.startin	Сканировать в заданном интервале (RANGE) от начала или последнего найденного блока (для совпадения в заданный интервал может попадать только начало шаблона). Задаётся в формате: <pre>.startin=<RANGE> [,<MODE>];</pre> где <RANGE> — это целое число, начиная с 1. Опциональные параметры (<MODE>) будут рассмотрены далее.
.at	Проверять наличие шаблона в заданной позиции. Важно! Данный модификатор не совместим с модификаторами .distance и .within. Задаётся в формате: <pre>.at=<RANGE> [,<MODE>];</pre> где <RANGE> — это целое число, начиная с 0. Опциональные параметры (<MODE>) будут рассмотрены далее.

В следующей таблице представлены опциональные параметры:

Наименование	Описание
start	Поиск с начала потока данных. Важно! Является значением по умолчанию для первого шаблона.
packet	Сканирование с начала пакета.
reverse	Поиск с конца пакета (удобно для проверки Next Protocol в ESP).
match	Поиск от последнего найденного шаблона. Важно! Является значением по умолчанию для второго и последующего шаблона.

Наименование	Описание
lastmark	Сканирование от последней метки, выставленной с помощью .mark pset .



Примечание

Если опциональный параметр для модификаторов **.distance** и **.within** совпадают, то отсчёт значения модификатора **.within** производится от значения **.distance**.

Например, запись:

```
.distance=10,match; .within=5,match
```

задаёт поиск в диапазоне с 10-го по 15-й байт от последнего найденного шаблона.

Примеры:

```
UASL(.name="sock5.proxy.detect"; .protocol=tcp; .flow=from_client; .seq=1,relative; .pattern="|05 01 00|"; .within=1;)
UASL(.name="block.google"; .protocol=tcp; .service=http;.pattern="google.com"; .within=512;)
```

.protocol

Данный модификатор позволяет указать протокол транспортного уровня, к которому будет применена сигнатура:

```
.protocol=<MODE>;
```

где <MODE> может принимать следующие значения:

- **icmp**: анализ трафика протокола ICMP.
- **udp**: анализ трафика протокола UDP.
- **tcp**: анализ трафика протокола TCP.

i Примечание

Можно задать только один протокол. Если протокол не указан, то сигнатура применяется только к трафику TCP и UDP.

Пример:

```
UASL(.name="block.google"; .protocol=tcp; .pattern="google.com";)
```

Частота срабатывания

При задании частоты срабатывание сигнатуры COV будет происходить не при каждом совпадении, а только после обнаружения заданного количества совпадений за указанный промежуток времени. Данный параметр может быть полезен при написании сигнатур для детектирования, например, атак типа брутфорс.

Для указания частоты срабатывания:

```
.rate=<count>, <period>;
```

где <count> — количество срабатываний;

<period> — интервал времени (в секундах), за который должно произойти заданное количество срабатываний.

Следующий параметр является необязательным и задаёт параметр, по которому совпадения будут сгруппированы:

```
.track=<MODE>;
```

где <MODE> — свойство, по которому происходит отслеживание пакетов.

<MODE> может принимать следующие значения:

- **src_ip** — отслеживание по IP-адресу источника;
- **dst_ip** — отслеживание по IP-адресу назначения.

Если **.track** не указан, то счётчик учитывает все совпадения, и при достижении заданного лимита происходит срабатывание сигнатуры.

Например:

```
UASL(.name="pop3.brute.force"; .protocol=tcp; .pattern="USER"; .flow=from_server; .rate=3,60; .track=src_ip;)
```

Срабатывание сигнатуры произойдёт после обнаружения шаблона USER (.pattern="USER";) в пакетах, отправленных с одного IP-адреса (.track=src_ip;), более 3-х раз за 60 секунд (.rate=3, 60;).

Направление анализа

Данный параметр является опциональным и позволяет применять сигнатуру к определённым потокам трафика. В результате можно создавать сигнатуры, которые будут анализировать трафик от клиента, от сервера или в обоих направлениях.

```
.flow=<MODE>;
```

где <MODE> может принимать следующие значения:

Наименование	Описание
from_client	Анализ трафика от клиента.
from_server	Анализ трафика от сервера.
bi_directional	Анализ трафика в обоих направлениях.

Поиск бинарных данных

Параметр **.byte_test** позволяет сравнить байт с заданным значением и применим к данным, представленным в двоичном или символьном форматах.

Общий формат записи:

```
.byte_test = <bytes>,<operator>,<value>,<offset>,[,<multiplier>]
[,<modifiers>];
```

Доступные параметры отображены в таблице:

Наименование	Описание
<bytes>	Количество байтов в текущей позиции с заданным смещением, считываемых из пакета. Может принимать значения 1, 2 или 4.
<size>	Длина строки; указывается для строковых данных.
*	Использование всех символов до первого нечислового символа.
<operator>	Оператор, использующийся для сравнения байта с заданным значением: • < — меньше; • > — больше; • = — равно; • != — не равно; • & — результат выполнения операции логического И для <bytes> и <MASK> (число, задающее интересующие биты) не равен 0; • ~ — результат выполнения операции логического И для <bytes> и <MASK> равен 0; • ^ — результат выполнения операции XOR для <bytes> и <MASK> не равен 0. Например: <pre>.byte_test=1,&,0x80,0;</pre> проверяет, что старший разряд первого байта поля данных пакета установлен в 1.
<value>	Значение, с которым выполняется сравнение, или размер пакета. Значение может быть задано с использованием префикса 0x; доступно использование арифметических операторов (+, -, *, /).
<offset>	Смещение в поле данных пакета: • relative: от последней точки совпадения.

Наименование	Описание
	Если параметр смещения не указан, то анализ, по умолчанию, производится с начала пакета.
<post_offset>	Число байтов, на которое необходимо сместить точку начала сканирования. Важно! Применим для .byte_jump .
<multiplier>	Числовое значение, на которое необходимо умножить извлечённое число перед сравнением или переносом точки начала сканирования; параметр является опциональным.
<modifiers>	Модификаторы (опционально): • big — обработка данных со старшего разряда; • little — обработка данных с младшего разряда; • string — данные в пакете являются строковыми; • hex — преобразование строки данных в шестнадцатеричное число; • dec — преобразование строки данных в десятичное число; • oct — преобразование строки данных в восьмеричное число; • align — округление числа конвертируемых байтов до следующей 32-битной границы; используется только для .byte_jump (например, 0 → 0; 1,2,3,4 → 4; 5,6 → 8 и т.д.).

Пример сравнения первых 4 байтов каждого из пакетов со значением 1234; данные в пакете представлены в символьном формате в десятичной системе счисления:

```
.byte_test=4,=,1234,0,string,dec;
```

Параметр **.byte_jump** переносит точку начала сканирования на указанное число байтов. Общий формат записи при обработке данных со старшего или младшего разряда (т.е. для модификаторов **big** и **little**):

```
.byte_jump = <bytes>,<offset>,<post_offset>[,<multiplier>]
[,<modifiers>];
```

Для строковых данных (модификатор **string**):

```
.byte_jump = (<size> | *),<offset>,<post_offset>[,<multiplier>]
[,<modifiers>];
```

Работа с метками

Для каждого потока данных может быть указана именованная метка. Для ее указания используется:

```
.mark <parameter>=<value>;
```

где <value> – название метки (указывается с использованием кавычек "");

<parameter> может принимать значения, представленные в таблице ниже.

Сопоставление шаблонов основано, в большинстве случаев, на работе с пакетами данных. Метки используются в случаях, если шаблон атак присутствует в нескольких пакетах. Сигнатура, сработавшая для предыдущего пакета, может поставить метку; наличие меток проверяется при отправке пакетов в рамках одной сессии.

Наименование	Описание
set	Установить именованную метку для текущего потока данных.
pset	Установить и запомнить последнюю выставленную метку для возможности её использования с модификаторами области поиска .distance и .within .
clear	Удалить именованную метку.
toggle	Изменить статус метки.
test	Проверить, существует ли метка.
reset	Сбросить все метки.

Протокольные анализаторы

В данном разделе будут рассмотрены поля протоколов ICMP, TCP, UDP, HTTP.

Т.к. для одной сигнатуры можно задать только один протокол, то использование ниже представленных параметров автоматически определяет его, т.е. равносильно использованию параметра **.protocol**.

Примечание

Указание параметров разных протоколов приведёт к ошибке.

ICMP

Для проверки свойств заголовка ICMP доступно использование следующих параметров:

Наименование	Описание
.icmp.type	Проверка типа ICMP. Доступно использование следующих операторов: =, !=.
.icmp.code	Проверка значения кода ICMP. Доступно использование следующих операторов: =, !=.
.icmp.id	Проверка значений идентификаторов ICMP. Доступно использование следующих операторов: =, !=.
.icmp.checksum	Проверка контрольной суммы, которая используется при обнаружении ошибок. Доступно использование следующих операторов: <, >, <=, >=, =, !=.
.icmp.data_size	Проверка размера поля данных пакета. Параметр используется для обнаружения пакетов аномальных размеров, зачастую использующихся для переполнения буфера. Доступно использование следующих операторов: <, >, <=, >=, =, !=. Если заданы несколько условий, то они объединяются логическим оператором И .

Примеры:

```
UASL(.name="Ping Death"; .protocol=icmp; .data_size>32000)
UASL(.name="Ping Death"; .icmp.data_size>32000)
```

TCP

Для проверки свойств заголовка TCP доступно использование следующих параметров:

Наименование	Описание
.tcp.sport	Проверка номера порта или диапазона портов источника. Доступно использование следующих операторов: =, !=.
.tcp.dport	Проверка номера порта или диапазона портов назначения. Доступно использование следующих операторов: =, !=.
.tcp.window_size	Проверка размера окна TCP. Поддерживаются следующие операторы: <, >, <=, >=, =, !=.
.tcp.checksum	Проверка контрольной суммы, используемой для проверки на наличие ошибок при передаче и/или приеме отправленного пакета. Доступно использование следующих операторов: <, >, <=, >=, =, !=.
.tcp.seq	Проверка значения порядковых номеров TCP. Поддерживаются следующие операторы: <, >, <=, >=, =, !=. Доступно использование модификатора relative — проверка относительно начального номера последовательности. Применение: <pre>.tcp.seq=<value>, relative;</pre> где <value> - порядковый номер TCP.
.tcp.flags	Проверка TCP-флагов: <pre>.tcp.flags=[<mod>]<tcp_flags>;</pre> где <mod> — модификатор. <tcp_flags> — флаг TCP, который может быть указан как в буквенном, так и в числовом (десятичной или шестнадцатеричной системах) форматах.

Наименование	Описание
	Флаги: • 0 — флаги не установлены; • F, 1, 0X001 — FIN; • S, 2, 0X002 — SYN; • R, 4, 0X004 — RST; • P, 8, 0X008 — PSH; • A, 16, 0X010 — ACK; • U, 32, 0X020 — URG; • E, 64, 0X040 — ECE; • C, 128, 0X080 — CWR; • N, 256, 0X100 — NS. Модификаторы: • * — должен быть установлен хотя бы один из заданных флагов, остальные не проверяются; • + — должны быть установлены все заданные флаги, остальные не проверяются; • ! — все заданные флаги должны быть сброшены, остальные не проверяются; • !0 — должен быть установлен хотя бы один флаг (любой). Важно! Если ни один из модификаторов не указан, то должны быть установлены все заданные флаги (строгое соответствие), остальные - сброшены.
.tcp.data_size	Размер полезной нагрузки пакета TCP (без учета заголовков). Поддерживаются следующие операторы: <, >, <=, >=, =, !=. Возможно указание как .data_size, тогда параметр будет относиться к протоколам TCP и UDP.

UDP

Для проверки свойств заголовка UDP доступно использование следующих параметров:

Наименование	Описание
.udp.port	Проверка номера порта или диапазона портов источника. Доступно использование следующих операторов: =, !=.

Наименование	Описание
<code>.udp.dport</code>	Проверка номера порта или диапазона портов назначения. Доступно использование следующих операторов: <code>=</code> , <code>!=</code> .
<code>.udp.checksum</code>	Проверка контрольной суммы. Доступно использование следующих операторов: <code><</code> , <code>></code> , <code><=</code> , <code>>=</code> , <code>=</code> , <code>!=</code> .
<code>.udp.data_size</code>	Размер полезной нагрузки пакета UDP (без учета заголовков). Поддерживаются следующие операторы: <code><</code> , <code>></code> , <code><=</code> , <code>>=</code> , <code>=</code> , <code>!=</code> . Возможно указание как <code>.data_size</code> , тогда параметр будет относиться к протоколам TCP и UDP.

HTTP

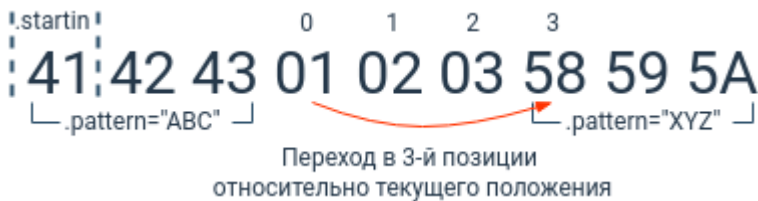
Для проверки свойств заголовка HTTP доступно использование следующих параметров:

Наименование	Описание
<code>.uri</code>	Проверка поля идентификатора ресурса (URI).
<code>.header</code>	Проверка произвольных заголовков HTTP.
<code>.body</code>	Проверка тела содержимого запроса или ответа HTTP.
<code>.host</code>	Проверка доменного имени узла.

Примеры

В данном разделе приведены примеры, написанные с использования UASL.

Пример 1



```
UASL(
  .id = 1;
  .pattern = "ABC"; .startin = 1;
  .pattern = "XYZ"; .at = 3, match;
)
```

В данном примере выполняется последовательный поиск 2-х шаблонов:

- поиск начала шаблона ABC в заданном диапазоне, т.е. первый байт заданного шаблона обязательно должен находиться в диапазоне. Значение модификатора `.startin` равно 1 (диапазон = 1, поиск шаблона с начала сессии, т.к. первый модификатор по умолчанию — `start`) — байт, входящий в этот диапазон должен быть равен началу шаблона ABC;
- поиск шаблона XYZ начиная с позиции 4 (**`.at=3;`**) от последнего найденного шаблона ABC.

Пример 2

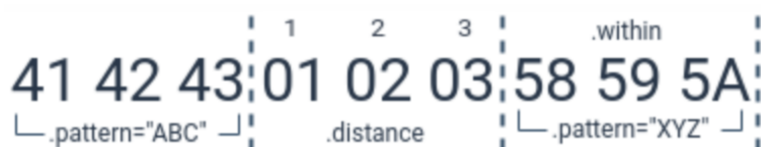
0		1	2	3	<code>.startin</code>
41	42	43	01	02	03
<code>.pattern="ABC"</code>			<code>.distance</code>	<code>.pattern="XYZ"</code>	

```
UASL(
  .id = 2;
  .pattern = "ABC"; .at = 0;
  .pattern = "XYZ"; .distance = 3, match; .startin = 1, match;
)
```

Выполняется последовательный поиск 2-х шаблонов:

- поиск начала шаблона ABC с начала пакета (**`.at=0;`**);
- пропустив 3 байта от последнего найденного шаблона ABC (**`.distance=3,match;`**) производится поиск начала шаблона XYZ; для срабатывания начало шаблона XYZ должно быть равно первому байту, с которого начинается поиск, т.к. **`.startin=1,match;`**.

Пример 3



```
UASL (
    .id = 3;
    .pattern = "ABC";
    .pattern = "XYZ"; .distance = 3, match; .within = 3, match;
)
```

Производится последовательный поиск 2-х шаблонов:

- поиск шаблона ABC;
- через 3 байта от последнего найденного шаблона ABC (**.distance=3,match;**) производится поиск шаблона XYZ: шаблон XYZ должен полностью попадать в последующие 3 байта, т.к. **.within=3**.

USERGATE POLICY LANGUAGE (UPL)

UserGate Policy Language (Описание)

UPL (UserGate Policy Language) — язык описания политик UserGate. Термин "политика" употребляется здесь в контексте конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента.

Правила настраиваются с использованием действий, условий и свойств.

Для каждого правила настраивается одно из действий. **Действия** — настройки, которые управляют обработкой транзакции (OK, WARNING, PASS, DENY, FORCE_PASS, FORCE_DENY). При настройке правил, в которых не предусмотрено указание действия (например, правила DNS, NAT и маршрутизации, пропускной способности и т.п.), необходимо указать действия PASS или OK.

Условия задаются знаками равно (=) или не равно (!=), например, зоны, адреса, GeoIP источников и назначения, сервисы, приложения и т.д.; все условия в

правиле проверяются по логическому И, т.е. правило сработает, если будут выполнены все условия.

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

Примечание

При настройке правил сначала указывается действие, потом условия и затем свойства.

С помощью UPL в интерфейсе CLI создаются правила политик сети и безопасности для следующих разделов:

- Настройки DNS-прокси (уровень: **network dns dns-proxy dns-rules**).
- Captive-портал (уровень: **users captive-portal**).
- Межсетевой экрана (уровень: **network-policy firewall**).
- NAT и маршрутизация (уровень: **network-policy nat-routing**).
- Пропускная способность (уровень: **network-policy traffic-shaping**).
- Фильтрация контента (уровень: **security-policy content-filtering**).
- Веб-безопасность (уровень: **security-policy safe-browsing**).
- Инспектирование туннелей (уровень: **security-policy tunnel-inspection**).
- Инспектирование SSL (уровень: **security-policy ssl-inspection**).
- Инспектирование SSH (уровень: **security-policy ssh-inspection**).
- Защита почтового трафика (уровень: **security-policy mail-security**).
- ICAP-правила (уровень: **security-policy icap-rules**).
- Правила защиты DoS (уровень: **security-policy dos-rules**).
- Веб-портал (уровень: **global-portal web-portal**).
- Правила reverse-прокси (уровень: **global-portal reverse-proxy-rules**).
- Серверные правила VPN (уровень: **vpn server-rules**).

Клиентские правила VPN (уровень: **vpn client-rules**).

Структура команды для создания правила:

```
Admin@nodename# create <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо создать правило.

<position> — позиция, на которую будет помещено правило.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для обновления существующего правила:

```
Admin@nodename# set <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо обновить правило.

<position> — номер правила, которое необходимо обновить.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для удаления правила:

```
Admin@nodename# delete <level> <position | all>
```

где <level> — уровень, на котором необходимо удалить правило.

<position> — номер правила, которое необходимо удалить.

<all> — удалить все правила.

Структура команды для отображения правила:

```
Admin@nodename# show <level> <position | all>
```

где <level> — раздел, правила которого нужно отобразить.

<position> — номер правила, которое необходимо отобразить.

<all> — отобразить все правила.

Пример создания правила межсетевого экрана с использованием UPL (использован многострочный ввод):

```
Admin@nodename# create network-policy firewall 1 upl-rule \
...DENY \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = known \
...service = HTTPS \
...time = lib.time("Working hours") \
...rule_log(session)\
...name("Example of firewall rule created in CLI") \
...enabled(true)
```

После создания правило отобразится в начале списка правил межсетевого экрана (на позиции 1). Данное правило запрещает HTTPS-трафик из зоны Trusted в зону Untrusted пользователям, идентифицированным системой. Правило работает в соответствии с расписанием "Working hours". При срабатывании правила в журнал будет записана информация о начале сессии.

В последующих статьях данного раздела можно найти более подробную информацию об [общих положениях](#) языка UPL, [определениях](#), [встроенных библиотеках](#), [условиях](#), [действиях](#), [свойствах](#) и [типах правил](#).

Общие положения

Комментарии

Любая строка, начинающаяся с символа "%", является комментарием. Символ процента "%" после пробела или табуляции вводит комментарий, который продолжается до конца строки (кроме случаев, когда символ процента отображается внутри кавычек (""), как часть выражения).

Пример:

```
% Это комментарий
DENY("Too many Host headers") request.header.Host.count = 2.. % и это
тоже
```

Комментарии могут быть в любом месте файла с описанием политик.

Правила

Правило политики (rule) состоит из условий и некоторого количества действий, записанных в любом порядке. Есть также свойства (properties), которые синтаксически выглядят как действие, но при этом активных действий не производят. Например, свойство *name* просто добавляет атрибут "имя" в правило.

Правила обычно пишутся в одной строке, но могут быть разбиты на строки с помощью специального символа — обратного слеша "\".

Когда правило выполняется, условие проверяется для текущей конкретной транзакции. Если условие оценивается как *True* (истина), выполняются все перечисленные действия и текущий слой заканчивается при наличии префиксов *PASS / FORCE_PASS / DENY / FORCE_DENY / WARNING / OK*. Если сработавшее правило не имеет префиксов *PASS / FORCE_PASS / DENY / FORCE_DENY / WARNING / OK*, то выполняются действия и дальше обрабатывается уже следующее правило. Если условие оценивается как *False* для этой транзакции, то дальше обрабатывается уже следующее правило.

Все условия в правиле проверяются по логическому "И". Другими словами, правило работает, когда будут выполнены все условия.

В свою очередь, условие является логической комбинацией триггеров. Триггеры — это отдельные тесты, которые можно выполнить с компонентами запроса, ответа, связанными пользователями или состоянием системы.

Действия — это настройки, которые управляют обработкой транзакции. Например, запретить (*deny*) или обработать объект (изменить заголовок — *rewrite*).

Синтаксис:

```
Rule ::= (PASS | FORCE_PASS | DENY | ( DENY (' string ') ) | FORCE_DENY |
FORCE_DENY(' string ') | WARNING | OK)? Conditions '\'? Actions
```

```
Conditions ::= condition '\'? Conditions
```


Actions ::= action '?' Actions

Пример:

Запрос будет запрещен, когда сработают оба триггера:

- домен будет example.com
- время будет между 9 и 17 часами

```
DENY url.domain = "example.com" time=09:00..17:00
```

Слой

Слой (layer)— это конструкция UPL, используемая для группировки правил и принятия одного решения. Раздельные принятия решения помогают контролировать сложность политики. Это делается путем написания каждого решения в отдельном слое.

У любого правила в слое может быть префикс *PASS / FORCE_PASS / DENY / FORCE_DENY / OK / WARNING*, когда срабатывает правило с таким префиксом, все остальные правила в слое пропускаются.

В случае если сработало правило с префиксом *FORCE_PASS* или *FORCE_DENY*, то это является окончательным результатом обработки, в противном случае обработка переходит на следующий слой. После обработки всех слоев запрос будет заблокирован или пропущен в зависимости от того, что было последним — *PASS / FORCE_PASS* или *DENY / FORCE_DENY*. Если процессинг остановится на *WARNING*, будет добавлено предупреждение в тело ответа.

Префикс *OK* подразумевает остановку обработки правил в текущем слое при выполнении условий и действий (если таковые указаны). Если префикс отсутствует при выполнении условий и действий, то остановка не подразумевается.

Действия *FORCE_PASS* и *FORCE_DENY* похожи на *PASS* и *DENY*, за исключением того, что они могут быть переопределены на последующих слоях. *FORCE_DENY* и *FORCE_PASS* немедленно прекращают проверку правил как на текущем, так и на последующих слоях, и этот результат является окончательным.

Синтаксис:

Layer ::= '[' layer_type layer_name ']'

```
layer_type ::= ssl | ssh | captive | content | shaper | firewall | safebrowsing | dns | icap |
mailsecurity | dos | webportal | reverseproxy | nat_routing | byod | vpn_server |
vpn_client | idps | tunnel | scenarios | ipvs_server | icap_balancing |
reverseproxy_balancing
```

```
layer_name ::= string
```

```
atom ::= [a-z][0-9a-zA-Z_]+
```

```
string ::= "" произвольная строка ""
```

Пример 1:

```
[content "L1"]
DENY enabled(true) % по умолчанию все запрещено

[content "Devs"]
DENY group != Developers enabled(true)
%... дальше идут правила, которые будут применяться только для группы
Developers
```

Пример 2:

```
[content "Admin"]
FORCE_PASS group = Admins enabled(true)

[content "L2"]
DENY enabled(true) % по умолчанию все запрещено
```

Динамические значения

Значения "адрес запроса" (*url*, *url.host*, *url.path*), "IP-адрес источника/назначения" (*src.ip*, *dst.ip*), "имя пользователя" (*user*), "значения заголовков" (*request* и *response*) и "параметры запроса" (*qparam*) могут сравниваться между собой, а также использоваться в качестве аргумента в действиях (actions), где это предусмотрено.

Условия

Условие (condition) в языке UPL является логической комбинацией триггеров. Триггеры — это отдельные тесты, которые можно выполнить с компонентами запроса, ответа, связанными пользователями или состоянием системы. Все триггеры условия сравниваются со значениями с помощью операторов "=" и "!=". В роли значения могут выступать константные значения, такие как строки, целочисленные значения, диапазоны значений, динамические значения.

Синтаксис:

condition ::= condition_name ('=' | '!=') condition_value

condition_value ::= pattern | list

list ::= '(' ((pattern ';') pattern)? ')'*

pattern ::= word | string | integer | float | boolean | range | condition_name

string ::= ''' произвольная строка '''

*word ::= [a-zA-Z][0-9a-zA-Z_]**

boolean ::= yes | no | true | false

range ::= integer .. [integer] | [integer] .. integer | float .. [float] | [float] .. float

numeric ::= integer | range

http.connect

Проверка наличия *HTTP CONNECT*.

Синтаксис:

http.connect = yes | no | true | false

http.method

Проверка используемого HTTP-метода. Метод можно указывать как в кавычках, так и без.

Синтаксис:

http.method = GET | CONNECT | DELETE | HEAD | POST | PUT | TRACE | OPTIONS | TUNNEL | LINK | UNLINK | PATCH | PROPFIND | PROPPATCH | MKCOL | COPY | MOVE | LOCK | UNLOCK | MKDIR | INDEX | RMDIR | COPY | MOVE

http.request.version

Проверка версии HTTP-запроса.

Синтаксис:

http.request.version = 0.9 | 1.0 | 1.1

http.response.version

Проверка версии HTTP-ответа.

Синтаксис:

http.response.version = 0.9 | 1.0 | 1.1

http.response.code

Проверка HTTP-кода ответа. Валидные значения: 100 - 999.

Синтаксис:

http.response.code = NNN %(где NNN число от 100 до 999)

http.request.body, http.request.body.nocase, http.response.body и http.response.body.nocase

Проверка тела запроса/ответа HTTP на содержание определенной сигнатуры.

Пример:

```
DENY http.response.body.nocase = "<title>index of" http.response.body = ">"
```

category

Проверка домена на принадлежность к определенной категории сайтов (список определенных в системе категорий смотрите в статье [Категории URL](#)).

Категорию можно указать как по имени, так и по ее идентификатору. Если имя категории содержит пробелы или спецсимволы, ее необходимо указывать в кавычках.

Синтаксис:

category = *word* | *string* | *integer* | *list* | *lib*

lib ::= *lib.category* '(' *list_libs* ')'

list_libs ::= *lib_name* ';' *list_libs*

lib_name ::= *word* | *string*

Пример:

Запретить категории *Job Search* и *Gambling*:

```
DENY category = ("Job Search", Gambling)
```

Запретить все категории из библиотеки *Restricted cats*:

```
DENY category = lib.category("Restricted cats")
```

morphology

Проверка тела ответа морфологическими словарями.

Синтаксис:

morphology = *word* | *string* | *list* | *lib*

lib ::= *lib.morphology* '(' *list_libs* ')'

list_libs ::= *lib_name* ';' *list_libs*

lib_name ::= *word* | *string*

Пример:

Запретить контент, если сработает категория морфологии из словаря *BadWords*:

```
DENY morphology = BadWords
```

Запретить морфологические категории из библиотек **Special Words**, **BadWords**

```
DENY morphology = ("Special Words", BadWords)
DENY morphology = lib.morphology("Special Words", BadWords) %
аналогично предыдущему правилу
```

request.header.<h_name> и response.header.<h_name>

Проверка HTTP-заголовка запроса/ответа. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

```
request.header.<h_name>[.base64][.nocase] = string
```

Пример:

```
DENY url="http://usergate.com" request.header.Pragma="no-cache"

PASS request.header.User-Agent = lib.useragent("Browsers")
PASS request.header.Content-Type = lib.mime("Applications")
DENY request.header.Connection.substring = "Upgrade"
```

request.header.<h_name>.substring и response.header.<h_name>.substring

Проверка HTTP-заголовка запроса/ответа на вхождение подстроки. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

```
request.header.<h_name>[.base64]substring[.nocase] = string
```

Пример:

```
DENY request.header.User-Agent.substring = "curl/"
```

request.header.<h_name>.regex и response.header.<h_name>.regex

Проверка HTTP-заголовка запроса/ответа на регулярное выражение PCRE. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

```
request.header.<h_name>[.base64].regex = string
```

Пример:

```
DENY("Accept only digits in content length") request.header.Content-  
Length.regex != "[0-9]*"
```

request.header.<h_name>.re2 и response.header.<h_name>.re2

Проверка HTTP-заголовка запроса/ответа на регулярное выражение RE2. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

```
request.header.<h_name>[.base64].re2 = string
```

Пример:

```
DENY("Accept only digits in content length") request.header.Content-  
Length.re3 != "[0-9]*"
```

request.header.<h_name>.count и response.header.<h_name>.count

Проверка количества заголовков <h_name> в HTTP-запросе/ответе. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

request.header.<h_name>.count = integer | range

Пример:

```
DENY("Too many Host headers") request.header.Host.count = 2..
```

request.header.<h_name>.length и response.header.<h_name>.length

Проверка длины значений всех заголовков <h_name> в HTTP-запросе/ответе. *h_name* может принимать одно из поддерживаемых значений (смотрите статью [Список поддерживаемых HTTP-заголовков](#)).

Синтаксис:

request.header.<h_name>.length = integer | range

Пример:

```
DENY("Too much Cookie data") request.header.Cookie.length = 2048..
```

request.header_names, request.header_values, response.header_values и response.header_values

Проверка имени/значения всех HTTP-заголовков запроса/ответа на значение.

Синтаксис:

request.header_values[.base64].regex = string

request.header_values[.base64].re2 = string

request.header_values[.base64].substring[.nocase] = string

request.header_values.count = integer | range

request.header_values.length = integer | range

request.x_header.<xh_name> и response.x_header.<xh_name>

Проверка HTTP-заголовок запроса/ответа на значение. *xh_name* — произвольный HTTP-заголовок.

Синтаксис:

request.x_header.<xh_name>[.base64][.nocase] = string

request.x_header.<xh_name>[.base64].regex = string

request.x_header.<xh_name>[.base64].re2 = string

request.x_header.<xh_name>[.base64].substring[.nocase] = string

request.x_header.<xh_name>.count = integer | range

request.x_header.<xh_name>.length = integer | range

Пример:

```
DENY url="http://usergate.com" request.x_header.Test="test1"
```

Возможны также суффиксы **length**, **count**, **regex**, **re2** как и в случае с *<h_name>*.

```
DENY("Too much X-Test data") request.x_header.X-Test.length = 2048..
DENY("Too much X-Test2 headers data") request.x_header.X-Test2.count =
2..
PASS request.x_header.Test.regex = "[0-9]*"
```

request.header.Cookie.<cookie_name>

Проверка заголовок запроса Cookie на значение.

Синтаксис:

```
request.header.Cookie.<cookie_name>[.base64][.(nocase / substring /  
substring.nocase / regex / re2)] = string
```

Пример:

```
DENY http.method = POST request.header.Cookie.csrf_token !=  
qparam.CSRF_TOKEN enabled(true) name("Check CSRF")
```

time, day, hour, minute

Проверка соответствия текущего времени заданному условию. Если не указан суффикс *utc*, время берется локальное, иначе — по Гринвичу.

Синтаксис:

```
day[.utc] = monday / tuesday / wednesday / thursday / friday / saturday / sunday / DD /  
list
```

```
time[.utc] = HH:MM / range / lib.time(<name>)
```

```
hour[.utc] = HH / range
```

```
minute[.utc] = MM / range
```

```
HH ::= 00 - 23
```

```
MM ::= 00 - 59
```

```
DD ::= 1 - 31
```

Пример:

```
PASS time = 12:00..13:00 % разрешить каждый день с 12 до 13 часов  
PASS time = lib.time("Праздники") % использовать библиотеку "Праздники"  
DENY day = (sunday, saturday) % запретить на выходных  
DENY day = (monday, 15) hour = 9..18 % запретить каждый понедельник и  
каждое 15 число месяца с 9 до 18 часов
```

Открытые интервалы учитываются по границе суток/часа.

PASS hour = 18.. % означает, что разрешено с 18 часов до полуночи
minute = ..10 % первые 10 минут каждого часа

url, url.host и url.address

Проверка url или его части на значение. Проверка использует нормализованный URI с декодированными *%*.

Синтаксис:

url[(prefix | substring | suffix | regex | re2)] = string

url.host[(prefix | substring | suffix | regex | re2)] = string

url.domain[(prefix | substring | suffix | regex | re2)] = string

url.address = ip_address | subnet | subnet_label

url.port = [low_port]..[high_port] | port

url.path[.base64][(prefix | substring | suffix | regex | re2)] = string

url.is_absolute = yes | no % полный или нет URL

prefix ::= string % начало строки

substring ::= string % подстрока

suffix ::= string % окончание строки

regex ::= string % регулярное выражение PCRE

re2 ::= string % регулярное выражение RE2

url.address — это, по сути, синоним *dst.ip*.

Пример:

```
DENY url.path.base64.re2 = "(?i)\bondisconnecting\W*" enabled(true)
name("ondisconnecting (URI)")
```

qparam.<name>, qparam.values и qparam.names

Проверка значения параметров запроса. Проверка использует имена и значения параметров с декодированными *%*.

Синтаксис:

qparam.length = numeric % проверить общую длину query-параметров

qparam.count = numeric % проверить количество query-параметров
qparam.<name>[(length | count)] = numeric

qparam.<name>[.base64][(nocase | substring | substring.nocase | regex | re2)] = string

qparam.values[.base64].substring[.nocase] = string % проверить все значения на вхождение подстроки

qparam.names[.base64].substring[.nocase] = string % проверить все имена на вхождение подстроки

qparam.values[.base64].regex = string % проверить все значения на регулярное выражение

qparam.names[.base64].regex = string % проверить все имена на регулярные выражения

qparam.values[.base64].re2 = string % проверить все значения на регулярное выражение

qparam.names[.base64].re2 = string % проверить все имена на регулярные выражения
numeric ::= integer | range % число либо диапазон

regex ::= string % регулярное выражение PCRE

re2 ::= string % регулярное выражение RE2

Пример:

```
DENY("limit arguments total length") qparam.length =
1024..                              % total
DENY("Limit argument value length") qparam.values.length =
1024..                              % for each
DENY("Limit argument name length") qparam.names.length =
1024..                              % for each
```

```
DENY("Maximum number of arguments in request limited") qparam.count =
12.. % total
DENY("PHP injection attempt") qparam.values.base64.substring.nocase =
"${@print}"
```

user и group

Проверка текущего пользователя или его группы.

Синтаксис:

user = word / string / known / unknown

group = word / string

user.guid = string

group.guid = string

known — используется для указания авторизованного (известного) пользователя;

unknown — используется для указания неавторизованного (неизвестного) пользователя.

Пример:

```
PASS user = known % разрешить известных пользователей
DENY group = "Отдел продаж" category = "Pornography/Sexually
Explicit" % запретить категорию порно для группы "Отдел продаж"
```

src и dst

Проверка условия на IP-адрес, зону или GeoIP источника/назначения.

Синтаксис:

src.ip = ip_address / subnet / subnet_label / list / lib

dst.ip = ip_address / subnet / subnet_label / list / lib

src.zone = integer / zone_name

dst.zone = integer / zone_name

src.geoip = iso3166 | list

dst.geoip = iso3166 | list

src.mac = mac_address | list

dst.mac = mac_address | list

lib ::= lib.(network | url) '(' list_libs ')'

list_libs ::= lib_name ';' list_libs

lib_name ::= word | string

iso3166 ::= [A-Z][A-Z]

url.address — это, по сути, синоним *dst.ip*.

scenario

Проверка активности определенного сценария.

Синтаксис:

scenario = string | word | list

Пример:

```
DENY scenario = Torrents desc("Запретить, если активен сценарий
Torrents")
```

virus_heuristic и virus_usergate

Проверка тела ответа на вирусы.

Синтаксис:

virus_heuristic = yes | no | true | false % (по умолчанию false)

virus_usergate = yes | no | true | false % (по умолчанию false)

heuristic — эвристический анализатор (медленный);

usergate — проверка по хэшам (быстрый).

bridge_vlan_filter

Фильтрация трафика по VLAN-тегам для интерфейса в режиме моста (bridge).

Синтаксис:

bridge_vlan_filter '!=' list | number | number..number

Пример:

```
DENY bridge_vlan_filter = (10, 100..200) desc("Запретить трафик по VLAN-тегам")
```

service

Детектирование трафика определенного сервиса для межсетевого экрана.

Синтаксис:

service = string | word | list

Пример:

```
DENY service = POP3 desc("Запретить сервис POP3")
```

application

Детектирование трафика определенного приложения на уровне L7 для межсетевого экрана.

Синтаксис:

application = string | word | list

Пример:

```
DENY application = Tor desc("Запретить Tor")
```

envelope_from и envelope_to

Проверка email-адреса отправителя/адресата сообщения.

Синтаксис:*envelope_from '='!'!=' string | list**envelope_to '='!'!=' string | list***Пример:**

```
PASS envelope_from = "Email froup from" envelope_to = "Email froup to"
service = SMTP mark_hdr(Subject) enabled(true) name("Mail Pass Rule")
```

response_time

Проверка времени ответа в миллисекундах.

Синтаксис:*response_time = integer*

hip_profile

HIP-профили для проверки соответствия конечного устройства требованиям безопасности. Действительно только для правил межсетевого экрана.

Синтаксис:*hip_profile = string | word | list*

Встроенные библиотеки

Библиотеки (*lib*) — это элементы языка UPL, которые служат для доступа к встроенным и пользовательским библиотекам. Как правило, это достаточно большие списки, которые неудобно описывать через определения `def`. Обращение к библиотекам происходит по их именам.

Синтаксис:*library ::= lib.<url | morphology | category | useragent | mime | network | time | applicationgroup | servicegroup>(list_names)**list_names ::= name list_names*

name ::= *word* / *string*

url — список URL;

morphology — список морфологических словарей;

category — группа категорий;

useragent — список юзерагентов;

mime — список типов контента;

network — список сетей/IP-адресов;

time — библиотека с промежутками времени.

Пример:

```
DENY src.ip = lib.network("Bad ips", "Test ips")
DENY dst.ip = lib.network("Bad ips")
DENY dst.ip = lib.url("Bad urls") % в данном случае домены будут
резолвиться в ip-адреса

DENY morphology = lib.morphology("Porno words", "Bad words")
DENY category = lib.category("Restricted categories") category =
lib.category(Productivity)

PASS request.header.User-Agent = lib.useragent("Browsers")
PASS request.header.Content-Type = lib.mime(Applications)
DENY time = lib.time(Weekends)
```

Определения

В файлах политик определения (def) служат для объединения наборов условий или действий. Каждое определение должно иметь уникальное пользовательское имя, по которому к нему можно обратиться из правил.

def condition

Наборы условий. Все условия в одной строке проверяются по логическому *И*. Перевод строки означает логическое *ИЛИ*. Символ экранирования — обратный слэш ("\") в конце строки позволяет перенести условие по *И* на следующую строку.

Синтаксис:

```

def condition label_name

    conditions

end

conditions ::= condition '\'? [conditions]

condition ::= name '=' value

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

```

def scenario_cond

Список условий сценария. Каждое условие сценария обычно пишется в одной строке, но при необходимости условие может быть разбито на строки с помощью специального символа — обратного следа ("\`\`").

Синтаксис:

```

def scenario_cond label_name

    scenario_conditions

end

scenario_conditions ::= Conditions '\'? Properties

Conditions ::= condition '\'? Conditions

Properties ::= property '\'? Properties

scenario_cond ::= name '=' value

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

```

def var

Определение переменных. Служит для подсчета некоторых событий за определенный интервал времени. Для изменения значения предназначены действия *inc* и *dec*.

Синтаксис:

```

def var label_name

    init ::= integer

    window ::= time

    key ::= condition_name / condition_list

end

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

condition_list ::= '(' condition_name , condition_list ')'

```

init — это начальное значение переменной, к которому она вернется по истечении времени *window*;

key — поле или список полей, по которым группируются значения переменной (необязательный параметр).

Свойства

Свойства (properties) — это некие атрибуты правила, например, *name* или *enabled*. Они используются для предоставления дополнительной информации в процессе обработки правил.

Синтаксис свойств точно такой же, как у действий.

Синтаксис:

```

property = prop_name / prop_name '(' list_params ')'

prop_name ::= name / desc / id / rule_log / enabled / scenario

list_params ::= value ',' list_params

```

name и desc

Атрибуты *имя* и *описание* для правила.

Синтаксис:

```

Name ::= name '(' string/word ')'

```

Description ::= desc (' string ')

Пример:

```
DENY hour = 9..18 category = News name("Запретить News")
desc("Запретить категорию News в рабочее время")
```

enabled

Атрибут, который включает или выключает работу правила.

Синтаксис:

Enable ::= enabled (' boolean ')

boolean ::= yes | no | true | false % (по умолчанию false)

rule_log

Устанавливает атрибут журналирования правила.

Значение *session* действительно только для правил межсетевого экрана, защиты от dos-атак и пропускной способности.

Синтаксис:

Logging ::= rule_log (' boolean | session ')

LoggingFwRule ::= rule_log (' boolean , interval, burst')

boolean ::= yes | no | true | false % (по умолчанию no)

interval ::= "integer/[s,m,h,d]"

burst ::= integer

interval — среднее число пакетов, попадающих под условие *limit* в единицу времени (1/s, 1/m, 1/h, 1/d) , default = 3/h;

burst — максимальное число пакетов, попадающих в под условие *limit* за один раз (default = 5).

profile

Устанавливает профиль правила.

Синтаксис:

Profile ::= profile '(' string | word | list ')'

certificate

Сертификат, используемый для поддержки HTTPS-соединения. Действительно только для правил reverse-прокси.

Синтаксис:

CertAuthEnabled ::= cert_auth_enabled '(' boolean ')'

Certificate ::= certificate '(' certificate_name ')'

certificate_name ::= string | word

gateway

Шлюз. Имя одного из существующих шлюзов. Действительно только для правил NAT и маршрутизации, и для условий сценария "Проверка состояния".

Синтаксис:

Gateway ::= gateway '(' string | word ')'

Свойства правил межсетевого экрана**reject_with**

Устанавливает способ, с помощью которого будет блокироваться трафик. Действительно только для правил межсетевого экрана.

Синтаксис:

Reject ::= reject_with '(' "tcp-reset-both" | "tcp-rst" | "host-unreach" ')'

fragmented

Проверка на фрагментированность пакетов. Действительно только для правил межсетевого экрана.

Синтаксис:

Fragmented ::= fragmented '(' boolean ')'

boolean ::= yes / no / true / false

yes — проверяются только фрагментированные пакеты;

no — проверяются только нефрагментированные пакеты;

—, если свойство *fragmented* не указано, то будут проверяться все пакеты.

ips_profile

Устанавливает профиль IPS. Действительно только для правил межсетевого экрана.

Синтаксис:

IPS_Profile ::= ips_profile '(' string | word ')'

l7_profile

Устанавливает профиль приложения. Действительно только для правил межсетевого экрана.

Синтаксис:

L7_Profile ::= l7_profile '(' string | word ')'

Свойства правил инспектирования SSL

block_invalid_cert

Блокирование сайтов с некорректными сертификатами. Действительно только для правил инспектирования SSL.

Синтаксис:

InvalidCertificate ::= block_invalid_cert '(' boolean ')'

boolean ::= yes / no / true / false

check_revoc_cert

Проверка по списку отозванных сертификатов. Действительно только для правил инспектирования SSL.

Синтаксис:

ChekRevocation ::= check_revoc_cert '(' boolean ')'

boolean ::= yes / no / true / false

block_expired_cert

Блокировка сертификатов с истекшим сроком действия. Действительно только для правил инспектирования SSL.

Синтаксис:

ExpiredCertificate ::= block_expired_cert '(' boolean ')'

boolean ::= yes / no / true / false

block_self_signed_cert

Блокировка самоподписанных сертификатов. Действительно только для правил инспектирования SSL.

Синтаксис:

SelfSignedCertificate ::= block_self_signed_cert '(' boolean ')'

boolean ::= yes / no / true / false

ssl_profile

Профиль SSL. Действительно только для правил инспектирования SSL, reverse-прокси, веб-портала.

Синтаксис:

SslProfile ::= ssl_profile '(' string | word ')'

ssl_forward_profile

Профиль пересылки SSL. Действительно только для правил инспектирования SSL.

Синтаксис:

SslForwardProfile ::= ssl_forward_profile '(' string | word ')'

profile_id ::= integer

Свойства правил пропускной способности

bandwidth_pool

Полоса пропускания. Действительно только для правил пропускной способности.

Синтаксис:

BandwidthPool ::= bandwidth_pool '(' bandwidth ')'

bandwidth ::= "100 Kbps" | "512 kbps" | "1 Mbps" | "2 Mbps" | "5 Mbps" | "10 Mbps" | "20 Mbps" | "50 Mbps" | "100 Mbps"

Пример:

```
scenario = "Сценарий обнаружения torrent" bandwidth_pool("1 Mbps")
enable(true) name("Пропускная способность torrent")
```

Свойства правил защиты почтового трафика

mark

Маркировка. Текст тега, который маркирует письмо. Действительно только для правил защиты почтового трафика.

Синтаксис:

Mark ::= mark '(' string | word ')'

mark_hdr

Заголовок. Поле, куда помещается тег маркировки. Действительно только для правил защиты почтового трафика.

Синтаксис:

MarkHeader ::= mark_hdr '(' word ')'

antispam_kav

Проверка антиспамом. Действительно только для правил защиты почтового трафика.

Синтаксис:

AntispamKav ::= antispam_kav '(' boolean ')'

boolean ::= yes | no | true | false

antispam_usergate

Проверка антиспамом UserGate. Действительно только для правил защиты почтового трафика.

Синтаксис:

AntispamUsergate ::= antispam_usergate '(' boolean ')'

boolean ::= yes | no | true | false

Пример:

```
DENY("with error") envelop_to = UserGate antispam_usergate(yes)
```

dnsbl

DNSBL-проверка (только SMTP). Действительно только для правил защиты почтового трафика.

Синтаксис:

DNSBLacklistCheck ::= dnsbl '(' boolean ')'

boolean ::= yes | no | true | false

Пример:

```
DENY service = SMTP dnsbl(yes)
```

Свойства правил NAT и маршрутизации**target_ip**

Адрес назначения DNAT, если задано действие *dnat* или *port_mapping*.

Новая IP-сеть/маска, если задано действие *netmap*.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

TargetIp ::= target_ip '(' ipv4 | ipv4_with_mask ')'

Пример:

```
PASS target_ip("192.168.1.20") dnat
```

target_snat

Включение SNAT. При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

TargetSnat ::= target_snat '(' boolean ')'

boolean ::= yes | no | true | false

snat_target_ip

SNAT IP (внешний адрес). Явно указывает IP-адрес, на который будет заменен адрес источника при подмене адресов пакетов.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

SnatTargetIp ::= snat_target_ip '(' ip_address ')'

port_map

Порт-форвардинг. Переопределение портов публикуемых сервисов. Действительно только для правил NAT и маршрутизации.

Синтаксис:

PortMap ::= port_map '(' protocol, port_from, port_to ')'

protocol ::= tcp | udp | smtp | smpts

port_from ::= integer

port_to ::= integer

port_from — номер TCP/UDP-порта, на который пользователи шлют запросы;
port_to — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.

direction

Направление подмены сетей. Действительно только для правил NAT и маршрутизации.

Синтаксис:

Direction ::= direction '(' input | output ')'

input — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике;

output — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике.

Свойства правил DNS-прокси

dns_server

Список IP-адресов DNS-серверов. Действительно только для правил DNS-прокси.

Синтаксис:

DnsServer ::= dns_server '(' ip_address | ip_address_list ')'

Свойства правил reverse-прокси

cert_auth_enabled

Аутентификация по сертификату. Действительно только для правил Reverse-прокси.

Синтаксис:

CertAuthEnabled ::= cert_auth_enabled '(' boolean ')'

boolean ::= yes | no | true | false

is_https

Включение поддержки HTTPS. Действительно только для правил Reverse-прокси.

Синтаксис:

```
IsHttps ::= is_https '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

rewrite_path

Подмена путей. Действительно только для правил Reverse-прокси.

Синтаксис:

```
RewritePath ::= rewrite_path '(' path_from, path_to ')'
```

path_from — изменить с (домен и/или путь URL, которые требуется изменить);
path_to — изменить на (домен и/или путь URL, на которые требуется заменить старые).

Свойства правил веб-портала

icon

Иконка, которая будет отображаться на веб-портале для данной закладки. Действительно только для правил веб-портала.

Синтаксис:

```
Icon ::= icon '(' string | word ')'
```

additional_url

Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей.

Действительно только для правил веб-портала.

Синтаксис:

```
AdditionalUrl ::= additional_url '(' string | word | list ')'
```

rdp_check_session_alive

Проверка авторизации для RDP-сессий. Действительно только для правил веб-портала.

Синтаксис:

```
RdpCheckSessionAlive ::= rdp_check_session_alive '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

transparent_auth

Включение прозрачной аутентификации пользователя. Действительно только для правил веб-портала.

Синтаксис:

```
TransparentAuth ::= transparent_auth '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

Свойства правил веб-безопасности (Safe browsing)

enable_adblock

Блокировка рекламы.

Синтаксис:

```
EnableAdblock ::= enable_adblock '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

url_list_exclusions

URL-список сайтов исключений, для которых блокировать рекламу не требуется.

Синтаксис:

```
UrlListExclusions ::= url_list_exclusions '(' list_libs ')'
```

```
list_libs ::= lib_name ',' list_libs
```

```
lib_name ::= word | string
```

enable_injector

Позволяет вставить произвольный код во все веб-страницы.

Синтаксис:

```
EnableInjector ::= enable_injector '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

custom_injector

Код инжектора.

Синтаксис:

```
CustomInjector ::= custom_injector '(' string ')'
```

safe_search

Функция безопасного поиска.

Синтаксис:

```
SafeSearch ::= safe_search '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

search_history_logging

Запись в журнал поисковых запросов пользователей.

Синтаксис:

```
SearchHistoryLogging ::= search_history_logging '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

social_sites_block

Блокировка приложения в популярных социальных сетях.

Синтаксис:

```
SocialSitesBlock ::= social_sites_block '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

Свойства BYOD

max_device_number

Максимальное количество устройств, с которых пользователь может получать доступ в сеть.

Действительно только для правил BYOD.

Синтаксис:

MaxDeviceNumber ::= max_device_number '(' integer ')'

max_active_device_number

Максимальное количество устройств, с которых пользователь одновременно может получать доступ в сеть.

Действительно только для правил BYOD.

Синтаксис:

MaxActiveDeviceNumber ::= max_active_device_number '(' integer ')'

device_type

Тип устройств, для которых применяется данное правило политики BYOD.

Действительно только для правил BYOD.

Синтаксис:

DeviceType ::= device_type '(' word | string | list ')'

approving_required

Подтверждение администратора.

Действительно только для правил BYOD.

Синтаксис:

ApprovingRequired ::= approving_required '(' boolean ')'

boolean ::= yes | no | true | false

Свойства инспектирования SSH

block_ssh_shell

Блокировка удалённого запуска shell. Действительно только для правил инспектирования SSH.

Синтаксис:

BlockSshShell ::= block_ssh_shell '(' boolean ')'

boolean ::= yes | no | true | false

block_ssh_exec

Блокировка удалённого выполнения команд по SSH. Действительно только для правил инспектирования SSH.

Синтаксис:

BlockSshExec ::= block_ssh_exec '(' boolean ')'

boolean ::= yes | no | true | false

block_sftp

Блокировка соединения SFTP (Secure File Transfer Protocol). Действительно только для правил инспектирования SSH.

Синтаксис:

BlockSftp ::= block_sftp '(' boolean ')'

boolean ::= yes | no | true | false

ssh_command

Команда linux, которую требуется передать, в формате ssh user@host 'command'.

Действительно только для правил инспектирования SSH.

Синтаксис:

SshCommand ::= ssh_command '(' string ')'

Свойства правил VPN-сервера

auth_profile

Профиль аутентификации. Действительно только для правил VPN-сервера.

Синтаксис:

```
AuthProfile ::= auth_profile '(' string | word ')'
```

vpn_network

Сеть VPN. Действительно только для правил VPN-сервера.

Синтаксис:

```
VpnNetwork ::= vpn_network '(' string ')'
```

interface

Интерфейс VPN. Действительно только для правил VPN-сервера и VPN-клиента.

Синтаксис:

```
Interface ::= interface '(' word ')'
```

Свойства правил VPN-клиента

server_address

IP-адрес сервера. Действительно только для правил VPN-клиента.

Синтаксис:

```
ServerAddress ::= server_address '(' ip_address ')'
```

password

Пароль. Действительно только для правил VPN-клиента.

Синтаксис:

```
Password ::= password '(' word ')'
```

last_error

Последняя ошибка VPN. Информационное поле, недоступное для редактирования. Действительно только для правил VPN-клиента.

Синтаксис:

```
LastError ::= last_error '(' string ')'
```

status

Статус. Информационное поле, недоступное для редактирования. Действительно только для правил VPN-клиента.

Синтаксис:

```
Status ::= status '(' string ')'
```

Свойства правил сценариев

trigger

Тип срабатывания сценария. Действительно только для правил сценариев.

Синтаксис:

```
Trigger ::= trigger '(' trigger_type ')'
```

```
trigger_type ::= all_users | one_user
```

duration

Продолжительность. Время в минутах, в течение которого сценарий будет активным после его активации. Действительно только для правил сценариев.

Синтаксис:

```
Duration ::= duration '(' integer ')'
```

operation_mode

Сценарий срабатывает при совпадении одного или всех условий.

Синтаксис:

```
OperationMode ::= operation_mode '(' mode ')'
```

mode ::= all | any

Свойства условий сценария

scond_type

Тип условий сценария. Действительно только для условий сценария.

Синтаксис:

SCondType ::= scond_type '(' type ')'

SCondType ::= scond_type '(' type ')'

count_interval

Количество срабатываний. Действительно только для условий сценария "Категория URL" (url_category), "Приложение" (app), "Тип контента" (mime_type) и "Проверка состояния" (health_check).

Синтаксис:

CountInterval ::= count_interval '(' integer ')'

max_event_count

Интервал времени в минутах, за который было обнаружено *count_interval* срабатываний. Действительно только для условий сценария "Категория URL" (url_category), "Приложение" (app), "Тип контента" (mime_type) и "Проверка состояния" (health_check).

Синтаксис:

MaxEventCount ::= max_event_count '(' integer ')'

packet_size

Размер пакета. Размер пакета в трафике пользователя превысил указанное значение. Действительно только для условий сценария "Размер пакета" (net_packet_size).

Синтаксис:

PacketSize ::= packet_size '(' size ')'

size ::= integer | integer KB | integer MB | integer GB

64 — размер в байтах;
2MB — размер в мегабайтах.

traffic_limit

Объем трафика. Действительно только для условий сценария "Ограничение трафика" (traffic).

Синтаксис:

TrafficLimit ::= traffic_limit '(' size ')'

size ::= integer | integer KB | integer MB | integer GB

period

Период времени. Действительно только для условий сценария "Ограничение трафика" (traffic).

Синтаксис:

Period ::= period '(' time_period ')'

time_period ::= minute | hour | day | week | month

ips_tl

Уровень угрозы COB. Действительно только для условий сценария "COB" (ips).

Синтаксис:

IpsTl ::= ips_tl '(' level ')'

level ::= integer | very_low | low | medium | high | very_high

ips_tl(2) scond_type(ips);
ips_tl(low) scond_type(ips).

health_check_method

Метод проверки. Действительно только для условий сценария "Проверка состояния" (health_check).

Синтаксис:

CheckMethod ::= health_check_method '(' method ')'

method ::= ping | dns | get

health_result

Результат. Действительно только для условий сценария "Проверка состояния" (health_check).

Синтаксис:

result ::= health_result '(' result ')'

result ::= positive | negative

health_request_timeout

Тайм-аут подключения (сек). Действительно только для условий сценария "Проверка состояния" (health_check).

Синтаксис:

RequestTimeout ::= health_request_timeout '(' integer ')'

health_answer_timeout

Тайм-аут ответа (сек). Действительно только для условий сценария "Проверка состояния" (health_check), "Метод проверки HTTP GET" (get).

Синтаксис:

ut ::= health_answer_timeout '(' integer ')'

health_type_request

Тип DNS-запроса. Действительно только для условий сценария "Проверка состояния" (health_check), "метод проверки DNS" (dns).

Синтаксис:

TypeRequest ::= health_type_request '(' type_name ')'

type_name ::= word | string

Свойства правил балансировки нагрузки

scheduler

Метод балансировки. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

Scheduler ::= scheduler '(' balancing_type ')'

balancing_type ::= wrr | rr | lc | wlc

wrr — Weighted round robin;

rr — Round robin;

lc — Least connections;

wlc — Weighted least connections.

real_server

Реальные серверы. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

RealServer ::= real_server '(' mode, ipv4[:port], weight ')'

mode ::= gate | masq | masq_snat

port ::= integer

weight ::= integer

gate — шлюз;

masq — маскарадинг;

masq_snat — маскарадинг с подменой IP-адреса источника (SNAT).

Пример:

```
OK \
    url.address = 172.168.13.100 \
```

```

url.port = 10000 \
service = tcp \
scheduler(wlc) \
real_server(masq_snat, 172.168.13.11:10000, 50) \
ipvs_fallback(gate, 172.168.13.12)
monitor_kind(ping) \
monitor_interval(60) \
monitor_timeout(60) \
monitor_failurecount(10) \
enabled(true) \
name("TCP/UPD load balancing")

```

ipvs_fallback

Аварийный режим сервера. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

IpvsFallback ::= ipvs_fallback '(' mode, ipv4[:port] ')'

mode ::= gate | masq | masq_snat

port ::= integer

monitor_kind

Режим. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorKind ::= monitor_kind '(' kind ')'

kind ::= ping | connect | negotiate

monitor_service

Сервис. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorService ::= monitor_service '(' service ')'

service ::= http | dns

monitor_request

Запрос. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorRequest ::= monitor_request '(' string ')'

monitor_response

Ожидаемый ответ. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorResponse ::= monitor_response '(' string ')'

monitor_interval

Интервал проверки. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorInterval ::= monitor_interval '(' integer ')'

monitor_timeout

Время ожидания. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorTimeout ::= monitor_timeout '(' integer ')'

monitor_failurecount

Число неудачных попыток. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

MonitorFailurecount ::= monitor_failurecount '(' integer ')'

Действия

Действие (action) — это то, что будет выполнено, если условия в правиле истинны. В качестве параметров могут использоваться константные значения, или динамические значение там, где это предусмотрено.

Синтаксис:

```
action = action_name | action_name '(' list_params ')'
```

```
action_name ::= warning | log_message | append | delete | set | replace | encrypt | incl  
dec | reset | redirect | encrypt_body_url | decrypt_path | body_inject |  
set_cookie_token | body_replace | lookup_and_auth | encode_cookie |  
decode_cookie | sma | nat | dnat | route | port_mapping | netmap | forward | ignore |  
action_label
```

```
action_label ::= 'action'!<action_label_name>
```

```
action_label_name ::= atom
```

```
list_params ::= value ';' list_params
```

warning

Действия, которые разрешаются без выхода из обработки правил на текущем слое. *warning* ставит отметку о том, что необходимо вставить код с предупреждением в тело ответа.

Пример:

```
[L1]
category = lib.category(Productivity) warning
DENY user = user1
```

log_message

Записать сообщения в журнал.

Пример:

```
DENY category = lib.category(Productivity) log_message("Deny porno")
```

append

Добавить заголовок к HTTP-запросу/ответу. Список поддерживаемых заголовков приведен в [Приложении](#).

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

```
append([request | response,] <headername>, value)
```

headername — см. в [Приложении](#).

value ::= *string* | *numeric* | *condition_name*.

set

Переписать значение конкретному HTTP-заголовку. Список поддерживаемых заголовков см. в [Приложении](#).

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

```
set([request | response,] <headername>, value)
```

headername — см. в [Приложении](#).

value ::= *string* | *numeric* | *condition_name*.

delete

Удалить HTTP-заголовок. Список поддерживаемых заголовков см. в [Приложении](#).

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

```
delete([request | response,] <headername>)
```

headername — см. в [Приложении](#).

replace

Модифицировать значение HTTP-заголовка. Список поддерживаемых заголовков см. в [Приложении](#).

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

replace([request | response,] <headername>, regex, value)

regex ::= string % регулярное выражение

value ::= string | condition_name

headername — см. в [Приложении](#).

Пример 1:

Добавить заголовок Referer:

```
PASS append(Referer, "http://example.com") enabled(true)
```

Удалить заголовок:

```
PASS delete(Referer)
```

Переписать заголовок:

```
PASS set(request, Cache-Control, no-cache)
```

Модифицировать заголовок Location:

```
PASS response.header.Location.count = 1.. replace(response, Location,
"http://example.com", url.host) enabled(true)
```

Пример 2:

```
define action delete_referer
  log_message("Referer header deleted")
  delete(request, Referer)
end
```

encrypt

Шифровать часть пути в HTTP-заголовке. Список поддерживаемых заголовков см. в [Приложении](#).

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

encrypt([*request* | *response*,] <headername>, <url>[, <user_key>[, <add_ip>]])

url ::= string % часть url для фильтрации

user_key ::= string % пользовательский ключ шифрования (необязательный параметр)

add_ip ::= boolean % добавлять ли IP к ключу шифрования (логическое значение, необязательный параметр)

boolean ::= yes | no | true | false

headername — см. в [Приложении](#).

encrypt_body_url

Шифровать часть пути в ссылках тела ответа.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

encrypt_body_url(<url>[, <user_key>[, <add_ip>]])

url ::= string % часть url для фильтрации

user_key ::= string % пользовательский ключ шифрования (необязательный параметр)

add_ip ::= boolean % добавлять ли IP к ключу шифрования (логическое значение, необязательный параметр)

boolean ::= yes | no | true | false

decrypt_path

Дешифровать часть пути запроса.

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

decrypt_path(<path>[, <user_key>[, <add_ip>]])

path ::= string % часть пути для фильтрации

user_key ::= string % пользовательский ключ шифрования (необязательный параметр)

add_ip ::= boolean % добавлять ли IP к ключу шифрования (логическое значение, необязательный параметр)

boolean ::= yes | no | true | false

Пример:

Шифровать все относительные пути в заголовке *Location* и теле ответа, и дешифровать путь запроса:

```
decrypt_path("/", "User_Key", true) enabled(true) name("Path decode")
http.response.code = 302 encrypt(Location, "/", "User_Key", true)
enabled(true) name("Encrypt Location header")
encrypt_body_url("/", "User_Key", true) enabled(true) name("Encrypt all
relative URL")
```

body_inject

Вставить скрипт в тело ответа.

Синтаксис:*body_inject(inject_text)**inject_text ::= string***set_cookie_token**

Добавить в ответ заголовок 'Set-Cookie' со сгенерированным токеном.

Синтаксис:*set_cookie_token(cookie_name, parameter, expires_date)**cookie_name ::= string**parameter ::= string**expires_date ::= [DD_]HH:MM % время которое будет прибавлено к текущему времени***Пример:**

Реализация CSRF защиты:

```

DENY http.method = POST request.header.Referer.substring = "/login.php"
qparam.UCSRF_TOKEN != request.header.Cookie.ucsrftoken enabled(true)
name("Check CSRF")
url.path.prefix = "/login.php" set_cookie_token(ucsrftoken, "path=",
01_00:00) body_inject("<script language='JavaScript'>
    var tokenName = 'UCSRF_TOKEN';

    document.addEventListener('DOMContentLoaded', function()
    {
        var t_res = document.cookie.match(/ucsrftoken=(.+?) (;|$)/);
        var tokenValue = t_res ? t_res[1] : '';

        var forms = document.getElementsByTagName('form');
        for(i=0; i<forms.length; i++)
        {
            var html = forms[i].innerHTML;
            html += '<input type=hidden name=' + tokenName + ' value='
+ tokenValue + ' />';

```

```

        forms[i].innerHTML = html;
    }
});
</script>") enabled(true) name("Inject")

```

encode_cookie

Шифровать значения Cookie в заголовке Set-Cookie с заданным именем.

Синтаксис:

```
encode_cookie(cookie_name[, condition_name][, user_kry_string][, f_encrypt])
```

cookie_name ::= string

condition_name % условие используемое для кодирования (по умолчанию src.ip)

user_kry_string ::= string % пользовательский ключ шифрования (по умолчанию "")

f_encrypt := true % необходимо шифрование (по умолчанию false)

decode_cookie

Дешифровать токен в заголовке Cookie с заданным именем.

Синтаксис:

```
decode_cookie(cookie_name[, condition_key][, user_kry_string][, f_decript])
```

cookie_name ::= string

condition_name % условие используемое для декодирования (по умолчанию src.ip)

user_kry_string ::= string % пользовательский ключ шифрования (по умолчанию "")

f_encrypt := true % необходимо шифрование (по умолчанию false)

Пример:

Шифрование и дешифрование Cookie с именем security:

```
response.header.Set-Cookie.count != 0 encode_cookie("security", src.ip,
true) enabled(true) name("encode_cookie")
request.header.Cookie.count != 0 decode_cookie("security", src.ip,
true) enabled(true) name("decode_cookie")
```

body_replace

Модифицировать тело ответа. Выполняется не более двух (первых) модификаций для каждого ответа.

Синтаксис:

body_replace(<regex>, <value>)

regex ::= string % регулярное выражение

value ::= string

Пример:

```
PASS \
body_replace("(\\+7|8)[\\s()?(\\d\\{3})[\\s)]?(\\d\\{3})[\\s-]?((\\d\\{2})[\\s-]?((\\d\\{2}))", "+\\1 (\\2) \\3-XX-XX") \
body_replace("(\\w{1})[\\w\\.]*((\\w{1})@([\\w]+)\\.([\\w]+)", "\\1***\\2@\\3.\\4") \
enabled(true) \
name("Replace mail and phone")
```

lookup_and_auth

Аутентифицировать пользователя. В случае если IP не указан, запрос маркируется именем пользователя.

Синтаксис:

lookup_and_auth(<user_login>[, <ip_address>[, <session_timeout>]])

user_login ::= string | condition_name % Логин аутентификации

ip_address ::= string | condition_name % IP адрес

session_timeout ::= integer % тайм-аут сессии, по умолчанию 0.

Пример:

```
lookup_and_auth(request.x_header.X-Authenticated-User,
request.x_header.X-Forwarded-For, 300) enabled(true) name("User
authentication")
lookup_and_auth(request.x_header.X-Authenticated-User) enabled(true)
name("Mark request")
```

redirect

При блокировке перенаправить пользователя на адрес, который указан в редиректе.

Синтаксис:

Redirect ::= redirect(RespCode[, RedirectText], Url)

RespCode ::= 301 | 302 | 305 | 307

RedirectText ::= string

Url ::= string

Пример:

```
DENY src.zone = Trusted redirect(302, "Custom test (Moved)", "https://
block.captive/block")
DENY src.zone = Untrusted redirect(302, "https://block.captive/block")
```

inc и dec

Используются для изменения значения переменных, объявленных как *def var*.

Синтаксис:

inc(var.<var_name>, integer)

dec(var.<var_name>, integer)

Пример:

На каждый `http.response.code = 500` увеличивается значение `rps` на 1. Если превысили 10 таких запросов за 5 минут, блокируем дальнейшие ответы. Через 5 минут переменная `rps` будет сброшена в 0:

```
def var rps
  init = 0
  window = 00:05
  key = src.ip
end

http.response.code = 500 var.rps=..10 inc(var.rps, 1) enabled(true)

PASS var.rps = 5 log_message("Warning!") enabled(true)

DENY var.rps=11.. log_message("Too many 500 errors!") enabled(true)
```

reset

Сбросить значения переменных, объявленных как *init* в *def var*, в начальное значение.

Синтаксис:

```
reset(var.<var_name>)
```

sma

Используются для подсчета среднего значения в окне времени, которое определяется в переменной как *window* в *def var*.

Синтаксис:

```
sma(var.<var_name>, integer)
```

Пример:

Блокируются запросы, когда среднее время запроса за 30-секундный интервал превысит 2 секунды:

```
def var avg_time
  init = 0
```

```

    window = 00:00:30
    key = src.ip
end

src.zone = Untrusted sma(var.avg_time, response_time) enabled(true)
name("sma")
DENY src.zone = Untrusted var.avg_time = 2000.. enabled(true) name("sma
res")

```

nat

NAT — подмена сетевых IP-адресов.

Пример:

```
PASS src.zone = Trusted dst.zone = Untrusted nat
```

dnat

DNAT — подмена IP-адреса назначения.

Пример:

```
PASS dnat target_ip("192.168.1.20")
```

port_mapping

Порт-форвардинг — перенаправление трафика на указанный IP-адрес с изменением номера порта публикуемого сервиса.

Пример:

```
PASS port_mapping target_ip("192.168.1.20") port_map(tcp, 2000, 2001)
```

netmap

Network mapping — позволяет произвести замену IP-адресов источника или назначения одной сети на другую.

Пример:

```
PASS netmap target_ip("192.168.32.0/24") direction(output)
```

route

Policy-based routing — позволяет маршрутизировать IP-пакеты на основе расширенной информации, например, сервисов, MAC-адресов или серверов (IP-адресов).

SNAT IP — Адрес, на который будет заменен адрес источника для трафика NAT.

Пример:

```
PASS service = HTTP route gateway(Шлюз1)
```

ignore

Игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации.

Пример:

```
OK profile("Example ICAP server") enabled(true) name("ICAP rule")  
ignore
```

forward

Переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL.

Пример:

```
OK url = lib.url(ZAPRET_INFO_BLACK_LIST_DOMAIN)ssl_profile("Default SSL  
profile") ssl_forward_profile("Forward SSL profile") enabled(false)  
name("Decrypt rule") forward
```

Типы правил

Правила контентной фильтрации

Префиксы

Имя	Описание
PASS	Разрешение посещения.
DENY	Блокировка веб-страницы.
WARNING	Предупреждение пользователя о том, что страница нежелательна для посещения.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[category](#), [morphology](#), [scenario](#), [time](#), [url](#), [user](#).

[request.header.Referer](#) — Список URL, в котором указаны рефереры для текущей страницы.

[request.header.User-Agent](#) — Useragent пользовательских браузеров.

[response.header.Content-Type](#) — Списки типов контента.

[http.method](#) — Метод, используемый в HTTP-запросах.

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [virus_heuristic](#).

Пример

```
[content "Content Rules"]
% ----- 1 --- "Content Rules" -----
PASS \
    url = lib.url("Education institutions") \
    src.zone = Trusted \
    desc("Content filtering rule which allows access to the list of
URLs. This is an example rule which can be changed or deleted if
```

```

necessary.") \
    rule_log(yes) \
    enabled(true) \
    name("Example white list")
% ----- 2 --- "Content Rules" -----
DENY("Blockpage (EN)") \
    url = lib.url("Education institutions") \
    dst.zone = Untrusted \
    rule_log(yes) \
    enabled(false) \
    name("Example block RU RKN by URL list")
% ----- 3 --- "Content Rules" -----
DENY \
    url = lib.network("Private IPs") \
    morphology = lib.morphology(Drugs) \
    src.zone = Trusted \
    time = lib.time(Weekdays) \
    rule_log(yes) \
    redirect(302, "https://bing.com") \
    enabled(false) \
    name("Example redirect to safesearch engines")

```

Правила межсетевого экрана

Префиксы

Имя	Описание
PASS	Разрешение трафика.
DENY	Блокировка трафика.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[service](#), [scenario](#), [time](#), [url](#), [user](#), [hip_profile](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [reject_with](#), [ips_profile](#), [l7_profile](#).

Пример

```
[firewall "Firewall rules"]
% ----- 1 -----
DENY \
    scenario = "Example torrent detection scenario" \
    dst.zone = Untrusted \
    dst.ip = lib.network("Botnets IP list") \
    rule_log(session) \
    reject_with("host-unreach") \
    enabled(true) \
    name("Example block RU RKN by IP list")
% ----- 2 -----
PASS \
    scenario = "Example torrent detection scenario" \
    src.zone = Trusted \
    dst.zone = Untrusted \
    hip_profile = "HIP profile" \
    ips_profile("Default IDPS profile") \
    l7_profile("Pass all applications") \
    rule_log(yes, "3/h", 5) \
    enabled(true) \
    name("Allow trusted to untrusted")
```

Правила NAT и маршрутизации

Префиксы

Имя	Описание
OK	Всегда ОК.

Тип правила определяется действием ([Action](#)):

- **nat** — правило NAT;
- **dnat** — правило DNAT;

- [port_mapping](#) — правило порт-форвардинга;
- [netmap](#) — правило Network mapping;
- [route](#) — правило policy-based.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[service](#), [scenario](#), [time](#), [url](#), [user](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [direction](#), [target_ip](#), [target_snat](#), [snat_target_ip](#),
[port_map](#), [gateway](#).

Пример

```
[nat_routing "NAT and Routing Rules"]
% ----- 1 -----
OK \
    src.zone = Trusted \
    service = (HTTP, HTTPS) \
    snat_target_ip("192.168.13.210") \
    rule_log(session) \
    enabled(true) \
    name("NAT Rule")\
    nat
% ----- 2 -----
OK \
    src.zone = Management \
    dst.ip = (lib.network("Private IPs"), lib.url("Microsoft Windows
Internet checker")) \
    target_ip("171.168.1.1") \
    target_snat(yes) \
    snat_target_ip("192.168.1.1") \
    enabled(true) \
    name("DNAY Rule")\
    dnat
% ----- 3 -----
```



```
OK \
  target_ip("172.168.1.1") \
  snat_target_ip("192.168.1.1") \
  port_map(tcp, 2000, 2000) \
  enabled(true) \
  name("Port-forwarding Rule")\
  port_mapping
% ----- 4 -----
OK \
  user = example \
  scenario = "Example torrent detection scenario" \
  gateway(My) \
  enabled(true) \
  name("Policy-base Rule")\
  route
% ----- 5 -----
OK \
  dst.geoip = (RW, S0) \
  target_ip("172.168.1.1") \
  direction(input) \
  enabled(true) \
  name("Network mapping Rule")\
  netmap
```

Правила Captive-портала

Префиксы

Имя	Описание
PASS	Не использовать аутентификацию.
OK	Использовать Captive-профиль.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[time](#), [url](#), [category](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [profile](#).

Пример

```
[captive "Captive Rules"]
% ----- 1 -----
PASS \
    category = lib.category(Threats) \
    url = lib.url("Microsoft Windows Internet checker") \
    time = lib.time(Weekends) \
    rule_log(yes) \
    enabled(true) \
    name("Skip auth for Microsoft Internet checker")
% ----- 2 -----
OK \
    src.zone = Trusted \
    profile("Example Captive profile") \
    enabled(true) \
    name("Example Captive portal")
```

Правила инспектирования SSL

Префиксы

Имя	Описание
PASS	Не расшифровывать передаваемые данные.
OK	Расшифровать передаваемые данные.

Пересылка определяется действием ([Action](#)):

- **forward** — в случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL ([ssl_forward_profile](#)).

Условия

[src.zone](#), [src.geoip](#), [src.ip](#),

[dst.geoip](#), [dst.ip](#),

[time](#), [service](#), [user](#), [category](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [ssl_profile](#), [ssl_forward_profile](#).

[block_invalid_cert](#), [check_revoc_cert](#), [block_expired_cert](#), [block_self_signed_cert](#).

Пример

```
[ssl "Decrypt Rules"]
% ----- 1 -----
PASS \
    category = (Finance, "Information Security") \
    rule_log(yes) \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example DO NOT Decrypt rule for Finance and Security sites")
% ----- 2 -----
OK \
    category = lib.category(Threats) \
    rule_log(yes) \
    block_invalid_cert(yes) \
    check_revoc_cert(yes) \
    block_expired_cert(yes) \
    block_self_signed_cert(yes) \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example decrypt rule for parental control")
% ----- 3 -----
OK \
    url = lib.url("Default SSL profile") \
    rule_log(yes) \
    ssl_profile("Default SSL profile") \
    ssl_forward_profile("SSL forward profile") \
    enabled(false) \
    name("Example decrypt RU RKN")\
    forward
```

Правила инспектирования SSH

Префиксы

Имя	Описание
PASS	Не расшифровывать передаваемые данные.
OK	Расшифровать передаваемые данные.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#),

[dst.geoip](#), [dst.ip](#),

[time](#), [service](#), [user](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#),

[block_ssh_shell](#), [block_ssh_exec](#), [block_sftp](#), [ssh_command](#).

Пример

```
[ssh "SSH inspection Rules"]
% ----- 1 -----
PASS \
    service = "Any UDP" \
    rule_log(yes) \
    enabled(true) \
    name("Bypass Rule")
% ----- 2 -----
OK \
    service = IMAP \
    block_ssh_shell(yes) \
    block_ssh_exec(yes) \
    block_sftp(yes) \
    ssh_command("command") \
    rule_log(yes) \
```

```
enabled(true) \  
name("Decrypy Rule")
```

DNS-правила

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

[url.domain](#).

Свойства

[name](#), [desc](#), [enabled](#), [dns_server](#).

Пример

```
[dns "DNS Rules"]  
% ----- 1 -----  
OK \  
    url.domain = "*.example.com" \  
    dns_server(1.2.3.4) \  
    enabled(true) \  
    name("Dns rule")
```

DoS-правила

Префиксы

Имя	Описание
PASS	Разрешение трафика.
DENY	Безусловная блокировка трафика.
WARNING	Применение профиля защиты от DoS-атак.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#),

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[time](#), [service](#), [user](#), [scenario](#),

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [profile](#).

Пример

```
[dos "DoS Rules"]
% ----- 1 -----
PASS \
    scenario = "Example torrent detection scenario" \
    user = example \
    src.ip = lib.url("Microsoft Windows Internet checker") \
    dst.geoip = RW \
    service = FTP \
    rule_log(session) \
    enabled(true) \
    name("DoS Allow Rule")
% ----- 2 -----
DENY \
    desc(api_dos_rule) \
    rule_log(yes, "3/h", 5) \
    enabled(true) \
    name("DoS Deny Rule")
% ----- 3 -----
WARNING \
    user = "CN=VPN users,DC=LOCAL" \
    time = lib.time("Working hours") \
    profile("DoS Profile") \
    enabled(false) \
    name("DoS Protect Rule")
```

ICAP-правила

Префиксы

Имя	Описание
PASS	Пропуск. Не посылать данные на ICAP-сервер.
OK	Пересылка данных на ICAP-сервер.

Действие ([Action](#)):

- [ignore](#) — игнорировать ответ от ICAP-сервера.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[url](#), [category](#), [user](#), [service](#), [http.method](#), [response.header.Content-Type](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [profile](#).

Пример

```
[dos "DoS Rules"]
% ----- 1 -----
PASS \
    scenario = "Example torrent detection scenario" \
    user = example \
    src.ip = lib.url("Microsoft Windows Internet checker") \
    dst.geoip = RW \
    service = FTP \
    rule_log(session) \
    enabled(true) \
    name("DoS Allow Rule")
% ----- 2 -----
DENY \
    desc(api_dos_rule) \
```

```
rule_log(yes, "3/h", 5) \
enabled(true) \
name("DoS Deny Rule")
% ----- 3 -----
WARNING \
user = "CN=VPN users,DC=LOCAL" \
time = lib.time("Working hours") \
profile("DoS Profile") \
enabled(false) \
name("DoS Protect Rule")
```

Правила защиты почтового трафика

Префиксы

Имя	Описание
PASS	Пропуск трафика без изменений.
DENY ("with error")	Блокировка письма, при этом сообщается об ошибке доставки письма на сервер.
DENY	Блокировка письма без уведомления о блокировке.
WARNING	Маркировка почтовых сообщений.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[user](#), [service](#), [envelope_from](#), [envelope_to](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [mark_hdr](#), [mark](#), [antispam_usergate](#), [dnsbl](#).

Пример

```
[mailsecurity "Mail Security Rules"]
% ----- 1 -----
```



```

PASS \
    user = (example, "CN=VPN users,DC=LOCAL") \
    envelope_from = "Email froup from" \
    envelope_to = "Email froup to" \
    service = SMTP \
    rule_log(yes) \
    mark_hdr(Subject) \
    enabled(true) \
    name("Mail Pass Rule")
% ----- 2 -----
DENY("with error") \
    service = (SMTPS, SMTP) \
    rule_log(yes) \
    mark_hdr(Subject) \
    antispam_usergate(yes) \
    enabled(true) \
    name("Mail Drop Rule")
% ----- 3 -----
DENY \
    src.zone = Untrusted \
    service = SMTP \
    mark_hdr(Subject) \
    dnsbl(yes) \
    enabled(false) \
    name("DNSBL spam drop rule")
% ----- 4 -----
WARNING \
    src.zone = Untrusted \
    service = (SMTP, POP3, SMTPS, POP3S) \
    mark_hdr(Subject) \
    mark("[SPAM]") \
    antispam_usergate(yes) \
    enabled(false) \
    name("SMTP and POP3 filtering")

```

Правила reverse-прокси

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[user](#), [request.header.User-Agent](#), [url.port](#).

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [profile](#),
[certificate](#), [cert_auth_enabled](#), [is_https](#), [ssl_profile](#),
[rewrite_path](#).

Пример

```
[reverseproxy "Reverse proxy Rules"]
% ----- 1 -----
OK \
    url.port = 80 \
    src.zone = Untrusted \
    desc("Example reverse proxy rule. This is an example rule which can
be changed or deleted if necessary. ") \
    profile("Example reverse proxy server") \
    rewrite_path("example.com/path1", "example.local/path1") \
    enabled(true) \
    name("Example reverse proxy rule")
```

Правила веб-безопасности

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[time](#), [user](#),

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#).

[enable_adblock](#), [safe_search](#), [search_history_logging](#), [social_sites_block](#), [enable_injector](#),

[custom_injector](#), [url_list_exclusions](#).

Пример

```
[safebrowsing "Safe browsing Rules"]
% ----- 1 -----
OK \
    rule_log(yes) \
    enable_adblock(yes) \
    safe_search(yes) \
    search_history_logging(yes) \
    social_sites_block(yes) \
    enable_injector(yes) \
    custom_injector(code) \
    url_list_exclusions(FISHING_BLACK_LIST) \
    desc("Safebrowsing rule for all users. This is an example rule
which can be changed or deleted if necessary.") \
    enabled(false) \
    name("Example safebrowsing")
```

Правила пропускной способности

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[time](#), [user application](#), [service](#), [scenario](#),

Свойства

[name](#), [desc](#), [enabled](#), [rule_log](#), [bandwidth_pool](#).

Пример

```
[shaper "Shaper Rules"]
% ----- 1 -----
OK \
    scenario = "Example torrent detection scenario" \
    service = "HTTP Proxy" \
    rule_log(session) \
    bandwidth_pool("1 Mbps") \
    enabled(true) \
    name("Example Bandwidth rule")
% ----- 2 -----
OK \
    scenario = "Example torrent detection scenario" \
    src.zone = Trusted \
    application = lib.category("Coin Miners", Business) \
    rule_log(yes, "3/h", 5) \
    bandwidth_pool("100 Kbps") \
    enabled(true) \
    name("Example torrent shaper")
```

Правила инспектирования туннелей

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.zone](#), [dst.geoip](#), [dst.ip](#).

[service](#).

Свойства

[name](#), [desc](#), [enabled](#).

Пример

```
[tunnel "Tunnel inspection Rules"]
% ----- 1 -----
PASS \
    src.zone = Trusted \
    dst.zone = Untrusted \
    service = gre \
    enabled(true) \
    name("Example Tunnel Inspection Bypass rule")
% ----- 2 -----
OK \
    dst.geoip = YE \
    service = gtpu \
    enabled(true) \
    name("Example Tunnel Inspection Rule")
```

Правила веб-портала

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[url](#), [user](#), [url.domain](#).

Свойства

[name](#), [desc](#), [enabled](#).

[icon](#), [ssl_profile](#), [certificate](#), [additional_url](#), [rdp_check_session_alive](#), [transparent_auth](#).

Пример

```
[webportal "Web portal Rules"]
% ----- 1 -----
OK \
    user = "CN=Default Group,DC=LOCAL" \
    url = "http://www.intranet.loc" \
    icon("default.svg") \
    rdp_check_session_alive(yes) \
    transparent_auth(yes) \
    certificate("CA (Default)") \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example http application published via web portal")
```

Правила VPN-сервера

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[dst.geoip](#), [dst.ip](#).

[user](#),

Свойства

[name](#), [desc](#), [enabled](#).

[profile](#), [auth_profile](#), [vpn_network](#), [interface](#).

Пример

```
[vpn_server "VPN server Rules"]
% ----- 1 -----
OK \
    user = "CN=VPN users,DC=LOCAL" \
    src.zone = Untrusted \
    profile("Remote access VPN profile") \
    auth_profile("Example user auth profile") \
    vpn_network("Remote access VPN network") \
    interface(tunnel1) \
    enabled(false) \
    name("Remote access VPN rule")
```

Правила VPN-клиента

Префиксы

Имя	Описание
OK	Всегда ОК.

Свойства

[name](#), [desc](#), [enabled](#).

[profile](#), [interface](#), [server_address](#).

[last_error](#), [status](#) — информационное поле, недоступное для редактирования.

Пример

```
[vpn_client "VPN client Rules"]
% ----- 1 -----
OK \
  server_address("10.10.10.10") \
  last_error(Disabled) \
  status(disconnected) \
  profile("Client VPN profile") \
  interface(tunnel3) \
  enabled(true) \
  name("Client VPN rule")
```

Правила сценариев

Префиксы

Имя	Описание
OK	Всегда ОК.

Условия

[scenario_cond](#).

Свойства

[name](#), [desc](#), [enabled](#).

[operation_mode](#), [trigger](#), [duration](#).

Условия сценария

Категория URL ([url_category](#))

Условия

[category](#)

Свойства

[count_interval](#), [max_event_count](#), [scond_type](#)

Обнаружение вируса (virus_detection)

Свойства

[scond_type](#)

Приложение (app)

Условия

[application](#)

Свойства

[count_interval](#), [max_event_count](#), [scond_type](#)

COB (ips)

Свойства

[ips_tl](#), [scond_type](#)

Тип контента (mime_type)

Условия

[response.header.Content-Type](#)

Свойства

[count_interval](#), [max_event_count](#), [scond_type](#)

Размер пакета (net_packet_size)

Свойства

[packet_size](#), [scond_type](#)

Сессий с одного IP (sessions_per_ip)**Свойства**[sessions_limit](#), [scond_type](#)**Объем трафика (traffic)****Свойства**[traffic_limit](#), [period](#), [scond_type](#)**Проверка состояния (health_check)****Условия**[url.address](#), [url.domain](#)**Свойства**[health_check_method](#), [health_result](#), [health_request_timeout](#), [health_type_request](#),
[health_answer_timeout](#), [count_interval](#), [max_event_count](#), [scond_type](#)**Пример**

```
[scenarios "Scenario Rules"]
% ----- 1 -----
def scenario_cond example_scenario_define
    category = (lib.category(Threats), "Advertisements & Pop-Ups")
    count_interval(10) max_event_count(3) scond_type(url_category)
    scond_type(virus_detection)
    application = lib.category(Threats) count_interval(2)
    max_event_count(1) scond_type(app)
    ips_tl(medium) scond_type(ips)
    response.header.Content-Type = lib.mime("Java script")
    count_interval(0) max_event_count(0) scond_type(mime_type)
    packet_size(200MB) scond_type(net_packet_size)
    sessions_limit(50) scond_type(sessions_per_ip)
    traffic_limit(2GB) period(hour) scond_type(traffic)
    url.address = "192.168.100.100" url.domain = "example.com"
```

```
health_check_method(dns) \  
    health_result(negative) health_request_timeout(4)  
health_type_request(a) \  
    count_interval(5) max_event_count(3) scond_type(health_check)  
    url.domain = "example.com" health_check_method(get) \  
    health_result(negative) health_request_timeout(5)  
health_answer_timeout(10) \  
    count_interval(0) max_event_count(0) scond_type(health_check)  
end  
OK \  
    scenario_cond = example_scenario_define \  
    operation_mode(all) \  
    trigger(one_user) \  
    duration(5) \  
    enabled(false) \  
    name("Example torrent detection scenario")
```

Правила балансировки нагрузки TCP/UDP

Префиксы

Имя		Описание	
OK		Всегда ОК.	

Условия

[src.zone](#), [src.geoip](#), [src.ip](#), [src.mac](#).

[service](#), [url.address](#), [url.port](#).

Свойства

[name](#), [desc](#), [enabled](#).

[scheduler](#), [real_server](#), [ipvs_fallback](#)

[monitor_kind](#), [monitor_service](#), [monitor_request](#), [monitor_response](#), [monitor_interval](#),

[monitor_timeout](#), [monitor_failurecount](#)

Пример

```
[ipvs_server "TCP/UDP load balancing Rules"]
% ----- 1 -----
OK \
    src.geoip = RW \
    url.address = 192.168.1.100 \
    url.port = 80 \
    service = tcp \
    scheduler(rr) \
    real_server(gate, 1.1.1.1:80, 50) \
    ipvs_fallback(masq_snat, 8.8.8.8:10000) \
    monitor_kind(negotiate) \
    monitor_service(http) \
    monitor_request("example.com") \
    monitor_interval(60) \
    monitor_timeout(60) \
    monitor_failurecount(10) \
    enabled(true) \
    name("TCP load balancing")
```

Правила балансировки ICAP

Префиксы

Имя	Описание
OK	Всегда ОК.

Свойства

[name](#), [desc](#), [enabled](#), [profile](#).

Пример

```
[icap_balancing "ICAP load balancing Rules"]
% ----- 1 -----
OK \
    profile("Example ICAP server") \
```

```
enabled(true) \  
name("ICAP load balancing")
```

Правила балансировки reverse-прокси

Префиксы

Имя	Описание
OK	Всегда OK.

Свойства

[name](#), [desc](#), [enabled](#), [profile](#).

Пример

```
[reverseproxy_balancing "Reverse proxy load balancing Rules"]  
% ----- 1 -----  
OK \  
    profile("Example reverse proxy server") \  
    enabled(true) \  
    name("Reverse-proxy load balancing")
```

Список поддерживаемых HTTP-заголовков

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Accept	Request	✓	✓	✓
Accept-Charset	Request	✓	✓	✓
Accept-Encoding	Request	✓	✓	✓
Accept-Language	Request	✓	✓	✓
Accept-Ranges	Response	✓	✓	✓
Age	Response			

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Allow	Request/ Response	✓	✓	✓
Authorization	Request			
Cache-Control	Request/ Response	✓	✓	✓
Client-IP	Request	✓	✓	
Connection	Request/ Response		✓	
Content-Encoding	Request/ Response		✓	
Content-Language	Request/ Response		✓	
Content-Length	Request/ Response			
Content-Location	Request/ Response		✓	✓
Content-Range	Request/ Response			
Content-Type	Request/ Response			
Cookie	Request	✓	✓	✓
Date	Request/ Response			
ETag	Response	✓	✓	
Expect	Request	✓		
Expires	Request/ Response		✓	✓
From	Request	✓	✓	
Host	Request			

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
If-Match	Request	✓		
If-Modified-Since	Request			
If-None-Match	Request	✓		
If-Range	Request			
If-Unmodified-Since	Request			
Last-Modified	Request/ Response			
Location	Response	✓	✓	
Max-Forwards	Request			
Meter	Request/ Response		✓	✓
Pragma	Request/ Response		✓	✓
Proxy-Authenticate	Response	✓		
Proxy-Authorization	Request	✓		
Proxy-Connection	Request	✓		
Range	Request	✓	✓	
Referer	Request	✓	✓	
Retry-After	Response	✓	✓	
Server	Response	✓	✓	
Set-Cookie	Response	✓	✓	✓
TE	Request	✓		
Trailer	Request/ Response		✓	

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Transfer-Encoding	Request/ Response		✓	
Upgrade	Request/ Response		✓	
User-Agent	Request	✓	✓	
Vary	Response	✓	✓	✓
Via	Request/ Response	✓	✓	✓
Warning	Request/ Response	✓	✓	✓
WWW-Authenticate	Response			

ДАШБОРД

Работа с дашбордами и виджетами

В UserGate NGFW можно отслеживать текущее состояние устройства, объемы трафика, проходящего через него, статус лицензии и различные статистические данные, связанные с сетевой безопасностью. Эти данные представлены в виде виджетов на странице **Дашборды**. Вы можете настраивать виджеты в соответствии с вашими требованиями.



Примечание

Просмотр и изменение дашбордов доступны, если в профиле доступа вашей учетной записи настроены соответствующие разрешения.

Вы можете добавлять новые дашборды, переименовывать их и удалять, выбирать нужные виджеты из поставляемых с продуктом коллекций, изменять состав виджетов на дашбордах, их расположение и размер. По умолчанию

созданы дашборды с виджетами NOC (Network Operation Center) и SOC (Security Operation Center).

В зависимости от типа данных виджеты поделены на три коллекции:

- **Центр управления сетью;**
- **Центр управления безопасностью;**
- **Группа VPN.**

В виджетах из коллекций **Центр управления безопасностью** и **Группа VPN** в графическом виде представлены данные из журналов UserGate NGFW. Поэтому, чтобы данные отображались в виджете, необходимо настроить соответствующие правила и включить для них журналирование событий. Например, если настроена сеть VPN и ведется запись соответствующих событий, вы сможете отслеживать статистику по виджетам из коллекции **Группа VPN**.

По умолчанию в виджете отображаются данные за последний час. Вы можете изменить период для каждого из виджетов, выбрав предустановленный вариант в верхней правой части виджета. В виджетах с графиками также можно выделить часть периода, чтобы подробнее ознакомиться с определенной частью графика. Возвращение к исходному масштабу выполняется по двойному нажатию левой кнопкой мыши.

Настройка виджета

Для некоторых виджетов вы можете фильтровать данные и настраивать способ их отображения. Если настройка доступна, в правом верхнем углу виджета отображается значок шестеренки.

Чтобы настроить виджет:

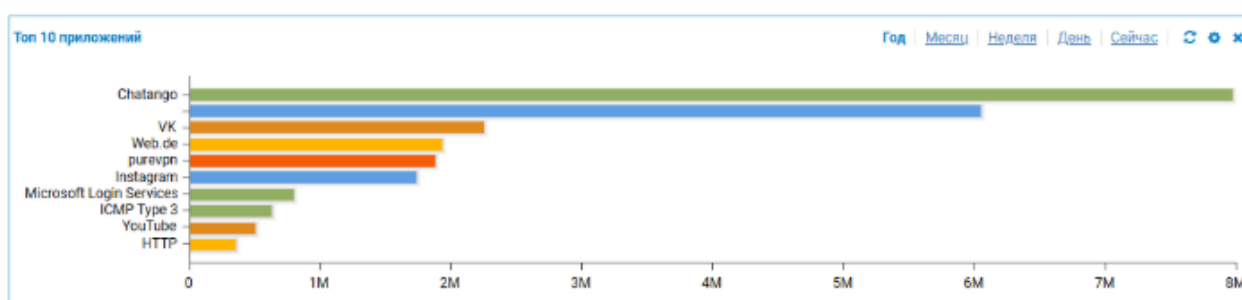
1. Нажмите на значок шестеренки в правом верхнем углу нужного виджета.
2. В окне **Настройка виджета** выполните одно или несколько действий (в зависимости от типа виджета набор параметров может отличаться):
 - измените название виджета;
 - укажите максимальное количество записей, которые будут отображаться в виджете;
 - выберите, по какому значению будут сгруппированы данные в виджете;

- выберите, в виде какой диаграммы или таблицы будут представлены данные;
- с помощью SQL-запроса настройте фильтрацию данных, отображаемых в виджете;
- добавьте описание виджета.

1. Нажмите **Сохранить**.

Пример фильтрации данных в виджете

На дашборд добавлен виджет **Топ-10 приложений**, в котором по умолчанию представлены разные приложения, в том числе не представляющие угрозы.



Чтобы по виджету можно было отслеживать только опасные приложения, необходимо в окне **Настройка виджета** в поле **Запрос фильтра** настроить дополнительную фильтрацию данных с помощью SQL-запроса.

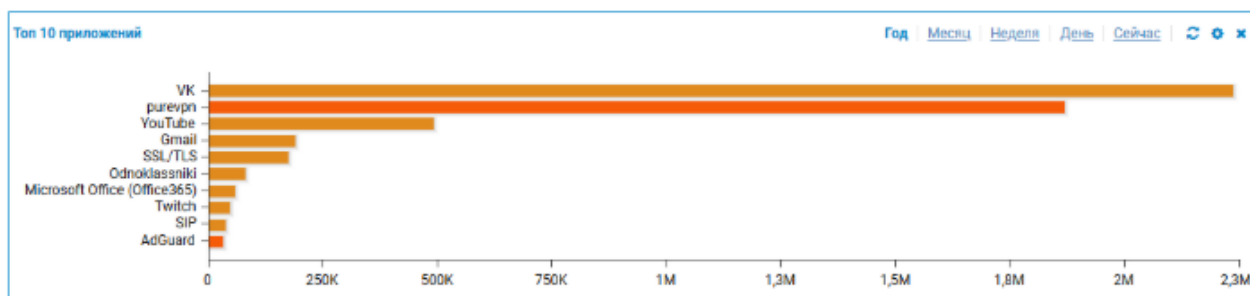
В SQL-запросах используется тот же синтаксис, что и в журналах для поиска и фильтрации данных. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации «[Поиск и фильтрация данных](#)». Значения параметров собираются из событий в журнале.

При вводе запроса в поле отображается список доступных операторов, параметров и их значений, из которых можно сформировать нужный запрос.

Запрос на фильтрацию опасных и очень опасных приложений выглядит следующим образом:

```
applicationThreat in (high, 'very high')
```

После завершения настройки и обновления данных в виджете будут представлены только опасные и очень опасные приложения.



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Раздел технической поддержки

Раздел технической поддержки [на сайте компании](#) содержит дополнительную информацию по настройке устройства. Здесь же вы можете оставить заявку на решение возникшей проблемы с оборудованием.

Аварийные ситуации

Сбои в работе устройства могут возникнуть при некорректной установке обновлений программного обеспечения.

Для профилактики аварийных ситуаций:

1. Перед установкой обновления сделайте резервную копию устройства. Подробнее — в разделе «[Управление резервным копированием](#)».
2. Во время установки обновления создайте [точку восстановления системы](#). Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении устройства:

1. Восстановите предыдущую стабильную версию ПО. Подробнее — в разделе «[Обновление ПО](#)».
2. Обратитесь в службу технической поддержки в зависимости от уровня вашего сервисного контракта:
 - Premium-поддержка: позвоните по выделенному телефону для экстренной помощи.
 - Brilliant-поддержка: свяжитесь с вашим выделенным техническим специалистом.
 - Базовая поддержка: обратитесь за квалифицированной помощью [на странице поддержки](#).

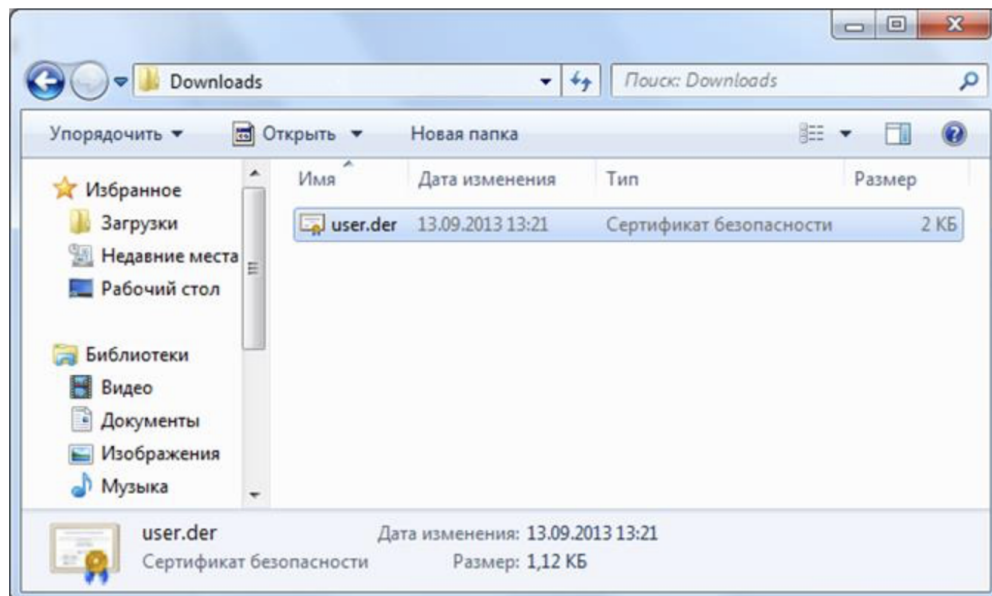
ПРИЛОЖЕНИЯ

Установка сертификата локального удостоверяющего центра

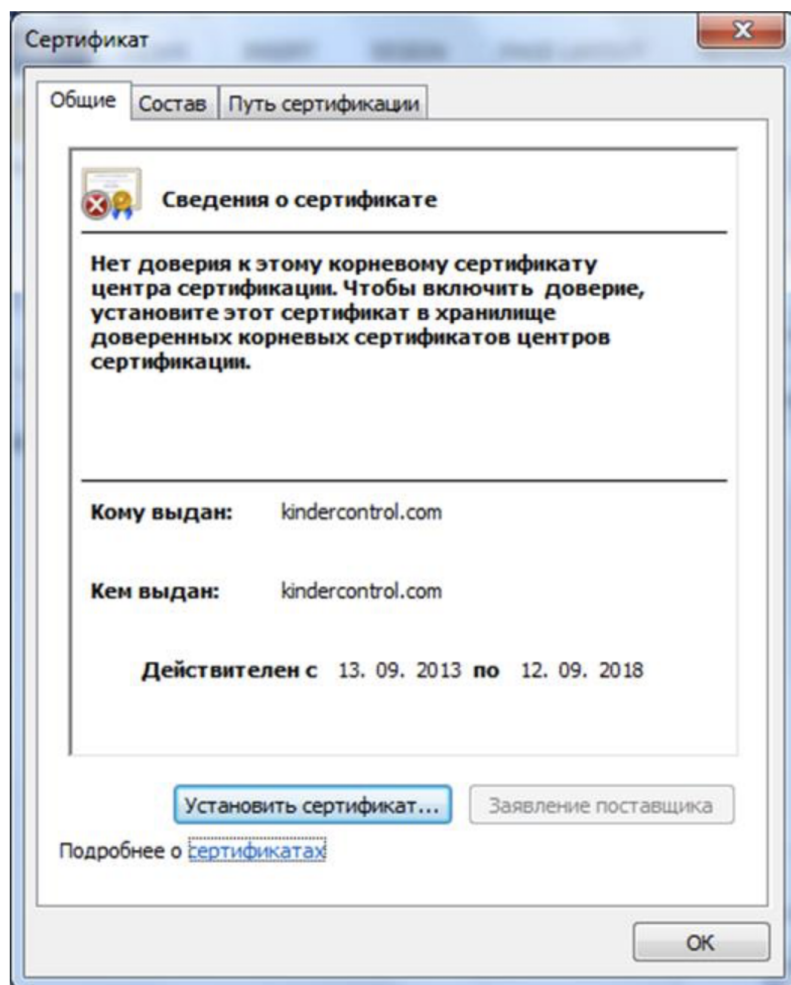
Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

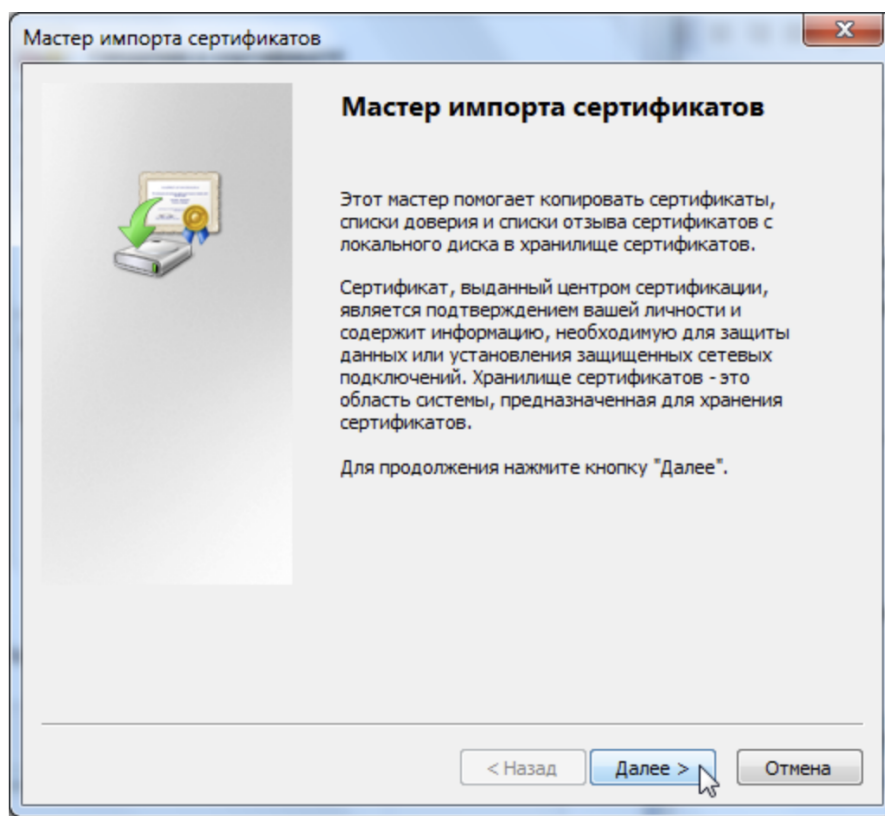
Откройте папку, куда вы скачали рет-сертификат, переименуйте его в `user.der` и дважды нажмите на него:



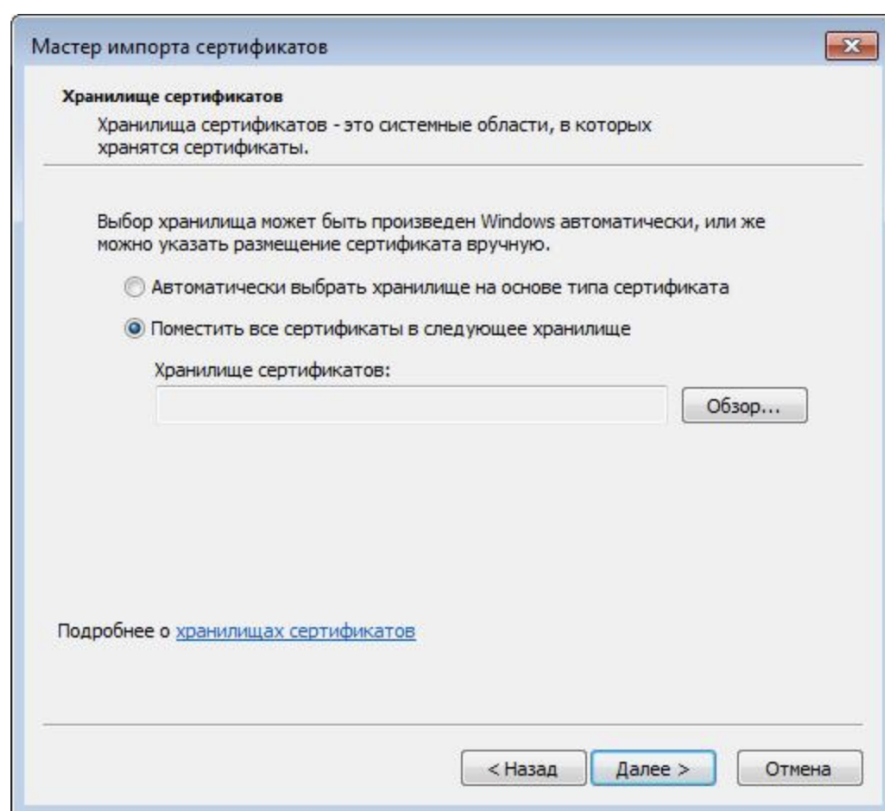
Откроется информация о сертификате. Нажмите **Установить сертификат**:



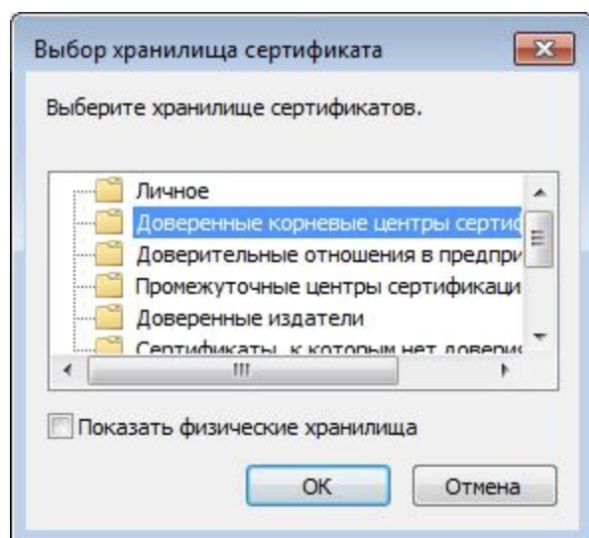
Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:



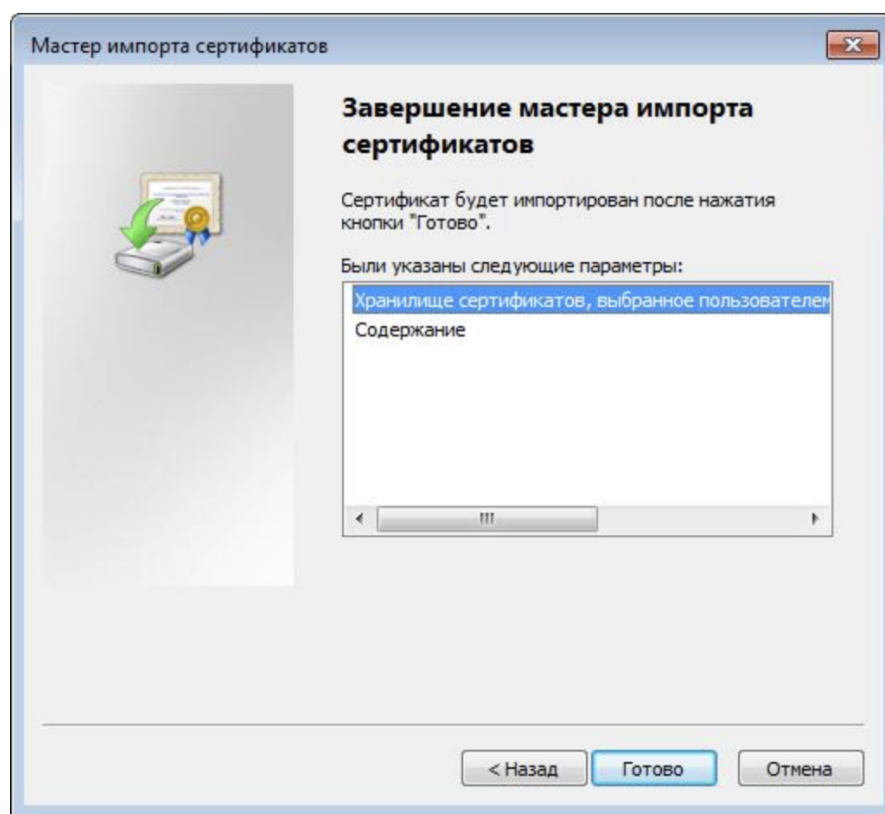
Выберите хранилище сертификата и нажмите **Обзор**:



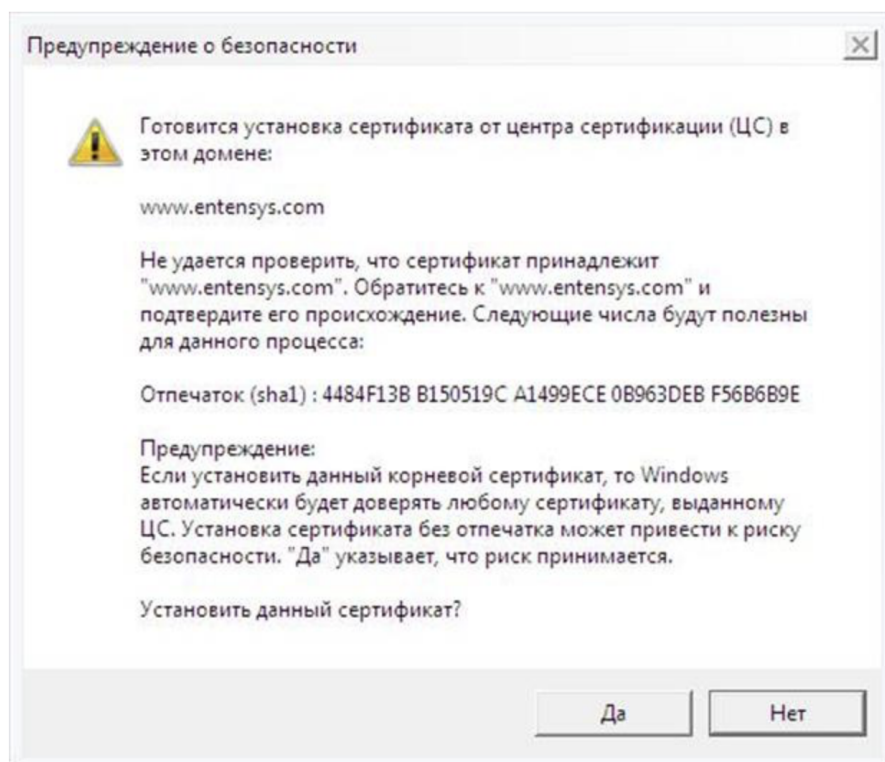
Выберите **Доверенные корневые центры сертификации** и нажмите **ОК**:



Нажмите **Готово**:



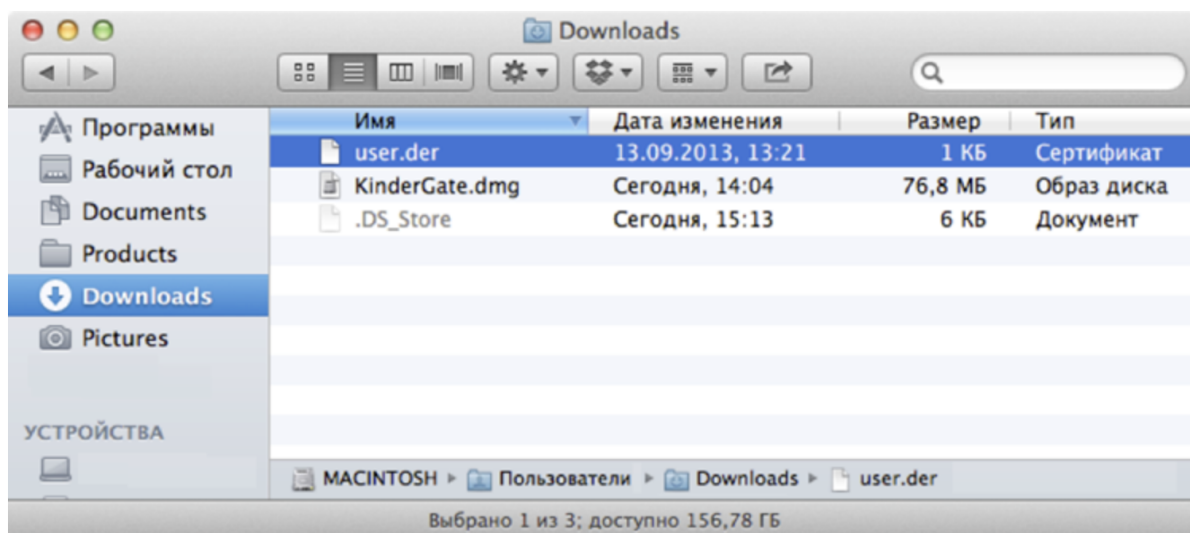
Когда появится предупреждение системы безопасности, нажмите **Да**:



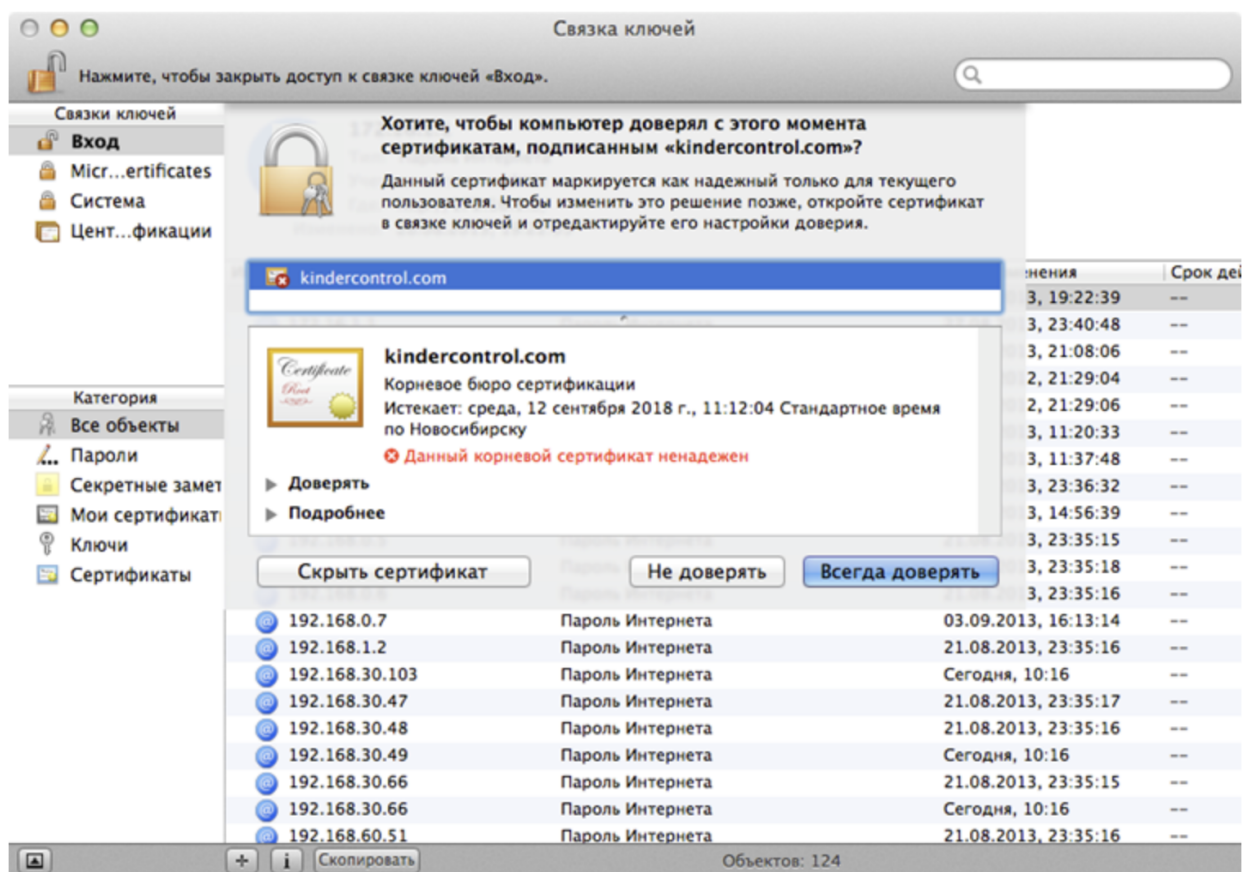
Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в ОС MacOSX

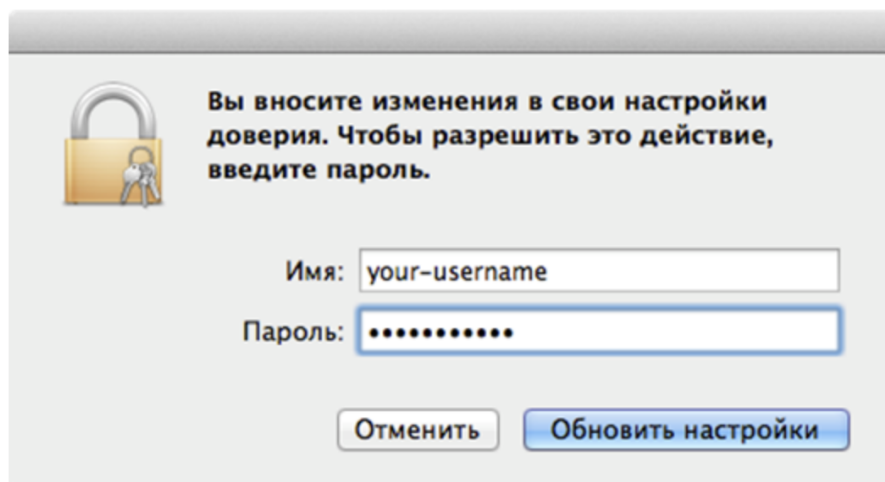
Перейдите в папку, куда вы скачали рет-сертификат и дважды нажмите на него:



Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:



Введите свой пароль для подтверждения данной операции:

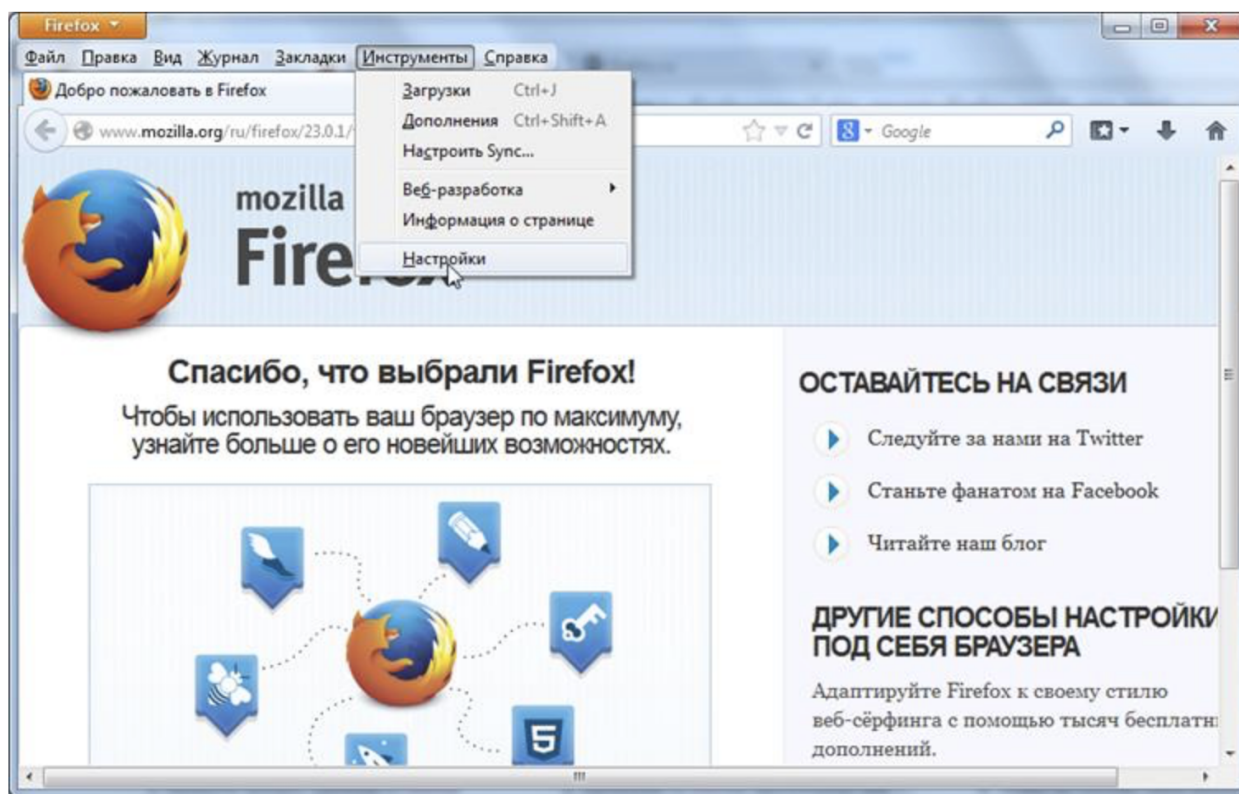


Сертификат установлен.

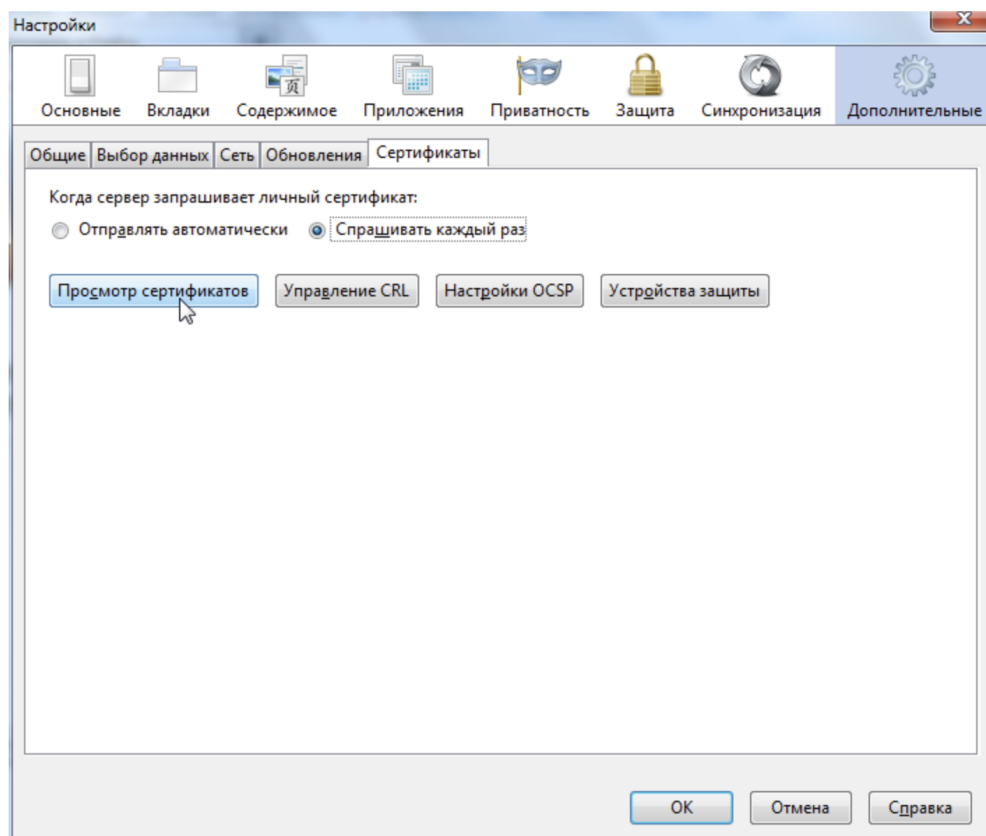
Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется одинаково для всех операционных систем. Рассмотрим установку на примере ОС Windows.

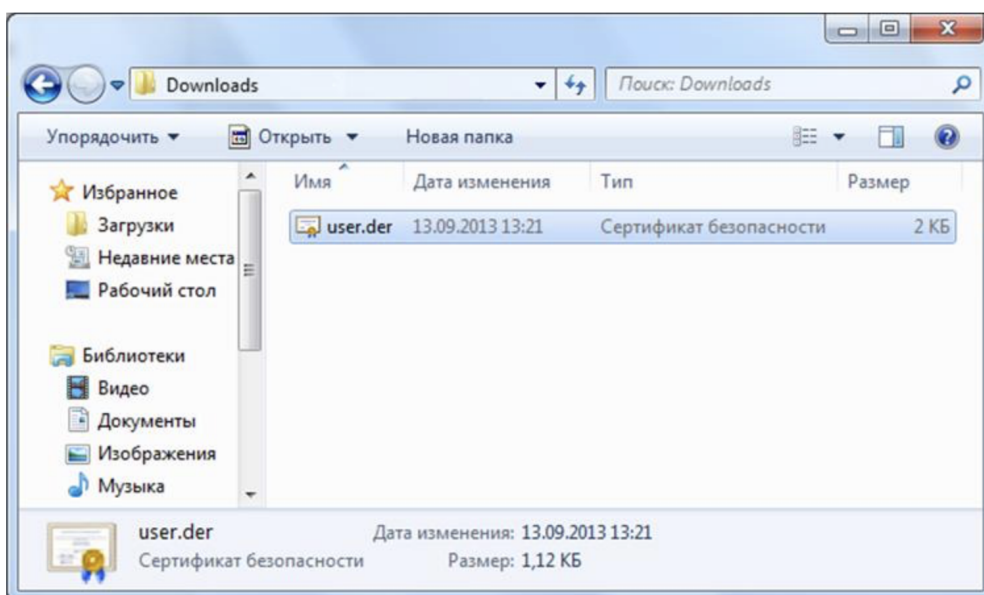
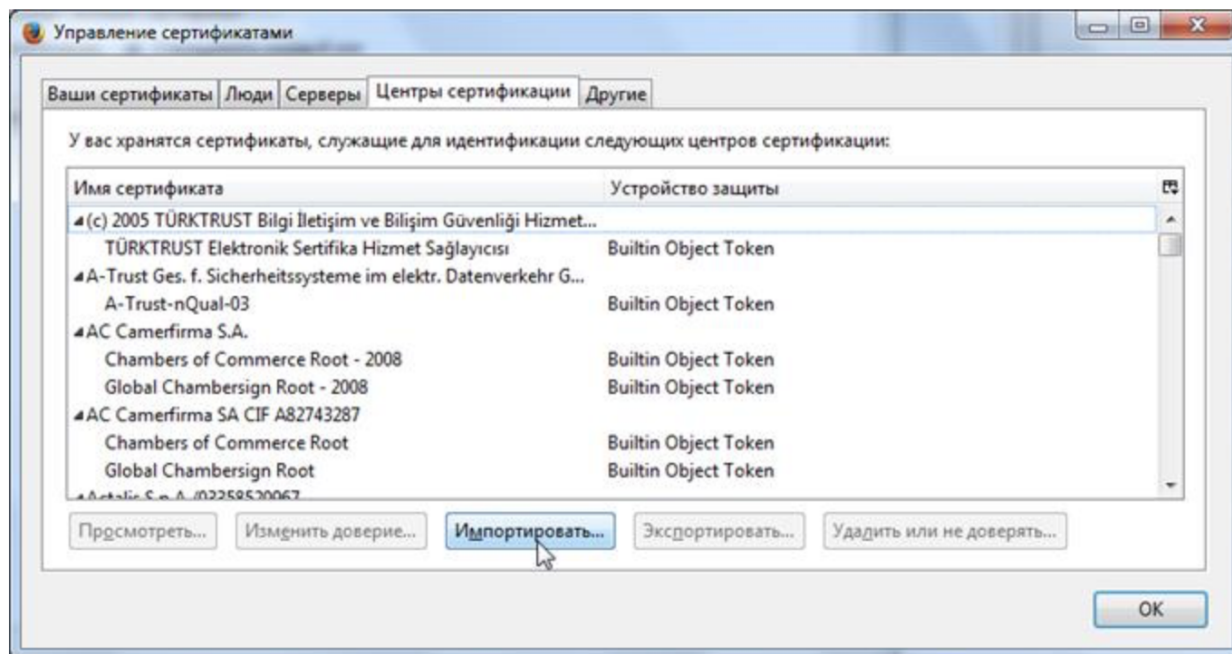
Откройте настройки браузера Firefox (**Инструменты** → **Настройки**):



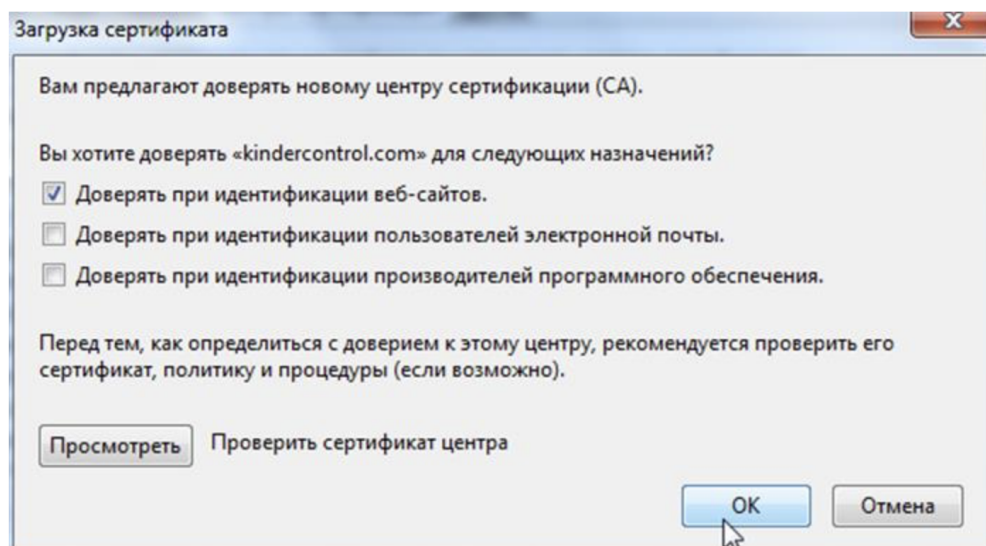
Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**.
Нажмите **Просмотр сертификатов**:



Нажмите **Импортировать** и укажите путь к скачанному рет-сертификату:



Установите флажок **Доверять при идентификации веб-сайтов** и нажмите **ОК**:



Установка сертификата завершена.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Криптомайнеры
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
	Мода и красота
	Отдых и оздоровление
	Рестораны и еда
	Спорт
	Путешествия
Здоровье и медицина	Здоровье и медицина
	Половое воспитание
Злоупотребление свободой СМИ - информация с ограниченным доступом. Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций	Оружие
Злоупотребление свободой СМИ - информация, содержащая скрытые вставки и иные технические способы воздействия на под-104Nº п/п Тематическая категория Содержание скрытое воздействие сознание людей и (или) оказывающая вредное влияние на их здоровье	Сайты сомнительного содержания
Злоупотребление свободой СМИ - наркотические средства, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и	Ненависть и нетерпимость

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Насилие
Злоупотребление свободой СМИ - экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпимость
	Насилие
Знакомства	Знакомства
Информация с ограниченным доступом. Информация, составляющая государственную или иную охраняемую законом тайну	Политика
	Правительство
Информация, пропагандирующая порнографию	Порнография и насилие
Компьютерные игры	Игры
Корпоративные сайты	Бизнес
	Финансы
	Общие
	Недвижимость
Корпоративные сайты, интернет- представительства	Некоммерческие и неправительственные организации

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
негосударственных учреждений	
Личная и немодерируемая информация. Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги	Персональные сайты
	Частные IP-адреса
	Социальные сети
	Потоковое мультимедиа и загрузки
	Веб-почта
Модерируемые доски объявлений (ресурсы данной категории, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты	Социальные сети
	Чаты
Наркотические средства. Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Наркотики
Нелегальная помощь школьникам и студентам. Банки готовых рефератов, эссе, дипломных работ и пр.	Школьные мошенничества

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной продукции и табачных изделий	Алкоголь и табак
Неприличный и грубый юмор. Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека	Сайты сомнительного содержания
Нижнее белье, купальники	Нудизм
Обеспечение анонимности пользователя, обход контентных фильтров. Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам	Анонимайзеры
	Переводчики
Образовательные ресурсы	Образование
Онлайн-казино и тотализаторы	Азартные игры
Отправка SMS с использованием интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS- сообщений	Реклама и всплывающие окна
Платные сайты	Паркованные домены
Поиск работы, резюме, вакансии	Поиск работы
Преступления - Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или	Преступная деятельность

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
подрывающих его репутацию)	
Преступления-клевета, экстремизм	Преступная деятельность
Программное обеспечение	Компьютеры и технологии
	Нелегальное ПО
	Информационная безопасность
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение	Ненависть и нетерпимость
Религии и атеизм	Религиозные культы
	Религия
Система поиска изображений	Обмен картинками
	Поисковые системы и порталы
СМИ	Форумы и новостные ленты
	Новости
Табак, реклама табака, пропаганда потребления табака. Сайты,	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
пропагандирующие потребление табака; реклама табака и изделий из него	
Торговля и реклама	Реклама и всплывающие окна
	Покупки
Убийства, насилие	Жестокое обращение с детьми
	Насилие
Чаты	Чаты
	Сервисы мгновенных сообщений
Экстремистские материалы или экстремистская деятельность (экстремизм)	Ненависть и нетерпимость

Требования к сетевому окружению

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб- консоли UserGate NGFW)	Доступ к веб- интерфейсу управления устройством .
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API.
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS. Доступен в версии 7.3.3 и выше.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверам технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)/ Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного времени)	Синхронизация времени.
DNS	TCP/UDP	53	Входящий (от клиентов к серверу)	Сервис получения информации

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			UserGate, если он выступает в качестве DNS-сервера)	(IP-адрес) о доменах.
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
		9000-9100	Входящий (приём конфигураци и от первого узла кластера)	Передача информации об изменении конфигураци и кластера (реплика настроек)
Связь с UserGate Management Center	TCP	9712	Исходящий (от UG NGFW до UGMC)	Первоначаль ная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG NGFW до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Связь с UserGate Log Analyzer	TCP	9713	Входящий (от LogAn к UG NGFW)	Первоначаль ная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer.
		2023	Входящий (от LogAn к UG NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
	TCP	Для версий 6.1.x: 1269 (передача данных на LogAn 6.1.x), 22699 (передача данных на LogAn 7.x.x) Для версий 7.0.x: 22699 (передача данных на LogAn 6.1.x), 22711 (передача данных на LogAn 7.x.x, с использованием SSL)	Исходящий (от UG NGFW к LogAn)	Передача журналов и телеметрии на сервер LogAn.
Подключение конечных устройств с установленным ПО UserGate Client (доступно начиная с версии 7.1.0)	TCP	4045	Входящий (от конечного устройства на UG NGFW)	Подключение конечных устройств и приём телеметрии для проверки комплаенса.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 – для LDAP и 636 – для LDAP over SSL).
Captive-портал и страница блокировки	TCP	443, 8043	Входящий (от браузера клиента на UG NGFW)	Отображение страницы авторизации Captive-портала и страницы блокировки.
Kerberos	TCP/UDP	88	Исходящий (на сервер)	Аутентификация

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			аутентификации (Kerberos)	пользователю по протоколу Kerberos.
NTLM	TCP	445	Исходящий (на сервер аутентификации NTLM)	Аутентификация пользователей по протоколу NTLM.
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
Агент терминального сервиса	UDP	1812, 1813	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Прокси-агент	UDP	8090	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимы для работы прокси-агента, предоставляющего доступ в Интернет пользователям, работающим на ОС Windows.
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
ICAP	TCP	1344	Исходящий (до серверов ICAP)	Сервис работы с серверами ICAP.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)/ Входящий (UserGate выступает в качестве DHCP-сервера)	Сервис службы DHCP.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
BGP	TCP	179	Исходящий (передача информации соседним BGP-маршрутизаторам)/ Входящий (получение информации от соседних BGP-маршрутизаторов)	Сервис динамическо й маршрутиза ции BGP.
OSPF	89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам / Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамическо й маршрутиза ции OSPF.
RIP	UDP	520	Исходящий (распростра нение соседним маршрутизат орам RIP-маршрутов)/ Входящий (получение от соседних маршрутизат оров RIP-маршрутов)	Сервис динамическо й маршрутиза ции RIP.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

Опции DHCP

Формат значений опций соответствует [RFC 2132](#).

Наименование	Описание
1	Маска подсети, из которой был получен адрес.
2	Разница во времени в подсети клиента относительно UTC (указывается в секундах).
3	Список IP-адресов доступных шлюзов.
6	Список DNS-серверов.
7	Список лог-серверов (MIT-LCS UDP).
9	Список LPR-серверов (RFC 1179).
13	Размер загрузочного образа для клиентов.
15	Имя домена.
16	Swap-сервер.
17	Путь корневого каталога для клиента.
18	Путь расширений BOOTP.
19	Применение пересылки IP-датаграмм.
20	Использование маршрутизации удаленного источника.

Наименование	Описание
21	Политика фильтрации IP-адресов.
22	Максимальный размер датаграммы.
23	Значение TTL для IP по умолчанию.
26	Значение MTU для данного интерфейса.
27	Признак, что все подсети используют текущую конфигурацию MTU.
31	Определение использования сообщений ICMP для обнаружения маршрутизаторов.
32	Адрес, который используется для обращения к маршрутизатору.
33	Статичный список маршрутизации; состоит из пар «адрес назначения» — «адрес роутера».
34	Использование концевиков (trailers) при запросах ARP.
35	Тайм-аут кэш-памяти ARP.
36	Необходимость использования инкапсуляции данных Ethernet.
37	Значение TTL для TCP-пакетов.
38	Интервал отправки контрольных пакетов TCP (TCP keep-alive).
40	Домен NIS.
41	Список серверов NIS.
42	Список серверов времени NTP.
44	Список IP-адресов серверов NetBIOS.
45	Список IP-адресов серверов рассылки датаграмм NetBIOS.
46	Тип узла NetBIOS.
47	Область NetBIOS.

Наименование	Описание
48	IP-адреса серверов шрифтов X Windows (X Window System Font).
49	Диспетчер дисплея X Windows.
58	Время T1 — интервал времени, в течение которого клиент должен отправить запрос на обновление IP-адреса.
59	Время T2 — интервал времени (в секундах), в течение которого клиент должен отправить запрос на повторное связывание.
60	Опция используется клиентом DHCP для указания поставщика.
64	Имя домена NIS+.
65	Список серверов NIS+.
66	Имя сервера TFTP.
67	Название загрузочного файла.
68	Адреса домашних агентов (Mobile IP Home Agent).
69	Список серверов SMTP.
70	Список серверов POP3.
71	Список серверов NNTP.
74	Список серверов IRC.
77	Класс пользователя.
80	Опция позволяет получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
93	Архитектура системы клиента DHCP.
94	Идентификатор сетевого интерфейса клиента DHCP.
97	Идентификатор клиента на основе UUID/GUID.
119	Список поиска DNS.

Наименование	Описание
120	Список серверов SIP.
121	Список бесклассовых статических маршрутов.
125	Указание информации о поставщике.
255	Конец списка опций; обязательно должен присутствовать последним.

Примеры генерации сертификатов для IKEv2 VPN

Генерация сертификатов на Linux с использованием OpenSSL

Пример генерации сертификатов в ОС Linux с помощью библиотеки OpenSSL на основе самоподписанного корневого сертификата.

Действия на стороне VPN-сервера

1. Создать самоподписанный корневой сертификат rootCA.

```
$ openssl genrsa -aes256 -passout pass:1234 -out rootCA.key 4096

$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out
rootCA.pem -subj "/C=RU/ST=Sib/L=Nsk/O=ep.local/OU=ep.local/CN=QA"
```

где rootCA.pem — это корневой сертификат.

Проверить, что сертификат корневой (в выводе должна быть строка: CA:TRUE):

```
$ openssl x509 -in rootCA.pem -text
```

2. На основе корневого сертификата создать сертификат для VPN-сервера.

- Требования — **key usage: server auth**;
- Указать subjectAltName соответствующее DNS-имени VPN-сервера.

```
$ openssl genrsa -aes256 -passout pass:1234 -out server.pass.key 4096

$ openssl rsa -passin pass:1234 -in server.pass.key -out server-key.pem
```

где server-key.pem — это приватный ключ.

Для генерации запроса на выпуск сертификата создать файл openssl-server.cnf с данными для запроса сертификата. **Пример** заполненного данными файла:

```
[ req ]
prompt = no
days = 365
req_extensions = v3_req
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
C = Ru
ST = Sib
L = Nsk
O = ep.local
OU = ep.local
CN = vpnserver.ep.local #dns name vpn-сервера
emailAddress = mail1@ep.local

[ v3_req ]
keyUsage = critical, digitalSignature
extendedKeyUsage = serverAuth
subjectAltName = @sans

[ sans ]
DNS.0 = vpnserver.ep.local # dns name vpn-сервера
```

Создать запрос на выпуск сертификата с учетом данных из созданного выше файла openssl-server.cnf. На этом этапе прописывается секция Subject сертификата:


```
$ openssl req -new -key server-key.pem -out server.csr -config openssl-
server.cnf
```

Подписать запрос корневым сертификатом. На этом этапе прописывается секция X509v3 extensions сертификата:

```
$ openssl x509 -CAcreateserial -req -extfile openssl-server.cnf -
extensions v3_req -days 365 -in server.csr -CA rootCA.pem -CAkey
rootCA.key -out server-cert.pem
```

где server-cert.pem — это сертификат VPN-сервера.

3. Импортировать сертификат VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера (server-cert.pem) и приватного ключа (server-key.pem).

4. Импортировать корневой сертификат в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированный файл самоподписанного корневого сертификата (rootCA.pem) без указания приватного ключа.

5. Создать профиль клиентских сертификатов в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле для авторизации **Common-name** или **Subject alt name** для получения имени пользователя.

6. На этапе настройки VPN будет необходимо создать профиль безопасности VPN. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля безопасности VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера необходимо перейти в раздел **VPN** → **Серверные профили безопасности** и нажать кнопку **Добавить**. В открывшемся окне указать необходимые параметры профиля безопасности (подробнее смотрите в разделе [Настройка VPN](#)). При использовании протокола IKEv2 для организации

VPN необходимо указать импортированный в пункте 3 сертификат VPN-сервера и профиль пользовательского сертификата, созданного в пункте 5, если в качестве режима аутентификации будет указан PKI.

Действия на стороне VPN-клиента

1. Создать сертификат для VPN-клиента.

Для генерации запроса на выпуск сертификата для VPN-клиента создать файл `openssl-client.cnf` с данными для запроса сертификата. **Пример** заполненного данными файла.

```
[ req ]
prompt          = no
days           = 365
req_extensions  = v3_req
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
C               = Ru           #              необязательный параметр
ST             = Sib          #              необязательный параметр
L             = Nsk           #              необязательный параметр
O             = ep.local      # имя домена, необязательный параметр
OU            = ep.local      # имя домена, необязательный параметр
CN            = user1@ep.local #Обязательный.
Идентификатор пользователя, которому выдан сертификат

[ v3_req ]
keyUsage        = critical, digitalSignature
extendedKeyUsage = clientAuth
subjectAltName   = email:user1@ep.local # Пользователь, под учетной
записью которого будет выполняться подключение к VPN-серверу.
```

Пример файла `openssl-client.cnf` с запросом на выпуск сертификата, когда VPN-пользователь добавлен локально на UG NGFW (без домена).

```
[ req ]
prompt          = no
days           = 365
req_extensions  = v3_req
```

```
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
C                = Ru                #                необязательный параметр
ST               = Sib               #                необязательный параметр
L               = Nsk                #                необязательный параметр
O               = ep.local           # имя домена, необязательный параметр
OU              = ep.local           # имя домена, необязательный параметр
CN              = user1              # обязательный. Идентификатор
пользователя, которому выдан сертификат

[ v3_req ]
keyUsage          = critical, digitalSignature
extendedKeyUsage  = clientAuth
subjectAltName    = otherName:msUPN;UTF8:user1
```

Где `user1` — логин учетной записи пользователя, созданной в UG NGFW.
 Подробнее о создании локальных учетных записей — в разделе «[Пользователи и группы](#)».



Примечание

Для каждого пользователя необходимо выпускать свой сертификат, изменяя файл `openssl-client.cnf`.

Поле `subjectAltName` используется, если в профиле клиентского сертификата поле для получения имени пользователя будет указано, как **Subject alt name**.

Сгенерировать приватный ключ для VPN-клиента:

```
$ openssl genrsa -aes256 -passout pass:1234 -out client.pass.key 4096

$ openssl rsa -passin pass:1234 -in client.pass.key -out client-key.pem
```

Создать запрос на выпуск сертификата с учетом данных из созданного выше файла `openssl-client.cnf` и подписать его корневым сертификатом:

```
$ openssl req -new -key client-key.pem -out client.csr -config openssl-
client.cnf
```

```
$ openssl x509 -CAcreateserial -req -extfile openssl-client.cnf -
extensions v3_req -days 365 -in client.csr -CA rootCA.pem -CAkey
rootCA.key -out client-cert.crt
```

3. Для использования в клиентах с ОС Windows в сценарии Remote Access VPN создать файл client.pfx, содержащий закрытый ключ и сертификат пользователя. Файл загружается в Windows и используется для подключения к VPN.

```
$ openssl pkcs12 -export -passout pass:1234 -out client.pfx -inkey
client-key.pem -in client-cert.crt
```

4. Файл client.pfx импортировать в Windows и расположить в разделе **Локальный компьютер**, хранилище — **Личное**.

5. Для использования клиентского сертификата на стороне узла — VPN-клиента в сценарии Site-to-Site VPN с IKEv2 необходимо импортировать созданный сертификат VPN-клиента. Для этого в консоли администратора NGFW, исполняющего роль VPN-клиента перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-клиента (client-cert.crt) и приватного ключа (client-key.pem). Далее, на этапе настройки VPN при создании клиентского профиля безопасности VPN необходимо перейти в раздел **VPN → Клиентские профили безопасности** и нажать кнопку **Добавить**. В открывшемся окне указать необходимые параметры профиля безопасности (подробнее — в разделе «[Профили клиентских сертификатов](#)»). При использовании протокола IKEv2 для организации VPN необходимо в поле Сертификат клиента указать импортированный ранее сертификат VPN-клиента.

Генерация сертификатов Центром Сертификации Microsoft Server

Пример генерации сертификатов Центром Сертификации Microsoft Server для сценария Remote Access VPN.

1. Выпустить Центром Сертификации корневой сертификат (rootCA).

2. Выпустить на основе корневого сертификата (rootCA) сертификат VPN-сервера.

- Указать требования — **key usage: server auth**;
- Минимальный размер ключа - **4096**;
- Указать **subjectAltName** соответствующее **DNS-имени VPN-сервера**.
- Создать шаблон для выдачи пользовательских сертификатов. UPN атрибут пользователя должен совпадать с атрибутами сертификата CN и\или SAN:principal name.

Действия на стороне VPN-сервера

1. Импортировать корневой сертификат (rootCA) в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Сертификаты** и нажать кнопку **Импортировать**.

2. Импортировать сертификат VPN-сервера в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Сертификаты** и нажать кнопку **Импортировать**.

3. Создать профиль клиентского сертификата в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate** → **Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный ранее корневой сертификат и выбирать поле для авторизации **Common-name** или **Subject alt name** для получения имени пользователя.

4. В разделе **VPN** → **Серверные профили безопасности** добавить в **Remote access VPN profile**:

- Сертификат в поле **Сертификат сервера**.
- Выбрать созданный **Профиль пользовательского сертификата**.
- Выбрать **Режим аутентификации** — посредством сертификатов **PKI**.

Свойства серверного профиля безопасности

Общие

Фаза 1

Фаза 2

Название:

RA_VPN

Описание:

ИКЕ версия:

IKEv2

Режим ИКЕ:

Основной

Тип идентификации:

отсутствует

Значение идентификации:

Общий ключ:

Общий ключ (повтор):

Сертификат сервера:

rootCA_vpn_CERT

Режим аутентификации:

PKI

Профиль сертификата пользователя:

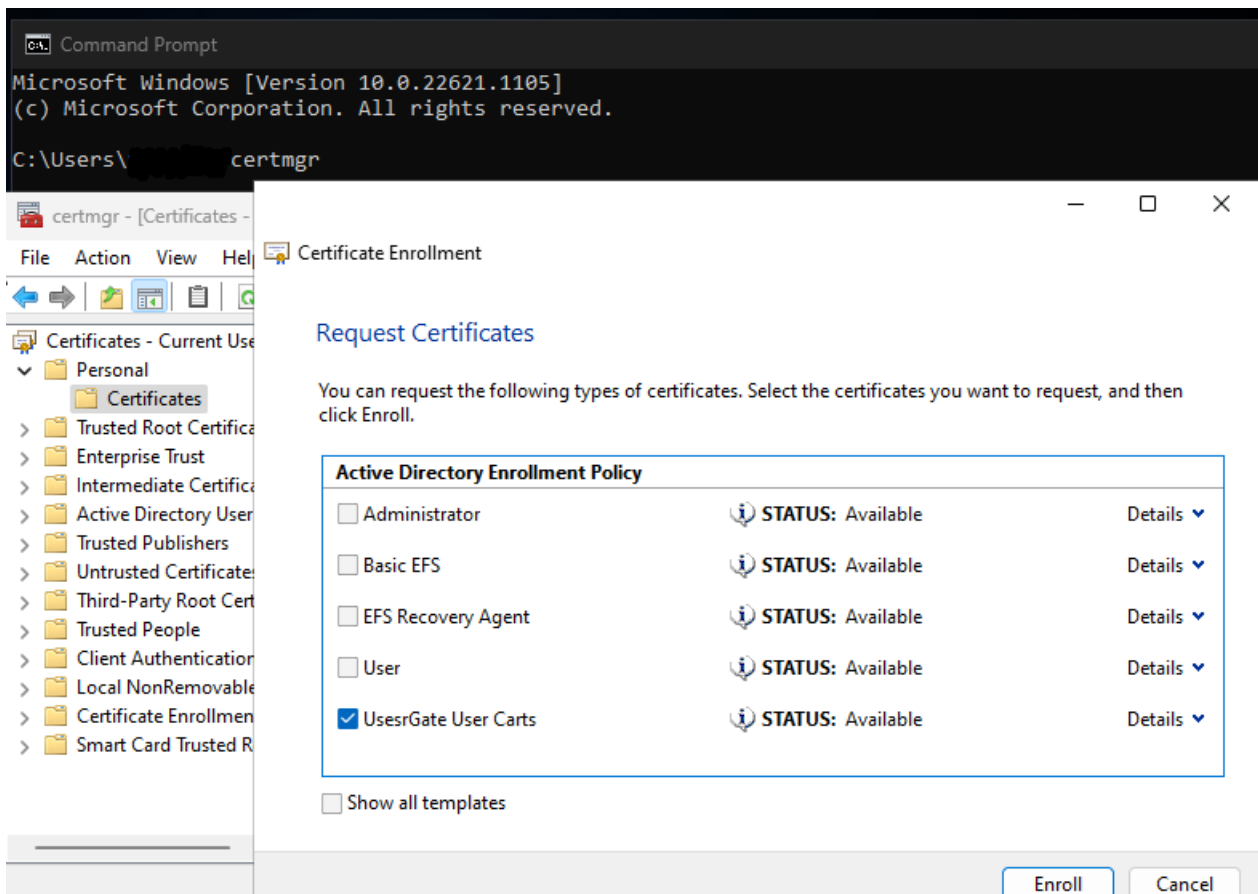
client_CERT

Сохранить

Отмена

Действия на стороне VPN-клиента

1. Запросить сертификат на клиентской машине согласно созданному ранее шаблону пользовательского сертификата.



2. Полученный сертификат расположить в репозиторий Локальный компьютер, хранилище — Личное.

