UserGate

NGFW 7.1.x Руководство администратора

Оглавление

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 (СОВ) 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 СОВ для защиты определенных сервисов и включать их в профили СОВ наряду с сигнатурами, поставляемыми UserGate. Профили СОВ интегрируются в правила межсетевого экрана. При срабатывании сигнатур такого профиля будет произведено действие, настроенное в сигнатурах и произведена соответствующая запись в Журнале СОВ.

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.

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.

Управление АСУ ТП

В новой версии платформы появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП) и управления ей. Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий. Это позволяет автоматизировать основные операции технологического процесса,

сохраняя при этом возможность контроля и вмешательства человека при необходимости.

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 приоритезировать 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-северами, 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 и Syslog. Для этого агент UserID осуществляет запросы посредством протокола WMI на серверы AD, а в случае с syslog, осуществляет прослушивание порта syslog и сбор информации, которую присылают серверы syslog. 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 NGFW, 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 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, СОВ 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

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

Платформа UserGate 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 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.

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. Помимо этого, существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

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.

ЛИЦЕНЗИРОВАНИЕ

Лицензирование (Описание)

Внимание!

Лицензионные ключи версий 6 и 7 *несовместимы*! Перед обновлением до версии 7, необходимо запросить у менеджера ключ для 7-й версии.

Базовая лицензия

Лицензирование UserGate NGFW осуществляется по параметрам производительности платформы и зависит от:

- типа аппаратной платформы (для программно-аппаратного комплекса);
- количества поддерживаемых ядер виртуальной машины (для виртуального образа).

При попытке регистрации некорректного оборудования ключом с ограничением по производительности появится ошибка: **Введенный ПИН-код выписан для другого устройства UserGate, или конфигурация сервера не соответствует лицензированным характеристикам, например, увеличено число ядер процессора**.

Примечание

Если виртуальная машина зарегистрирована корректным ключом, а в дальнейшем в неё будут добавлены дополнительные ядра, то активным в виртуальной машине будет только разрешенное лицензией количество ядер.

Базовая лицензия на продукт является бессрочной (без обновлений).

Дополнительно лицензируемые модули

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • Обновлений ПО UserGate. • Обновлений сигнатур системы обнаружения вторжений.

Наименование	Описание
	• Обновлений сигнатур приложений L7. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений необходимо продление лицензии.
Модуль Advanced Threat Protection (ATP)	Модуль ATP включает в себя следующие опции: • Годовая подписка на базу категорий сайтов UserGate URL filtering. • Годовая подписка на обновляемые списки URL (списки запрещенных сайтов Роскомнадзора, список phishing-сайтов, Белый список UserGate, Черный список UserGate, итд.). • Годовая подписка на морфологические базы, предоставляемые компанией UserGate. • Годовая подписка на работу сервиса веб-безопасности (блокировка рекламы, история поиска, безопасный поиск, блокировка приложений социальных сетей). Модуль выписывается на 1 год, по истечении данного срока: • UserGate URL filtering перестает работать. • Фильтрация с помощью морфологии перестает работать. • Списки URL продолжают работать, но обновления будут недоступны. • Сервис веб-безопасности (блокировка рекламы, история поиска, безопасный поиск, блокировка приложений социальных сетей) перестает работать.
Модуль Mail security	Mail security включает в себя годовую подписку на проверку почтового трафика с помощью модуля антиспама UserGate.
Модуль Потоковый антивирус UserGate	Модуль включает в себя подписку на потоковый антивирус UserGate сроком на 1 год. По истечению данного срока антивирус UserGate перестает работать.
Модуль Cluster	Модуль включает лицензию на работу устройств UserGate в режиме "кластер".
Модуль Контроль доступа в сеть на уровне МЭ	Модуль предназначен для взаимодействия с конечными устройствами с установленным ПО UserGate Client,

Наименование	Описание
	являющимся компонентом экосистемы UserGate SUMMA. Подписка на данный модуль включает в себя: • Контроль доступа конечных устройств в сеть на уровне межсетевого экрана UserGate, при подключении через VPN, по результатам проверки соответствия требованиям политик безопасности (комплаенса), реализованной на основе профилей HIP. • Передачу телеметрии состояния конечных устройств на SIEM системы. • Доступ к обновлениям библиотеки HIP профилей. Модуль выписывается на срок кратный 1 году (до 5 лет). По истечении срока подписки правила межсетевого экрана, настроенные на NGFW и использующие профили HIP в качестве одного из условий, перестают работать.

Онлайн-активация лицензии

При онлайн-активации устройство\ПО UserGate обращается к серверу лицензировании https://reg2.usergate.com. На сервер передается следующая техническая информация: **номер версии ПО UserGate, пин-код, название продукта, модель устройства** и т.д. В ответ приходят данные о сроке действия лицензии и списке модулей, разрешенных данной лицензией.

Если модули, ранее присутствующие в системе, отсутствуют в этом списке, то они деактивируются, а их лицензия аннулируется. Вновь появившиеся модули активируются.

В дальнейшем при работе устройства\ПО UserGate проверка лицензии происходит 1 раз в сутки. Если все в порядке — ничего не происходит и устройство будет работать в штатном режиме. При успешной проверке в журналах отображается запись об этом событии.

При недоступности серверов лицензирования делается 14 попыток с интервалом в 120 секунд. В случае неуспеха попытки прекращаются на сутки, после чего снова следуют 14 попыток подключения к серверу активации. В случае, если в течении периода действия лицензии так и не удается подключиться к серверу активации, лицензия блокируется по истечении срока действия (модули, лицензия которых просрочена, перестают работать). При каждой ошибке подключения к серверу активации в журналы заносится сообщение об ошибке.

Порядок действий при онлайн-активации

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в **Дашборд**.	Нажать на пиктограмму **Дашборд** в правом верхнем углу.
Шаг 2. В разделе **Информация о лицензии** зарегистрировать продукт.	В разделе **Лицензия** нажать на ссылку **Нет лицензии**, ввести ПИН-код и заполнить регистрационную форму. При нахождении узла NGFW в закрытом контуре без прямого доступа в интернет возможна активация/обновление лицензии через прокси-сервер. Для этого необходимо выбрать режим **Использовать прокси-сервер для активации и апдейтов**. Далее указать IP-адрес и порт вышестоящего прокси-сервера. При необходимости указать логин и пароль для аутентификации на прокси-сервере.

Офлайн-активация лицензии

> **Примечание**
> **Доступно с версии 7.1+**

В случае, если UserGate NGFW не имеет доступа в сеть Интернет, возможно проведение офлайн-активации лицензии. При офлайн-активации поведение NGFW аналогично поведению при недоступности сервера активации. По истечении времени действия по локальному счетчику времени лицензия блокируется и соответствующие модули прекращают работу.

> **Примечание**
> **Процедура офлайн-активации производится через Вашего менеджера.**

Порядок действий при офлайн-активации

Наименование	Описание
Шаг 1. Открыть в браузере страницу активации.	В браузере перейдите по адресу *https://IP-address:8001?features=offline-reg* (где IP-address — IP-адрес устройства).

Наименование	Описание
Шаг 2. Перейти в **Дашборд**.	Перейдите в **Дашборд**, найдите виджет **Лицензия** и нажмите **Нет лицензии**. Также можно нажать **Не зарегистрированная версия** в левом верхнем углу веб-интерфейса управления.
Шаг 3. Начать процедуру офлайн-активации.	В окне активации продукта выберите **Начать активацию в автономном режиме** и введите ПИН-код. Нажмите **Далее**.
Шаг 4. Получить файл запроса для процедуры офлайн-активации.	Мастер активации предложит скачать файл с запросом для регистрации. Скачайте файл и перешлите его Вашему менеджеру. Если Вы не знаете Вашего менеджера, то необходимо обратиться в службу технической поддержки.
Шаг 5. Дождаться ответа менеджера со специальным файлом ответа для завершения процедуры офлайн-активации.	Менеджер должен прислать письмо или любым другим способом передать вам файл ответа для завершения процедуры офлайн-активации.
Шаг 6. Используя полученный файл, завершить процедуру активации.	После получения файла откройте окно активации продукта и завершите активацию лицензии: нажмите **Завершить активацию в автономном режиме** и загрузите полученный файл.

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Описание

Межсетевой экран UserGate поставляется в виде программно-аппаратного комплекса (ПАК, appliance) 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 такие вендоры как VMWare, Oracle VirtualBox, и 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.**

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и 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.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb и добавьте по 1Gb на каждые 100 пользователей.
Шаг 4. Важно! Самостоятельно добавьте дополнительный диск, нужного размера	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 200Gb или более. Рекомендованный размер — 300Gb или более. Для систем виртуализации QEMU-KVM: размер системной области, по умолчанию, составляет 8Гб. Система, при первом запуске, сама определит наличие дополнительного диска и расширит свои системные разделы. Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:

Наименование	Описание
	`qemu-img create -f qcow2 -o preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_size=4K имя-вашего-диска.qcow2 100G`
Шаг 5. Настройте виртуальные сети	UserGate 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.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину UserGate. Во время загрузки выберите **Support Menu** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.

Примечание

Если сетевые интерфейсы на виртуальной машине с NGFW были удалены средствами гипервизора, они будут помечены как удаленные в веб-интерфейсе с помощью иконки

.

Примечание

Если vm UserGate клонируется через vSphere, то в vmx-файле настроек склонированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие vm источника.

Автоматизация развертывания UserGate NGFW с помощью Cloud-init

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

- Настройка с помощью команд CLI (файл с заголовком #utm-config). Возможно использовать все CLI-команды для полной настройки инстанса.
- Активация 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")
```

В данный файл можно добавлять все доступные для администратора команды CLI. Подробно о CLI-командах смотрите в разделе Интерфейс командной строки (CLI).

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

Если необходимо активировать создаваемый инстанс, то это можно сделать через указание параметров для лицензирования в отдельном файле. Следует учитывать, что активация возможна только при наличии у инстанса 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 multipart формат:

```
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:

1. Методами, реализуемыми облачными провайдер, например, у провайдера 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 у других поставщиков облачных услуг.
2. Через подключаемый iso-диск. Диск должен содержать файлы meta-data, user-data, vendor-data следующего содержимого:

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 в 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 межсетевого экрана UserGate должен иметь доступ до следующих серверов, расположенных в сети интернет:

- Сервер регистрации — reg2.usergate.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate — updates.usergate.com, порты TCP 80, 443.

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

- Обеспечение репликации настроек — порты TCP 4369, TCP 9000-9100.
- Сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности читайте 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, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

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

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления.	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить NGFW. После загрузки NGFW укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить NGFW. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Произвести первоначальную инициализацию в интерфейсе командной строки или подключиться к веб-консоли NGFW по указанному адресу, он должен выглядеть примерно следующим образом: https://NGFW_IP_address:8001. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).
Шаг 2. Выбрать язык.	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль.	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Настроить зоны, IP-адреса интерфейсов, подключить UserGate в сеть предприятия.	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0.

Наименование	Описание
	• Зона Trusted (LAN). • Зона Untrusted (Internet). • Зона DMZ. • Зона Cluster. • Зона VPN for remote access. • Зона VPN for Site-to-Site. • Зона Tunnel inspection zone.
Шаг 5. Настроить шлюз в Интернет.	В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет, зона **Untrusted**. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 6. Указать системные DNS-серверы.	В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Настройка DNS.
Шаг 7. Настроить время сервера.	В разделе **UserGate → Настройки → Настройка времени сервера** настроить синхронизацию времени с серверами NTP.
Шаг 8. Зарегистрировать NGFW.	Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ NGFW в Интернет. Более подробно о лицензировании продукта читайте в главе Лицензирование.
Шаг 9. Создать правила NAT.	В разделе **NAT и Маршрутизация** создать необходимые правила NAT. Для доступа в интернет пользователей сети **Trusted** правило NAT уже создано: «**NAT from Trusted to Untrusted**». Подробно о правилах NAT читайте в главе NAT и маршрутизация.
Шаг 10. Создать правила межсетевого экрана.	В разделе **Межсетевой экран** создать необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети **Trusted** правило межсетевого экрана уже создано — «**Allow trusted to untrusted**», необходимо только включить его. Подробно о правилах межсетевого экрана читайте в главе Межсетевой экран.
Шаг 11. Создать дополнительных	

Наименование	Описание
администраторов (опционально).	В разделе **Администраторы UserGate** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).
Шаг 12. Настроить авторизацию пользователей (опционально).	В разделе **Пользователи и устройства** создать необходимые методы авторизации пользователей. Самый простой вариант — это создать локальных пользователей NGFW с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя **Any** во всех правилах). Для других вариантов авторизации пользователей смотрите главу Пользователи и устройства.
Шаг 13. Создать правила контентной фильтрации (опционально).	В разделе **Фильтрация контента** создать правила фильтрации HTTP(S). Более подробно о фильтрации контента читайте в главе Фильтрация контента.
Шаг 14. Создать правила веб-безопасности (опционально).	В разделе **Веб-безопасность** создать дополнительные правила защиты веб. Более подробно о веб-безопасности читайте в главе Веб-безопасность.
Шаг 15. Создать правила инспектирования SSL (опционально).	В разделе **Инспектирование SSL** создать правила для перехвата и расшифровывания HTTPS-трафика. Более подробно о дешифровании HTTPS читайте в главе Инспектирование SSL.

После выполнения вышеперечисленных действий NGFW готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

НАСТРОЙКА УСТРОЙСТВА

Общие настройки

Раздел **Общие настройки** определяет базовые установки UserGate NGFW:

Наименование	Описание
Часовой пояс	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.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Режим аутентификации веб-консоли	Способ аутентификации пользователя (администратора) при входе в веб-консоль управления. Возможны следующие варианты: • **По имени и паролю**. Администратор должен ввести имя и пароль для получения доступа к веб-консоли. • **По X.509-сертификату**. Для аутентификации по сертификату необходимо иметь сертификат пользователя, подписанный сертификатом удостоверяющего центра веб-консоли и установленный в браузер. При включении этого режима аутентификации режим аутентификации по имени и паролю отключается. Вернуть режим аутентификации по имени и паролю можно с помощью команд CLI. • **Профиль сертификата пользователя.** Аутентификаци и посредством сертификатов (PKI) использует профиль пользовательского сертификата, это позволяет управлять сертификатами для обеспечения безопасности и подтверждения подлинности в сетевых соединениях.
Профиль SSL для веб-консоли	Выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробно о профилях SSL смотрите в главе Профили SSL.
Профиль SSL для страниц блокировки/авторизации	Выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации Captive-портала. Подробно о профилях SSL смотрите в главе Профили SSL.
Таймер автоматического закрытия сессии (мин.)	Настройка таймера автоматического закрытия сессии в случае отсутствия активности администратора в веб-консоли.
Профиль SSL конечного устройства	Выбор профиля SSL для построения защищенного канала общения NGFW и конечных устройств UserGate Client. Подробно о профилях SSL смотрите в главе Профили SSL.

Наименование	Описание
Сертификат конечного устройства	Сертификат, который будет использоваться для построения защищённого канала связи между NGFW и конечными устройствами UserGate Client. **Важно!** Конечные устройства запоминают сертификат, поэтому при изменении необходимо распространить корневой сертификат удостоверяющего центра (Root CA) на подключенные конечные устройства; сертификат должен быть установлен в хранилище доверенных корневых центров сертификации локального компьютера.
Настройка времени сервера	Настройка параметров установки точного времени. • **Использовать NTP** — использовать сервера NTP из указанного списка для синхронизации времени. • **Основной сервер NTP** — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org. • **Запасной сервер NTP** — адрес запасного сервера точного времени. • **Время на сервере** — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Модули	Позволяет настроить модули NGFW: • **HTTP(S)-прокси порт** — позволяет указать нестандартный (дополнительный) номер порта, который будет использоваться для подключения к встроенному прокси-серверу. По умолчанию используется порт TCP 8090; при изменении порт продолжает функционировать. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100. • **Домен auth captive-портала** — служебный домен, который используется NGFW при авторизации пользователей через Captive-портал. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес NGFW, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя auth.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Домен logout captive-портала** — служебный домен, который используется пользователями NGFW для окончания сессии (logout). Необходимо, чтобы

Наименование	Описание
	пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес NGFW, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя logout.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Домен страницы блокировки** — служебный домен, который используется для отображения страницы блокировки пользователям. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес NGFW, то резолвинг настроен автоматически. По умолчанию используется имя block.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **FTP поверх HTTP** — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. Требуется явное указание прокси-сервера для протокола FTP в браузере пользователя. Администратор может ограничивать доступ к ресурсам FTP с помощь правил контентной фильтрации (только по условиям Пользователи и URL). • **FTP поверх HTTP домен** — служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса NGFW, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя ftpclient.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Зона для инспектируемых туннелей** — включение/выключение модуля инспектирования туннелей и указание зоны для их инспектирования. • **Пароль агентов терминального сервиса** — настройка пароля для подключения агентов авторизации терминальных серверов. • **Настройка LLDP** — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети,

Наименование	Описание
	оповещать устройства о своём 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, изменение имени хоста или адреса управления. Может принимать значения от 1 до 3600; задаётся 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.
Настройка кэширования HTTP	Настройка кэша прокси-сервера: • **Включен/Выключен** — включение или отключение кэширования. • **Исключения кэширования** — список URL, которые не будут кэшироваться. • **Максимальный размер объекта**, Мбайт — объекты с размером более, чем указано в данной настройке, не будут кэшироваться. Рекомендуется оставить значение по умолчанию — 1 Мбайт. • **Размер RAM-кэша**, Мбайт — размер оперативной памяти, отведенный под кэширование. Не рекомендуется ставить более 20% от объема оперативной памяти системы.
Log Analyzer	Настройки модуля LogAn: • **Локальный сервер/Внешний сервер**. Выберите внешний сервер, если у вас есть внешний сервер LogAn, в противном случае выберите локальный сервер. • **Состояние** — показывает текущее состояние сервиса статистики. **Важно!** При указании внешнего LogAn обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.
Web-портал	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (SSL VPN).

Наименование	Описание
	Подробное описание данных настроек смотрите в главе Веб-портал.
Настройка PCAP	Настройка записи трафика при срабатывании сигнатур системы обнаружения вторжений. Настройка захвата пакетов: • **Без захвата**. • **Один пакет**. • **Предшествующие пакеты** (от 4 до 30 пакетов). • **Предшествующие и последующие пакеты** (предшествующие: от 4 до 30; последующие: от 2 до 15). **Важно!** Большой размер PCAP может вести к значительному замедлению обработки данных.
Настройка учета изменений	При включении данной опции и создания **Типов изменений** любое изменение в конфигурацию, вносимое администратором через веб-консоль, будет требовать указание типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • Распоряжение. • Приказ. • Регламентные работы, и т.д. Количество типов изменений не ограничено.
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления (UGMC), позволяющей управлять парком устройств UserGate из одной точки; для подключения к серверу UGMC используются порты TCP 2022 и TCP 9712. • **Включен/Выключен** — включение или отключение управления с помощью UGMC. • **Адрес UserGate Management Center** — адрес сервера в формате IPv4-адреса или FQDN (возможно использование IDN-адреса). • **Код устройства** — токен, требуемый для подключения к UGMC. UGMC может использоваться как источник обновления ПО и сигнатур.
Расписание скачивания обновлений	Настройки для управления скачиванием обновлений программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по

Наименование	Описание
	подписке (база категорий URL-фильтрации, СОВ, списки IP-адресов, URL, типов контента и другие). • **Обновления ПО** — настройка расписания проверки наличия новых обновлений UGOS и скачивания обновлений. • **Обновления библиотек** — настройка расписания проверки наличия новых обновлений библиотек и скачивания библиотек. Чекбокс **Единое расписание для всех обновлений** применяет расписание ко всем библиотекам, иначе для каждой библиотеки необходимо настроить собственное расписание. При задании расписания 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".
Вышестоящий прокси	Настройки параметров вышестоящего прокси-сервера для перенаправления пользовательского трафика. В качестве параметров указывается тип вышестоящего прокси-

Наименование	Описание
	сервера (HTTP(S), SOCKS5), IP-адрес и порт вышестоящего прокси-сервера, логин и пароль при необходимости для аутентификации на вышестоящем прокси-сервере.

Управление устройством

Раздел **Управление устройством** определяет следующие настройки NGFW:

- **Кластеризация.**
- **Настройки диагностики.**
- **Операции с сервером.**
- **Резервное копирование.**
- **Экспорт и импорт настроек.**

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• **Off** — ведение журналов диагностики отключено. • **Error** — журналировать только ошибки работы сервера. • **Warning** — журналировать только ошибки и предупреждения. • **Info** — журналировать только ошибки, предупреждения и дополнительную информацию. • **Debug** — максимум детализации. Рекомендуется установить значение параметра **Детализация диагностики** в **Error** (только ошибки) или **Off** (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность NGFW.
Журналы диагностики	• **Скачать журналы** — скачать диагностические журналы для передачи их в службу поддержки UserGate; для скачивания доступны журналы веб-консоли и/или журналы системы. Для скачивания необходимо выбрать журналы и нажать **Начать архивирование журналов**; после архивирования

Наименование	Описание
	журналы будут доступны для скачивания (кнопка **Скачать**). • **Очистить журналы** — удалить содержимое папки крэш-логов.
Удаленный помощник	• **Включено**/**Отключено** — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate для диагностики и решения проблем. Для успешной активации удаленного помощника NGFW должен иметь доступ к серверу удаленного помощника по протоколу SSH. • **Идентификатор удаленного помощника** — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • **Токен удаленного помощника** — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** — перезагрузка NGFW. • **Выключить** — выключение NGFW.
Обновления	Выбор канала обновлений ПО UserGate • **Стабильные** — проверка наличия стабильных обновлений ПО. • **Бета** — проверка наличия экспериментальных обновлений.
Обновления сервера	Индикация имеющихся обновлений NGFW. Запуск процесса обновления сервера с возможностью создания точки восстановления. Просмотр списка изменений ПО в обновлении.
Офлайн обновления	Загрузка файла для офлайн обновления.

Наименование	Описание
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО NGFW. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере.

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование). При наличии обновлений в разделе **Управление устройством → Операции с сервером** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя NGFW.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния NGFW, как это описано в разделе Системные утилиты. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки NGFW будет перезагружен.

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием NGFW: настройка правил экспорта конфигурации, создание резервной копии, восстановление NGFW.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе **Управление устройством → Управление резервным копированием** нажать **Создание резервной копии**. Система сохранит текущие настройки сервера под следующим именем:

Наименование	Описание
	backup_PRODUCT_NODE-NAME_DATE.gpg, где: *PRODUCT* — тип продукта: NGFW, LogAn, MC; *NODE-NAME* — имя узла UserGate; *DATE* — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки **Остановить**. Запись о создании резервной копии отобразится в журнале событий устройства.

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе **Управление устройством → Управление резервным копированием** нажать **Восстановление из резервной копии** и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

Дополнительно администратор может настроить сохранение файлов на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе **Управление устройством → Управление резервным копированием** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки. Путь на сервере должен уже существовать. Сама система несуществующие папки не создаст! В случае использование SSH-сервера возможно использование авторизации по ключу. Для импорта или

Наименование	Описание
	генерации ключа необходимо выбрать **Настроить SSH-ключ** и указать **Сгенерировать ключи** или **Импортировать ключ**. **Важно!** При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей **/home/user/.ssh/** в файле **authorized_keys**. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка **Проверить соединение**); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. **Важно!** Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его 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 и тире используются 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".

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки NGFW в файл и впоследствии восстановить эти настройки на этом же или другом NGFW. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Экспорт настроек является кластерной функцией. Работает это следующим образом: при создании правила экспорта настроек на одном из узлов кластера

оно автоматически реплицируется на остальные узлы кластера. При этом сами файлы экспорта создаются и отправляются отдельно на каждом узле.

Примечание

Экспорт/импорт настроек не восстанавливает состояние кластера и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать NGFW с помощью имеющегося ПИН-кода и заново создать кластер, если это необходимо.

Примечание

В случае использования мультифакторной аутентификации через TOTP, ключи TOTP не сохраняются; необходима повторная инициализация.

Имеется возможность сделать экспорт всех настроек (за исключением вышеперечисленных), либо сделать только экспорт сетевых настроек. При экспорте только сетевых настроек сохраняется информация о:

- Настройки DNS.
- Настройки DHCP.
- Настройки всех интерфейсов, включая туннели.
- Настройки шлюзов.
- Настройки виртуальных маршрутизаторов (VRF).
- Настройки WCCP.
- Настройки зон.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Экспорт → Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит текущие настройки сервера под именем utm-utmcore@nodename_version-YYYYMMDD_HHMMSS.bin, где: nodename — имя узла NGFW version — версия UGOS

Наименование	Описание
	YYYYMMDD_HHMMSS — время выгрузки настроек в часовом поясе UTC, например: utm-utmcore@heashostatot_6.1.1.10462R-1_20210511_095942

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать **Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен.

Примечание

Для корректного импорта правил, использующих обновляемые списки UserGate (приложения, категории URL и т.п.), необходимо наличие лицензии на модули SU и ATP, а также загруженных списков UserGate.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе **Управление устройством → Экспорт и импорт настроек** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль/Подтверждение пароля** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки.

Наименование	Описание
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его 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 и тире используются 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.

Управление доступом к консоли UserGate NGFW

Доступ к веб-консоли UserGate NGFW регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети. Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

> **Примечание**
>
> **При первоначальной настройке NGFW создается локальный суперпользователь Admin.**

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора.	В разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант: • **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • **Добавить пользователя LDAP** — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • **Добавить группу LDAP** — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • **Добавить администратора с профилем авторизации** – создать пользователя, назначить созданный ранее профиль администратора и профиль авторизации (необходимы корректно настроенные серверы авторизации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Разрешения для API	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Объекты описаны документации API. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Наименование	Описание
Разрешения для веб-консоли	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для CLI	Позволяет разрешить доступ к CLI. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Администратор NGFW может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей.	В разделе **Администраторы → Администраторы** нажать кнопку **Настроить**.
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • **Сложный пароль** — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как — минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • **Число неверных попыток аутентификации** — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**. • **Время блокировки** — время, на которое блокируется учетная запись.

> **Примечание**
>
> **Дополнительные параметры защиты учетной записи администратора применимы только к локальным учетным записям. Если в качестве администратора устройства выбирается учетная запись из внешнего каталога (например, LDAP), то параметры защиты для такой учетной записи определяются этим внешним каталогом.**

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8001).

> **Примечание**
>
> **Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.**

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

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

Для включения данного режима необходимо выполнить следующие действия (в качестве примера используется утилита openssl):

Наименование	Описание
Шаг 1. Создать учетные записи дополнительных администраторов.	Произвести настройку, как это описано ранее в этой главе, например, создать учетную запись администратора с именем Administrator54.
Шаг 2. Создать или импортировать существующий сертификат типа УЦ (удостоверяющего центра) авторизации веб-консоли.	Создать или импортировать существующий сертификат удостоверяющего центра (достаточно только публичного ключа) в соответствии с главой Управление сертификатами. **Важно!** Существующий сертификат удостоверяющего центра — сертификат, которым непосредственно подписаны сертификаты администраторов, а не корневой. Например, для создания eудостоверяющего центра с помощью утилиты openssl требуется выполнить команды:

Наименование	Описание

	`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`
	
	В файле ca-key.pem будет находиться приватный ключ сертификата, в ca.pem — публичный ключ. Импортировать публичный ключ в NGFW.

Шаг 3. Создать сертификаты для учетных записей администраторов.	С помощью средств сторонних утилит (например, openssl) создать сертификаты для каждого из администраторов. Необходимо, чтобы поле сертификата **Common name** в точности совпадало с именем учетной записи администратора, как она была создана в NGFW. Для openssl и пользователя Administrator54 команды будут следующими: `openssl req -subj '/C=RU/ST=Moscow/O=MyCompany /CN=Administrator54' -out admin.csr -newkey rsa:2048 -keyout admin-key.pem -nodes`

Шаг 4. Подписать сертификаты администраторов, созданным на шаге 2 сертификатом удостоверяющего центра.	С помощью средств сторонних утилит (например, openssl) подписать сертификаты администраторов сертификатом удостоверяющего центра веб-консоли.
	Для openssl команды будут следующими:
	`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 'Administrator54 client certificate'`
	
	Файл admin.p12 содержит подписанный сертификат администратора.

Шаг 5. Добавить подписанные сертификаты в ОС, с которой администраторы	Добавить подписанные сертификаты администраторов (admin.p12 в нашем примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой

Наименование	Описание
будут авторизоваться в веб-консоль.	администраторы будут авторизоваться в веб-консоль. Более подробно смотрите руководство по используемой вами ОС.
Шаг 6. Переключите режим авторизации веб-консоли в авторизацию по сертификатам x.509.	В разделе **Настройки** поменяйте **Режим авторизации веб-консоли** на **По X.509 сертификату**.

Примечание

Переключить режим авторизации веб-консоли можно с помощью команд CLI.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования NGFW. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Кластеризация и отказоустойчивость

UserGate NGFW поддерживает 2 типа кластеров:

1. **Кластер конфигурации**. Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. **Кластер отказоустойчивости**. До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости.

Кластер конфигурации

Ряд настроек уникален для каждого из узлов кластера, например, настройка сетевых интерфейсов и IP-адресация. Список уникальных настроек:

Наименование	Описание
Настройки, уникальные для каждого узла	Настройки Log Analyzer. Настройки диагностики. Настройки интерфейсов. Настройки шлюзов. Настройки DHCP.

Наименование	Описание
	Маршруты. Настройки OSPF. Настройки BGP.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	Смотрите главу Первоначальная настройка.
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе **Зоны** создать выделенную зону для репликации настроек кластера или использовать существующую (**Cluster**). В настройках зоны разрешить следующие сервисы: • Консоль администрирования • Кластер Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера. Именно этот интерфейс будет использоваться для отправки VRRP ADVERTISEMENT сообщений.	В разделе **Управление устройством** в окне **Кластер конфигурации** выбрать текущий узел кластера и нажать на кнопку **Редактировать.** Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать **Секретный код** на первом узле кластера.	В разделе **Управление устройством** нажать на кнопку **Сгенерировать секретный код.** Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.
Шаг 5. Подключить второй узел в кластер.	Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В

Наименование	Описание
	противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и все настройки первого кластера реплицируются на второй. Состояние узлов кластера конфигурации можно определить по цветовой индикации напротив названия узла UserGate в разделе **UserGate → Управление устройством → Кластер конфигурации**: • **Зелёный**: узел доступен. • **Жёлтый**: происходит синхронизация между узлами кластера конфигурации. • **Красный**: связь до узла потеряна, узел недоступен.
Шаг 6. Назначить зоны интерфейсам второго узла.	В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

Примечание

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

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько, например, в кластер конфигурации добавлены узлы A, B, C и D на основе которых создано 2 кластера отказоустойчивости — A-B и C-D.

Поддерживаются 2 режима кластера отказоустойчивости — **Актив-Актив** и **Актив-Пассив**. Состояние узлов кластера можно определить по цвету

индикатора около названия узла NGFW в разделе **UserGate → Управление устройством → Кластеры отказоустойчивости**:

- **Красный**: нет связи с соседними узлами конфигурации.
- **Жёлтый**: кластер отказоустойчивости не запущен на узле.

Отсутствие индикатора напротив названия узла говорит о доступности узла кластера.

Кластер отказоустойчивости Актив-Пассив

В режиме Актив-Пассив один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. 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 Актив-Пассив 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 роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (смотрите раздел Настройка шлюзов), и доступ в интернет отсутствует через все имеющиеся шлюзы.

  Если хост, указанный в свойствах проверки сети, недоступен на всех узлах кластера, то кластер отказоустойчивости будет отключен.
- Сбой в работе ПО UserGate.

Отключение одного или нескольких сетевых интерфейсов, на которых назначены виртуальные IP-адреса понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-сервера будет равен 248, приоритет резервного — 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250 (справедливо для случая если виртуальные адреса сконфигурированы на двух и более интерфейсах. Если на одном, то роль мастера не возвращается).

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

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

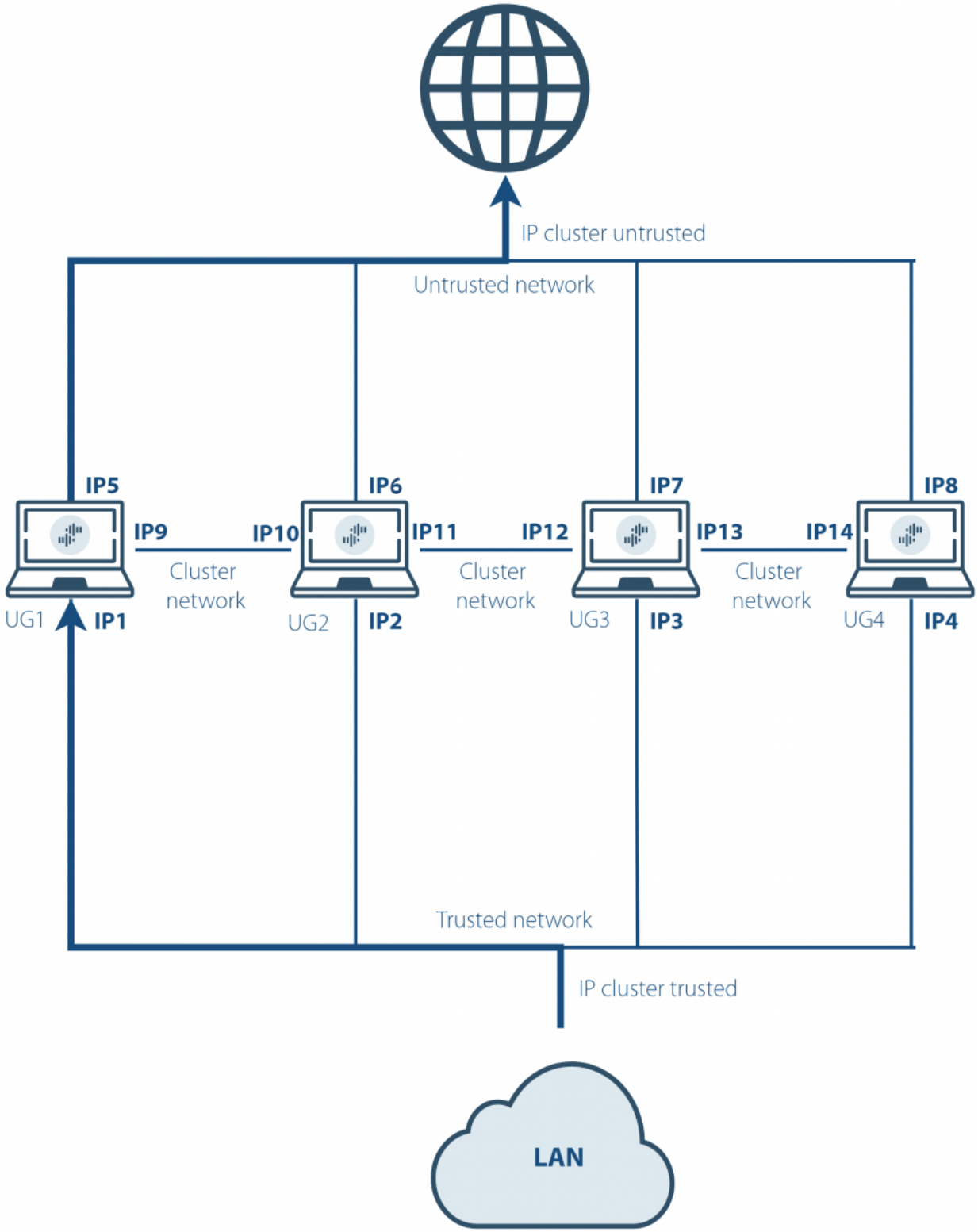
> **Примечание**
>
> **Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается NGFW каждую минуту и при переезде роли мастера на запасной сервер.**

Ниже представлена пример сетевой диаграммы отказоустойчивого кластера в режиме Актив-Пассив. 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 настроек.

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



Отказоустойчивый кластер в режиме Актив-Пассив

Кластер отказоустойчивости Актив-Актив

В режиме Актив-Актив один из серверов 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**
>
> **Режим Актив-Актив 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 роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (смотрите раздел Настройка шлюзов), и доступ в интернет отсутствует через все имеющиеся шлюзы.
- Сбой в работе ПО NGFW.

Отключение одного или нескольких сетевых интерфейсов **мастер-узла**, на которых назначены виртуальные IP-адреса, понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-

сервера будет равен 248, приоритет резервного — 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250.

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, а также исключает данный узел из балансировки трафика. Тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

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

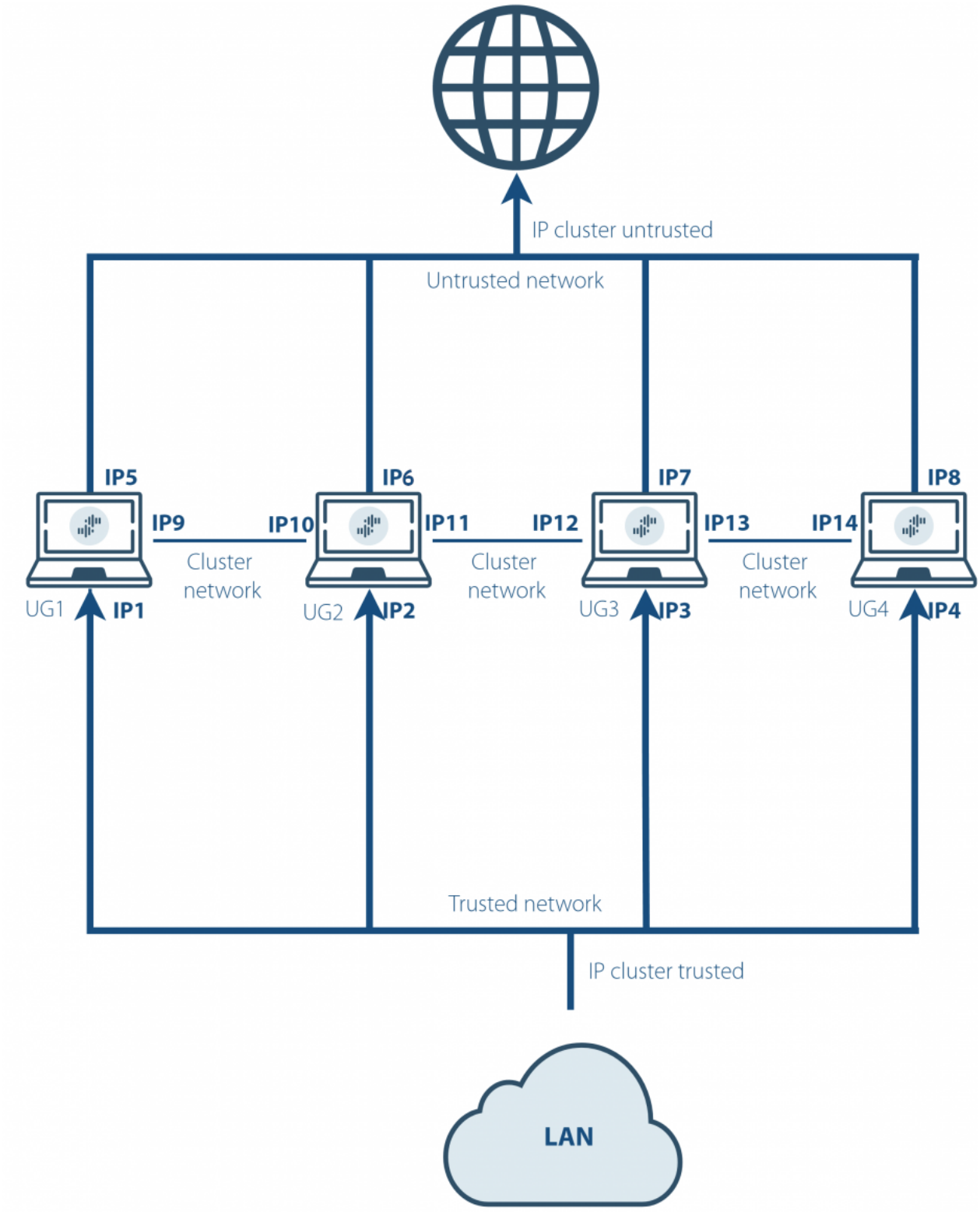
Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылает служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме Актив-Актив пакет GARP отсылается NGFW только при переходе роли мастера на запасной сервер.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. 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 настроек.

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



Отказоустойчивый кластер в режиме Актив-Актив

Примечание

Для корректной обработки трафика необходимо, чтобы обратный трафик от сервера к клиенту вернулся через тот же узел 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 данной задачи – это использование NAT из сети клиента в сеть сервера (NAT из Trusted в Untrusted).

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать кластер конфигурации.	Создать кластер конфигурации, как это описано на предыдущем шаге.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	В разделе **Зоны** следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зоны **Trusted** и **Untrusted** на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости.	В разделе **Управление устройством → Кластер отказоустойчивости** нажать на кнопку **Добавить** и указать параметры кластера отказоустойчивости.
Шаг 4. Указать виртуальный IP-адрес для хостов auth.captive, logout.captive, block.captive, ftpclient.captive.	Если предполагается использовать авторизацию с помощью Captive-портала, то необходимо, чтобы системные имена хостов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, резолвились в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более детально эти параметры описаны в разделе Общие настройки.

Параметры отказоустойчивого кластера:

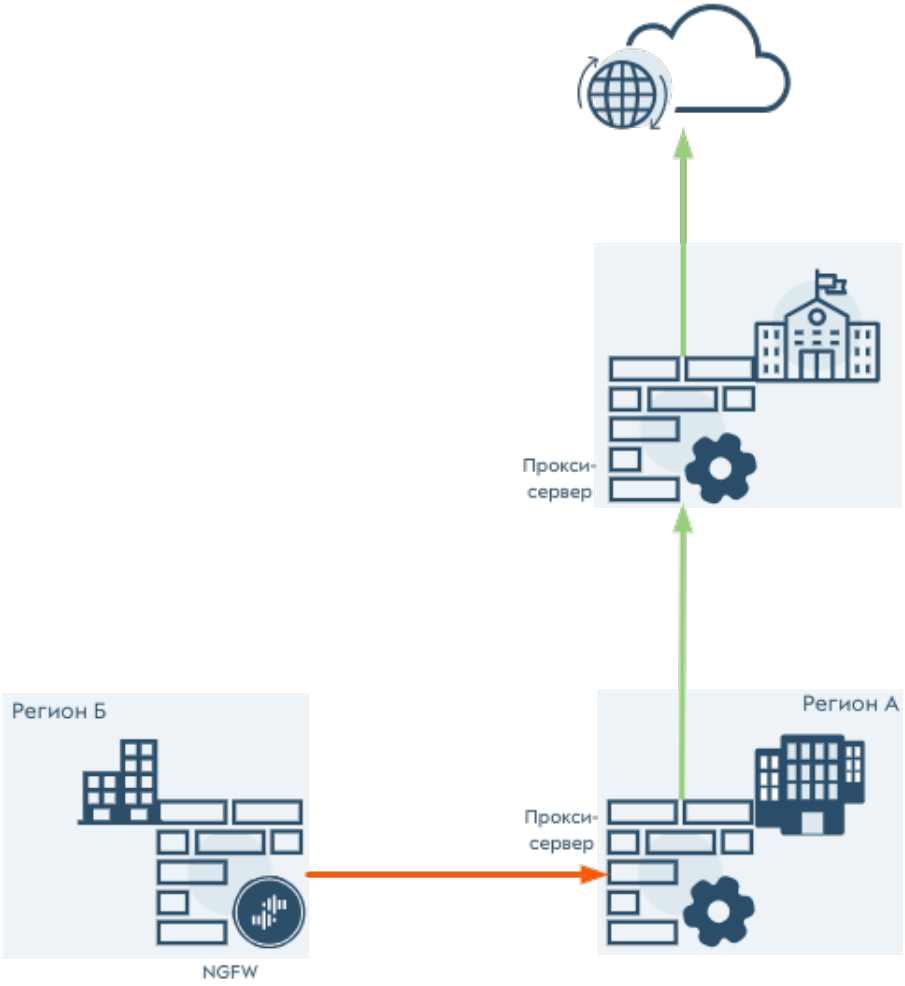
Наименование	Описание
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: • **Актив-Актив** — нагрузка распределяется на все узлы кластера.

Наименование	Описание
	• **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий между всеми узлами, входящими в кластер отказоустойчивости. Включение данной опции делает переключение пользователей с одного устройства на другое прозрачным для пользователей, но добавляет существенную нагрузку на платформу UserGate. Имеет смысл только для режима кластера Актив-Пассив.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.
Синхронизация UDP/ICMP	Управление режимом синхронизации пользовательских сессий: • **Синхронизовать все сессии** — включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка **Синхронизировать сессии** во вкладке **Общие** активирована, синхронизироваться будут только TCP сессии. • **Исключенные из синхронизации IP** — указание IP-адресов, с которыми не будут синхронизироваться пользовательские сессии.

Upstream Proxy

Описание

Upstream Proxy — это функциональность NGFW, позволяющая перенаправлять входящий HTTP(S) трафик на другой 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.

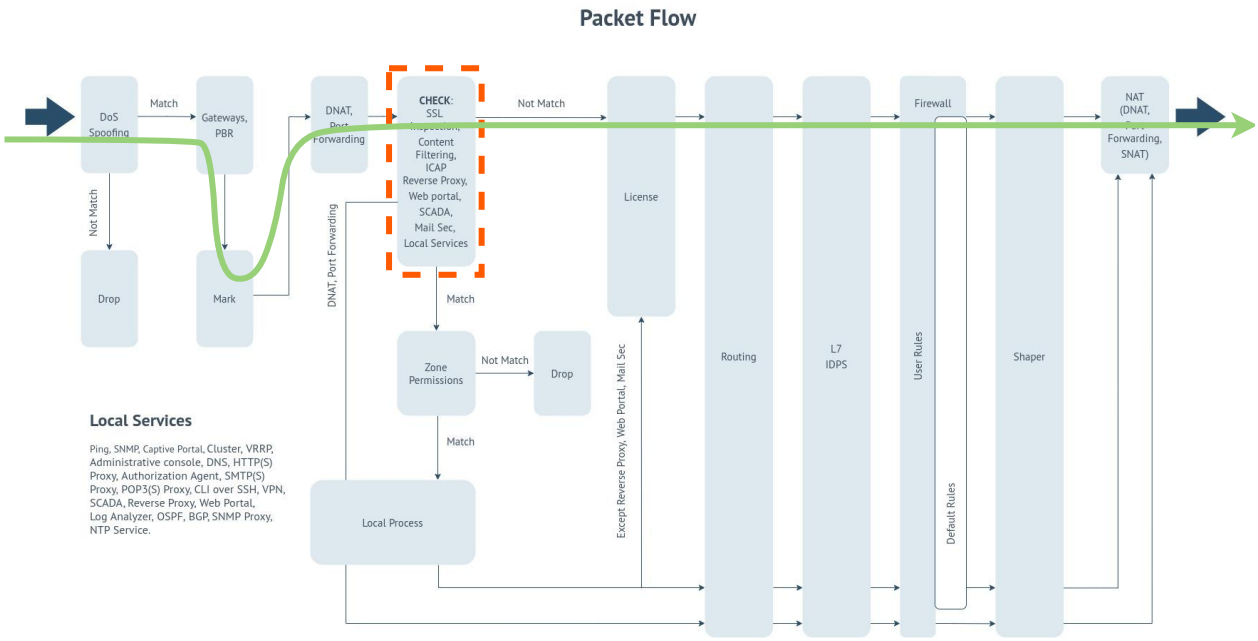


Upstream Proxy работает только если NGFW используется в режиме явного прокси-сервера (Explicit Proxy). На стороне клиента в веб-браузере или в других приложениях в явном виде указывается адрес и порт прокси-сервера NGFW .

При запросе клиентом внешнего ресурса формируется две TCP-сессии:

- Первая сессия: Клиент — NGFW. Обращение от клиента происходит непосредственно к NGFW и начинается с сообщения HTTP Connect.
- Вторая сессия: В отличие от классического сценария с явным прокси, сессия устанавливается не между NGFW и конечным сервером, а между NGFW и последующим (вышестоящим) прокси-сервером. Трафик от NGFW до вышестоящегог прокси-сервера является транзитным для блока Firewall. Необходимо понимать, что в режиме Upstream proxy адресом назначения становится IP-адрес вышестоящего прокси-сервера. Если ранее было настроено запрещающее правило по IP-адресам назначения, то такое правило работать не будет.

Алгоритм обработки трафика (packet flow) аналогичен алгоритму обработки в режиме явного прокси-сервера.



Поступая на интерфейс, пакеты проходят проверку соответствия правилам зоны в блоке **DoS, Spoofing**. Для корректной работы функциональности Upstream Proxy в NGFW необходимо в настройках зоны разрешить сервис HTTP(s)-прокси, иначе пакеты будут отброшены.

Далее пакеты обрабатываются в блоке **Gateways**, **PBR**, в котором маркируются для дальнейшего использования в правилах маршрутизации.

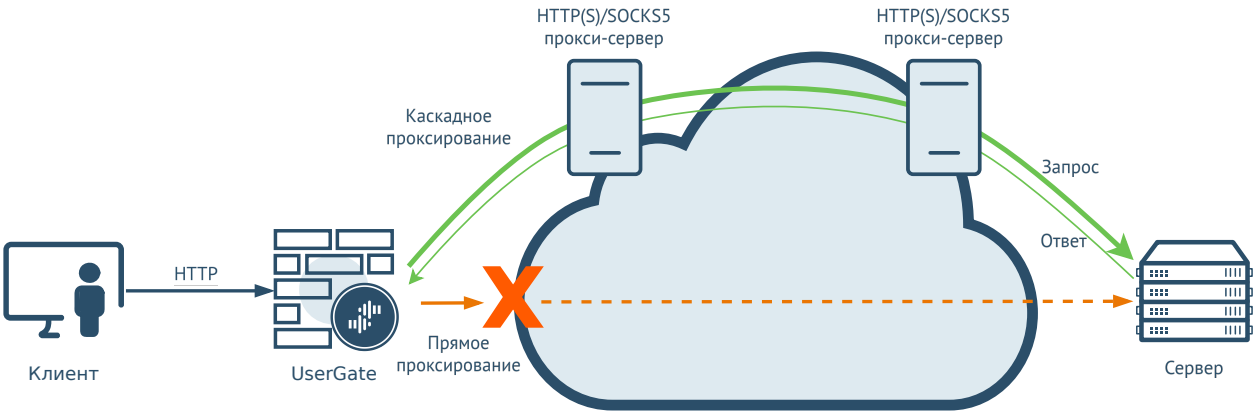
Затем пакеты без изменений проходят в блок с условным названием **CHECK**, где весь трафик проходит проверку соответствия условиям правил инспектирования, контентной фильтрации, а также принадлежности сервисам ICAP, reverse-прокси, веб-портала, АСУ ТП и защиты почтового трафика.

Проверка осуществляется путём поэтапного анализа трафика в соответствие с параметрами алгоритма блока CHECK (подробнее в статье UserGate NGFW packet flow). После обработки в блоке **CHECK** трафик будет направлен в блоки License, Routing и далее.

Сценарии использования

Proxy forwarding (без классификации трафика)

Весь входящий на NGFW HTTP трафик, прошедший через правила фильтрации на NGFW, перенаправляется на следующий (вышестоящий) прокси-сервер по цепочке. В качестве вышестоящего прокси-сервера может быть любой HTTP(S) или SOCKS5 прокси-сервер. Поддерживается опциональный режим с аутентификацией на вышестоящем прокси-сервере по логину/паролю.

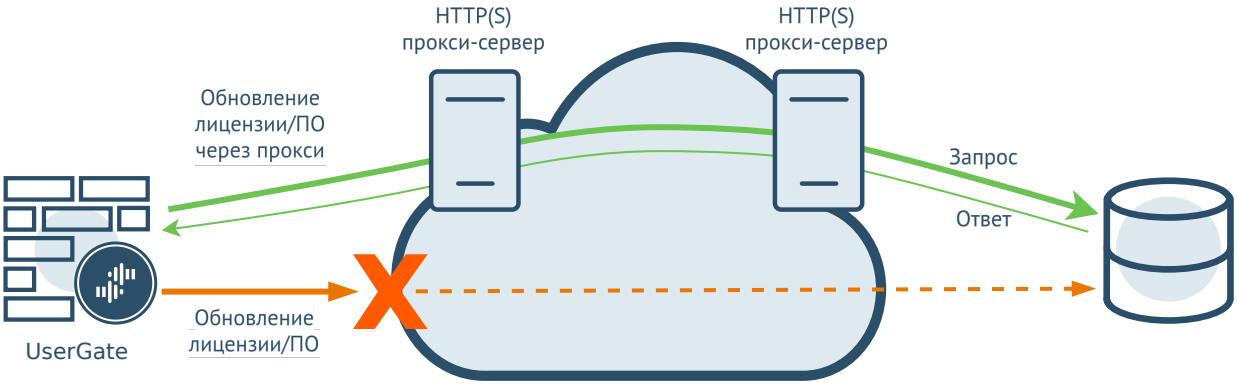


Журналирование перенапрявляемого на вышестоящий прокси-сервер трафика производится в Журнале веб-доступа, но в качестве IP-адреса назначения указывается IP-адрес вышестоящего прокси-сервера.

Этот сценарий может использоваться для обеспечения доступа к контенту с региональными ограничениями, для интеграции сети регионального офиса с существующей глобальной сетевой иерархией компании, для обеспечения конфиденциальности внешних коммуникаций компании.

Update via proxy

Активация лицензии или обновление ПО узлов UserGate (NGFW, MC, LogAn) проходит через внешний прокси-сервер. В качестве такого прокси может быть любой HTTP(S) прокси-сервер. Поддерживается опциональный режим с аутентификацией на внешнем прокси-сервере по логину/паролю.



Журналирование событий лицензирования или обновления ПО через внешний прокси-сервер производится в Журнале событий. В описании каждого такого обновления добавляется тег **proxy** с адресом и портом прокси-сервера. Например, **proxy: https://10.10.0.1:3128**.

Активация лицензий или ПО через внешний прокси-сервер может производиться на NGFW, UGMC, LogAn, SIEM.

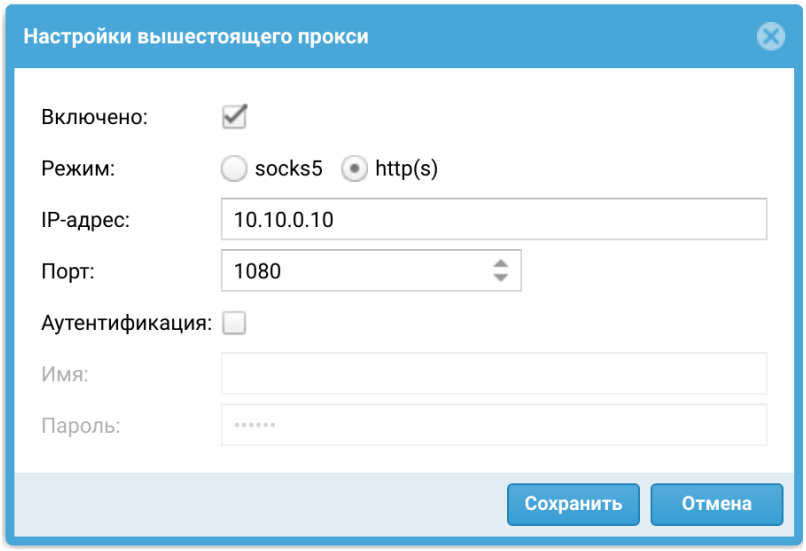
Одним из примеров использования такого сценария может быть случай, когда оборудование UserGate (например, UGMC, LogAn) находится внутри организации с закрытым контуром, без прямого выхода в интернет для обновления ПО.

> **Примечание**
>
> **Настройки функциональности Upstream Proxy для NGFW, LogAn могут прописываться в соответствующих шаблонах на UGMC и применяться к управляемым узлам через UGMC.**

Настройки Upstream Proxy

Настройка Upstream Proxy в консоли администратора

Настройка **сценария перенаправления трафика** на вышестоящий прокси-сервер производится в разделе **UserGate —>Настройки —> Вышестоящий прокси**.

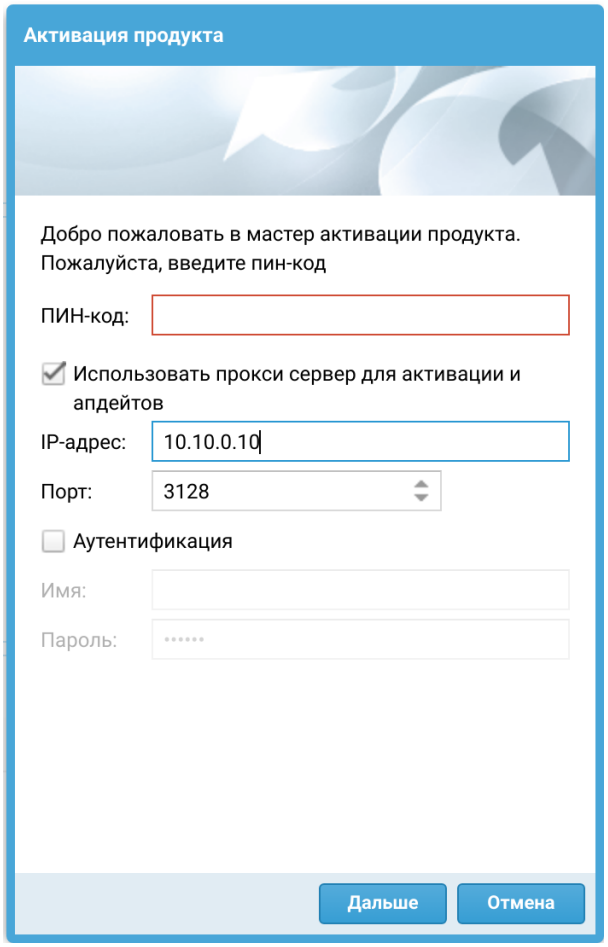


Необходимо указать режим работы вышестоящего прокси-сервера (HTTP(S)) или SOCKS5), его IP-адрес и порт. Если для доступа к вышестоящему прокси-серверу требуется аутентификация, необходимо указать соответствующий логин и пароль.

Сценарий обновления лицензии или ПО узла UserGate через внешний прокси-сервер имеет одинаковую сквозную настройку для активации лицензии и для обновления ПО. Настройку можно сделать либо в разделе **Лицензия** в **Дашборде,** либо в разделе У**правление устройством** в **Настройках**. Параметры, установленные в одном из этих разделов, будут отображаться и во втором.

Настройки в **Дашборде**:

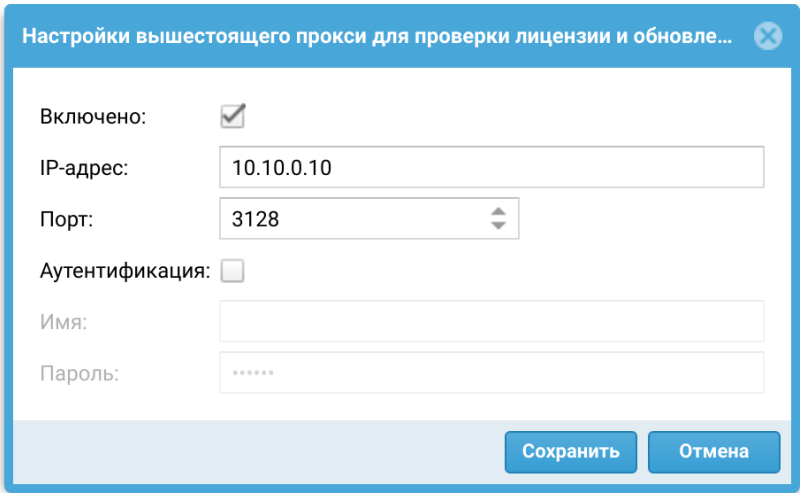
Перейти в раздел **Дашборд → Лицензия** и нажать на строку регистрации. В окне активации нажать на строку **настройки вышестоящего прокси**.



В открывшемся окне настройки необходимо указать IP-адрес и порт внешнего HTTP прокси-сервера. Если для доступа к внешнему прокси-серверу требуется аутентификация, необходимо указать соответствующий логин и пароль.

Настройки в разделе **Управление устройством**:

Перейти в раздел **UserGate → Управление устройством → Операции с сервером** и нажать **Настроить** для операции настройки вышестоящего прокси для проверки лицензий и обновлений.



В открывшемся окне настройки необходимо указать IP-адрес и порт внешнего HTTP прокси-сервера. Если для доступа к внешнему прокси-серверу требуется аутентификация, необходимо указать соответствующий логин и пароль.

Настройка Upstream Proxy в CLI

Описание настроек Upstream Proxy в интерфейсе командной строки (CLI) смотрите в разделе Настройка Upstream Proxy.

Управление сертификатами

Общие сведения

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

Для выполнения данных функций NGFW использует различные типы сертификатов:

Наименование	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, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. Этот сертификат должен быть выпущен со следующими параметрами: • Subject name — значение, установленное для домена **Домен Auth captive-портала**, определенного на странице **Настройки**. • Subject Alternative names — необходимо указать все домены, для которых используется данный сертификат, как они заданы на странице **Настройки**: ◦ домен Auth captive-портала. ◦ домен Logout captive-портала. ◦ домен страницы блокировки. ◦ домен FTP поверх HTTP.

Наименование	Описание
	◦ домен для веб-портала, указанный в настройках веб-портала. По умолчанию используется подписанный с помощью сертификата инспектирование SSL сертификат, выпущенный для домена auth.captive, со следующими параметрами: • Subject name = auth.captive • Sunject alternative names = auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive Если администратор не загрузил свой собственный сертификат для обслуживания этой роли, то NGFW самостоятельно в автоматическом режиме перевыпускает данный сертификат при изменении администратором одного из доменов на странице **Настройки** (домены для auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive). **Примечание** **Если администратор использует отдельный сертификат для домена Captive-портала, то он обязательно должен 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, то при аутентификации через сертификат в браузере будет выдаваться ошибка безопасности.**
SSL инспектирование	Сертификат класса удостоверяющего центра. Он используется для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. Например, при перехвате HTTPS-трафика сайта yahoo.com оригинальный сертификат, выданный: Subject name = yahoo.com Issuer name = VeriSign Class 3 Secure Server CA — G3, подменяется на Subject name = yahoo.com Issuer name = компания, как она указана в сертификате центра сертификации, заведенного в NGFW.

Наименование	Описание
	Данный 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 для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.
SSL инспектирование (корневой)	Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.
Пользовательский сертификат	Сертификат, который назначается пользователю NGFW. Пользователь может быть, как заведен локально, так и получен из LDAP. 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 NGFW с сервером SSO SAML IDP. Подробно о настройке работы NGFW с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства.
Веб-портал	Сертификат, используемый для веб-портала. Если данный сертификат не указан явно, то NGFW использует сертификат SSL Captive-портала, выпущенный сертификатом для инспектирования SSL. Подробно о настройке веб-портала смотрите в соответствующем разделе руководства.

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

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку **Создать** в разделе **Сертификаты**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Страна** — страна, в которой выписывается сертификат. • **Область или штат** — область или штат, в котором выписывается сертификат. • **Город** — город, в котором выписывается сертификат. • **Название организации** — название организации, для которой выписывается сертификат. • **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • **E-mail** — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в NGFW. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата (SSL веб-консоли, инспектирование SSL, УЦ для авторизации в веб-консоли). В случае, если вы выбрали SSL веб-консоли, NGFW перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. Сертификат инспектирования SSL начинает работать немедленно после того, как его выбрали. Более детально об инспектировании HTTPS смотрите в главе Инспектирование SSL.

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

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	

Наименование	Описание
	Выбрать тип экспорта: • **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в приложении Установка сертификата локального удостоверяющего центра. • **Экспорт CSR** — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности UserGate не разрешает экспорт приватных ключей сертификатов.

Примечание

Пользователи могут скачать себе для установки сертификат инспектирования SSL с UserGate по прямой ссылке: http://UserGate_IP:8002/cps/ca

Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

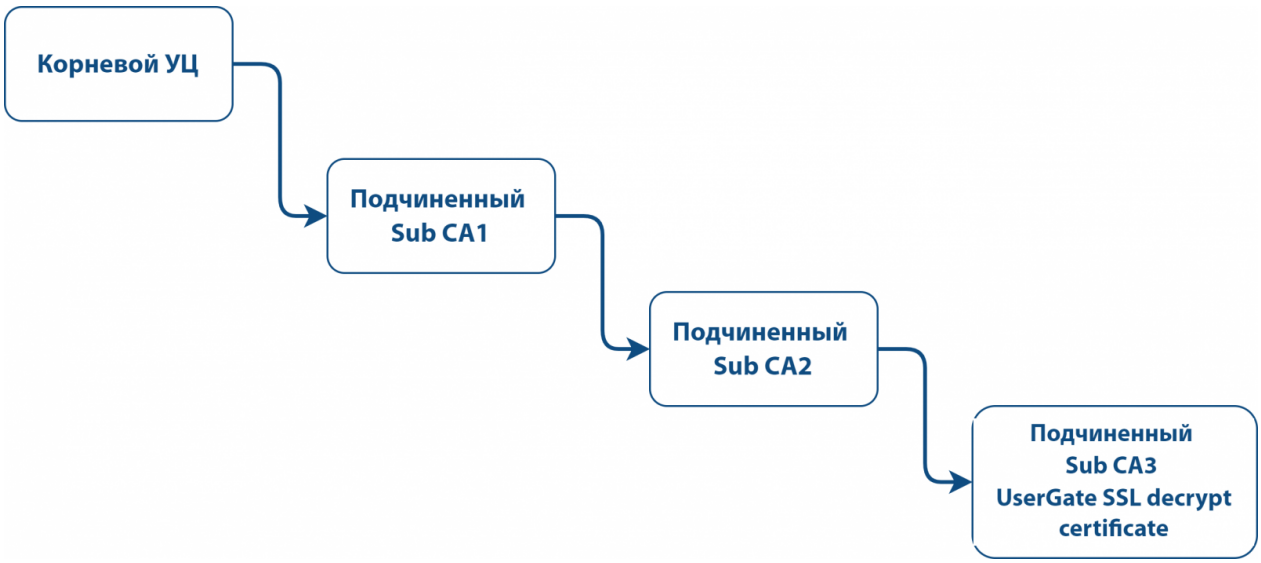
Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку **Импорт**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата.

Наименование	Описание
	• **Файл сертификата**: загрузите файл, содержащий данные сертификата. • **Приватный ключ**: загрузите файл, содержащий приватный ключ сертификата. • **Пароль** для приватного ключа, если таковой требуется. • **Цепочка сертификатов** – файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Использование корпоративного УЦ для создания сертификата инспектирования SSL

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

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



Пример структуры корпоративного УЦ

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

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

1. Сертификат класса удостоверяющего центра (CA):
    - В расширении X509v3 Basic Constraints (RFC 5280) сертификата должен быть атрибут CA:TRUE.
    - В разделе **UserGate → Сертификаты** консоли администратора такие сертификаты помечаются иконкой **Файл сертификата УЦ** слева от названия сертификата.
1. 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** раздела **UserGate → Сертификаты** консоли администратора для такого сертификата будет указано **Отсутствует**.
    - Если в сертификате используется расширение X509v3 Key Usage, то для инспектирования SSL обязательно должны присутствовать атрибуты digitalSignature и keyCertSign.
        - В столбце **Назначение сертификата** раздела **UserGate → Сертификаты** консоли администратора для такого сертификата будет указано **Digital signature** и **Certificate signing**.

> **Примечание**
>
> **UserGate не поддерживает алгоритм подписи rsassaPss. Необходимо, чтобы вся цепочка сертификатов, которая используется для выписывания сертификата для инспектирования SSL, не содержала данного алгоритма подписи.**

Для выполнения этой задачи следует выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать CSR-запрос на создание сертификата в NGFW.	Нажать на кнопку **Создать → Новый CSR**. Заполнить необходимые поля и создать CSR. Будет создан приватный ключ и файл запроса. С помощью кнопки **Экспорт** скачать файл запроса.
Шаг 2. Создать сертификат на основе подготовленного CSR.	В Microsoft CA создать сертификат на основе полученного на предыдущем шаге 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». Обратитесь к документации Microsoft за более подробной информацией. По окончании процедуры вы получите сертификат (публичный ключ), подписанный УЦ Sub CA2.
Шаг 3. Скачать полученный сертификат.	Из веб-консоли Microsoft CA скачать созданный сертификат (публичный ключ).
Шаг 4. Загрузить сертификат в созданный ранее CSR.	В NGFW выбрать созданный ранее CSR и нажать кнопку **Редактировать**. Загрузить файл сертификата и нажать **Сохранить**.
Шаг 5. Указать тип сертификата – инспектирование SSL.	В NGFW выбрать созданный ранее CSR и нажать кнопку **Редактировать**. В поле **Используется** указать **SSL инспектирование**.
Шаг 6. Скачать сертификаты для промежуточных УЦ (Sub CA1 и Sub CA2).	В веб-консоли Microsoft CA выбрать и скачать сертификаты (публичные ключи) для УЦ Sub CA1 и Sub CA2.
Шаг 7. Загрузить сертификаты Sub CA1 и Sub CA2 в NGFW.	С помощью кнопки **Импорт** загрузить скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2.
Шаг 8. Установить тип — инспектирование SSL (промежуточный) для сертификатов Sub CA1 и Sub CA2.	В UserGate выбрать загруженные сертификаты и нажать кнопку **Редактировать**. Указать в поле **Используется — Инспектирование SSL (промежуточный)** для обоих сертификатов.
Шаг 9. Загрузить сертификат Root CA в UserGate (опционально).	С помощью кнопки **Импорт** загрузить корневой сертификат организации в NGFW. С помощью кнопки **Редактировать** указать в поле **Используется — Инспектирование SSL (корневой)**.

Профили клиентских сертификатов

Профиль клиентского сертификата позволяет управлять сертификатами для обеспечения безопасности и подтверждения подлинности в сетевых соединениях. В профиле указываются сертификаты УЦ, методы проверки актуальности пользовательских сертификатов, методы выбора имени пользователя для аутентификации.

Профиль клиентского сертификата используется для валидации предоставленного клиентом сертификата. Сертификат клиента проверяется на валидность для каждого сертификата УЦ из списка.

При выборе режима аутентификации посредством сертификатов (PKI) указывается сконфигурированный ранее профиль клиентского сертификата, который в дальнейшем можно будет использовать в различных подсистемах NGFW, например, Captive-портал, VPN, web-портал, reverse proxy.

Чтобы создать профиль клиентского сертификата, необходимо в разделе **Настройки → UserGate → Профили клиентских сертификатов** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля клиентских сертификатов.
Описание	Опциональное описание профиля.
Получать имя пользователя из	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • Common-name — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • Subject altname email — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • Principal name — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, берется первый, указанный в сертификате.
Сертификаты УЦ	Сертификаты УЦ, назначаемые профилю.

Наименование	Описание
	Список сертификатов удостоверяющих центров. Используется для валидации предоставленного клиентом сертификата. Сертификат клиента проверяется на валидность для каждого сертификата УЦ из списка. Перебор списка идет сверху вниз.
Проверка отозванных сертификатов	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: • Не проверять — не проверять ни один сертификат. • Вся цепочка — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • Сертификат пользователя — проверять только сертификат клиента. • Считать валидным, если статус неизвестен — 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).
Тайм-аут проверки	Интервал времени, по истечению которого NGFW перестает ожидать ответа от службы списков отзыва сертификатов.

Расширение системного раздела

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить **новый** диск необходимого размера в свойствах виртуальной машины UserGate.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел **Support menu**. В открывшемся разделе выбрать **Expand data partition** и запустить процесс расширения раздела.
Шаг 3. Проверить размер системного раздела.	

Наименование	Описание
	После завершения процесса расширения загрузить узел и в разделе **Дашборд → Диски** проверить размер системного раздела.

> **Примечание**
>
> **Расширение системного раздела путем увеличения размера *имеющегося* диска виртуальной машины возможно только при сбросе узла до заводских настроек, т.е. при выполнении операции factory reset.**

Системные утилиты

Системные утилиты доступны администратору во время загрузки 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) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к NGFW. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
UGOS NGFW	Загрузка NGFW с выводом диагностической информации о загрузке в последовательный порт.
UGOS NGFW (failsafe)	Загрузка NGFW в упрощённом видеорежиме.
Support menu	Войти 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:

Наименование	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 NGFW. **Важно!** Для расширения системного раздела с сохранением данных и настроек NGFW необходимо средствами гипервизора добавить **новый** диск и затем выполнить операцию **Expand data partition**, как указано в статье руководства администратора Расширение системного раздела.
Create backup	Создать полную копию диска NGFW на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление NGFW с внешнего USB носителя.
Factory reset	**Сброс состояния NGFW. Версия ПО останется той, которая была установлена при запуске команды. Все данные и настройки будут утеряны.**
Exit	Выход и перезагрузка устройства.

НАСТРОЙКА СЕТИ

Настройка зон

Зона в NGFW — это логическое объединение сетевых интерфейсов. Политики безопасности 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.

Администраторы NGFW могут 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.	Нажать на кнопку **Добавить** и дать название зоне
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.

Наименование	Описание
	• **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 — 300 запросов в секунду, для порога отбрасывания пакетов — 600 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). • **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).

Наименование	Описание
	• **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). • **SCADA** — сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • **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** — 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 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.

Наименование	Описание
	• **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). 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 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

Наименование	Описание
	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

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN-интерфейсы. Раздел отображает все интерфейсы каждого узла кластера. Настройки интерфейсов специфичны для каждого из узлов, то есть не глобальны.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать 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.
- Назначить зону интерфейсу.

- Назначить профиль Netflow для отправки статистических данных на Netflow коллектор.
- Назначить профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Доступно только для интерфейсов типа адаптер.
- Назначить Алиас/Псевдоним — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.
- Изменить физические параметры интерфейса — MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
- Настроить работу DHCP-релея на выбранном интерфейсе. Для этого необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.
- Мост.
- PPPoE.
- VPN.
- Tunnel.
- Loopback.

Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает VLAN.

Наименование	Описание
Название	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN.
Описание	Опциональное описание интерфейса.
Тип интерфейса	Указать 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.
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов.
Имя узла	Имя узла в кластере, на котором создается данный VLAN.
Интерфейс	Физический интерфейс, на котором создается VLAN.
Зона	Зона, которой принадлежит VLAN.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе 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 — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
DHCP-релей	Настройка работы DHCP-релея на VLAN-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический

агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает бонд.
Название	Название бонда.
Имя узла	Узел кластера NGFW, на котором будет создан бонд.
Зона	Зона, к которой принадлежит бонд.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе 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	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **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 снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **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

Наименование	Описание
	применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **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. • **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. • **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, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет 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. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.

Наименование	Описание
Up delay (мсек)	Задает 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. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом 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 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. 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 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.
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • **Layer 2** — 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.

Наименование	Описание
	• **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • **Layer 3+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 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.
DHCP-релей	Настройка работы DHCP-релея на бонд-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Создание моста (bridge)

Сетевой мост работает на канальном уровне сетевой модели OSI (L2), при получении из сети кадра сверяет MAC-адрес последнего и, если он не принадлежит данному сегменту, передает (транслирует) кадр дальше; если кадр принадлежит данному сегменту, мост ничего не делает.

Интерфейс мост можно использовать в NGFW аналогично обычному интерфейсу. Кроме этого, через мост можно настроить фильтрацию передаваемого контента на уровне L2 без внесения изменений в сетевую инфраструктуру компании. Простейшая схема использования NGFW в качестве решения, обеспечивающего контентную фильтрацию на уровне L2, выглядит следующим образом:

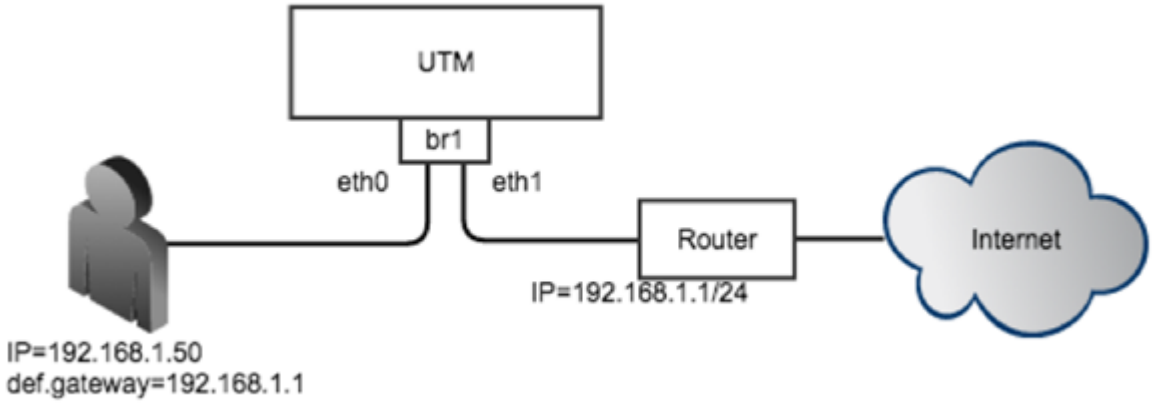


Рисунок 4 Использование моста

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

При выборе режима 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 АСУ ТП и Mail security. Контентная фильтрация работает в этом режиме.

> **Внимание!**
> **Функционал DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.**

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

Если мост создается в ПАК NGFW, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить 2 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 NGFW отключено.
- Система внутренней диагностики обнаружила проблему в работе ПО NGFW.

Более подробно о сетевых интерфейсах, поддерживающих режим байпас смотрите в спецификации на оборудование ПАК NGFW.

С помощью кнопки **Добавить мост** администратор может объединить несколько физических интерфейсов в новый тип интерфейса — мост. Необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает интерфейс мост.
Название	Название интерфейса.
Имя узла	Узел кластера NGFW, на котором создать интерфейс мост.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2.
Зона	Зона, к которой принадлежит интерфейс мост.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе 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 NGFW.
STP (Spanning Tree Protocol)	Включает использование STP для защиты сети от петель.
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.
DHCP-релей	Настройка работы DHCP-релея на bridge-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется

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

Интерфейс PPPOE

PPPoE (**Point-to-point protocol over Ethernet**) — сетевой протокол канального уровня передачи кадров PPP через Ethernet. С помощью кнопки **Добавить**, выбрав **Добавить PPPoE**, администратор может создать PPPoE интерфейс. При создании необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает интерфейс PPPoE.
Имя узла	Узел кластера NGFW, на котором создать интерфейс PPPoE.
Интерфейс	Указать интерфейс, на котором будет создаваться интерфейс PPPoE.
Зона	Зона, к которой принадлежит интерфейс PPPoE.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе 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.
Логин	Имя пользователя для соединения PPPoE.
Пароль	Пароль пользователя для соединения PPPoE.
Переподключаться автоматически	Включает переподключение соединения при обрыве связи.
Тип аутентификации	

Наименование	Описание
	Протоколы аутентификации, использующиеся в протоколе PPP: • **CHAP** — Challenge Handshake Authentication Protocol — протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём. • **PAP** — Password Authentication Protocol — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (без шифрования).
Интервал между попытками подключения (сек.)	Интервал времени в секундах после разрыва соединения перед повторным запуском.
Маршрут по умолчанию	Устанавливает интерфейс PPPoE в качестве маршрута по умолчанию.
Интервал проверки соединения (сек.)	Интервал проверки соединения.
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которого NGFW считает, что соединение отсутствует и разрывает его.
Использовать DNS-сервер провайдера	Если опция включена, то NGFW использует DNS-серверы, выданные провайдером.
Количество попыток подключения	Количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены.
PPPoE сервис	Имя сервиса необходимо прописывать в случае предоставления провайдером. Если имя сервиса не используется, поле необходимо оставить пустым.

Интерфейс VPN

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 NGFW, 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.

В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры:

Наименование	Описание
Название	Название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW будут также помещены в эту зону.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе 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 предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес. Для использования интерфейса, используемого в роли клиента, необходимо выбрать Динамический режим.
MTU	Размер MTU для выбранного интерфейса.

По умолчанию в системе уже созданы 3 VPN-интерфейса:

- **tunnel1**, который рекомендовано использовать для Remote access VPN.
- **tunnel2**, который рекомендовано использовать для серверной части Site-to-Site VPN.
- **tunnel3**, который рекомендовано использовать для клиентской части Site-to-Site VPN.

Интерфейс туннель

Интерфейс туннель — это виртуальный сетевой адаптер, который может использоваться для создания соединения точка-точка через IP-сеть. Поддерживаются следующие типы туннельных интерфейсов:

- GRE — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47.
- IPIP — это 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 Source IP — точкой входа в туннель, и Destination IP — точкой выхода из туннеля.
- VXLAN — это протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789.

Для создания туннельного интерфейса в разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить туннель.** Задайте следующие параметры:

Наименование	Описание
Включено	Включение или выключение данного интерфейса.
Название	Название интерфейса, должно быть в виде greN, где N — это порядковый номер туннельного интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относится данный 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 туннеля — GRE, IPIP, VXLAN.
MTU	Размер MTU для выбранного интерфейса.
Локальный IP	Локальный адрес point-to-point интерфейса.

Наименование	Описание
Удаленный IP	Удаленный адрес point-to-point интерфейса.
IP интерфейса	IP-адрес, назначенный туннельному интерфейсу.
VXLAN ID	Идентификатор VXLAN. Только для типа туннеля VXLAN.

Интерфейс loopback

Для создания loopback-интерфейса необходимо в разделе **Сеть → Интерфейсы** нажать кнопку **Добавить** и выбрать **Добавить loopback-интерфейс.** Далее необходимо задать следующие параметры:

Параметр	Описание
Включено	Включает интерфейс.
Название	Название интерфейса в виде loopbackN, где N — целое число.
Описание	Опциональное описание интерфейса.
Имя узла	Выбор узла кластера NGFW, на котором создается интерфейс.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2.
Зона	Зона, к которой принадлежит интерфейс.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
Профиль LLDP	Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol (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.
DHCP-релей	Настройка работы DHCP-релея на интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес UserGate** IP-

Параметр	Описание
	адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Настройка шлюзов

Для подключения NGFW к интернету необходимо указать IP-адрес одного или нескольких шлюзов. Если для подключения к интернету используется несколько провайдеров, то необходимо указать несколько шлюзов. Настройка шлюза уникальна для каждого из узлов кластера.

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

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок **Балансировка** и указать **Вес** каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз). При распределении трафика между шлюзами с разными весами происходит: 1.Вычисление хэша от адресов источника и назначения. 2.Выбор шлюза Трафик распределяется с учётом весов. Пусть настроены 2 шлюза: • **n1**, **n2** — сессии, проходящие через шлюзы. • **w1**, **w2** — веса шлюзов. Тогда сессии между шлюзами будут распределяться согласно **n1/w1 = n2/w2**.

Наименование	Описание
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить **Проверку сети**, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет (с помощью ping) с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли(в случае если в текущей сессии не менялся порядок сортировки отбражаемых шлюзов,смена порядка сортировки не влияет на процесс выбора шлюза). По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Состояние шлюза (доступен — зеленый, не доступен — красный) определяется следующим образом:

Наименование	Описание
Проверка сети отключена	Шлюз считается доступным, если NGFW может получить его MAC-адрес с помощью ARP-запроса. Проверка наличия доступа в интернет через этот шлюз не производится. Если MAC-адрес шлюза не может быть определен, шлюз считается недоступным.
Проверка сети включена	Шлюз считается доступным, если: • NGFW может получить его MAC-адрес с помощью ARP-запроса. • Проверка наличия доступа в интернет через этот шлюз завершилась успешно. В противном случае шлюз считается недоступным.

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.

NGFW может также выступать в качестве DHCP-релея, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный

DHCP-сервер. Более подробно о настройке DHCP-релея можно посмотреть в разделе Настройка интерфейсов.

В 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.
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

Данный раздел содержит настройки сервисов DNS и DNS-прокси.

Для корректной работы продукта необходимо, чтобы 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.

Наименование	Описание
	Внимание! **Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.**
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.
Только A и AAAA DNS-записи для не идентифицированных пользователей (защита от VPN поверх DNS)	Если защита включена, то UserGate отвечает только на запросы на записи A 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).

Наименование	Описание
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 (A-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

В крупных сетях зачастую множество логических сетей используют для прохождения трафика одни и те же сетевые устройства. Данный трафик должен быть разделен на сетевых устройствах, в первую очередь для уменьшения риска несанкционированного доступа между сетями.

Виртуальные маршрутизаторы или **Virtual Routing and Forwarding (VRF)** обеспечивают разделение трафика путем разделения сетевых интерфейсов в независимые группы. Трафик из одной группы интерфейсов не может попасть в другие группы интерфейсов.

Каждый виртуальный маршрутизатор имеет свою собственную таблицу маршрутизации. Таблица маршрутизации виртуального роутера может содержать запись о маршрутах, заданных статически или полученных с помощью протоколов динамической маршрутизации — BGP, OSPF, RIP.

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

Интерфейсы, не вошедшие ни в один из виртуальных маршрутизаторов, автоматически назначены в виртуальный маршрутизатор — **Виртуальный маршрутизатор по умолчанию.**

Виртуальные маршрутизаторы имеют следующие ограничения:

- Следующие сервисы могут быть использованы только в Виртуальном маршрутизаторе 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.
- Действие правил NAT, DNAT, Port forwarding распространяются на все виртуальные маршрутизаторы.
- Зоны глобальны, то есть настройки зоны, и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

Примечание

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

Для добавления виртуального маршрутизатора необходимо выполнить следующие действия:

Примечание!

Следующие префиксы не могут быть использованы для задания имени виртуального маршрутизатора: port, gre, egress, ingress, tun, tap, erspan, ppp, bond, bridge, pimreg.

Примечание!

При создании виртуального маршрутизатора его имя не должно содержать заглавных букв, и должно иметь длину не менее трех символов.

Наименование	Описание
Шаг 1. Создать виртуальный маршрутизатор.	В разделе **Сеть → Виртуальные маршрутизаторы** нажмите добавить и задайте имя и описание нового виртуального маршрутизатора. Укажите имя узла, на котором создается данный виртуальный маршрутизатор при наличии кластера.
Шаг 2. Добавить интерфейсы в созданный виртуальный маршрутизатор.	В закладке **Интерфейсы** укажите интерфейсы, которые должны быть помещены в данный виртуальный маршрутизатор. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, не могут быть добавлены; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие.
Шаг 3. Добавить статические маршруты (опционально).	Добавьте маршруты (кроме маршрута по умолчанию), которые будут применены к трафику в данном виртуальном маршрутизаторе. Подробнее читайте в разделе Статические маршруты. Маршрут по умолчанию добавляется в разделе **Сеть → Шлюзы**. Подробнее о настройке шлюзов читайте в разделе Настройка шлюзов.
Шаг 4. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации OSPF (опционально).	Настройте протокол OSPF для построения динамической карты маршрутов. Более подробно смотрите раздел руководства OSPF.
Шаг 5. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации BGP (опционально).	Настройте протокол BGP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства BGP.
Шаг 6. Добавить динамические маршруты, получаемые с помощью протокола	Настройте протокол RIP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства RIP.

Наименование	Описание
маршрутизации RIP (опционально).	
Шаг 7. Настроить мультикастинг (опционально).	Настройте параметры мультикастинга в данном виртуальном маршрутизаторе. Более подробно смотрите раздел руководства Мультикастинг.

Статические маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей. Маршрут применяется локально к тому узлу кластера и в тот виртуальный маршрутизатор, в котором он создается.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Задать название и описание данного маршрута.	В разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Статические маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 3. Указать тип данного маршрута.	Возожно указать следующие типы маршрутов: • Unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • Blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата. • 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).
Шаг 4. Указать адрес назначения.	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 5. Указать шлюз.	

Наименование	Описание
	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с NGFW.
Шаг 6. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то NGFW сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 7. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

Протоколы динамической маршрутизации

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

Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически.

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

NGFW поддерживает работу трех протоколов маршрутизации — OSPF, BGP, RIP.

OSPF

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

маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации — вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол 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). Подробно о работе протокола OSPF читайте в соответствующей технической документации.

> **Примечание**
>
> **При работе протокола OSPF в кластере отказоустойчивости в режиме Active-Passive, узел, который обладает ролью Slave, автоматически назначает стоимость для всех своих интерфейсов и для списков редистрибуции в 2 раза выше, чем установленная на узле стоимость. Тем самым обеспечивается приоритет Master-узла в маршрутизации трафика.**

Для настройки OSPF в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить OSPF-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **OSPF** и настройте OSPF-роутер.

При настройке OSPF-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного OSPF-роутера.
Идентификатор роутера	

Наименование	Описание
	IP-адрес роутера. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору).
Redistribute	Распространять другим OSPF-роутерам маршруты в непосредственно подключенные к NGFW сети (connected) или статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel).
Метрика	Установить метрику распространяемым маршрутам. Для задания метрики по-умолчанию укажите в этом поле значение 0. (Метрика по-умолчанию для Мастер ноды кластера равна 20. Метрика по-умолчанию для запасной ноды равна 40.)
Default originate	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию.

При настройке интерфейсов OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного интерфейса.
Интерфейс	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор.
Тип сети	Выбор типа сети для оптимизации процесса установления соседства. Доступны следующие параметры: • **Не установлен**. • **Broadcast**. • **Point-to-point**. • **Point-to-multipoint**.
Пассивный режим	Включение/отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается слать пакеты обновления протокола маршрутизации.
Стоимость	Стоимость (cost) канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и

Наименование	Описание
	используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1.
Приоритет	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.
Интервал hello	Время в секундах, через которое маршрутизатор посылает hello-пакеты. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд.
Интервал dead	Интервал времени в секундах, по истечении которого соседний маршрутизатор считается неработающим. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд.
Интервал повторения	Устанавливает временный интервал перед повторной отсылкой пакета LSA. Значение по умолчанию 5 секунд.
Задержка передачи	Устанавливает примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию 1 секунда.
Bfd profile	Определяет настройки BFD для мониторинга OSPF. Это позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF. Подробнее читайте в разделе Профили BFD.
Аутентификация **Вкл**	Включает требование аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов.
Тип аутентификации	Может быть: • **Plain** — передача ключа в открытом виде для аутентификации роутеров. Необходимо указать значение поля **Ключ**. • **Digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Необходимо указать **Ключ** и **MD5 key ID**. Эти параметры должны быть идентичными на всех роутерах для нормальной работы.

Наименование	Описание
	Значение параметра Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.

При настройке области OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данной области.
Имя	Имя для данной области.
Стоимость	Стоимость (cost) маршрута по умолчанию, анонсируемая в stub-область. Значение по умолчанию — 1. В случае, когда между stub-областью и другой областью есть несколько маршрутизаторов (ABR), администратор может назначить разные значения стоимости, анонсируемые из ABR в stub-область, для приоритизации трафика из stub-области через один из этих ABR.
Идентификатор области	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.
Тип авторизации	Может быть: • **Нет** — не требовать авторизацию OSPF-пакетов. • **Plain** — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. • **Digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Идентификация на уровне интерфейсов имеет приоритет над авторизацией на уровне зоны.
Тип области	Определяет тип области. Поддерживаются следующие типы областей: • **Нормальная** — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. • **Тупиковая (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

Наименование	Описание
	системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. • **NSSA** — Not-so-stubby. Зона NSSA определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR).
Не суммировать	Запрещает инжекцию суммированных маршрутов в тупиковые типы областей.
Интерфейсы	Выбор интерфейсов OSPF, на которых будет доступна данная зона.
Виртуальные ссылки	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.

BGP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол BGP.

BGP (Border Gateway Protocol) — динамический протокол маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — External Gateway Protocol). На текущий 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, использующими протоколы внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети. Подробно о работе протокола BGP читайте в соответствующей технической документации.

Для настройки BGP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить BGP-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **BGP** и настройте BGP-роутер.
Шаг 3. Задать фильтры и Routemap (опционально) для ограничения количества получаемых маршрутов.	В разделе **Фильтры** нажать на кнопку **Добавить** и настроить параметры Routemap/фильтров. Добавить столько Routemap/фильтров, сколько необходимо для работы BGP в вашей организации.
Шаг 4. Добавить хотя бы одного BGP-соседа (пира).	В разделе **BGP-соседи** нажать на кнопку **Добавить** и настроить параметры маршрутизатора, относящегося к соседней АС. Добавить столько соседей, сколько необходимо. **Важно!** Согласно требованиям RFC-8212 для каждого соседа необходимо обязательно указать входящие и исходящие фильтры. Без входящих фильтров роутер не будет принимать маршруты с данного соседа, при отсутствии исходящих фильтров роутер не будет анонсировать маршруты на данного соседа. Если интерфейсу NGFW, с которого устанавливается подключение к соседу, назначено несколько IP-адресов, то при настройке BGP-соседа, в случае отсутствия правила NAT, принудительно устанавливающего адрес источника для BGP-сессии с этим соседом, в качестве адреса NGFW необходимо указывать основной (primary) IP-адрес, т.е. адрес, который стоит первым в списке в настройках интерфейса.

При настройке BGP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного BGP-роутера.
Идентификатор роутера	IP-адрес роутера. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору.
Номер автономной системы (AC)	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.
Redistribute	Позволяет распространять другим BGP-маршрутизаторам маршруты в непосредственно подключенные к NGFW сети (connected), статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel), или маршруты, полученные по протоколу OSPF.
Multiple path	Включает балансировку трафика на маршруты с одинаковой стоимостью.
Сети	Список сетей, относящихся к данной AC.

Для добавления BGP-соседей нажмите кнопку **Добавить** и укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного соседа.
Host	IP-адрес соседа.
Описание	Произвольное описание соседа.
Удаленная ASN	Номер автономной системы, к которой относится сосед.
Вес	Вес данных маршрутов, получаемых от данного соседа.
TTL	Максимальное количество хопов, разрешенное до этого соседа.
Bfd profile	Настроить с помощью профиля BFD мониторинг BGP для возможности более быстрого обнаружения неисправностей соединений.

Наименование	Описание
	Для более подробной информации о настройке BFD смотрите 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.
Multihop для eBPGP	Указывает, что до этого соседа непрямое соединение (более одного хопа).
Route reflector client	Указывает, является ли этот сосед клиентом Route reflector.
Soft reconfiguration	Использовать soft reconfiguration (без разрыва соединений) для обновления конфигурации.
Default originate	Анонсировать этому соседу маршрут по умолчанию.
Аутентификация	Включает аутентификацию для данного соседа и задает пароль для аутентификации.
Фильтры BGP-соседей	Ограничивает информацию о маршрутах, получаемых от соседей или анонсируемых к ним.
Routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами.

Routemap позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов. Для создания routemap необходимо указать следующие параметры:

Наименование	Описание
Название	Имя для данного routemap.
Действие	Устанавливает действие для данного routemap, может принимать значения: • **Разрешить** — разрешает прохождение данных, попадающих под условия routemap. • **Запретить** — запрещает прохождение данных, попадающих под условия routemap.
Сравнивать по	

Наименование	Описание
	Условия применения routemap, может принимать значения: • **IP**. Если выбрано данное условие, то в закладке IP-адреса надо добавить все необходимые IP-адреса для данного условия. • **AS путь**. Если выбрано данное условие, то в закладке AS-путь надо добавить все необходимые номера автономных сетей для данного условия. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (_), который интерпретируется как: • Пробел. • Запятая. • Начало строки. • Конец строки. • AS set delimiter { and }. • AS confederation delimiter (and). • **Community**. Если выбрано данное условие, то в закладке Community надо добавить строки всех необходимых BGP community для данного условия.
Установить next hop	Установить для отфильтрованных маршрутов значение next hop в указанный IP-адрес.
Установить вес	Установить для отфильтрованных маршрутов вес в указанное значение.
Установить метрику	Установить для отфильтрованных маршрутов метрику в указанное значение.
Установить предпочтение	Установить для отфильтрованных маршрутов предпочтение в указанное значение.
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для данного маршрута.
Community	Установить значение для BGP community для отфильтрованных маршрутов.

Фильтр позволяет фильтровать маршруты при перераспределении. При создании фильтров необходимо указать следующие параметры:

Наименование	Описание
Название	Имя для данного фильтра.
Действие	Устанавливает действие для данного фильтра, может принимать значения: • **Разрешить** — разрешает прохождение данных, попадающих под условия фильтра. • **Запретить** — запрещает прохождение данных, попадающих под условия фильтра.
Фильтровать по	Условия применения фильтра, может принимать значения: • **IP**. Если выбрано данное условие, то в закладке **IP-адреса** надо добавить все необходимые IP-адреса для данного 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 данное условие, то в закладке **AS-путь** надо добавить все необходимые номера автономных сетей для данного условия.

RIP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол RIP.

RIP (Routing Information Protocol) — протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками (хоп, hop) в

качестве метрики маршрутизации. Подробно о работе протокола RIP читайте в соответствующей технической документации.

Для настройки RIP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить RIP-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и настройте RIP-роутер.
Шаг 3. Указать сети RIP.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и укажите сети RIP, для которых будет работать RIP протокол.
Шаг 4. Настройте интерфейсы RIP.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и произведите настройку интерфейсов RIP.

При настройке RIP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного RIP-роутера.
Версия RIP	Определяет версию протокола RIP. Как правило используется версия протокола 2.
Метрика по умолчанию	Стоимость маршрута. Обычно метрика равна 1 и не может превышать 15.
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 роутеры о том, что данный роутер имеет маршрут по умолчанию.

Маршрутизатор RIP будет слать обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. Необходимо указать 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 отправлять обновления.

При настройке интерфейсов RIP укажите следующие параметры:

Наименование	Описание
Интерфейс	Выберите интерфейс, который будет использоваться для работы протокола RIP. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Посылать версию	Укажите версию протокола RIP, которую маршрутизатор будет отсылать.
Принимать версию	Укажите версию протокола RIP, которую маршрутизатор будет принимать.
Пароль	Строка для авторизации, которая будет посылаться и приниматься в пакетах RIP. Все роутеры, 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 прибыло обновление.
Poison reverse	Метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отсылает его соседу, от которого его получил.
Пассивный режим	Устанавливает режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает их.

Параметры редистрибуции маршрутов позволяют указать какие из маршрутов необходимо отправлять соседям. Возможно задать для редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGPG, а также маршруты в непосредственно подключенные к 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 к тысячам и более потребителей, что особенно эффективно для доставки голосового и видео трафика. Традиционные методы доставки трафика — это unicast

(доставка от точки к точке) и broadcast (широковещательная посылка трафика). Мультикастинг (multicast) позволяет доставить трафик к группе хостов (мультикаст-группа). Хосты (получатели), которые хотят получать данный трафик, должны вступить (присоединиться) к соответствующей мультикаст-группе. Для присоединения хостов к мультикаст-группе используется протокол Internet Group Management Protocol (IGMP). Мультикаст-группа идентифицируется групповым адресом. Для мультикастовых адресов выделена подсеть класса D с верхними 4 битами, установленными в 1110. Таким образом диапазон адресов для мультикаст-трансляций определен как 224.0.0.0 — 239.255.255.255.

Далее маршрутизаторы должны обеспечить эффективную доставку трафика от источника трансляции к получателям. Protocol Independent Multicast (PIM) используется на маршрутизаторах для достижения данной цели.

Маршрутизаторы в мультикастинговой среде можно разделить на First Hop Router (FHR), Rendezvous Point (RP), Last Hop Router (LHR). FHR находится ближе всего к источнику трансляции и отвечает за регистрацию источника трансляции в сети. RP является каталогом доступных мультикаст-источников для Any Source Multicast (ASM) режима. 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, посылая сообщение IGMP membership report.

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

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

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

Режим работы Source Specific Multicast (SSM) используется, когда приемник трафика явно указывает известный ему адрес источника трансляции. В данном 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

Режим работы Any Source Multicast (ASM). В этом режиме приемник трансляции указывает мультикаст-группу, с которой хочет получать трансляцию. Для работы данного режима необходимо наличие маршрутизатора с ролью Rendezvous Point (RP). RP определяет источник трансляции для этой группы для данного приемника. После чего источник и приемник выбирают лучший сетевой путь для пересылки данного мультикаст-трафика. В данном 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 NGFW в качестве LHR мультикаст-роутера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настроить мультикаст-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Мультикаст маршрутизатор** и настройте его.
Шаг 2. Указать интерфейсы, на которых должен работать данный роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Интерфейсы** и произведите настройку интерфейсов. Будут доступны только те интерфейсы, которые относятся к данному виртуальному маршрутизатору.
Шаг 3. Задать Rendezvous points для режима ASM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Rendezvous points** и укажите их адреса.
Шаг 4. Установить необходимые ограничения на доступные мультикаст-группы для режима ASM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Rendezvous points** и укажите адреса разрешенных мультикаст-групп в закладке **Разрешенные группы ASM**. Если оставить этот список пустым, то будут разрешены все групповые адреса.
Шаг 5. Установить необходимые ограничения на доступные мультикаст-группы для режима SSM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Разрешенные группы SSM** и укажите адреса разрешенных мультикаст-групп Если оставить этот список пустым, то будут разрешены все групповые адреса.

При настройке мультикаст роутера возможно указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает мультикаст роутер в данном виртуальном маршрутизаторе.
Использовать ECMP	Разрешает распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). 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).
Использовать ECMP rebalance	Если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). При отключенной опции перераспределяются только те потоки, которые передавались через отключенный интерфейс.
Keep-alive таймер	Интервал в секундах (31-60000), через который маршрутизатор будет посылать сообщения keepalive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.

При настройке интерфейсов можно задать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного интерфейса для мультикастинга.
Интерфейс	Выберите интерфейс, который будет использоваться для работы мультикаста. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Интервал отправки HELLO сообщений	Интервал отправки PIM HELLO сообщений в секундах (1-180). PIM Hello сообщения отправляются периодически со всех интерфесов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг.
Приоритет выбора DR	Приоритет при выборе Designated router (DR) 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 данном интерфейсе.

Наименование	Описание
Использовать IGMPv2	Использовать версию IGMP v2, по умолчанию используется IGMP v3.

При настройке Rendevouz points можно указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данный RP.
Название	Название данного RP.
IP-адрес	Unicast IP-адрес данного RP.
Разрешенные руппы ASM	Список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Нет ограничений, если ничего не задано.

Разрешенные группы SSM — настройка мультикаст роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть укзаны любые сети из диапазона 232.0.0.0/8. Нет ограничений, если ничего не задано.

Исключения из SPT — настройка мультикаст роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

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.

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

Наименование	Описание
	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). 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

Наименование	Описание
	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 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. Система поддерживает следующие типы серверов аутентификации:

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.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. 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.
Секретный ключ	

Наименование	Описание
	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером 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**.
Шаг 2. Настроить DNS-серверы на NGFW.	В настройках NGFW в качестве системных DNS-серверов указать IP-адреса контроллеров домена.

Наименование	Описание
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). • 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

Наименование	Описание
	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. Подробно 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. **Важно!** В настройках NGFW имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из

Наименование	Описание
	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 текущем 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.	Создать пользователя в домене AD, например, kerb@domain.loc с опцией **password never expires**. Установите пароль пользователю kerb.

Наименование	Описание
	Важно! Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb. **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!): ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab Введите пароль пользователя kerb. **Важно!** Команда чувствительна к регистру букв. В данном примере: auth.domain.loc — DNS-запись, созданная для сервера UserGate на шаге 1 DOMAIN.LOC — Kerberos realm domain, обязательно большими буквами! kerb@DOMAIN.LOC — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Шаг 4. Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 5. Настроить синхронизацию времени с контроллером домена.	В настройках UserGate 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 Kerberos. Необходимо использовать отдельную учетную запись.

Наименование	Описание
	Подробно 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 UserGate, 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 текущем 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. Подробно 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 авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах NGFW, например, Captive-портал, VPN, веб-портал и т.д. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства → Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Профиль MFA	Профиль мультифакторной аутентификации. Должен быть предварительно создан в разделе **Профили MFA**, если планируется использовать мультифакторную аутентификацию. Профиль определяет способ доставки одноразового пароля для второго метода аутентификации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее. **Важно!** Мультифакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только те, где пользователь явно вводит свои учетные данные в веб-форму страницы авторизации. В связи с этим, мультифакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Данный параметр определяет, через сколько секунд NGFW переведет пользователя из **Known users** в **Unknown users** при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя).
Время жизни авторизованного пользователя	Данный параметр определяет, через сколько секунд NGFW переведет пользователя из **Known users** в **Unknown users**. По происшествии указанного времени пользователю потребуется повторно авторизоваться на Captive-портале.
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя.
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации.
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например, сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, то 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.

Наименование	Описание
	• **Принять политику** — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный 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 протоколов HTTP и 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.

- Для авторизации пользователей, работающих по протоколу HTTPS, необходимо настроить инспектирование SSL, иначе авторизация 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.
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 относятся 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 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).

Наименование	Описание
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.
HTTPS для страницы аутентификации	Использовать HTTPS при отображении страницы авторизации Captive-портала для пользователей. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. Более подробно о сертификатах смотрите в разделе Управление сертификатами.

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 создания профиля оповещения смотрите в главе Профили оповещений.
От	Указать, от имени кого будут отправляться оповещения.

Наименование	Описание
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.
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 срабатывание 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).

Наименование	Описание
	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. 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 IP-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. 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

После изменения файла конфигурации сервис терминального агента нужно перезапустить.

Таких пользователей также необходимо добавить в NGFW как локальных. О добавлении пользователей читайте в разделе Пользователи. При добавлении необходимо указать **Логин** в формате: «*имя компьютера_имя пользователя*»; пароль указывать не нужно.

> **Примечание**
> **Имя компьютера должно состоять из букв, цифр и знака подчёркивания; использование тире не допускается.**

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**: IP-адрес устройства UserGate, принимающего соединение от агента аутентификации.
- **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 (мультифакторной аутентификации)

Мультифакторная 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.

NGFW поддерживает мультифакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации и следующих типов в качестве второго:

- **TOTP** (Time-based One Time Password) токена в качестве второго. 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 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 NGFW или в доменной учетной записи в Active Directory.

Чтобы настроить мультифакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить авторизацию с помощью Captive-портала.	Мультифакторная авторизация работает только при авторизации пользователей с помощью Captive-портала. Смотрите раздел для подробной информации.
Шаг 2. Создать профиль мультифакторной авторизации.	В разделе консоли **Пользователи и устройства → Профили MFA** создать профиль мультифакторной 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

Наименование	Описание
	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).
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 будут заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Для способа доставки **MFA через email** необходимо указать следующие параметры:

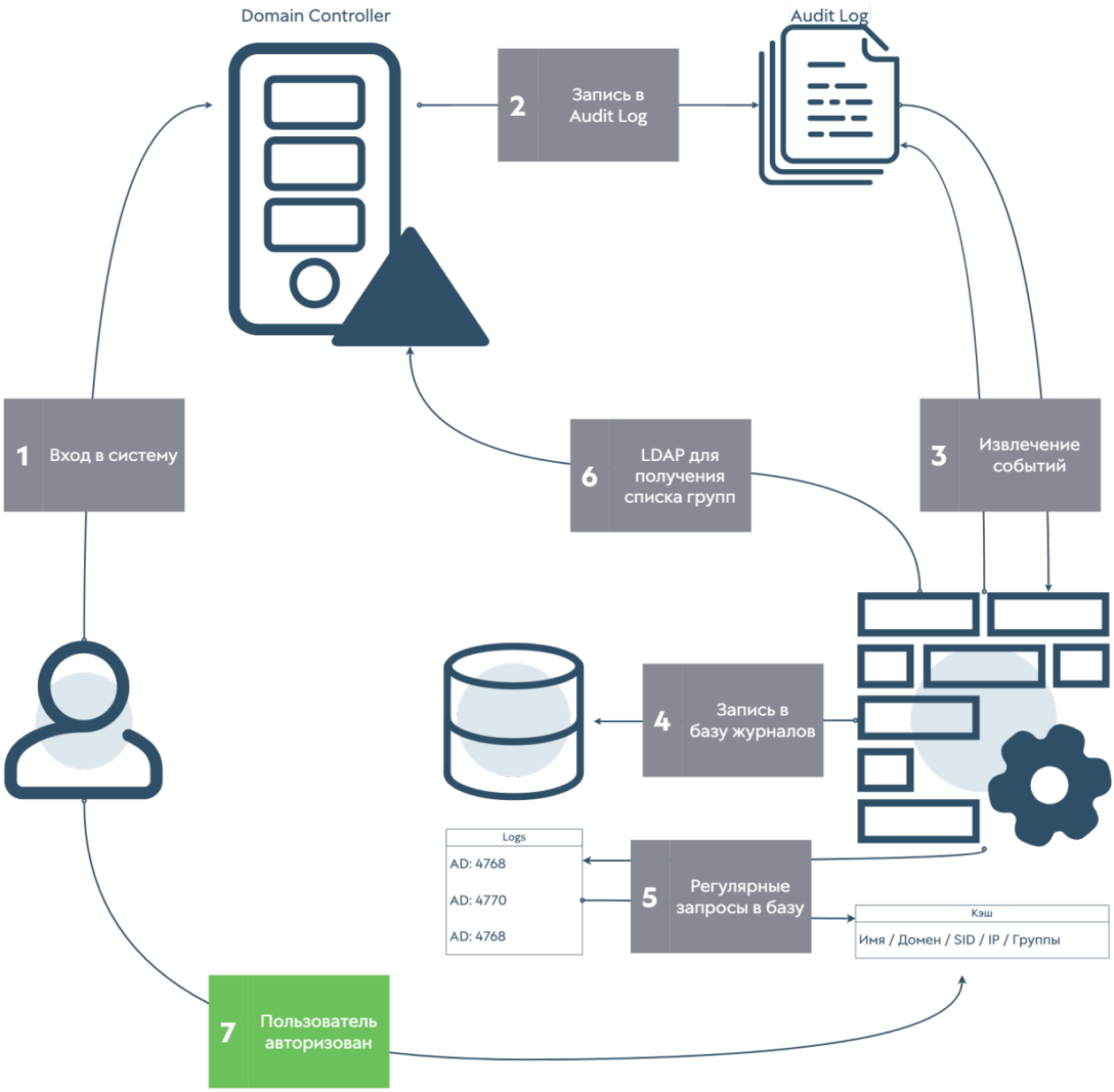
Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по электронной почте смотрите в разделе Профили 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 будут заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

UserID агент

Описание

Предназначен, для осуществления прозрачной аутентификации на выбранных устройствах NGFW. В качестве источника данных аутентификации используются журналы ActiveDirectory(посредством протокола WMI) и Syslog(посредством стандартизированного протокола syslog RFC 3164, RFC 5424, RFC 6587).

Схема работы



Данные для осуществления прозрачной авторизации берутся из журналов ActiveDirectory(AD) и\или Syslog. Для этого агент UserID осуществляет запросы посредством протокола WMI на сервера AD, а в случае с syslog, осуществляет прослушивание порта syslog (по умолчанию tcp\514) и сбор информации, которую присылают сервера syslog. Далее информация фильтруется по событиям входы\выхода, и заносится в Базу Данных.

UserID агент периодически делает запрос в Базу Данных для поиска событий входов\выходов пользователей. Поиск происходит только среди записей, полученных при помощи источников UserID, то есть другие записи (полученные через WMI sensors, Endpoints, Log collector) игнорируются. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя

отправляются на все устройства NGFW, указанные в Профиле редистрибуции источника и производится вход пользователя на NGFW. Таким образом производится авторизация пользователя на всех указанных устройствах. В случае выхода пользователя, ситуация аналогична(за исключением WMI-коннектора, там данные о выходе пользователя сейчас не обрабатываются). Информация о входе\выходе\ошибке сохраняется в журнал UserID.

> **Примечание**
>
> **События, полученные с источников, будут отображены в журналах Агент UserID во вкладке Журналы и отчёты.**

Настройка

В общем случае для настройки сбора информации с источников необходимо выполнить следующее:

Наименование	Описание
Шаг 1. Настроить аудит на серверах AD и Syslog	На серверах AD возможно потребуется включить аудит события безопасности следующих категорий: • Audit LogOn • Audit LogOff • Audit Kerberos Authentication Service • Audit Group Membership На серверах syslog необходимо настроить отправку журналов на IP адрес сборщика логов UserID.

Наименование	Описание
Шаг 2. Создать агента UserID.	Для этого в пункте: **Настройки** → **Пользователи и устройства** → **UserID агент**, нажмите кнопку **Добавить** и выберите нужный тип агента.
Шаг 3. Настроить параметры агента User ID.	Настройка осуществляется в разделе **Пользователи и устройства --> UserID агент**, кнопка **Настроить агент**.
Шаг 4. Настроить источник событий.	В качестве источников могут быть использованы Microsoft Active Directory или Syslog.

При настройке агента необходимо заполнить следующие поля:

Наименование	Описание
Вкладка «Общие»	Общие настройки агента
Интервал опроса (сек.)	Период опроса серверов Active Directory. Значение по умолчанию – 120 секунд.
Время жизни аутентифицированного пользователя (сек.)	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).
Интервал мониторинга syslog (сек.)	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
Вкладка «Настройки syslog сервера»	Предназначена для настройки агента для сбора журналов по протоколу syslog.
Протокол	Протокол для приёма журналов по протоколу syslog: • TCP; • UDP. Для выбора протокола необходимо отметить чекбокс **Включено** в соответствующем блоке.
Порт	Номер порта, использующегося для сбора Syslog событий. По умолчанию – порт 514.

Наименование	Описание
Максимальное количество сессий	Максимальное количество устройств, подключённых одновременно с целью отправки сообщений.
Безопасное соединение	Включение/отключение шифрования потока данных; параметр относится к настройке сервера syslog при выборе протокола TCP. Подробнее об использовании TLS в Syslog читайте в соответствующей документации.
Файл сертификата ЦС	Сертификат удостоверяющего центра (центра сертификации), который используется для установления безопасного соединения; параметр относится к настройке сервера Syslog при выборе протокола TCP.
Файл сертификата	Сертификат, созданный пользователем и подписанный центром сертификации (ЦС); необходимо указать при настройке безопасного соединения; параметр относится к настройке сервера Syslog при выборе протокола TCP.
Вкладка «Ignore network list»	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника по появится в журнале **UserID**. Список может быть создан в разделе **Библиотеки --> IP-адреса** или при настройке агента (кнопка **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов читайте в разделе IP-адреса. Данная настройка является глобальной и относится ко всем источникам.
Вкладка «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.

> **Примечание**
> **При подключении NGFW к Log Analyzer возможна одновременная работа агентов UserID, настроенных на обоих устройствах. Агенты устройств будут работать независимо друг от друга. События журналов агента UserID, полученные NGFW, как и события других журналов, будут переданы на LogAn.**

Microsoft Active Directory

В случае, если в качестве источника информации выступает Microsoft Active Directory необходимо:

Наименование	Описание
Шаг 1. Настроить параметры агента UserID для мониторинга Microsoft AD.	Параметры агента UserID были рассмотрены ранее.
Шаг 2. Настроить источник событий.	Настроить Microsoft Active Directory в качестве источника. Подробнее о параметрах источника читайте далее.

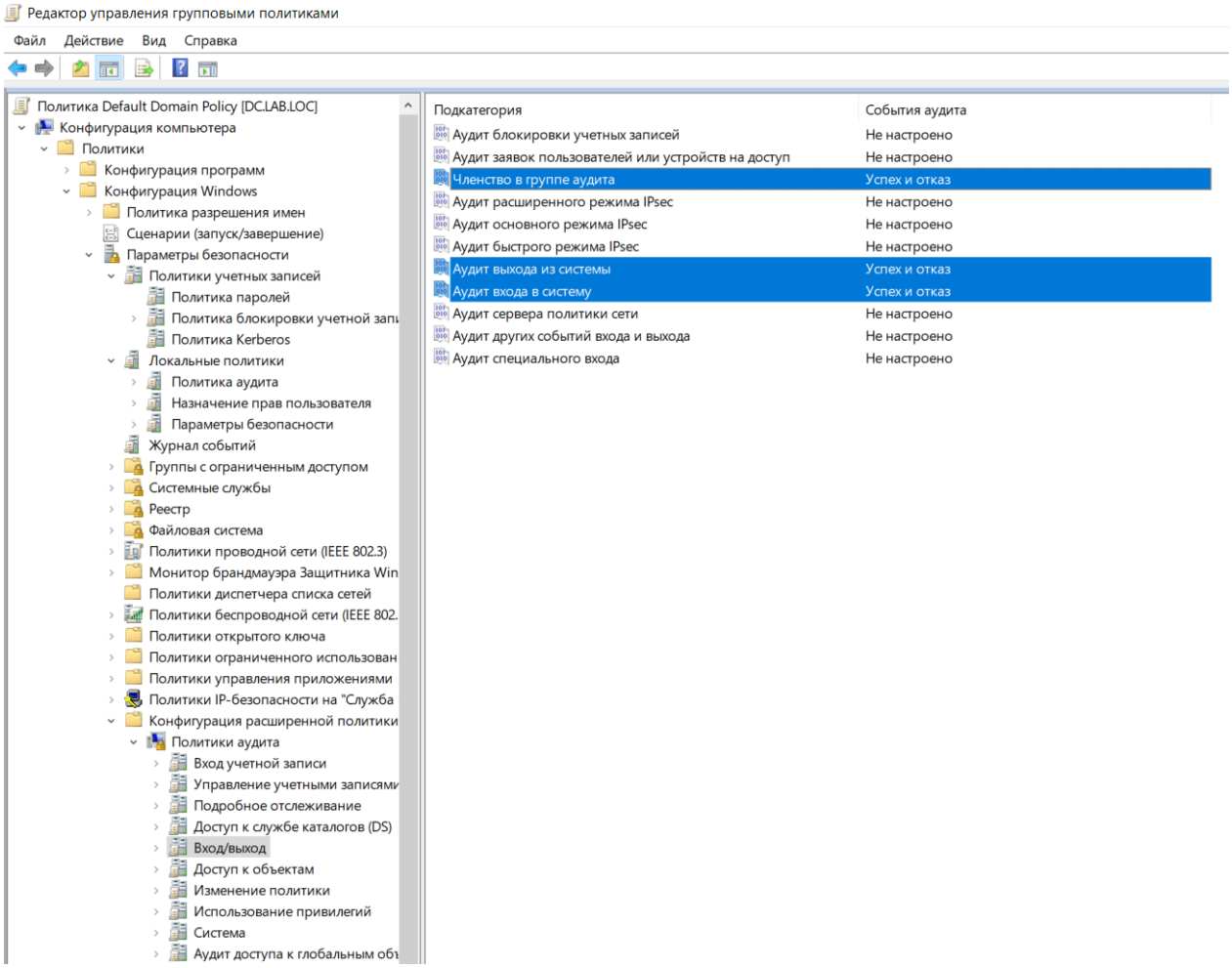
При использовании серверов AD в качестве источников событий NGFW выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). Периодичность выполнения запросов регулируется настройками агента UserID (параметр Интервал опроса). Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы** → **Агент UserID** → **Журнал Windows Active Directory**.
При добавлении источника событий типа Microsoft Active Directory необходимо указать следующие данные:

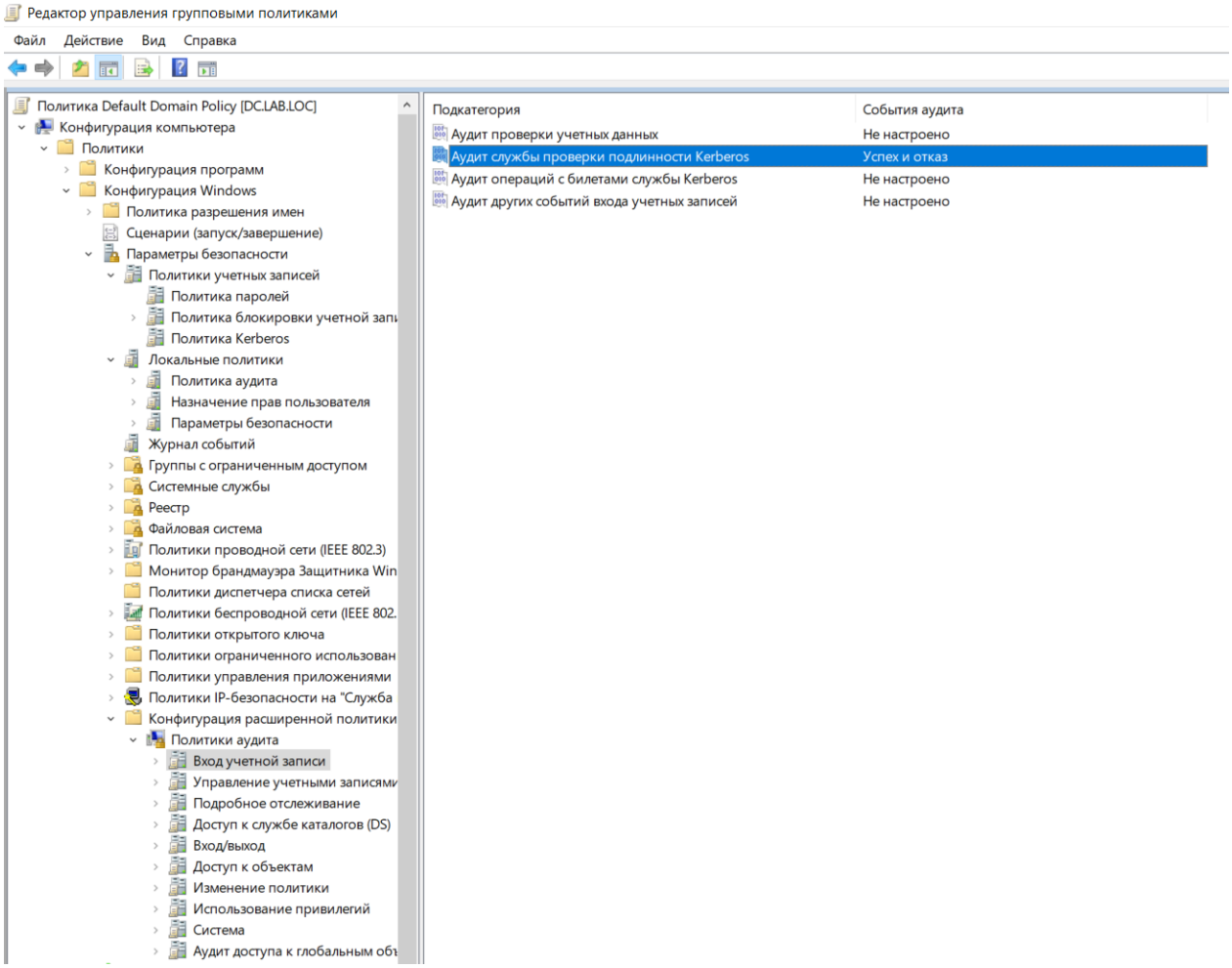
Наименование	Описание
Включено	Включение/отключение получения журналов с источника.
Название	Название источника.
Описание	Описание источника (опционально).
Адрес сервера	Адрес Microsoft Active Directory.
Протокол	Протокол доступа к AD (WMI).

Наименование	Описание
Имя	Имя пользователя для подключения к AD.
Пароль	Пароль пользователя для подключения к AD.
Профиль аутентификации	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD. Подробнее о профилях читайте в разделе Профили аутентификации.

Настройка аудита событий на сервере MS AD

Для включения аудита событий отредактируйте Политики Аудита в Политике домена по умолчанию и Конфигурацию расширенной политики, как указано на следующих снимках экрана, используя оснастку gpedit.msc





Для выполнения WMI-запросов необходимо создать пользователя с соответствующими привилегиями по процедуре, указанной ниже.

Создание пользователя с разрешениями Windows Management Instrumentation (WMI)

> **Внимание!**
>
> **Эти настройки нужны для подключения агента к WMI посредством учетной записи с ограниченными правами.**

Процедура создания и конфигурация пользователя на сервере Windows с разрешениями для просмотра WMI.

1. Создайте учетную запись пользователя на контроллере домена:

   - Перейдите в меню **Пуск > Диспетчер серверов > Средства > Active Directory - пользователи и компьютеры**

- В необходимом Подразделении (OU) создайте **Нового пользователя** для UserID.

2. Сконфигурировать членство в группах для новой учетной записи пользователя:

- Щелкните правой кнопкой мыши по новой учетной записи пользователя UserID и выберите **Свойства**.
- Нажать на вкладку **Членство в группах**.
- Нажать **Добавить > Дополнительно > Поиск**.
- Выбрать следующие группы:
  - **Пользователи DCOM**
  - **Пользователи журналов производительности**
  - **Пользователи удаленного рабочего стола**
  - **Читатели журнала событий**
- Нажать **OK**

3. Назначить права Distributed Component Object Model (DCOM):

- Перейти в меню Windows **Пуск —> Администрирование —> Службы компонентов**. Откроется окно **Службы компонентов**.
- Раскрыть **Службы компонентов —> Компьютеры —> Мой компьютер**.
- Нажать правой кнопкой мыши по **Мой компьютер** и выбрать **Свойства**. Откроется окно **Свойства: Мой компьютер**.
- Перейти во вкладку **Безопасность COM**.
- В области Права доступа нажать **Изменить ограничения.**
- Убедиться, что для **Пользователи DCOM** выбрано **Локальный доступ** и **Удаленный доступ**.
- Нажать **OK**, чтобы сохранить настройки.
- В окне **Свойства: Мой компьютер** нажать в области **Разрешения на запуск и активацию** на **Изменить ограничения.**

- Убедиться, что для **Пользователи DCOM** выбрано **Локальный запуск**, **Удаленный запуск**, **Локальная активация** и **Удаленная активация**.
- Нажать **OK**, чтобы сохранить настройки, и еще раз нажать **OK**, чтобы закрыть окно **Свойства: Мой компьютер**.
- Выбрать **Файл —> Выход**, чтобы закрыть окно **Службы компонентов**.

4. Сконфигурировать назначения защиты пространства имен WMI:

- Перейти в меню **Пуск —> Выполнить**.
- Ввести `wmimgmt.msc` и нажать **OK**.
- Нажать правой кнопкой мыши на **Элемент управления WMI (локальный)** и выбрать **Свойства**.
- перейти на вкладку **Безопасность**.
- Нажать **Безопасность —> Добавить —> Дополнительно —> Поиск**.
- Выбрать новую учетную запись пользователя, нажимать **OK**, пока вы не вернетесь в окно **Безопасность** для Root.
- Нажать **Дополнительно** и выбрать добавленную учетную запись пользователя.
- Нажать **Изменить**.
- В меню **Применяется к:** выбрать **Данное пространство и подпространство имен**.
- Убедиться, что выбрано **Выполнение методов**, **Включить учетную запись**, **Включить удаленно** и **Прочесть безопасность**.
- Нажать **OK,** пока вы не вернетесь в окно wmimgmt.
- Выбрать **Файл —> Выход**, чтобы закрыть окно wmimgmt.

Syslog

Примечание

Для корректной работы сборщика логов UserID, необходимо настроить сервер Syslog для отправки журналов на адрес агента UserID. Подробнее см. документацию Syslog.

Для настройки источника событий необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Разрешить сбор информации с удалённых устройств по протоколу syslog.	В разделе **Сеть → Зоны** разрешить сервис **UserID syslog коллектор** для зоны, в которой находятся сервера Syslog.
Шаг 2. Настроить параметры агента UserID для мониторинга сервера syslog.	Параметры агента UserID были рассмотрены ранее.
Шаг 3. Настроить источник событий.	Настроить сервер Syslog в качестве источника. Подробнее о параметрах источника читайте далее.

При добавлении источника событий типа Syslog необходимо указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение получения журналов с источника.
Название	Название источника.
Описание	Описание источника.
Адрес сервера	Адрес хоста, с которого 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.
Профиль аутентификации	Профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах syslog.
Фильтры	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.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

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 UserGate, 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.

Наименование	Описание
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: [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""

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**.

> **Примечание**
>
> **Адрес назначения "ServerIP" в настройках агента должен соответствовать адресу интерфейса на который приходят запросы агента.**

Установленный агент аутентификации отсылает 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 потребуется 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

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.

Наименование	Описание

	• **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 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.

Конечные устройства UserGate Client

ПО UserGate Client (UGC) является компонентом экосистемы UserGate SUMMA, которое позволяет администратору централизованно управлять парком управляемых устройств. Установка UGC на компьютеры пользователей позволяет получать с них 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 управляемых устройств UGC, будет постоянно расширяться.

Благодаря использованию ПО UserGate Client администратор может произвести гибкую настройку политик безопасности с помощью правил межсетевого экрана, позволяющих фильтровать трафик на основе адреса источника/назначения, пользователей, сервисов, списков и категорий URL, приложений и типов контента.

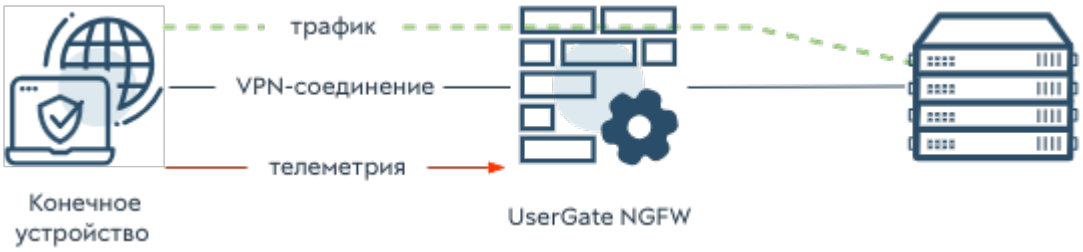
Телеметрическая информация, журналы Windows и другие данные о безопасности конечных устройств передаются в систему анализа событий LogAn и могут быть использованы для автоматического реагирования на угрозы безопасности.

На данный момент ПО UserGate Client может быть установлено 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. В дальнейшем планируется расширение списка платформ, для которых будет доступно использование ПО UserGate Client.

> **Примечание**
> **Под конечными устройствами будет подразумеваться пользовательский компьютер с установленным ПО UserGate Client.**

UserGate Client в связке с NGFW

Общение конечных устройств с NGFW производится по порту 4045 с использованием протокола HTTPS.



Регистрация конечного устройства происходит после подключения устройства к NGFW по VPN. При первом подключении конечное устройство проверяет валидность сертификата, указанного на NGFW для установки SSL-соединения, запоминает сертификат и далее использует его для проверки.

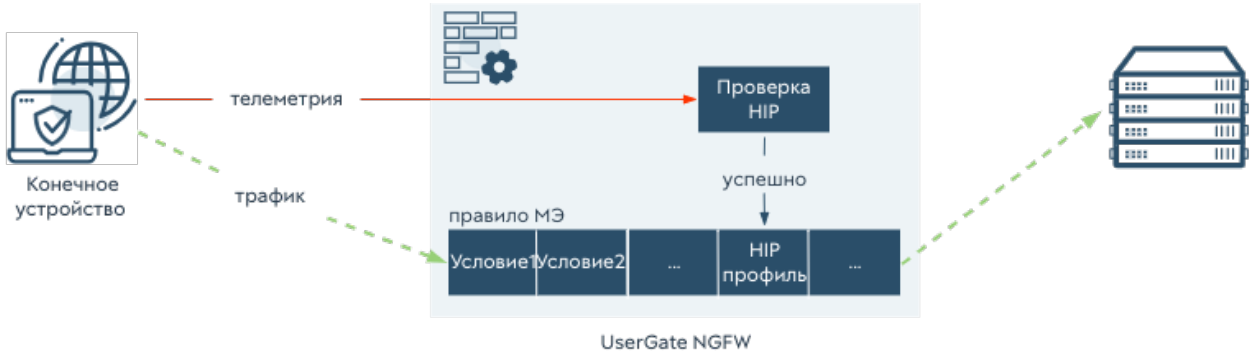
> **Примечание**
> **Если сертификат был изменен, то необходимо распространить корневой сертификат удостоверяющего центра (Root CA) на подключенные конечные устройства; сертификат должен быть установлен в хранилище доверенных корневых центров сертификации локального компьютера.**

После регистрации каждому новому конечному устройству присваивается уникальный идентификатор, который хранится в базе NGFW. Тайм-аут активности конечных устройств составляет 2 минуты, т.е., если в течение 2-х минут на 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 NGFW.

Проверка HIP на NGFW

Проверка на соответствие требованиям безопасности (комплаенса) происходит по следующей схеме:



Конечное устройство отправляет на 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 HIP 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 HIP 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.

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 NGFW

Подключение конечного устройства к 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.

Примечание

Если конечное устройство подключено к UGMC, перерегистрации на NGFW после установки VPN-соединения не произойдет.

Примечание

Для работы с конечными устройствами UserGate Client необходимо наличие лицензии. В случае отсутствия соответствующей лицензии регистрации конечного устройства на NGFW не произойдет; будет установлено только VPN-соединение.

> **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 раза. 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 NGFW.	В разделе **UserGate → Настройки** укажите сертификат и профиль для установки SSL-соединения. При подключении конечное устроство будет проверять валидность сертификата. В случае смены сертификата на 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 NGFW используется порт TCP 4045.
Шаг 3. Настроить NGFW в качестве VPN-сервера.	Настройте VPN на NGFW, к которому будет подключено конечное устройство. После установки VPN-соединения регистрация конечного устройства произойдет автоматически. Политики безопасности, настроенные на NGFW, также будут применены к конечным устройствам. **Важно!** Для проверки на соответствие требованиям безопасности (комплаенса) конечное устройство будет отправлять телеметрию на 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).**

ПОЛИТИКИ СЕТИ

Описание

Раздел **Политики сети** содержит следующие подразделы:

- Межсетевой экран.
- NAT и маршрутизация.
- Балансировка нагрузки.
- Пропускная способность.

С помощью политик сети администратор может настроить необходимый доступ в интернет для своих пользователей, опубликовать внутренние ресурсы сети в интернете, управлять скоростью передачи данных для определенных сервисов и приложений.

> **Примечание**
> **Правила, созданные в данных разделах, применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила.**

Для предоставления пользователям доступа в интернет необходимо:

Наименование	Описание
Шаг 1. Создать правило NAT (опционально).	Если необходимо наттирование трафика. Смотрите раздел NAT и маршрутизация.
Шаг 2. Создать разрешительное правило межсетевого экрана.	Смотрите раздел Межсетевой экран.

Для публикации внутреннего ресурса в интернете необходимо:

Наименование	Описание
Шаг 1. Создать правило DNAT или правило reverse-прокси.	Смотрите раздел Правила DNAT и Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси.

Чтобы указать для определенного сервиса или адреса выход в интернет через альтернативного провайдера, необходимо:

Наименование	Описание
Шаг 1. Создать правило Policy-based routing.	Смотрите раздел Policy-based routing.

Для того чтобы запретить или разрешить определенный тип трафика, проходящий через UserGate, необходимо:

Наименование	Описание
Шаг 1. Создать правило межсетевого экрана.	Смотрите раздел Межсетевой экран.

Для того чтобы распределить трафик между несколькими внутренними серверами, необходимо:

Наименование	Описание
Шаг 1. Создать правило Балансировки нагрузки.	Смотрите раздел Балансировка нагрузки.

Для того чтобы ограничить скорость для определенного сервиса или приложения, необходимо:

Наименование	Описание
Шаг 1. Создать правило Пропускной способности.	Смотрите раздел Пропускная способность.

Межсетевой экран

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate NGFW. В качестве условий правила могут выступать зоны и IP-адреса источника/назначения, пользователи, группы, сервисы.

События срабатывания правил межсетевого экрана отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

> **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**
> **Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).**

> **Примечание**
> **Если не создано ни одного правила, то любой транзитный трафик через NGFW запрещен.**

В настройках разрешающих правил межсетевого экрана могут быть добавлены профили СОВ и/или профили приложений (L7), содержащие определенные наборы сигнатур. После того, как трафик попадает в первое разрешающее правило межсетевого экрана, поток данных начинает анализироваться сигнатурами профилей СОВ и/или L7. При срабатывании сигнатур к трафику применяется действие, настроенное в правиле, и производится соответствующая запись в журналах (в **Журнале трафика** – для приложений и в **Журнале СОВ** – для СОВ), если в профилях была включена опция **Журналирование**.

Чтобы создать правило межсетевого экрана, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Межсетевой экран** и указать необходимые параметры.

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	**Запретить**: блокирует трафик. **Разрешить**: разрешает трафик.
Профиль приложений	Профиль приложений, созданный заранее в разделе **Библиотеки → Профили приложений**. Профиль приложений включает в себя набор релевантных сигнатур приложений, предназначенный для использования в правилах межсетевого экрана для анализа трафика на 7 уровне модели OSI. Подробнее о создании и настройке профилей приложений читайте в разделе Профили приложений. **Важно!** Профиль приложений является дополнительным параметром для активации механизма анализа трафика на 7 уровне модели OSI. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.
Профиль СОВ	Профиль СОВ, созданный заранее в разделе **Библиотеки → Профили СОВ**. Профиль СОВ представляет собой набор релевантных сигнатур, предназначенный для обнаружения вторжений и защиты определенных сервисов. Подробнее о создании и настройке профилей СОВ читайте в разделе Профили СОВ. **Важно!** Профиль СОВ является дополнительным параметром для активации правила СОВ. Может применяться только в правилах межсетевого экрана с разрешением прохождения трафика.
Отбросить и	Настройка данного параметра доступна для правил, блокирующих трафик (выбрано действие **Запретить**). Параметр может принимать одно из следующих значений: • **Не выбран**.

Наименование	Описание
	• **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	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.

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.
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). 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 или HTTPS.
Время	Интервалы времени, когда правило активно.
HIP профили	HIP профили, созданные в разделе **Библиотеки → HIP профили**. HIP профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). Подробнее о создании и настройке HIP профилей читайте в разделе HIP профили.

Наименование	Описание
	Важно! В случае выключения профиля HIP, он будет помечен серым цветом, а правило межсетевого экрана продолжает работать без условия проверки комплаенса.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. 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.

NAT и маршрутизация

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, DNAT, Порт-форвардинга, Policy-based routing и Network mapping. 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 NAT, DNAT, порт-форвардинга, Policy-based routing и Network mapping отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

> **Примечание**
>
> **GeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и порт-форвардинг.**

Правила NAT

Как правило, для предоставления пользователям доступа в интернет необходимо создать хотя бы одно правило NAT из зоны **Trusted** в зону **Untrusted**.

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

Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило NAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **NAT**.
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника при наттировании пакетов. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то 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 NGFW будет использовать все указанные адреса при Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана.
Журналирование	

Наименование	Описание
	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. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки 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!** Флажок **Инвертировать** не влияет на работу при использовании MAC-адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
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 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.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	

Наименование	Описание
	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.

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 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. Более подробно о публикации ресурсов с помощью правил reverse-прокси описано в главе Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. Для публикации серверов, работающих по протоколам, отличным от HTTP/HTTPS, необходимо использовать публикацию DNAT.

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**
>
> **Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).**

Чтобы создать правило DNAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **DNAT**.
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника при наттировании пакетов; если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса 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 во вкладке **DNAT** активировать Флажок **Включить SNAT**.
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. • **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

Наименование	Описание
	внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании MAC-адресов. **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	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. **Важно!** 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, например, HTTP. Если не указан сервис, то будут опубликованы все сервисы. **Важно!** Нельзя опубликовать сервисы, которые используют следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет.
Включить SNAT	При включении данной опции 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 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.

Правила порт-форвардинга

Правила порт-форвардинга работают аналогично правилам DNAT за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис. Чтобы создать правило порт-форвардинга, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

> **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**
>
> **Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).**

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Порт-форвардинг**.
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. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика.

Наименование	Описание
	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!** Флажок **Инвертировать** не влияет на работу при использовании MAC-адресов. **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, списки URL назначения 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.
Порт-форвардинг	Переопределения портов публикуемых сервисов: • **Оригинальный порт назначения** — номер TCP/UDP-порта, на который пользователи шлют запросы. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100. • **Новый порт назначения** — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.

Наименование	Описание
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернете.
Включить SNAT	При включении данной опции 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 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.

Policy-based routing

Правила policy-based routing обычно используются для указания определенного маршрута в интернет для определенных хостов и/или сервисов. Например, в организации используются 2 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 в интернет-шлюз провайдера 2 и настроить правило policy-based routing 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.

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**
>
> **Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).**

Чтобы создать правило policy-based routing, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Policy-based routing**.
Шлюз	Выбор одного из существующих шлюзов. Вы можете добавить шлюз в разделе **Сеть → Шлюзы**. **Важно!** Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
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. • **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!** Флажок **Инвертировать** не влияет на работу при использовании MAC-адресов.

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.
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). 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.
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.

Network mapping

Правила Network mapping позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией, например, 192.168.1.0/24, и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес хоста без изменений, например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 хост 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, 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 **Network mapping**, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Network mapping**.
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. • **Нет**. В этом случае информация не будет записываться.

Наименование	Описание
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!** Флажок **Инвертировать** не влияет на работу при использовании MAC-адресов. **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, 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). 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.
Network mapping	Задаются параметры подмены сетей. **Направление**: • Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике,

Наименование	Описание
	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.** • **Новая IP-сеть/маска** — адрес сети, на которую будет производится замена.
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.

Балансировка нагрузки

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/IP необходимо выбрать пункт **Добавить балансировщик TCP/IP** 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.
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 **weight**

Наименование	Описание
	ed 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. **Внимание!** **Поскольку в режиме *Шлюз* 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.**
Аварийный режим	Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо включить его и указать: • **IP-адрес** сервера. • **Порт** сервера. Порт, на который пересылать запросы пользователей. • **Режим**. Может быть три варианта: ◦ **Шлюз**: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ **Максарадинг**: 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.
Мониторинг	С помощью мониторинга можно настроить проверку реальных серверов на определение их работоспособности. Если проверка прошла неуспешно для реального сервера, он исключается из балансировки.

Наименование	Описание
Режим	Способ мониторинга реальных серверов. Возможны варианты: • **ping** — проверить доступность узла с помощью утилиты ping. • **connect** — проверить работоспособность узла, установив TCP-соединение на определенный порт. • **negotiate** — проверить работоспособность узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. Для настройки этого режима следует 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.

Наименование	Описание
Описание	Описание правила.
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритезации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе Полосы пропускания.
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 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.

Наименование	Описание
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. **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” и для определенной группы — “Социальные сети”. После того как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Включить и настроить параметры СОВ.
- Настроить проверку почтовых протоколов SMTP и POP3 на наличие спама.
- Настроить журналирование или блокировку определенных команд АСУ ТП.
- 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 система обнаружения и предотвращения вторжений — в журнале СОВ (**Журналы и отчёты → Журнал СОВ**).

Правила АСУ ТП — в журнале АСУ ТП (**Журналы и отчёты → Журнал АСУ ТП**).

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).

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 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.
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 срабатывание 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 сработает.
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.

Наименование	Описание
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 UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate 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, 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). 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, 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.

Наименование	Описание
	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. **Важно!** Начиная с версии UserGate 5.0.6R6 администратор может переопределить категорию на любой сайт, на который, по его мнению, категория назначена не верно 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, обновляемые компанией UserGate, в том числе список материалов, запрещенных Министерством Юстиции Российской Федерации, словари по темам «Суицид», «Терроризм», «Порнография», «Нецензурные выражения»,

Наименование	Описание
	«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.

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).

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.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание 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.
Инжектор	Позволяет вставить произвольный код во все веб-страницы. Для редактирования вставляемого кода необходимо нажать на кнопку **Код инжектора.**

Наименование	Описание
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.
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:

Наименование	Описание
	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.

> **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**.

> **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.
Описание	Описание правила инспектирования.
Действие	Действия правила инспектирования: • **Инспектировать**. • **Не расшифровывать**.
Инспектирование туннелей	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).

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.
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

С помощью данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу TLS/SSL, это в первую очередь HTTPS, а также почтовые протоколы SMTPS и POP3S. В UserGate используется известная технология man-in-the-middle (MITM), при которой контент расшифровывается на сервере, а затем анализируется.

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности. Дешифрование SMTPS и POP3S необходимо для блокирования спама.

С помощью правил данного 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.

После дешифрования данные шифруются сертификатом, выписанным центром сертификации, указанным в разделе **Сертификаты**. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить сертификат центра сертификации в доверенные корневые сертификаты. Более подробно это описано в разделе Установка сертификата локального удостоверяющего центра.

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.

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

Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Примечание

Если не создано ни одного правила, то SSL не перехватывается и не дешифруются, соответственно, контент, передаваемый по SSL, не фильтруется.

Чтобы создать правило инспектирования SSL, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование SSL** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание 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 необходимо указать **Профиль пересылки SSL** (о настройке профилей пересылки читайте 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 серверу UserGate, так и при построении SSL-соединения от сервера UserGate к запрашиваемому веб-ресурсу. Подробно о профилях SSL смотрите в главе 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 **Know**

Наименование	Описание
	n необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и 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 UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate 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.
Адрес назначения	Списки IP-адресов назначения 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.
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

Наименование	Описание
	доменные имена (www.example.com, а не http://www.example.com/home/). Более подробно о работе со списками URL читайте в главе Списки URL.
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 шифрованные 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.

Примечание

Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

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.
Описание	Описание правила.

Наименование	Описание
Действие	Расшифровывать или не расшифровывать передаваемые данные.
Записывать в журнал правил	Информация о срабатывание правила будет регистрироваться в Журнале инспектирования SSH.
Блокировать удаленный запуск shell	Запрет запуска командного интерпретатора на SSH-сервере. Пользователю будет разрешено запускать только команды на удаленном сервере, например: `ssh user@host command`
Блокировать удаленное выполнение по SSH	Запрет удаленного выполнения **любых** команд на SSH-сервере.
Редактировать команду SSH	**Опционально** для 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.

Наименование	Описание
Адрес назначения	Списки IP-адресов назначения 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.
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, 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 отсечь сообщения от очевидных и явных спамеров;

- маркировка сообщений по результатам проверки на спам; требует наличия также лицензии на модуль Mail security.

> **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.

Наименование	Описание
Шаг 2. Включить поддержку сервисов SMTP(S) и POP3(S) в зоне, подключенной к сети Интернет.	Смотрите раздел Настройка зон.
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.
Название	Название правила.
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). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во

Наименование	Описание
	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):

- 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.

- 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.

Защита от DoS атак

UserGate NGFW позволяет гранулировано 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.
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.

Наименование	Описание
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.

> **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.
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.

Наименование	Описание
	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 сработает.
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

Наименование	Описание
	типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идеунтификации 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). 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 (СОВ) 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. СОВ 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.

Сигнатуры СОВ 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 свое действие, журналирование, запись в файл pcap, включение/отключение сигнатуры. Подробнее о сигнатурах СОВ читайте в разделе Сигнатуры СОВ.

С помощью гибко настраиваемых фильтров наборы сигнатур добавляются в профили СОВ. Администратор может создать необходимое количество профилей СОВ для защиты различных сервисов. Подробнее о профилях СОВ читайте в разделе Профили СОВ.

Для активации системы обнаружения и предотвращения вторжений профиль СОВ добавляется в разрешающее правило межсетевого экрана. Таким образом, системой будут обрабатываются только те сигнатуры, которые попали в добавленные профили.

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем. Если в правиле определен профиль СОВ, 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 СОВ, если была включена опция журналирования. Если ни одна из сигнатур не была найдена, то трафик пропускается дальше.

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 СОВ/L7 IP-адреса** (подробнее читайте в разделе Заблокированные СОВ/L7 IP-адреса).

Работа с внешними ICAP-серверами

Описание

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 NGFW будет выступать в роли ICAP-клиента.

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.
Адрес сервера	IP-адрес ICAP-сервера.
Порт	TCP-порт ICAP-сервера, значение по умолчанию 1344.

Наименование	Описание
Максимальный размер сообщения	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
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. • **Название заголовка**, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — X-Authenticated-User.

Наименование	Описание
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.
Описание	Описание правила.
Действие	Возможны следующие варианты: • **Пропустить** — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор

Наименование	Описание
	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.
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).

Наименование	Описание
	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 защите почтового трафика смотрите в разделе Защита почтового трафика.

Работа с несколькими серверами ICAP

UserGate 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 UserGate 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.**

ГЛОБАЛЬНЫЙ ПОРТАЛ

Описание

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.

> **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).**

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	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: https://имя_хоста:порт.
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

Наименование	Описание
	использовать мультифакторную аутентификацию для доступа к веб-порталу. Более подробно о профилях аутентификации смотрите раздел руководства Профили аутентификации.
Шаблон страницы аутентификации	Выбрать шаблон страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Создать свою страницу аутентификации можно в разделе Шаблоны страниц.
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Создать свою страницу аутентификации можно 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. Подробно о профилях SSL смотрите в главе Профили SSL.
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. Более подробно о ролях сертификатов смотрите в разделе руководства 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. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами.

Настройке 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.
Домен прямого доступа	При указанном значении Домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Обязательно должен быть указан протокол (HTTP или HTTPS) и домен.
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. Подробно о профилях SSL смотрите в главе Профили SSL.
Сертификат	Сертификат, который будет использоваться для для создания HTTPS-соединения между UserGate и сервером. Если выбран режим **Выбрать сертификат**, то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Более подробно о ролях сертификатов смотрите в разделе руководства Управление сертификатами.
Иконка	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку.

Наименование	Описание
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 HTTP/HTTPS-ресурсов с помощью reverse-прокси

Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси.

В отличие от публикации с помощью правил DNAT, публикация с использованием reverse-прокси предоставляет следующие преимущества:

- Публикация по HTTPS серверов, работающих по HTTP и наоборот.
- Балансировка запросов на ферму веб-серверов.
- Возможность ограничения доступа к публикуемым серверам с определенных Useragent.
- Возможность подмены доменов и путей публикуемых серверов.

Чтобы опубликовать сервер, используя reverse-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервер reverse-прокси.	В разделе **Глобальный портал → Серверы reverse-прокси** нажать на кнопку **Добавить** и создать один или более публикуемых веб-серверов.

Наименование	Описание
Шаг 2. Создать правило балансировки на серверы reverse-прокси (опционально).	В случае, если требуется балансировка на ферму публикуемых серверов, создать в разделе **Политики сети → Балансировка нагрузки** балансировщик reverse-прокси. В качестве серверов используются серверы reverse-прокси, созданные на предыдущем шаге.
Шаг 3. Создать правило reverse-прокси.	В разделе **Глобальный портал → Правила reverse-прокси** создать правило, которое будет задавать условия публикации серверов или фермы серверов. **Важно!** Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в настройках правила.
Шаг 4. Разрешить сервис Reverse-прокси на зоне, с которой необходимо разрешить доступ к внутренним ресурсам.	В разделе **Сеть → Зоны** разрешите сервис Reverse-прокси для зоны, с которой необходимо разрешить доступ к внутренним ресурсам (обычно зона Untrusted).

Для создания сервера reverse-прокси разделе **Глобальный портал → Серверы reverse-прокси** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название публикуемого сервера.
Описание	Описание публикуемого сервера.
Адрес сервера	IP-адрес публикуемого сервера.
Порт	TCP-порт публикуемого сервера.
HTTPS до сервера	Определяет, требуется ли использовать протокол HTTPS до публикуемого сервера.
Проверять SSL-сертификат	Включает/отключает проверку валидности SSL-сертификата, установленного на публикуемом сервере.
Не изменять IP-адрес источника	Оставляет оригинальный IP-адрес источника в пакетах, пересылаемых на публикуемый сервер. Если отключено, то IP-адрес источника заменяется на IP-адрес NGFW.

Для создания правила балансировки на серверы reverse-прокси в разделе **Политики сети → Балансировка нагрузки** необходимо выбрать **Добавить → Балансировщик reverse-прокси** и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Серверы reverse-прокси	Созданный на предыдущем шаге список серверов reverse-прокси, на которые будет распределяться нагрузка.

Для создания правила reverse-прокси необходимо нажать на кнопку **Добавить** в разделе **Глобальный портал → Правила reverse-прокси** 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

Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Сервер reverse-прокси	Сервер reverse-прокси или балансировщик reverse-прокси, куда NGFW будет пересылать запросы.
Порт	Порт, на котором NGFW будет слушать входящие запросы.
Использовать HTTPS	Включает поддержку HTTPS.

Наименование	Описание
Профиль SSL	Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи.
Сертификат	Сертификат, используемый для поддержки HTTPS-соединения.
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.
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 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. Данная вкладка доступна только при использовании HTTPS и авторизации пользователя по сертификату.
Назначение	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. **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.
Useragent	UserAgent пользовательских браузеров, для которых будет применено данное правило. С помощью флажка **Инвертировать** можно заблокировать доступ к сервису, опубликованному через правило reverseproxy, для указанных в этом поле UserAgent.
Подмена путей	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2 **Изменить с** — домен и/или путь URL, которые требуется изменить. **Изменить на** — домен и/или путь URL, на которые требуется заменить старые. Если указан домен в поле **Изменить с**, то правило публикации будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.

НАСТРОЙКА VPN

VPN (Описание)

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 клиент UserGate Client, также поддерживаются стандартные клиенты большинства популярных операционных систем, например, таких, как Windows, Linux, Mac OS X, iOS, Android и другие.

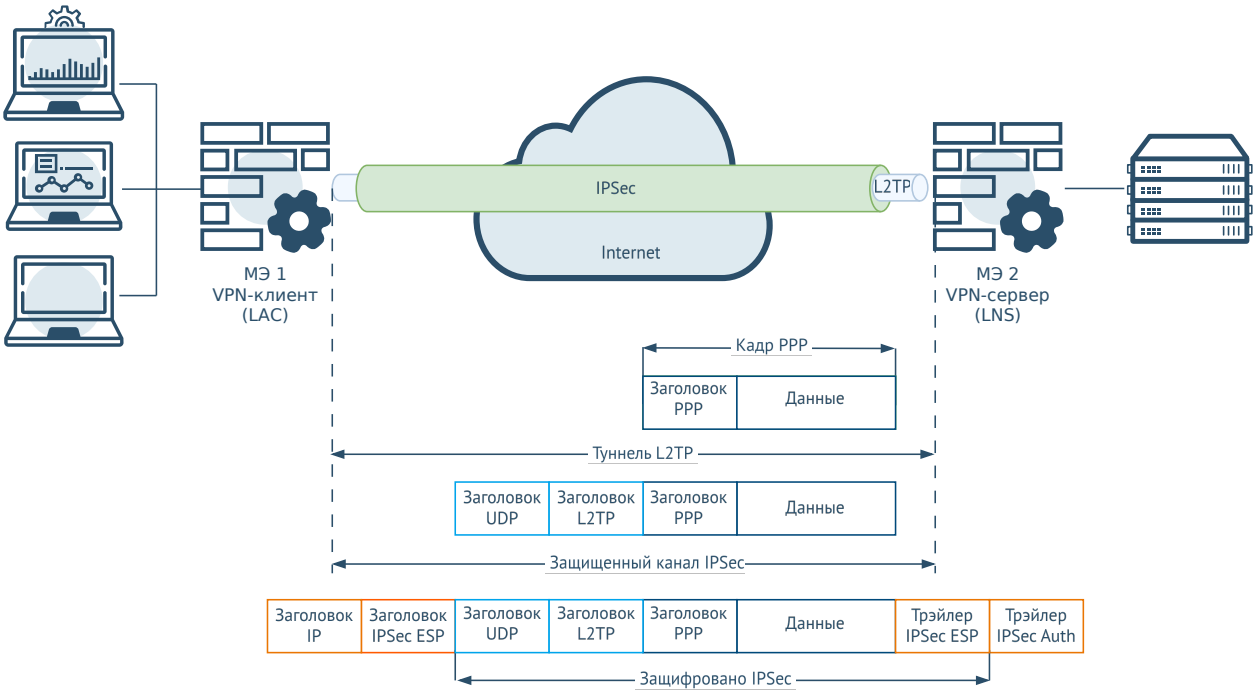
Варианты организации защищенных VPN-туннелей

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.

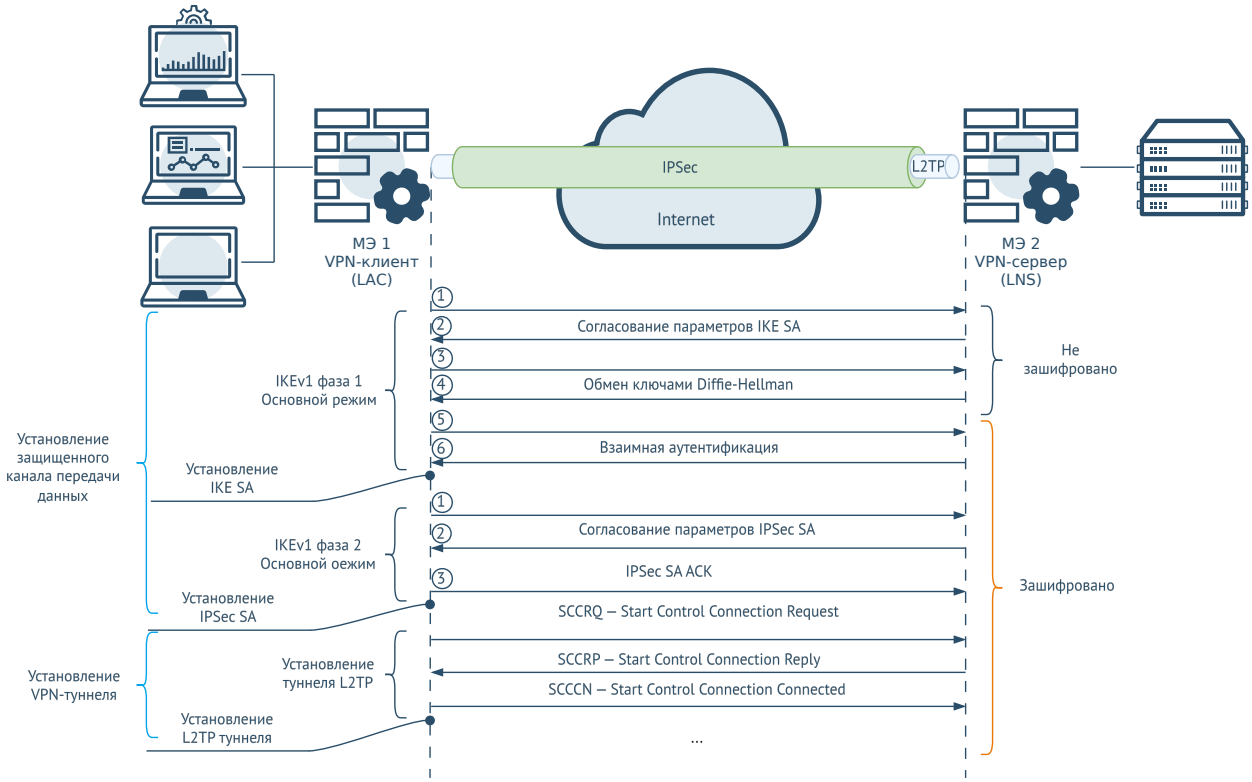


VPN имеет два уровня инкапсуляции — внутреннюю инкапсуляцию L2TP и внешнюю инкапсуляцию IPsec. Внутренний уровень имеет заголовки L2TP и UDP дополнительно к кадру PPP. Внешний уровень добавляет заголовок и трэйлер IPsec ESP. Трейлер проверки подлинности IPsec Auth обеспечивает проверку целостности сообщений и аутентификацию.

Процесс создания VPN состоит из следующих основных этапов:

1. Установление защищенного канала передачи данных.

2. Установление VPN-туннеля.



Установление 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 обеим 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. 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.

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. Основной 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.

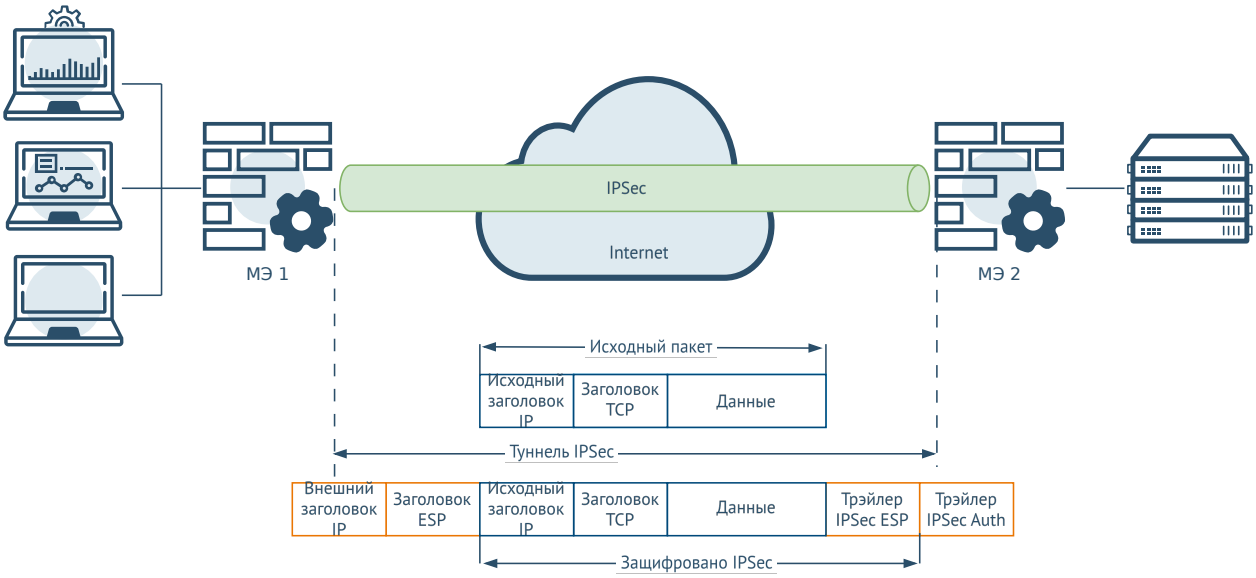
Установление VPN-туннеля

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.

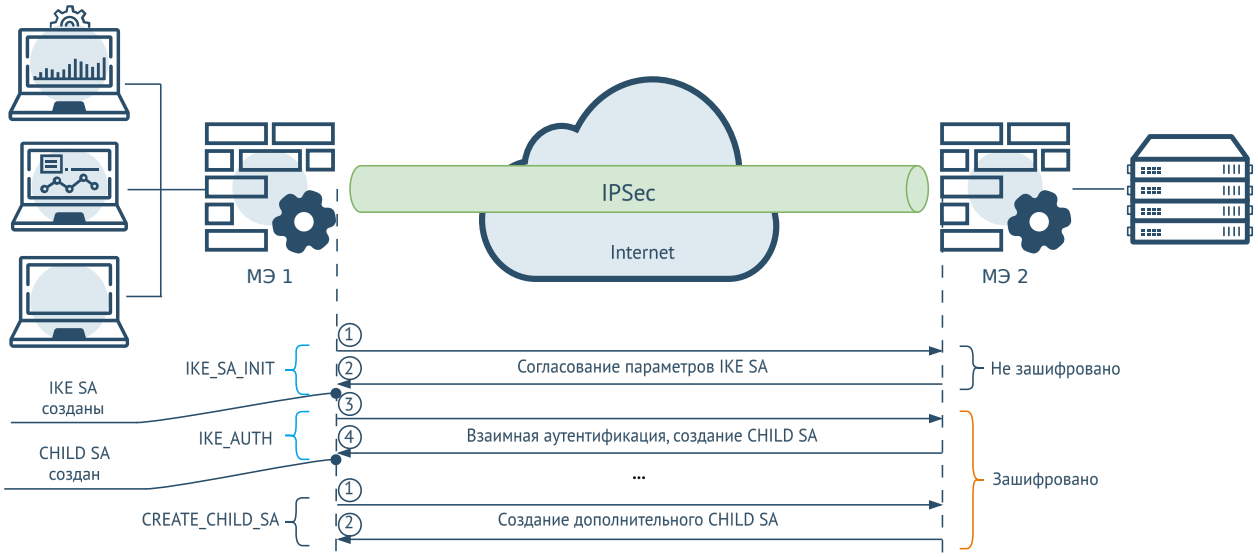
IPsec(IKEv2) VPN

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 работает в качестве VPN-клиента.

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 шифрованного 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. Важно! При настройке туннельного GRE интерфейса 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)

VPN-подключение, позволяющее соединить локальные сети удаленных офисов, называется Site-to-Site VPN.

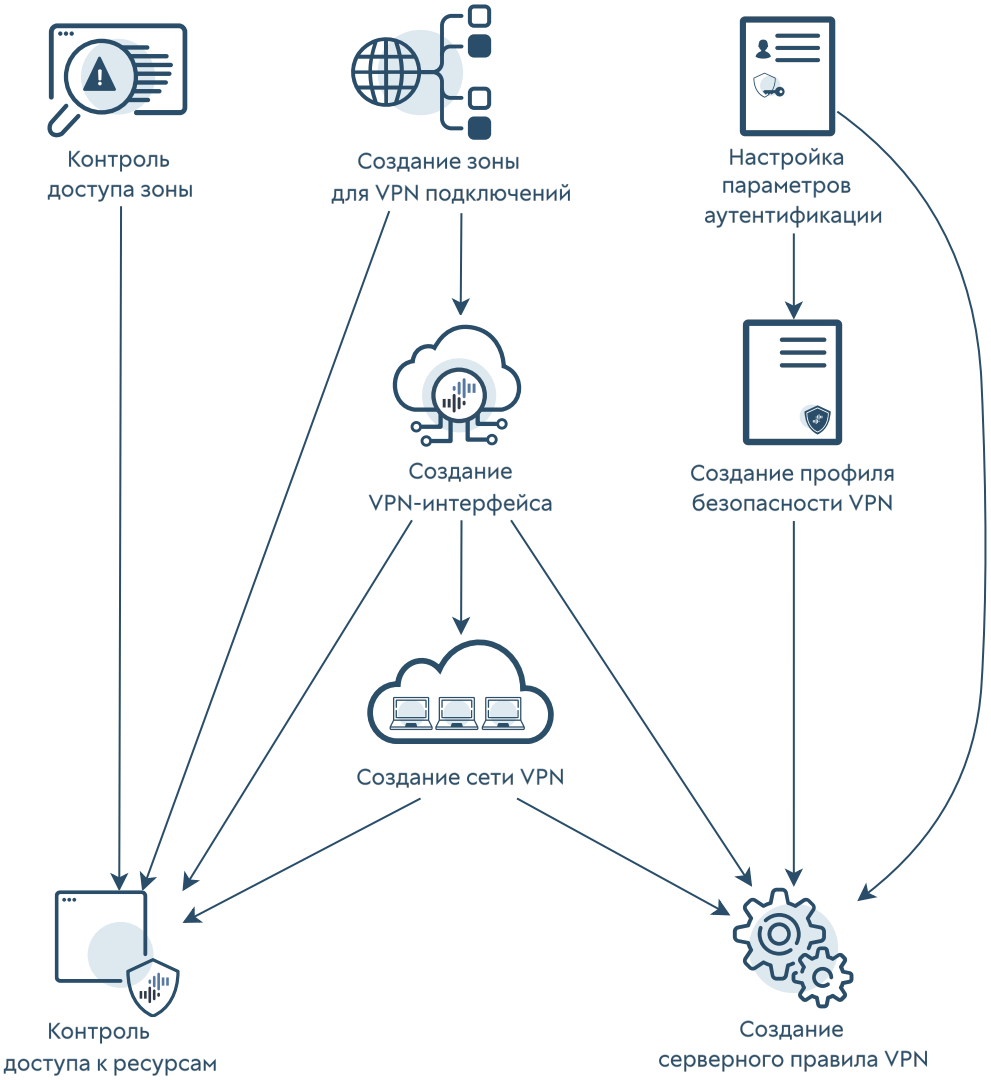
В этом подключении один межсетевой экран выступает в роли VPN-сервера, а другой — в роли VPN-клиента. Клиент инициирует соединение с сервером. Site-to-Site VPN может быть создан между двумя межсетевыми экранами UserGate, либо между межсетевым экраном UserGate и устройством другого производителя.

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

Настройка VPN-сервера на NGFW состоит из следующих основных этапов:



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.
8. 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.

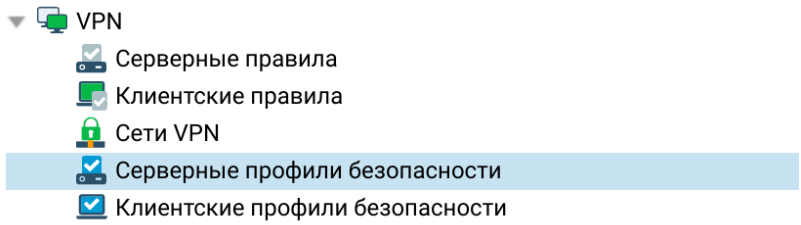
- Аутентификация посредством **сертификатов**, использующих инфраструктуру открытых ключей (PKI). Используется при выборе протокола **IKEv2** для организации защищенного соединения. Необходимо заранее создать сертификаты сервера и клиента и импортировать их в NGFW. О примерах создания и использования 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.

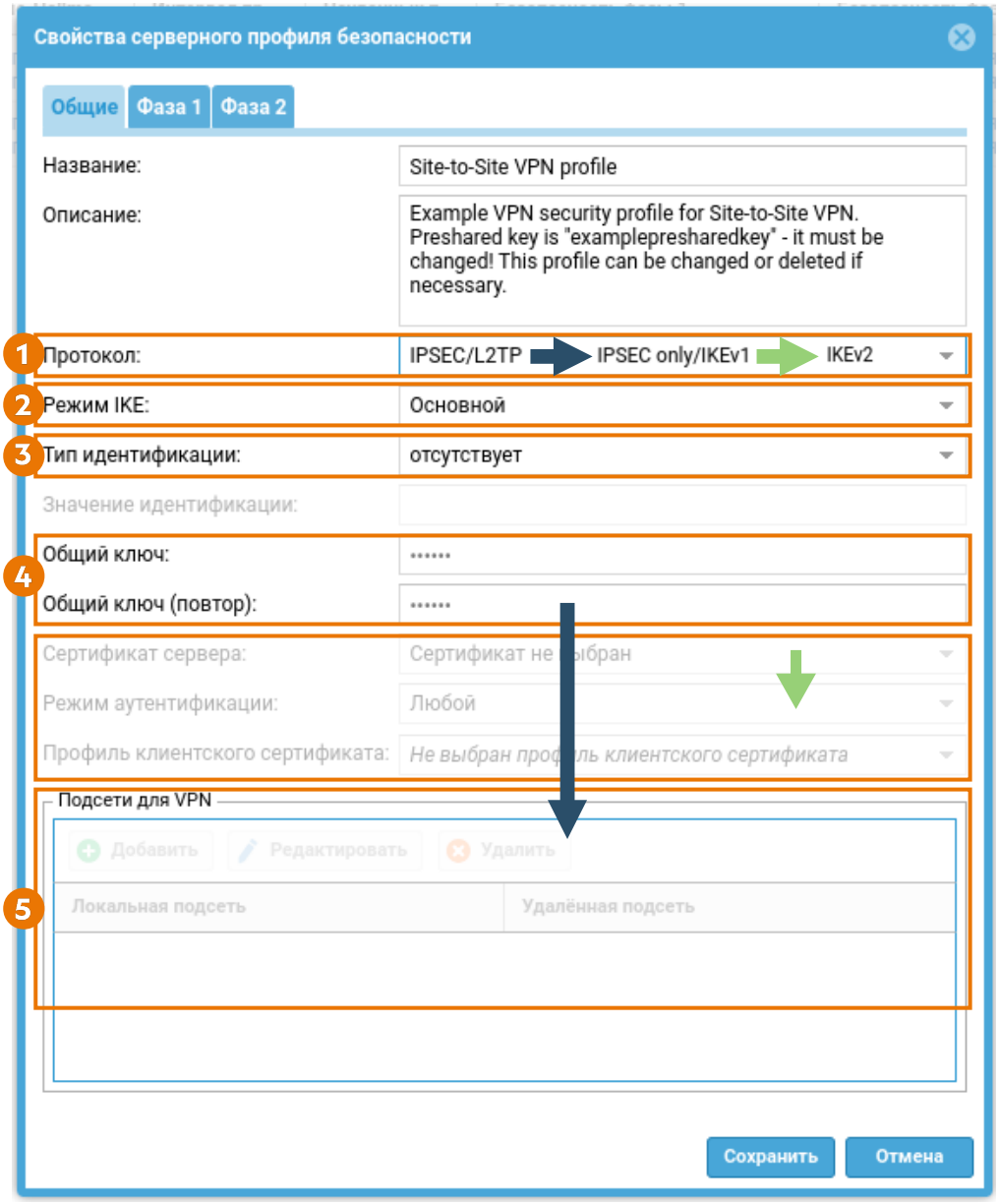
Создание профиля безопасности VPN

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 раздельно:



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:



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 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.

4. Тип аутентификация удаленного узла при установлении защищенного соединения.

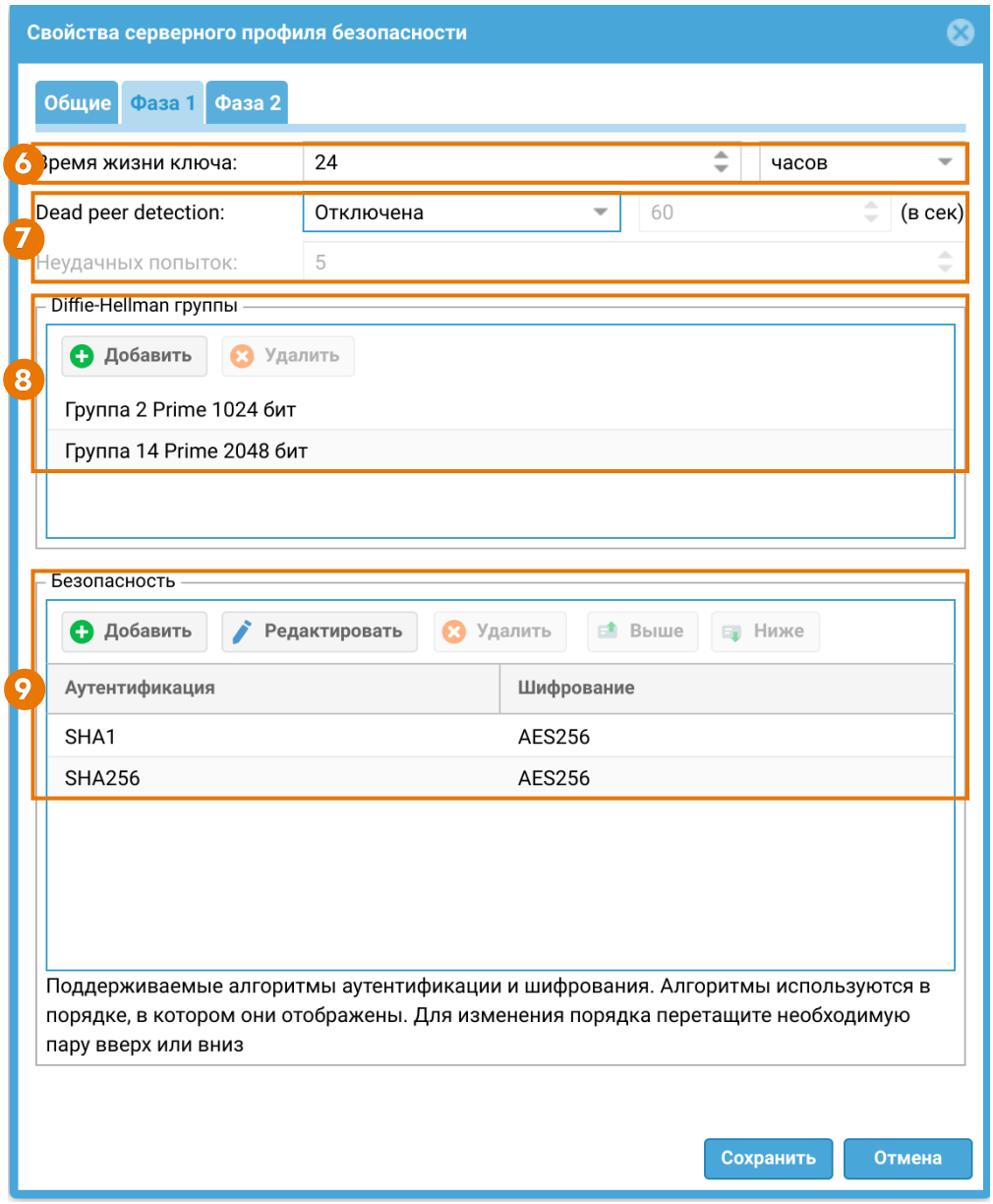
- При выборе протокола IKEv1 используется аутентификация с **общим ключом** (Pre-shared key). Необходимо задать общий ключ. Строка должна совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- При выборе протокола IKEv2 для организации туннеля Site-to-Site возможна аутентификация с помощью 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:



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

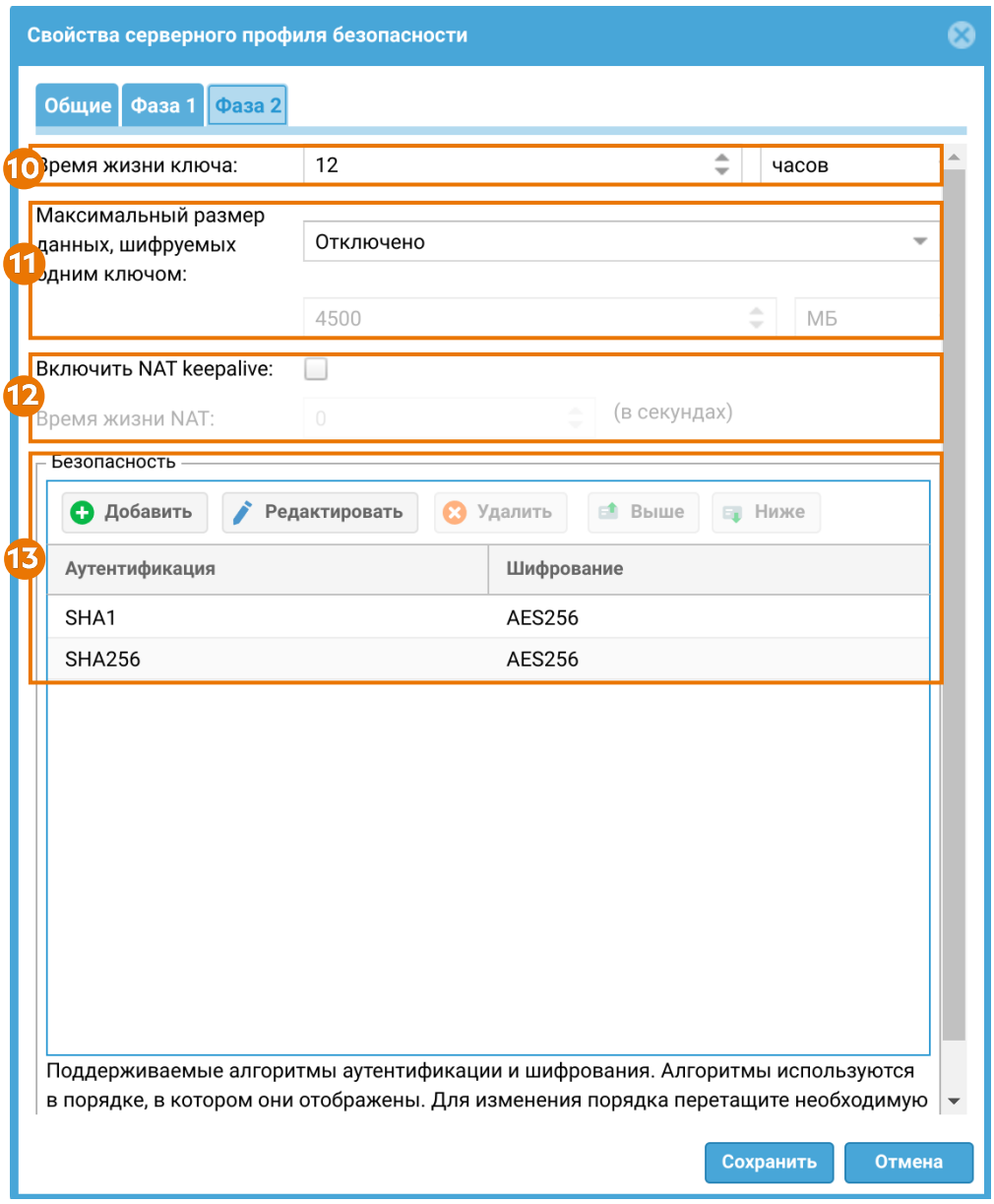
R-U-THERE для проверки доступности IPsec-соседа. Возможны 3 режима работы механизма:

- **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 будет 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:



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

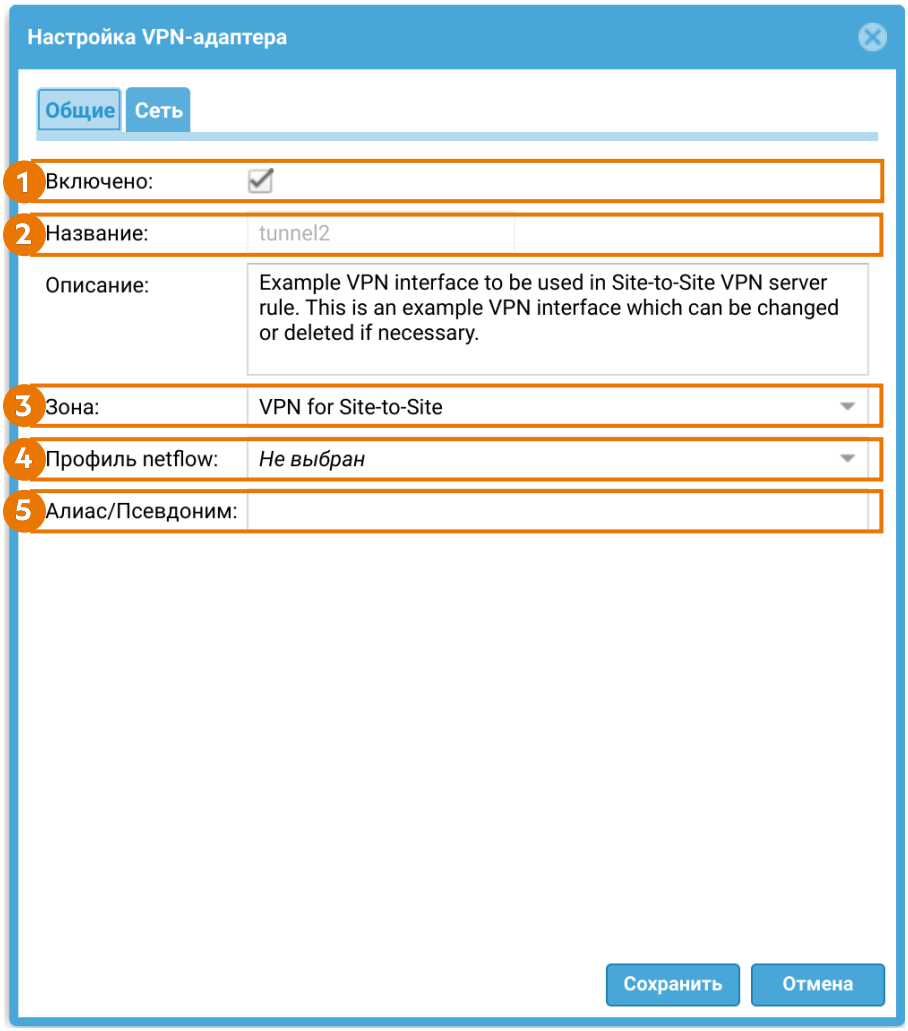
отправляет пакеты keepalive в сторону peer-узла для поддержания сессии NAT активной.

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:



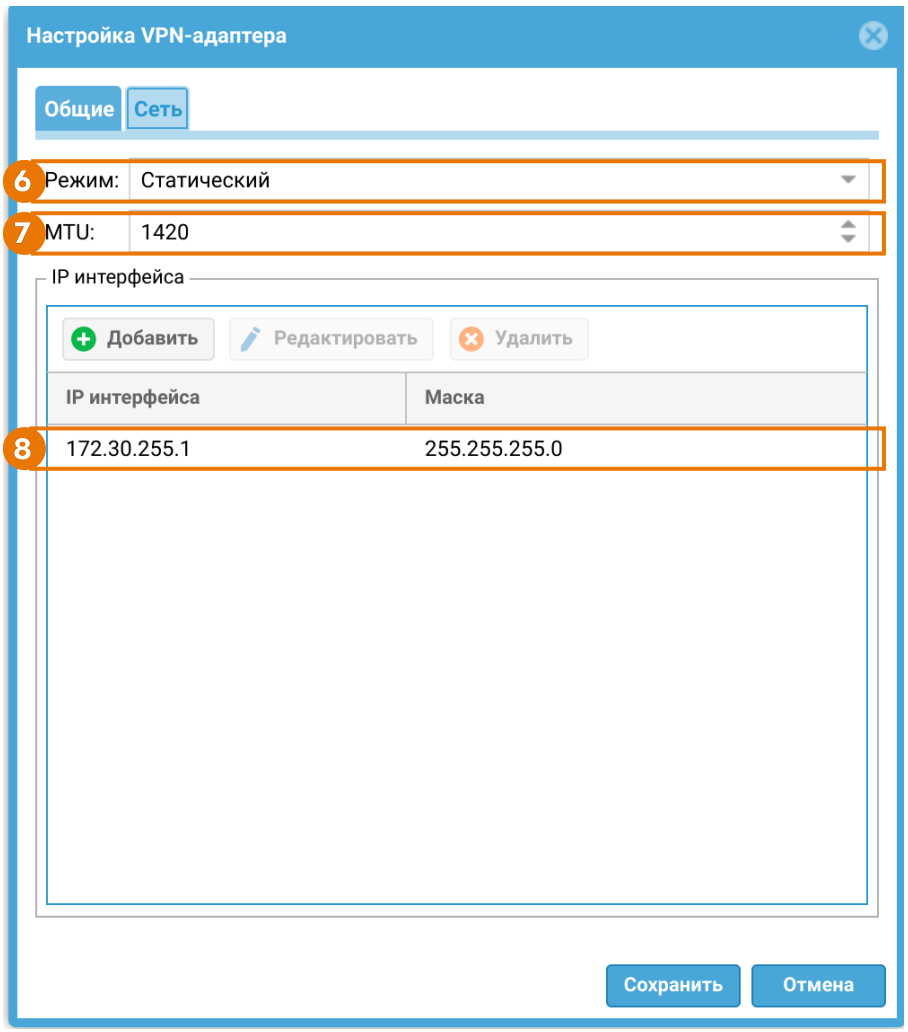
1. **Включено** — включение/отключение интерфейса.

2. **Название** — название интерфейса, должно быть в виде *tunnelN*, где *N* — это порядковый номер VPN-интерфейса.

3. **Зона**, к которой будет относится 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.



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.

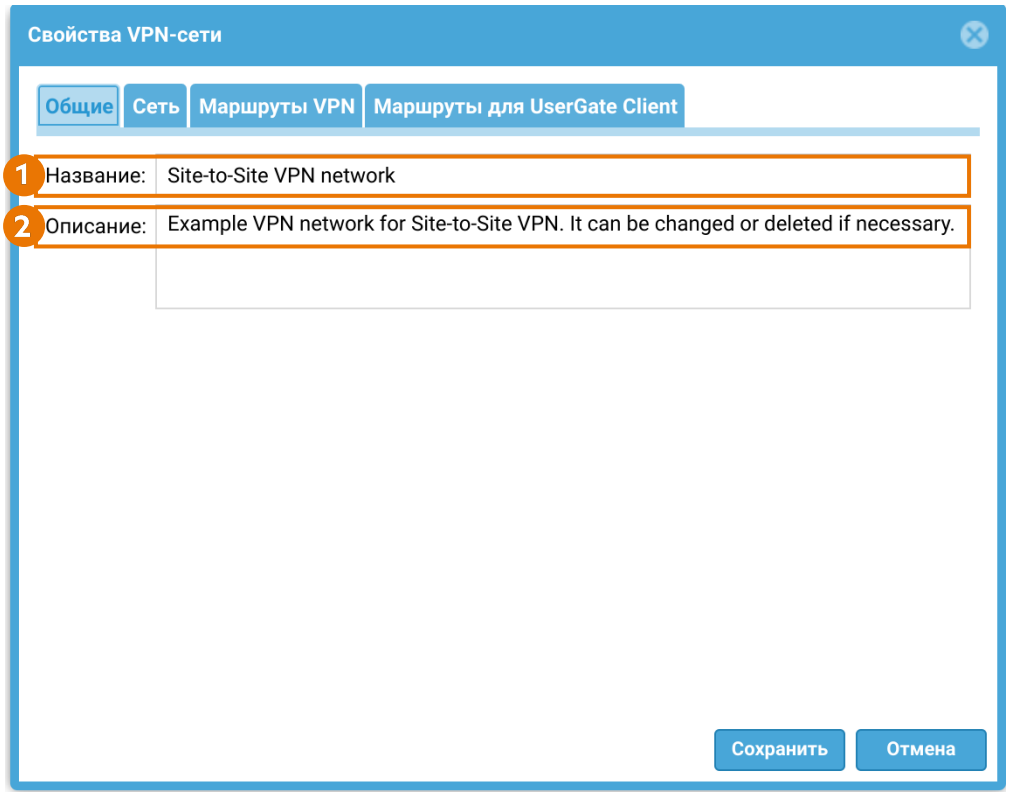
8. Поле добавления **IP-адреса** VPN-интерфейса в случае, если выбран статический режим присвоения адреса.

Создание сети VPN

Сеть VPN определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов

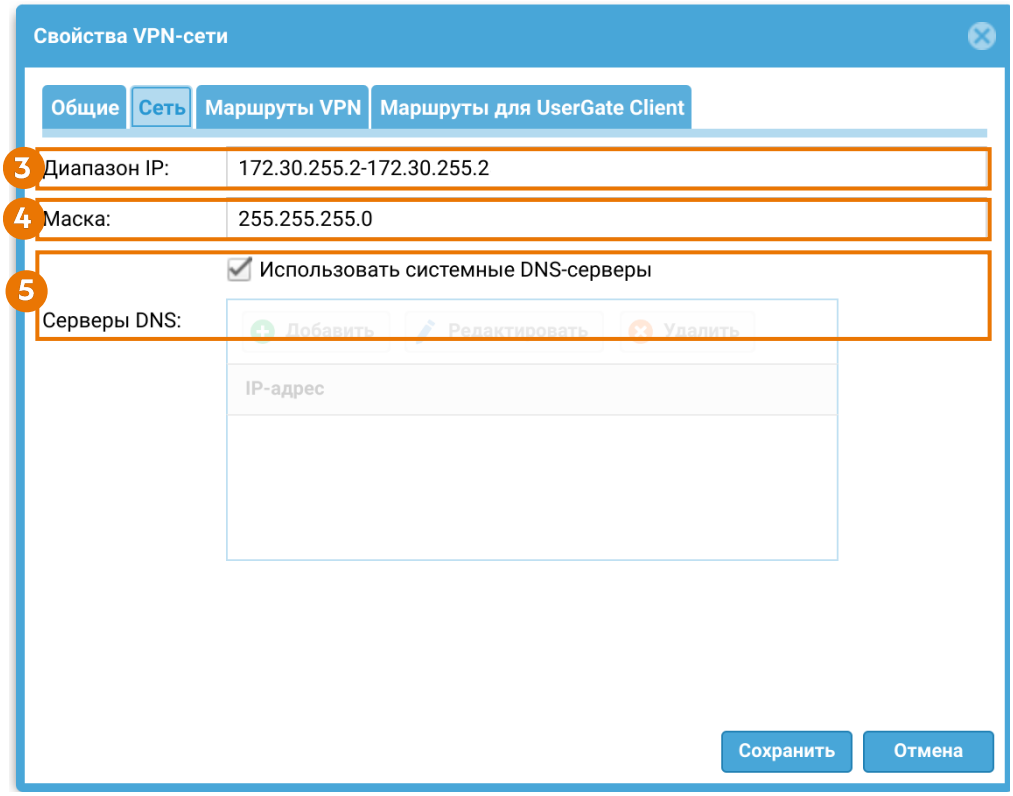
клиентам внутри туннеля, настройки DNS и маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов.

Сеть VPN в веб-консоли администратора создается в разделе **VPN → Сети VPN**, Необходимо нажать кнопку **Добавить** и заполнить необходимые поля в свойствах VPN-сети:



1. **Название** сети VPN.

2. **Описание** сети VP. Опциональный параметр.



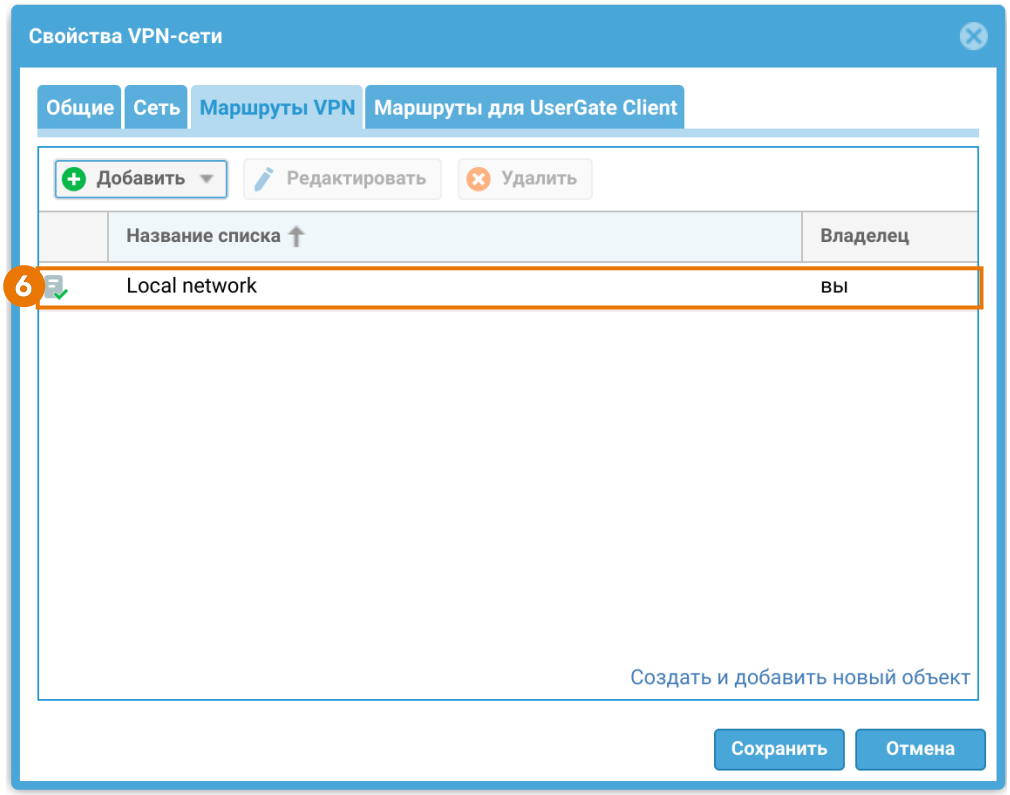
3. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен **VPN-интерфейсу** NGFW, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.

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.

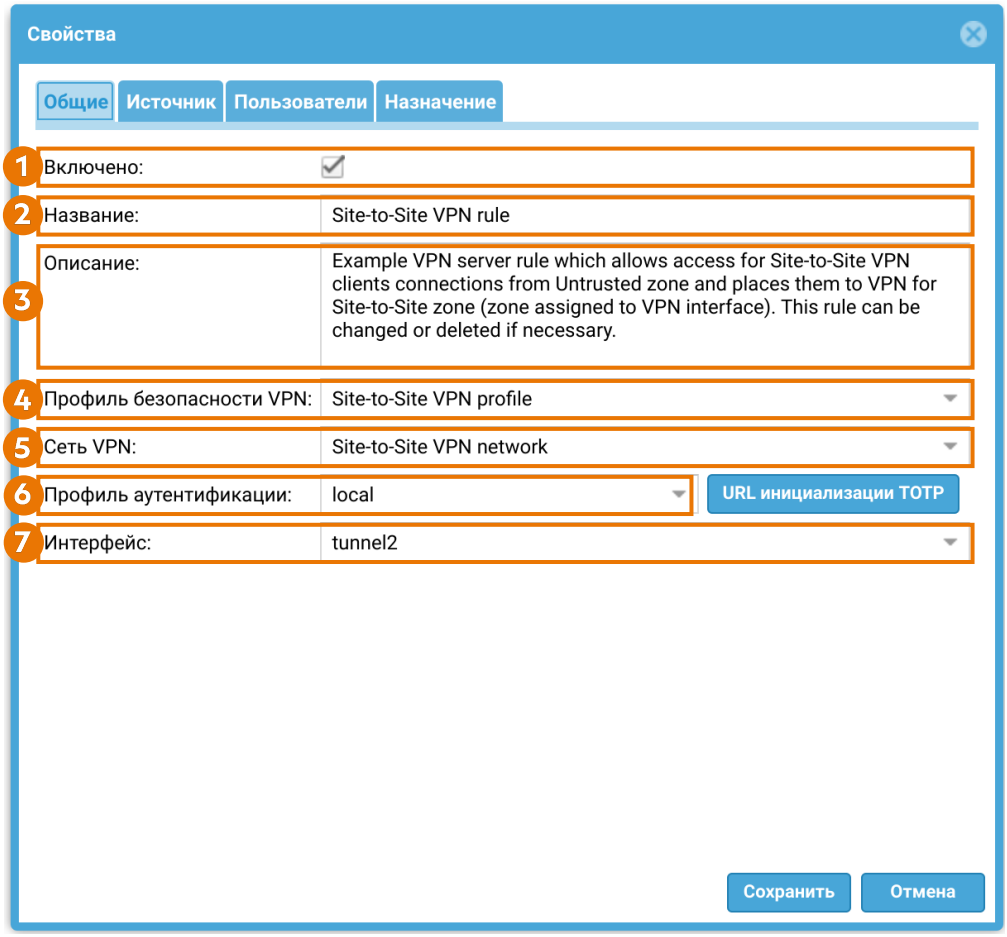


6. **Маршруты VPN** — маршруты, передаваемые VPN-клиенту в виде бесклассовой адресации (CIDR) или заранее созданного списка IP-адресов.

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:



1. **Включено** — включение/отключение правила VPN.

2. **Название** серверного правила VPN.

3. **Описание** серверного правила VPN. Опциональный параметр.

4. **Профиль безопасности VPN** — профиль безопасности, созданный ранее.

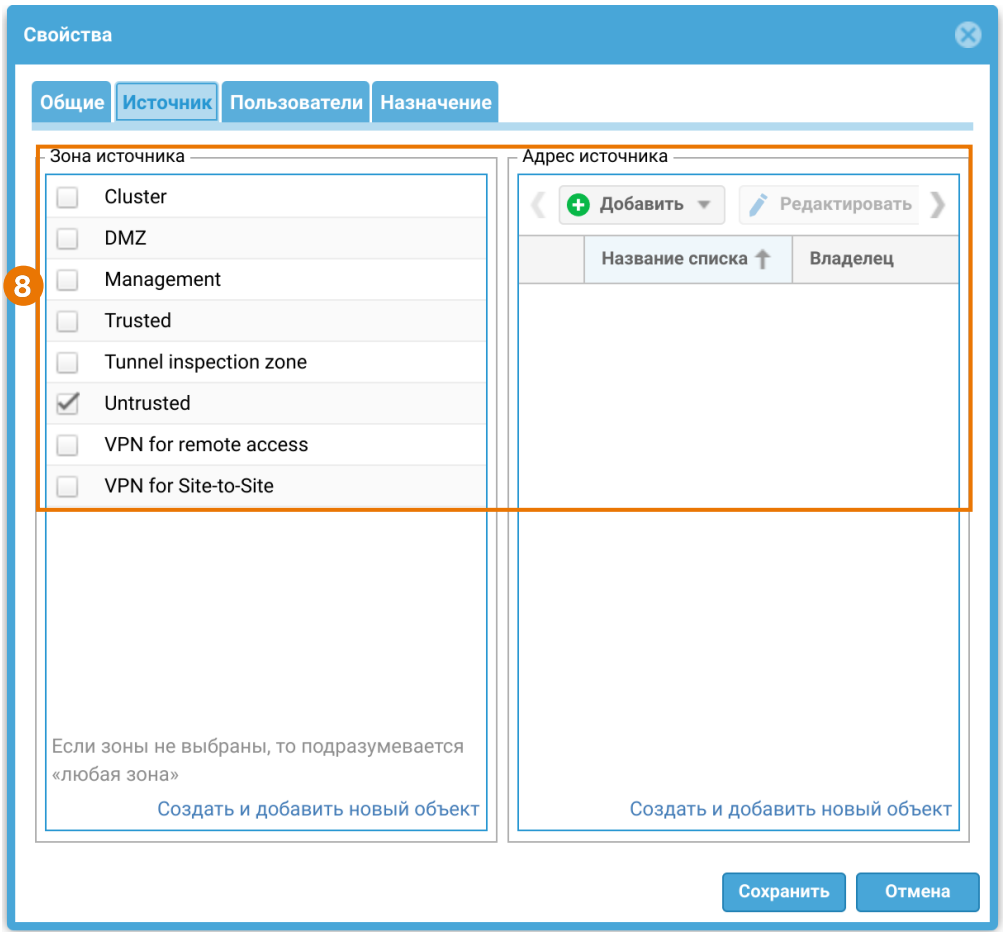
5. **Сеть VPN** — сеть, созданная ранее на этапе создания сети VPN. При настройке серверного правила для IPsec-туннеля, когда UserGate является VPN-сервером (указан протокол VPN **IPsec only/IKEV1** в свойствах серверного профиля безопасности) необходимо в данном поле выбрать опцию **Не использовать**.

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.

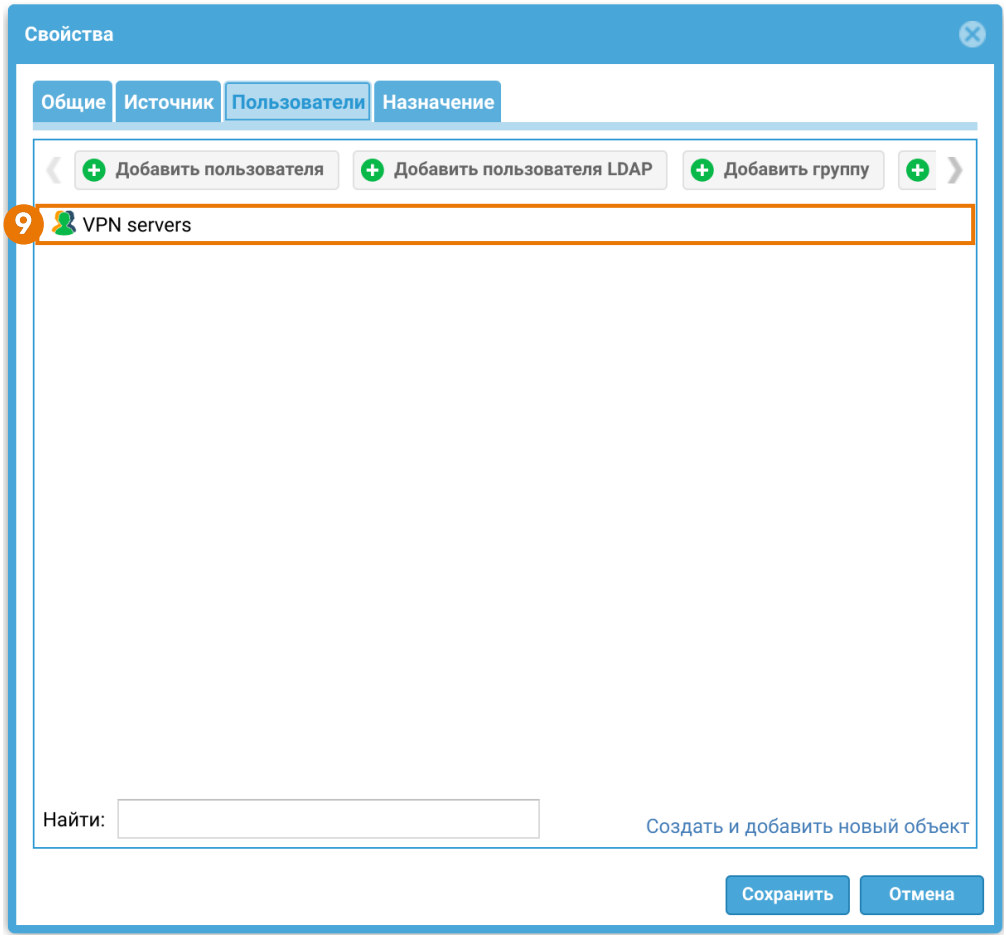


8. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

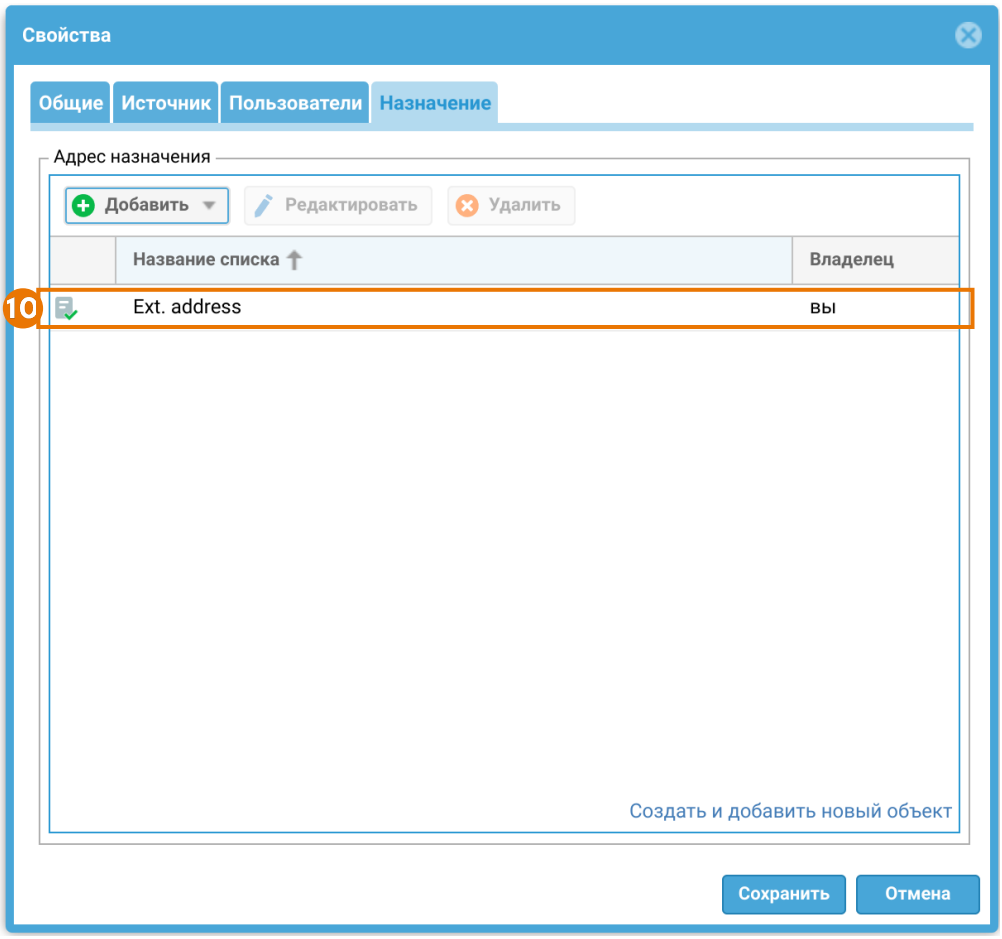
Важно!

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.



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.

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

Настройка VPN-клиента на NGFW состоит из следующих основных этапов:

1. Создание зоны для VPN подключений.
2. Создание VPN-интерфейса.
3. Контроль доступа к ресурсам.
4. Настройки параметров аутентификации.
5. Создание профиля безопасности VPN.
6. Создание клиентского правила VPN.

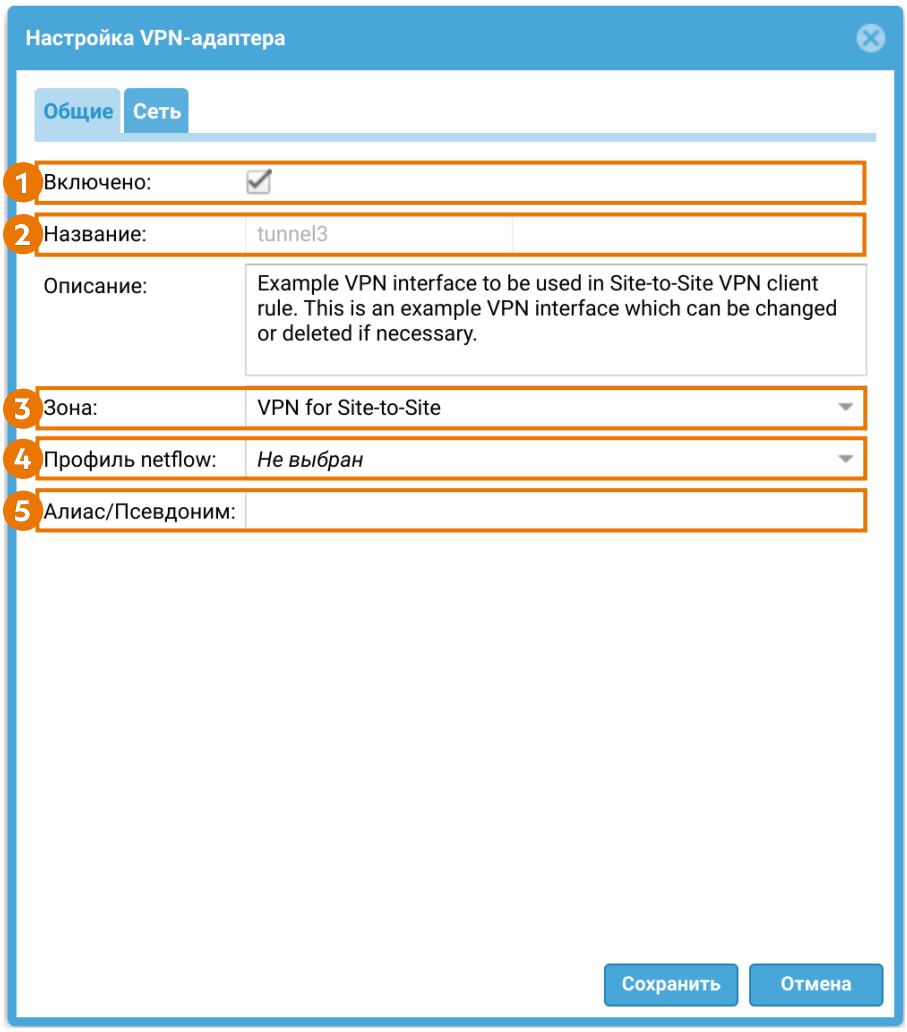
Создание зоны для VPN-подключений

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:



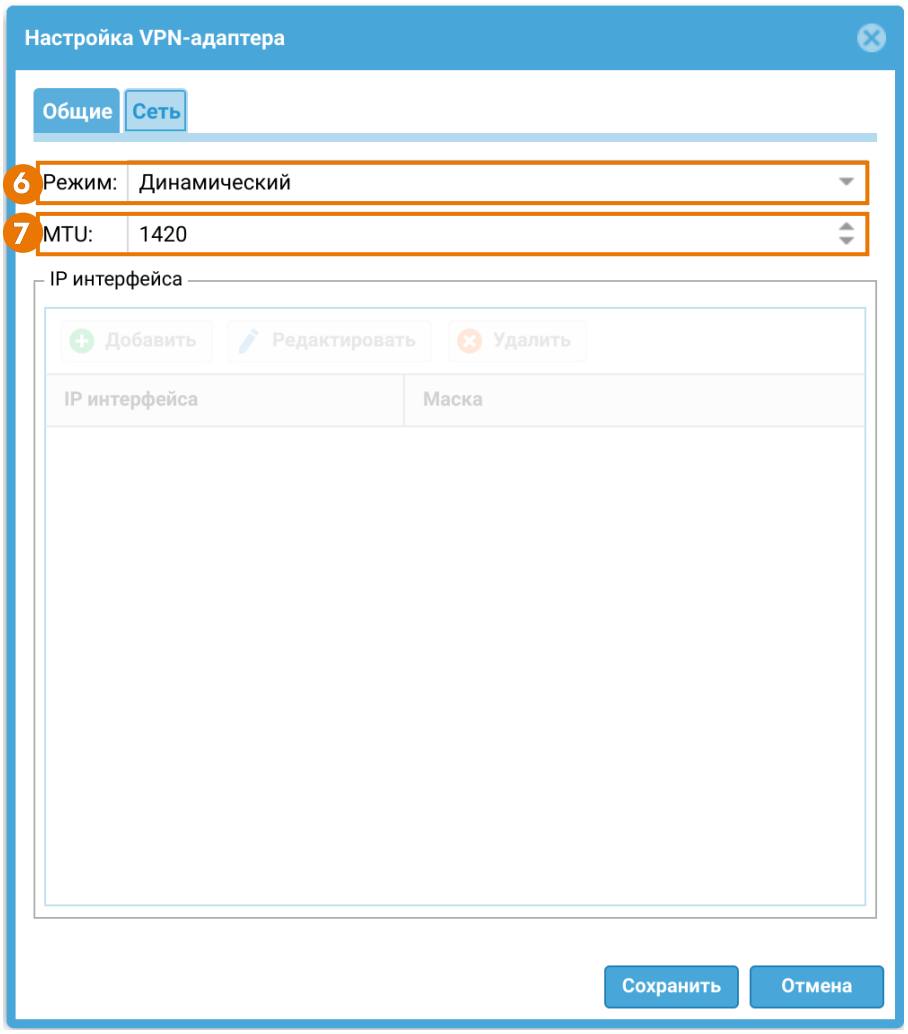
1. **Включено** — включение/отключение интерфейса.

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 относится 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.



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.

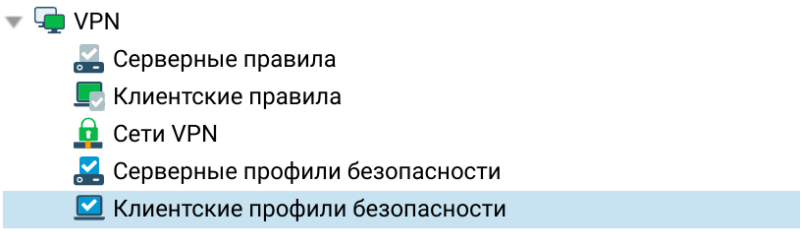
Настройки параметров аутентификации

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.

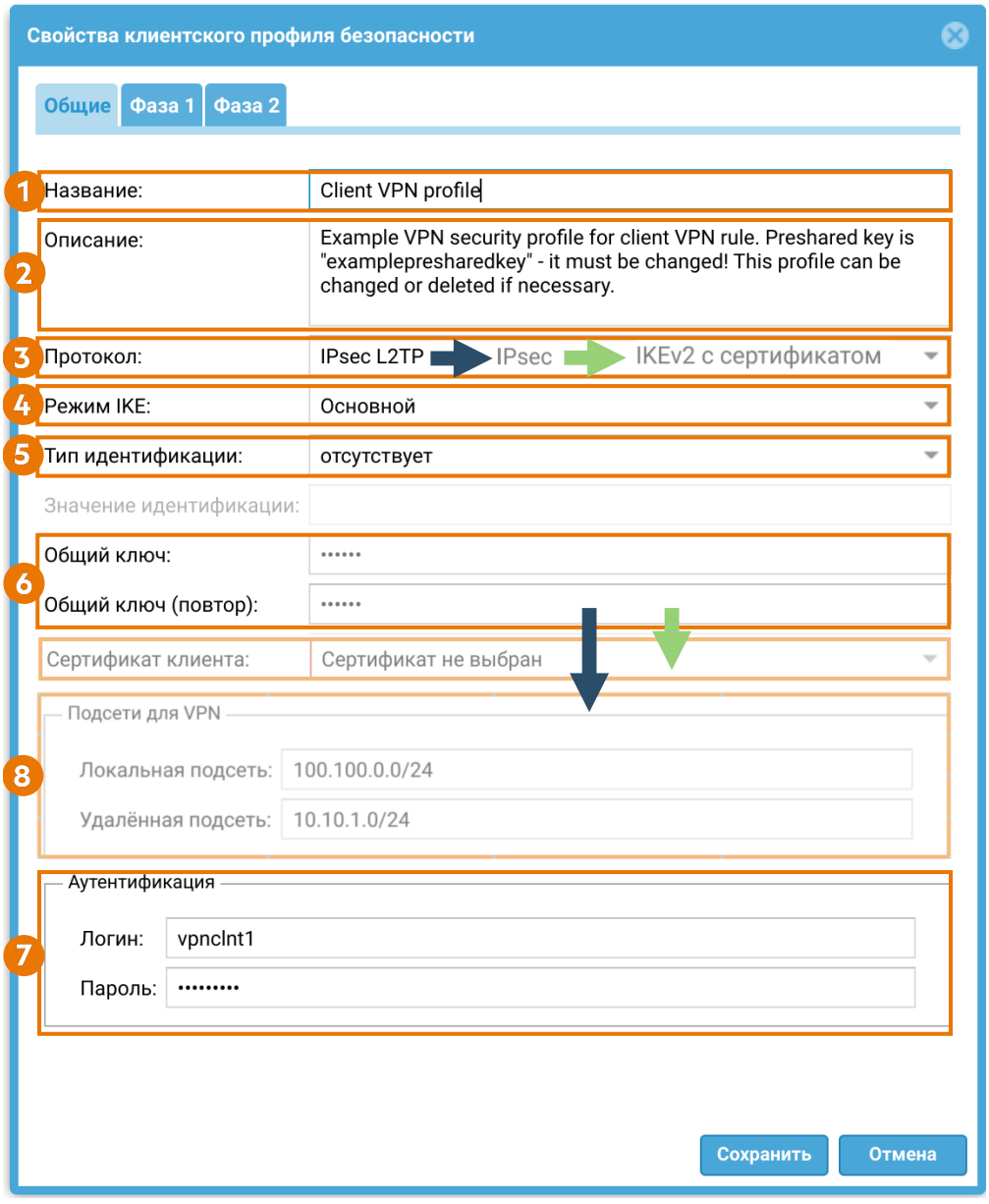
О примерах создания и использования сертификатов для IKEv2 VPN читайте в Приложении.

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 раздельно:



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:



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:

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

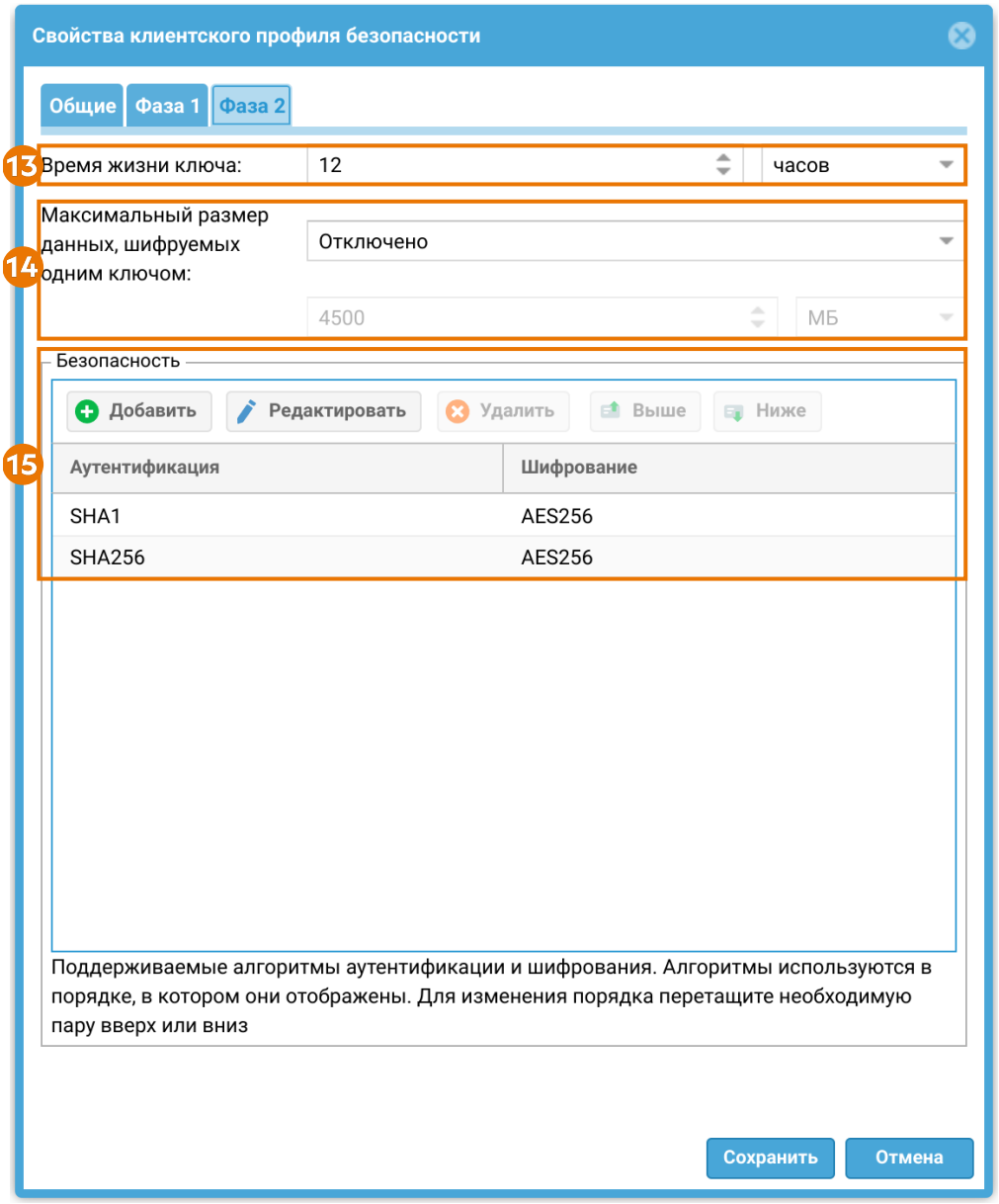
возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается.

- **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 будет 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:



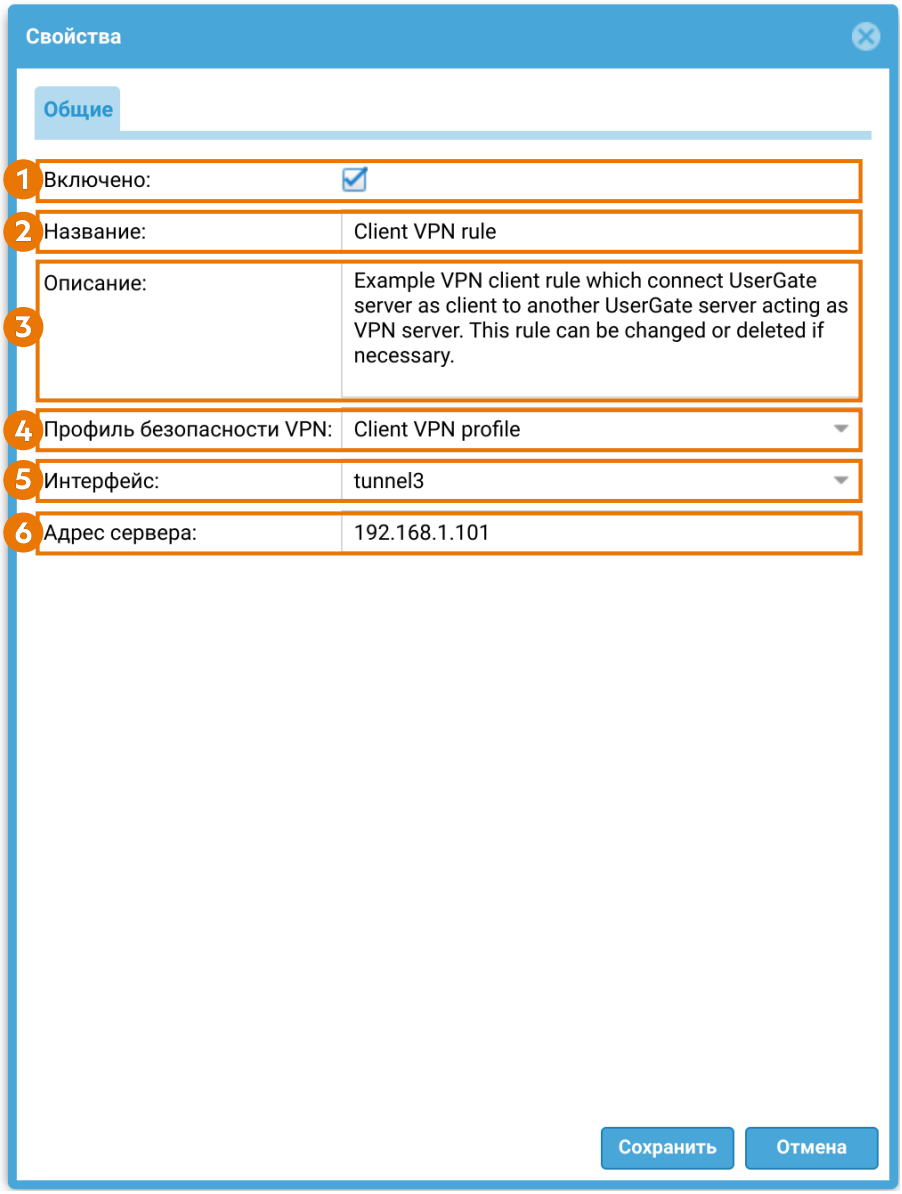
13. **Время жизни ключа** — по истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.

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**/**Ниже**.

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:



1. **Включено** — включение/отключение данного правила.

2. **Название** клиентского правила.

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.

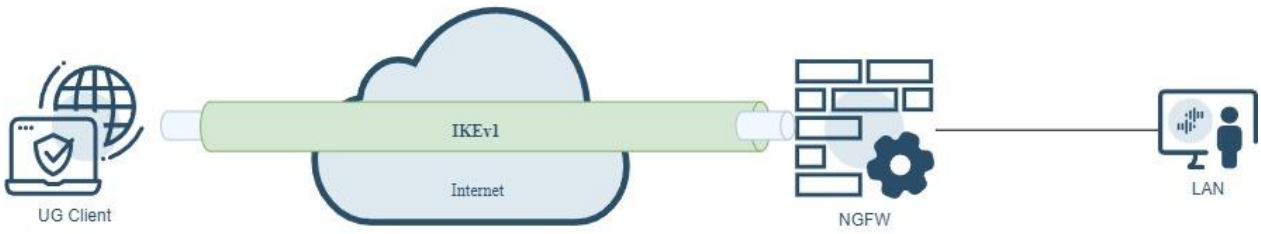
После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

VPN для удаленного доступа клиентов (Remote access VPN)

Remote Access VPN (Virtual Private Network) – виртуальная частная сеть с удаленным доступом, позволяет пользователям получать доступ к корпоративной сети своей компании. Реализует защищенное взаимодействие между сегментом корпоративной сети и одиночным пользователем, который подключается к корпоративным ресурсам через Интернет.

UserGate Client – это программное обеспечение для организации безопасного удаленного доступа к корпоративной сети через VPN-канал. Он обеспечивает шифрование данных и защищает передачу информации между удаленным устройством и корпоративной инфраструктурой. Совместим с операционной системой Windows. Аутентификация пользователей возможна с помощью логин/пароль, двухфакторную аутентификацию (2FA) и сертификаты, что гарантирует, что только авторизованные лица получат доступ. Централизованное управление UserGate Client осуществляется через UGMC, что позволяет администраторам настраивать политики доступа, определять, какие ресурсы доступны пользователям и группам пользователей, и контролировать уровни доступа. Подробнее о UserGate Client можно узнать в статье Конечные устройства UserGate Client.

UserGate Client IPsec L2TP



В данном случае NGFW выступает в качестве VPN сервера, а пользователь с установленным ПО UserGate Client выступают в качестве клиента 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.
Для этого необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе **Сеть → Зоны** отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервисы **VPN** и **Подключение конечных устройств**.
Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN клиенты.	В разделе **Сеть → Зоны** создать зону, в которую будут помещены подключаемые по VPN клиенты. Эту зону в дальнейшем можно использовать в политиках безопасности. Существует уже созданная по умолчанию зона **VPN for remote access.**
Шаг 3. Создать правило NAT для созданной зоны.	Для того чтобы подключенные VPN клиенты могли ходить в интернет через туннель NGFW , необходимо создать правило NAT из зоны **VPN for remote access** в зону **Untrusted**. Создайте соответствующее правило в разделе **Политики сети → NAT и маршрутизация**. Для примера в 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**.
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе **Политики сети → Межсетевой экран** создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. Чтобы трафик передавался на сервер из зоны клиента через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения. Для примера в NGFW создано правило из зоны удаленных VPN подключений **VPN for remote access,** разрешающее доступ в зоны **Trusted and Untrusted**.
Шаг 5. Создать профиль аутентификации.	В разделе **Пользователи и устройства → Профили аутентификации** создать профиль для пользователей VPN. Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP.

Наименование	Описание
Шаг 6. Создать серверный профиль безопасности VPN.	В настройках серверного профиля безопасности VPN определяются алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов. Для создания профиля безопасности **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** – название профиля безопасности. • **Описание** – описание профиля. • **IKE версия** – протокол IKE используется для создания защищенного канала связи между сетью и клиентом. Выбрать IKEv1 • **Режим IKE**: ◦ **Основной режим**. В основном режиме происходит обмен шестью сообщениями. ◦ **Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. • **Тип идентификации** – **Отсутствует.** Используется в случае, когда для установления соединения между VPN-сервером и UG Client не требуется использовать параметр IKE local ID. Тип параметра IKE local ID: ◦ **IPv4** — IP-адрес узла. ◦ **FQDN** – адрес узла в формате полностью определенного доменного имени (FQDN) • **Значение идентификации** – значение параметра IKE local ID в формате выбранного ранее типа. • **Общий ключ**. Аутентификация удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования туннеля. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа** – по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **Dead peer detection** — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве

Наименование	Описание
	связи используется механизм Dead Peer Detection (DPD). 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. • **Diffie-Hellman группы** – выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **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. • **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**

Наименование	Описание
	одним ключом), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **Включить 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 peer-узла для поддержания сессии NAT активной. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.
Шаг 7. Создать VPN-интерфейс.	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. В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** – название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** – описание интерфейса. • **Зона** – зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 2. • **Профиль Netflow** – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** – необходимо использовать статический IP-адрес. • **MTU** – размер MTU для выбранного интерфейса.
Шаг 8. Создать сеть VPN.	

Наименование	Описание
	VPN-сеть 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. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** – название сети. • **Описание** – описание сети. • **Диапазон IP-адресов**, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите **DNS-серверы**, которые будут переданы клиенту, или укажите четбокс **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. **Важно!** **Можно указать не более двух DNS-серверов.** • **Маршруты VPN** – укажите маршруты, передаваемые клиенту в виде IP-адреса с маской или заранее созданного списка IP-адресов. • **Маршруты для UserGate Client** – настройка функции раздельного туннелирования для UserGate Client. **Важно! Настройки маршрутов, передаваемых на конечные устройства UserGate Client, передаются только при VPN с IKEv2.**
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел **VPN →**

Наименование	Описание
	Серверные правила, нажать кнопку **Добавить** и заполнить следующие поля: • **Включено** – флажок включения/отключения правила. • **Название** – название правила. • **Описание** – описание правила. • **Профиль безопасности VPN** – серверный профиль безопасности, созданный ранее. • **Сеть VPN** – сеть VPN, созданная ранее. • **Профиль аутентификации** – профиль аутентификации, созданный ранее. • **Интерфейс** – интерфейс VPN, созданный ранее. • **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.** • **Назначение** – один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 1. • **Пользователи** – группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN.

Наименование	Описание
	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.**
Шаг 10. Настроить VPN на клиентском компьютере.	Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры: • Установка ПО UserGate VPN Client на рабочей с станции. • В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1. • В качестве общего ключа для подключения VPN L2TP/IPsec(IKEv1) (pre-shared key, shared secret) используйте общий ключ, указанный вами на шаге 6. • Укажите данные пользователя для аутентификации (Login/Password). Подробнее о конечных устройствах UserGate Client в связке с NGFW смотрите в разделе данного руководства Конечные устройства UserGate Client

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.

Настройка VPN для удаленного доступа с помощью интерфейса cli

Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.

Для редактирования параметров зоны используется следующая команда:

```
Admin@UGOS# 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@UGOS# set network zone Untrusted enabled-services [ VPN ]
```

Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN серверы.

Для создания зон используется следующая команда:

```
Admin@UGOS# create network zone <parameters>
```

Подробнее о командах и параметрах для создания/редактирования зон в cli смотрите в статье Зоны.

Пример создания зоны RA_VPN:

```
Admin@UGOS# create network zone name RA_VPN enabled-services [ VPN ]
```

Шаг 3. Создать правило NAT для созданной зоны.

Правила NAT создаются с помощью синтаксиса UPL командой:

```
Admin@UGOS# create network-policy nat-routing <position> upl-rule
<parameters>
```

Подробнее о порядке настройки правил межсетевого экрана в cli смотрите в статье Настройка правил NAT и маршрутизации.

Пример создания правила NAT из зоны RA_VPN в зону Zone1:

```
# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = RA_VPN \
...dst.zone = Zone1 \
...nat \
...rule_log(session) \
...name("RA NAT rule") \
...enabled true
```

Шаг 4. При необходимости создать разрешающее правило межсетевого экрана для разрешения трафика из созданной зоны в нужный сегмент сети.

Правила межсетевого экрана создаются с помощью синтаксиса UPL командой:

```
Admin@UGOS# create network-policy firewall <position> upl-rule
<commands>
```

Подробнее о порядке настройки правил межсетевого экрана в cli смотрите в статье Настройка правил межсетевого экрана.

Пример создания разрешающих правил межсетевого экрана для разрешения трафика из зоны RA_VPN в зону Zone1.

```
Admin@UGOS# create network-policy firewall 2 upl-rule PASS \
...src.zone = RA_VPN \
...dst.zone = Zone1 \
...rule_log(session) \
...name("RA_VPN to Zone1") \
...enabled(true)
```

Шаг 5. Создать профиль аутентификации для пользователей VPN.

Подробнее о порядке создания профилей аутентификации для пользователей в cli смотрите в статье Настройка профилей аутентификации.

Пример создания сервера аутентификации LDAP с названием New ldap server для домена testd.local и профиля аутентификации с названием New profile:

```
Admin@UGOS# create users auth-server ldap name "New ldap server"
address 192.168.1.2 domains [ test.local ] bind-dn test@test.local
password 12345 enabled on

Admin@UGOS# create users auth-profile name "New profile" auth-methods
ldap [ "New ldap server" ]
```

Шаг 6. Создать профиль безопасности VPN-сервера.

Для создания профиля безопасности VPN-сервера используется следующая команда:

```
Admin@UGOS# create vpn server-security-profiles <parameters>
```

Подробнее о порядке создания профилей безопасности VPN в cli смотрите в статье Настройка профилей безопасности VPN.

Пример создания профиля безопасности VPN-сервера с названием "VPN-server profile 2" для L2TP/IPsec VPN:

```
Admin@UGOS# create vpn server-security-profiles name "VPN-server
profile 2" ike-version 1 ike-mode main psk 12345 dh-groups [ "Group 2
Prime 1024 bit" "Group 14 Prime 2048 bit" ] phase1-security [ SHA1/
AES256 SHA256/AES256 ] phase2-security [ SHA1/AES256 SHA256/AES256 ]
Repeat preshared key:
Admin@UGOS#
```

Шаг 7. Создать VPN-интерфейс.

Для создания VPN-интерфейса используется следующая команда:

```
Admin@UGOS# create network interface vpn <parameters>
```

Подробнее о порядке создания VPN-интерфейса в cli смотрите в статье Интерфейсы.

Пример создания VPN-интерфейса tunnel1, входящего в зону RA_VPN:

```
Admin@UGOS# create network interface vpn interface-name 1 zone RA_VPN
ip-addresses [ 172.30.252.1/24 ] enabled on
```

Шаг 8. Создать сеть VPN.

Для создания сети VPN используется следующая команда:

```
Admin@UGOS# create vpn networks <parameters>
```

Подробнее о порядке создания сети VPN в cli смотрите в статье Настройка сетей VPN.

Пример создания сети VPN с названием "VPN network 2":

```
Admin@UGOS# create vpn networks name "VPN network 2" ip-range
172.30.252.2-172.30.252.254 mask 255.255.255.0 use-system-dns on
routes-ip-list [ "Int net address" ]
```

Шаг 9. Создать серверное правило VPN.

Правила для VPN-сервера создаются с помощью синтаксиса UPL командой:

```
Admin@UGOS# create vpn server-rules <position> upl-rule <commands>
```

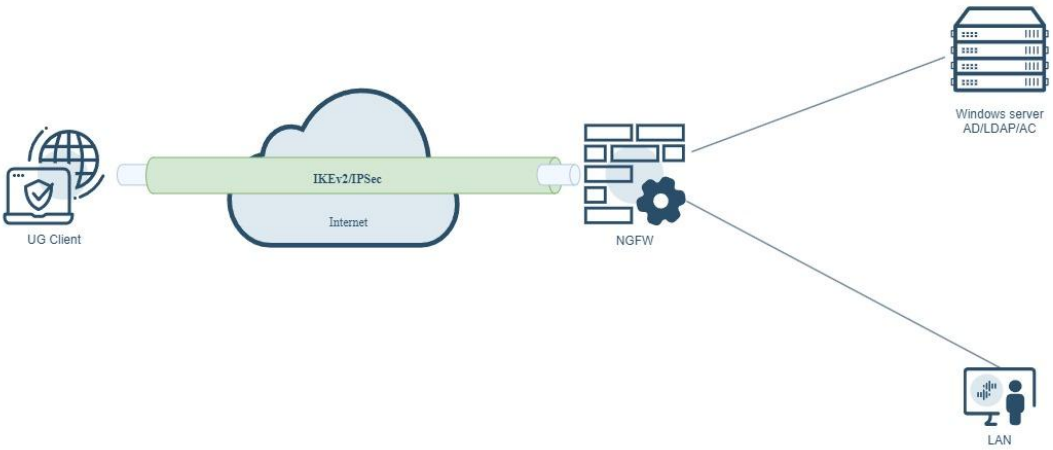
Подробнее о порядке настройки серверных правил VPN в cli смотрите в статье Настройка серверных правил.

Пример создания серверного правила VPN с названием "VPN-server rule 2", в котором используются ранее созданные: профиль безопасности VPN-сервера "VPN-server profile 2", сеть VPN "VPN network 2", профиль аутентификации пользователей "New profile", VPN-интерфейс tunnel1 и список с внешним IP-адресом VPN-сервера "Ext VPN address":

```
Admin@UGOS# create vpn server-rules 2 upl-rule OK \
...name("VPN-server rule 2") \
...profile("VPN-server profile 2") \
...vpn_network("VPN network 2") \
...auth_profile("New profile") \
```

```
...interface(tunnel1) \
...src.zone = Untrusted
...dst.ip = lib.network("Ext VPN address")
...enabled(true)
```

UserGate Client IKEv2 с сертификатом



Для подключения VPN-клиентов к корпоративной сети необходимо настроить NGFW для выполнения роли VPN-сервера, а пользователь с установленным ПО UserGate Client выступают в качестве клиента VPN. **При создании VPN с помощью IKEv2/IPsec, протокол** IKEv2 обменивается ключами, устанавливает и управляет защищенным соединением. Перед установкой туннеля IKEv2 IPsec, устройства должны аутентифицироваться друг перед другом, обеспечивая уверенность в том, что они являются легитимными. Это включает в себя использование предварительно согласованных сертификатов. Проверка сертификатов осуществляется:

- По шифрованному каналу vpn-клиент присылает пользовательский сертификат и зашифрованные данные, подписанные приватным ключом.
- VPN-сервер расшифровывает данные публичным ключом клиента и сравнивает со своим контрольным набором, проверяя наличие приватного ключа у клиента.
- VPN-сервер согласно настроенному профилю пользовательских сертификатов проверяет сертификат клиента на соответствие указанной цепочки сертификатов.
- VPN-сервер осуществляет проверку отозванных сертификатов.

- VPN-сервер осуществляет проверку UPN атрибутов пользователя указанного в профиле аутентификации с атрибутами в сертификате **CN и\или SAN:principal name.**
- Если не пройдет любой пункт из четырех, соединение не установится.
- Если все проверки пройдены, VPN-сервер со своей стороны отправляет свой сертификат и зашифрованные данные, подписанные своим приватным ключом, а также наличие второго фактора (если указано).
- Клиент проверяет подлинность подписи сервера и соответствие subjectAlternativeName тому адресу, куда он подключился.

Выполните следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе **Сеть → Зоны** отредактировать параметр контроля доступа для зоны **Untrusted**, к которой будут подключаться VPN-клиенты, разрешить сервисы **VPN** и **Подключение конечных устройств**.
Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN клиенты.	В разделе **Сеть → Зоны** создать зону **VPN for remote access**, в которую будут помещены подключаемые по VPN клиенты. Существует уже созданная по умолчанию зона **VPN for remote access.**.
Шаг 3. Создать правило NAT для созданной зоны.	Для того чтобы подключенные VPN клиенты могли ходить в интернет через туннель NGFW , необходимо создать правило NAT из зоны **VPN for remote access** в зону **Untrusted**. Создайте соответствующее правило в разделе **Политики сети → NAT и маршрутизация**. Для примера в 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**.
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе **Политики сети → Межсетевой экран** создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. Для примера в NGFW создано правило **VPN for remote access to Trusted and Untrusted**..
Шаг 5. Создать профиль аутентификации.	В разделе **Пользователи и устройства → Профили аутентификации** создать профиль для пользователей VPN. Укажите **Метод аутентификации.** Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP.

Наименование	Описание
	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*). Подробно о профилях аутентификации смотрите в разделе данного руководства Профили аутентификации.
Шаг 6. Создать группу пользователей.	В разделе **Пользователи и устройства → Группы** создать группу для пользователей VPN. Обратите внимание UPN атрибут пользователя должен совпадать с атрибутами CN и\или SAN: principal name в пользовательских сертификатах выписанных на клиенте.
Шаг 7. Создать сертификаты.	В разделе **UserGate → Сертификаты** создать или импортировать корневой сертификат удостоверяющего центра и сертификат с приватным ключом. Подробно о создание сертификатов смотрите Приложение 6. Примеры генерации сертификатов для IKEv2 VPN.
Шаг 8. Создать профиль пользовательского сертификата.	В разделе **UserGate → Профили пользовательских сертификатов** создать профиль. Подробно о профилях пользовательского сертификата смотрите в разделе данного руководства Профили клиентских сертификатов.
Шаг 9. Добавить сертификат в раздел настройки.	В разделе **UserGate → Настройки** указать в пункте **Сертификат конечного устройства** добавленный ранее сертификат с приватным ключом.
Шаг 10. Создать серверный профиль безопасности VPN.	В настройках серверного профиля безопасности VPN определяются алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов. В раздел **VPN → Серверные профили безопасности**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** – название профиля безопасности. • **Описание** – описание профиля. • **IKE версия** – **IKEv2** – для создания защищенного канала будет использоваться IKEv2. • **Тип идентификации** – **Отсутствует.** Используется в случае, когда для установления соединения между

Наименование	Описание
	VPN-сервером и UG Client не требуется использовать параметр IKE local ID. Тип параметра IKE local ID: ◦ **IPv4** — IP-адрес узла. ◦ **FQDN** – адрес узла в формате полностью определенного доменного имени (FQDN) • **Значение идентификации** – значение параметра IKE local ID в формате выбранного ранее типа. • **Сертификат сервера** – выбор сертификата сервера для аутентификации посредством сертификатов. • **Режим аутентификации** – посредством сертификатов (PKI). • **Профиль сертификата пользователя** — необходимо указать сконфигурированный профиль пользовательских сертификатов. Далее необходимо задать параметры первой и второй фаз согласования туннеля. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа** – по истечению данного времени происходят повторная аутентификация и согласование настроек первой фазы. • **Dead peer detection** — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи используется механизм Dead Peer Detection (DPD). 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

Наименование	Описание
	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. • **Diffie-Hellman группы** – выбор группы Диффи-Хеллмана, которая будет 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. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **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. • **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. • **Включить 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 peer-узла для поддержания сессии NAT активной. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, котором они отображены. Для изменения порядка перетащите

Наименование	Описание
	необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.
Шаг 11. Создать VPN-интерфейс.	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. В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** – название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** – описание интерфейса. • **Зона** – зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 2. • **Профиль Netflow** – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** – необходимо использовать статический IP-адрес. • **MTU** – размер MTU для выбранного интерфейса.
Шаг 12. Создать сеть VPN.	VPN-сеть 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. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** – название сети. • **Описание** – описание сети. • **Диапазон IP-адресов**, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не

Наименование	Описание
	указывайте здесь адреса сети и широковещательный адрес. • Укажите **DNS-серверы**, которые будут переданы клиенту, или поставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. **Важно!**Можно указать не более двух DNS-серверов. • **Маршруты VPN** – укажите маршруты, передаваемые клиенту в виде IP-адреса с маской или заранее созданного списка IP-адресов. • **Маршруты для UserGate Client** – вкладка для редактирования маршрутов, передаваемых клиентам, на которых установлен UserGate Client.
Шаг 13. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел **VPN → Серверные правила**, нажать кнопку **Добавить** и заполнить следующие поля: • **Включено** – флажок включения/отключения правила. • **Название** – название правила. • **Описание** – описание правила. • **Профиль безопасности VPN** – серверный профиль безопасности, созданный ранее. • **Сеть VPN** – сеть VPN, созданная ранее. • **Профиль аутентификации** – профиль аутентификации, созданный ранее. Подробнее о настройка двухфакторной аутентификации через TOTP для подключений по VPN смотрите в разделе Мультифакторная аутентификация с подтверждением через одноразовые временные пароли (TOTP) • **Интерфейс** – интерфейс VPN, созданный ранее. • **Источник** – зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**.

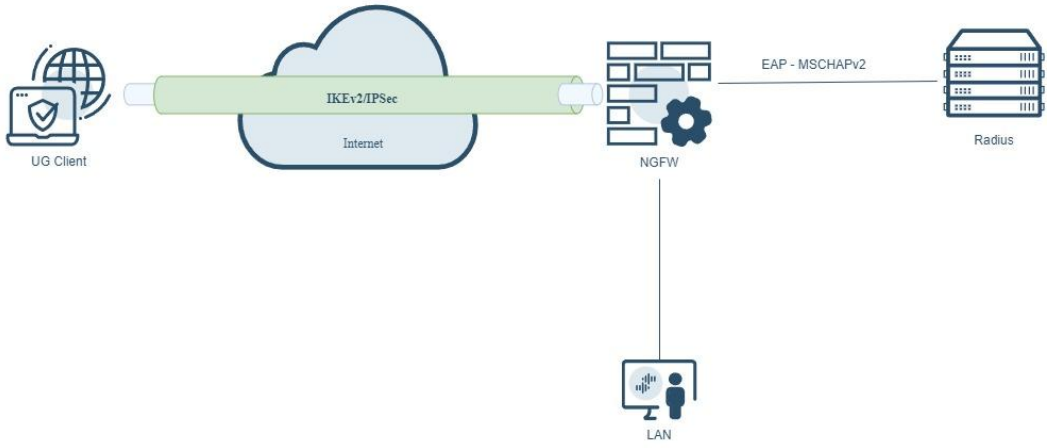
Наименование	Описание
	Важно! **Обработка трафика происходит по следующей логике:** **– условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;** **– условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.** • **Назначение** – один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 1. • **Пользователи** – группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN. **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.**
Шаг 14. Настроить VPN на клиентском компьютере.	При аутентификации с помощью сертификатов, использующих инфраструктуру открытых ключей (PKI), установите сертификат клиента на рабочую станцию в репозиторий – Локальный компьютер, хранилище – Автоматически выбрать хранилище. Подробнее о примерах генерации сертификатов для аутентификации можно посмотреть в Приложение. Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры: • Установка ПО UserGate VPN Client на рабочей с станции.

Наименование	Описание
	• Установите сертификат на рабочую станцию в репозиторий — Локальный компьютер, хранилище — Автоматически выбрать хранилище. • В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1. Подробнее о конечных устройствах UserGate Client в связке с NGFW смотрите в разделе данного руководства Конечные устройства UserGate Client

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.

UserGate Client IKEv2 аутентификации через Radius по логину-паролю



При инициализации VPN туннеля используя протокол IKEv2/IPsec аутентификация пользователя по логину и паролю через Radius. Для подключения VPN-клиентов к корпоративной сети необходимо настроить

NGFW для выполнения роли VPN-сервера, а пользователь с установленным ПО UserGate Client выступают в качестве клиента VPN.

VPN-клиент инициируют процесс установления VPN-туннеля с VPN-сервером, отправляя сообщении IKE_AUTH, сервер отвечает клиенту, что требуется авторизация через EAP-MSCHAPv2 . Клиент обменивается с сервером несколькими EAP-пакетами. VPN-сервер транслирует EAP-пакетами по radius на доменный радиус-сервер, который принимает решение об аутентификации. Далее, после того как получено положительный ответ от Radius-сервера, VPN-сервер по полученному логину запрашиваем домен на предмет этого пользователя и спрашиваем все его группы, далее принимается решение, можно ли данному пользователю подключаться к VPN-серверу.

Наименование	Описание
Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе **Сеть → Зоны** отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервисы **VPN** и **Подключение конечных устройств**. Как правило, это зона **Untrusted.**
Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN клиенты.	В разделе **Сеть → Зоны** создать зону, в которую будут помещены подключаемые по VPN клиенты. Эту зону в дальнейшем можно использовать в политиках безопасности.
Шаг 3. Создать правило NAT для созданной зоны.	Для того чтобы подключенные VPN клиенты могли ходить в интернет через туннель NGFW , необходимо создать правило NAT из зоны **VPN for remote access** в зону **Untrusted**. Создайте соответствующее правило в разделе **Политики сети → NAT и маршрутизация**. Для примера в 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**.
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе **Политики сети → Межсетевой экран** создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны.
Шаг 5. Создать профиль аутентификации.	В разделе **Пользователи и устройства → Профили аутентификации** создать профиль для пользователей VPN. Укажите **Метод аутентификации.** Следует учесть, что для аутентификации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP.

Наименование	Описание
	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*). Подробно о профилях авторизации смотрите в разделе данного руководства Профили аутентификации.
Шаг 6. Создать серверный профиль безопасности VPN.	В настройках серверного профиля безопасностии VPN определяются алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов. В разделе **VPN** создаются профили безопасности для VPN-сервера и для VPN-клиента. Для создания профиля безопасности **VPN-сервера** необходимо перейти в раздел **VPN → Серверные профили безопасности**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** – название профиля безопасности. • **Описание** – описание профиля. • **IKE версия** – используем **IKEv2** для создания защищенного канала будет использоваться IKEv2. • **Тип идентификации** – **Отсутствует.** Используется в случае, когда для установления соединения между VPN-сервером и UG Client не требуется использовать параметр IKE local ID. Тип параметра IKE local ID: ◦ **IPv4** — IP-адрес узла. ◦ **FQDN** – адрес узла в формате полностью определенного доменного имени (FQDN). • **Значение идентификации** – значение параметра IKE local ID в формате выбранного ранее типа. • **Режим аутентификации** – возможна аутентификация с помощью логина и пароля через RADIUS сервер (AAA). Далее необходимо задать параметры первой и второй фаз согласования туннеля. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа** – по истечению данного времени происходят повторная аутентификация и согласование настроек первой фазы.

Наименование	Описание
	• **Dead peer detection** — для проверки работоспособности канала и его своевременного отключения/переподключения при обрыве связи используется механизм Dead Peer Detection (DPD). 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. • **Diffie-Hellman группы** – выбор группы Диффи-Хеллмана, которая будет 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. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.

Наименование	Описание
	Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **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. • **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. • **Включить 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 peer-узла для поддержания сессии NAT активной. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.
Шаг 7. Создать VPN-интерфейс.	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. В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** – название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** – описание интерфейса.

Наименование	Описание
	• **Зона** – зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 2. • **Профиль Netflow** – профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** – необходимо использовать статический IP-адрес. • **MTU** – размер MTU для выбранного интерфейса.
Шаг 8. Создать сеть VPN.	VPN-сеть 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. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** – название сети. • **Описание** – описание сети. • **Диапазон IP-адресов**, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите **DNS-серверы**, которые будут переданы клиенту, или поставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. **Важно!**Можно указать не более двух DNS-серверов. • **Маршруты VPN** – укажите маршруты, передаваемые клиенту в виде IP-адреса с маской или заранее созданного списка IP-адресов. • **Маршруты для UserGate Client** – вкладка для редактирования маршрутов, передаваемых клиентам, на которых установлен UserGate Client.
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел **VPN →**

Наименование	Описание
	Серверные правила, нажать кнопку **Добавить** и заполнить следующие поля: • **Включено** – флажок включения/отключения правила. • **Название** – название правила. • **Описание** – описание правила. • **Профиль безопасности VPN** – серверный профиль безопасности, созданный ранее. • **Сеть VPN** – сеть VPN, созданная ранее. • **Профиль аутентификации** – профиль аутентификации, созданный ранее. Подробнее о настройка двухфакторной аутентификации через TOTP для подключений по VPN смотрите в разделе Мультифакторная аутентификация с подтверждением через одноразовые временные пароли (TOTP) • **Интерфейс** – интерфейс VPN, созданный ранее. • **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.** • **Назначение** – один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 1. • **Пользователи** – группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN. По умолчанию в NGFW создано серверное правило **Remote access VPN rule**, в котором используются необходимые настройки для **Remote Access VPN**, а доступ к VPN разрешен членам локальной группы **VPN users.**

Наименование	Описание
	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.**
Шаг 10. Настроить VPN на клиентском компьютере.	При аутентификации с помощью протокола EAP с методом MSCHAPv2 (AAA) укажите данные пользователя для аутентификации (Login/Password). Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры: • Установка ПО UserGate VPN Client на рабочей с станции. • В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1. • Укажите данные пользователя для аутентификации (Login/Password). Подробнее о конечных устройствах UserGate Client в связке с NGFW смотрите в разделе данного руководства Конечные устройства UserGate Client

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-

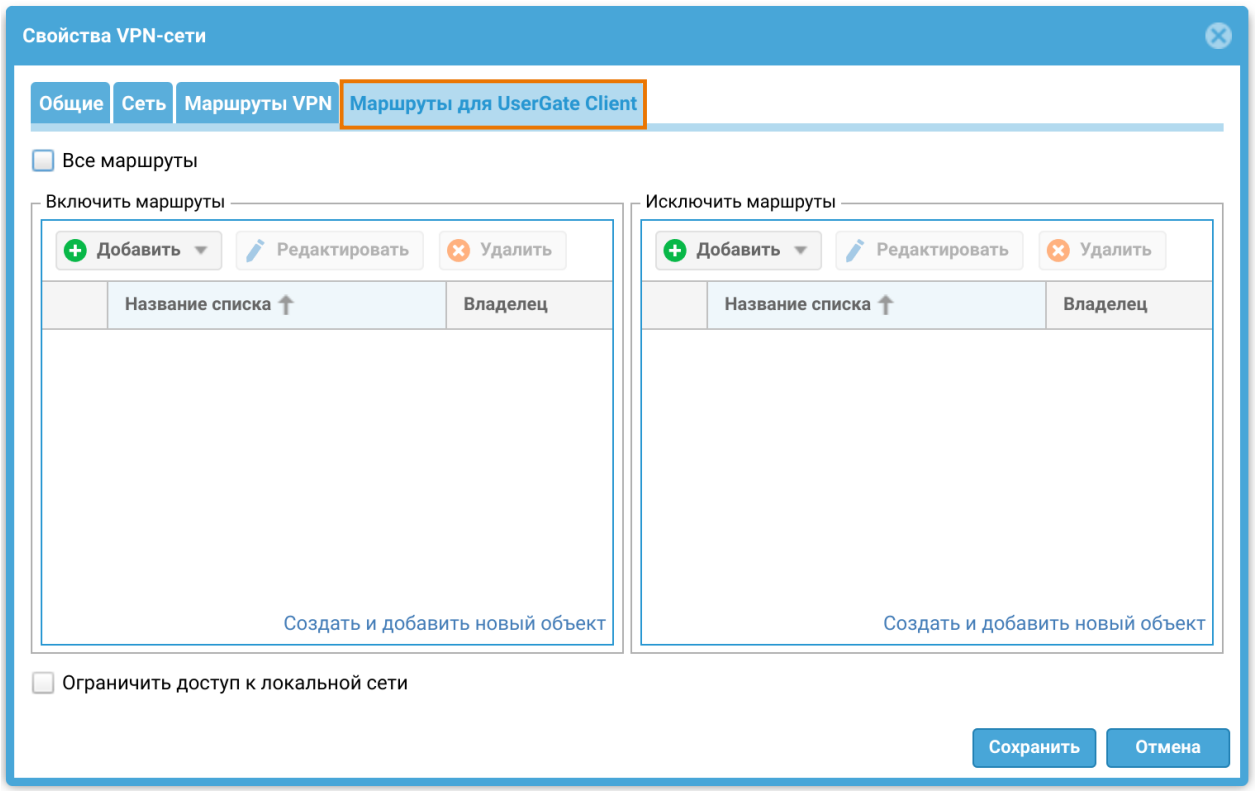
сессии локальные настройки маршрутизации на компьютере пользователя возвращаются в исходные.

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.

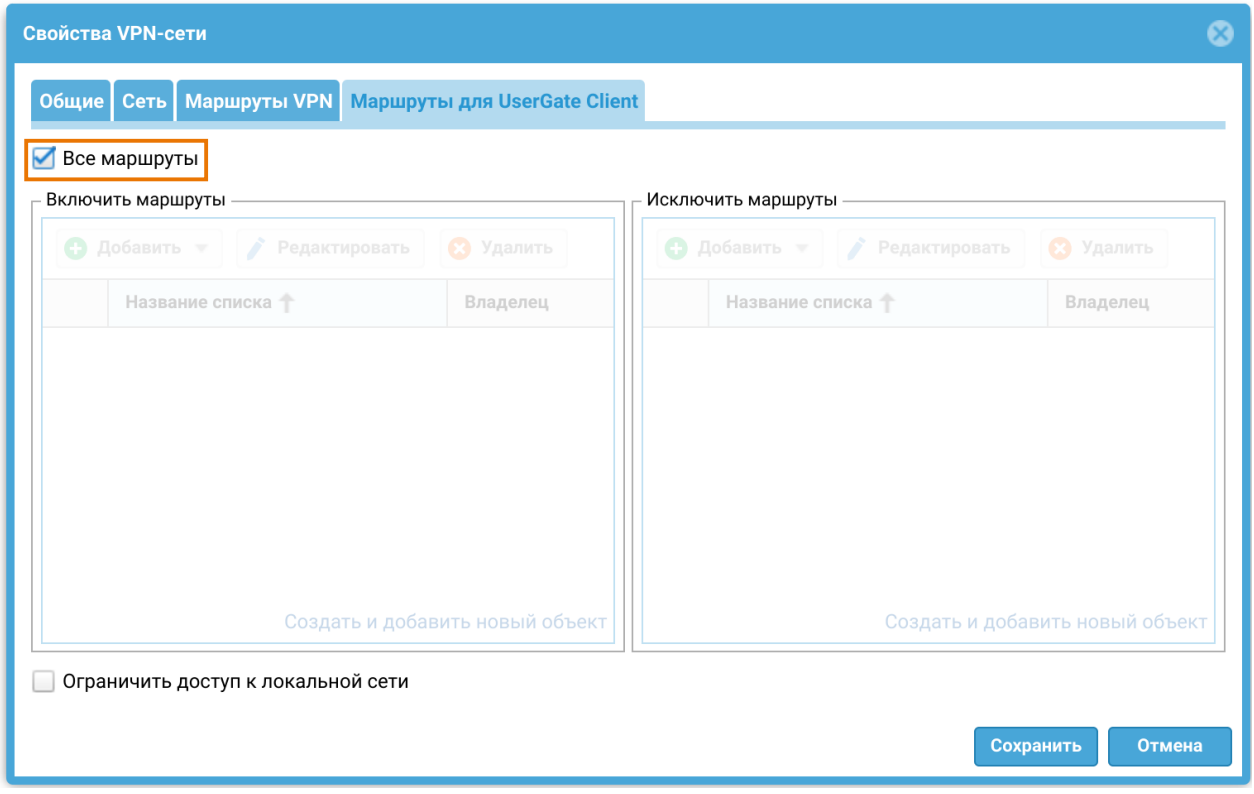
Локальные маршруты в обход VPN, изначально прописанные на компьютере пользователя, удаляются на время работы VPN. После отключения VPN-соединения эти маршруты возвращаются.

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**.

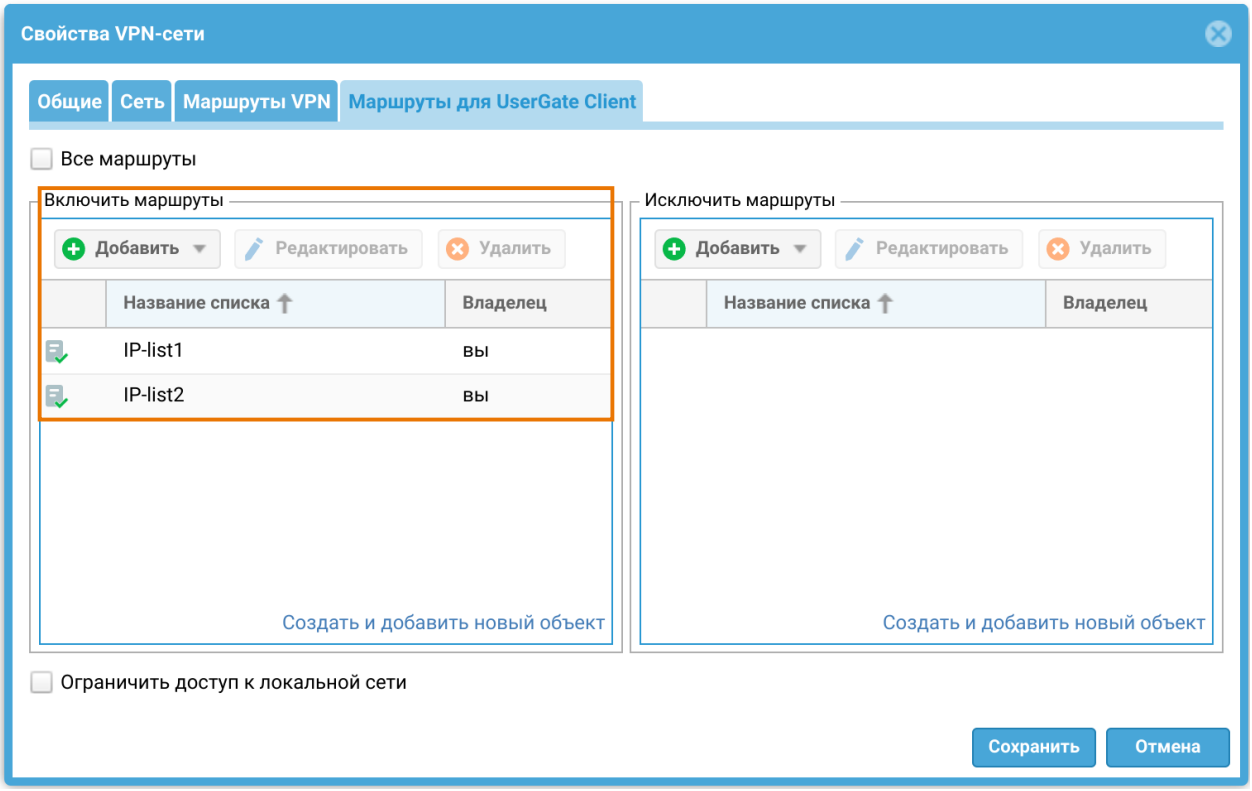


Рассмотрим подробнее возможные сценарии настроек раздельного туннелирования.

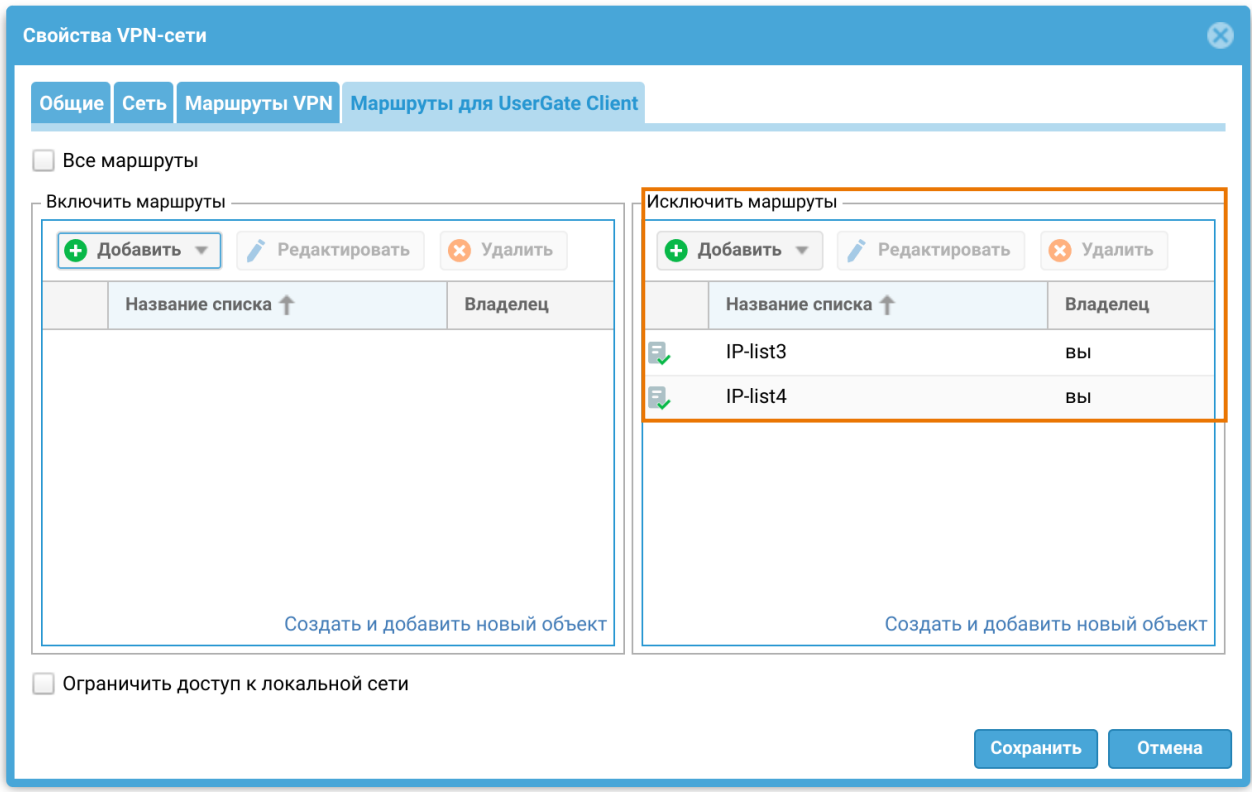
а) Если поставлен флажок **Все маршруты**, в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию (default route) вида *0.0.0.0/0* ➜ *VPN-шлюз*. Имеющийся ранее маршрут по умолчанию будет удален из таблицы.



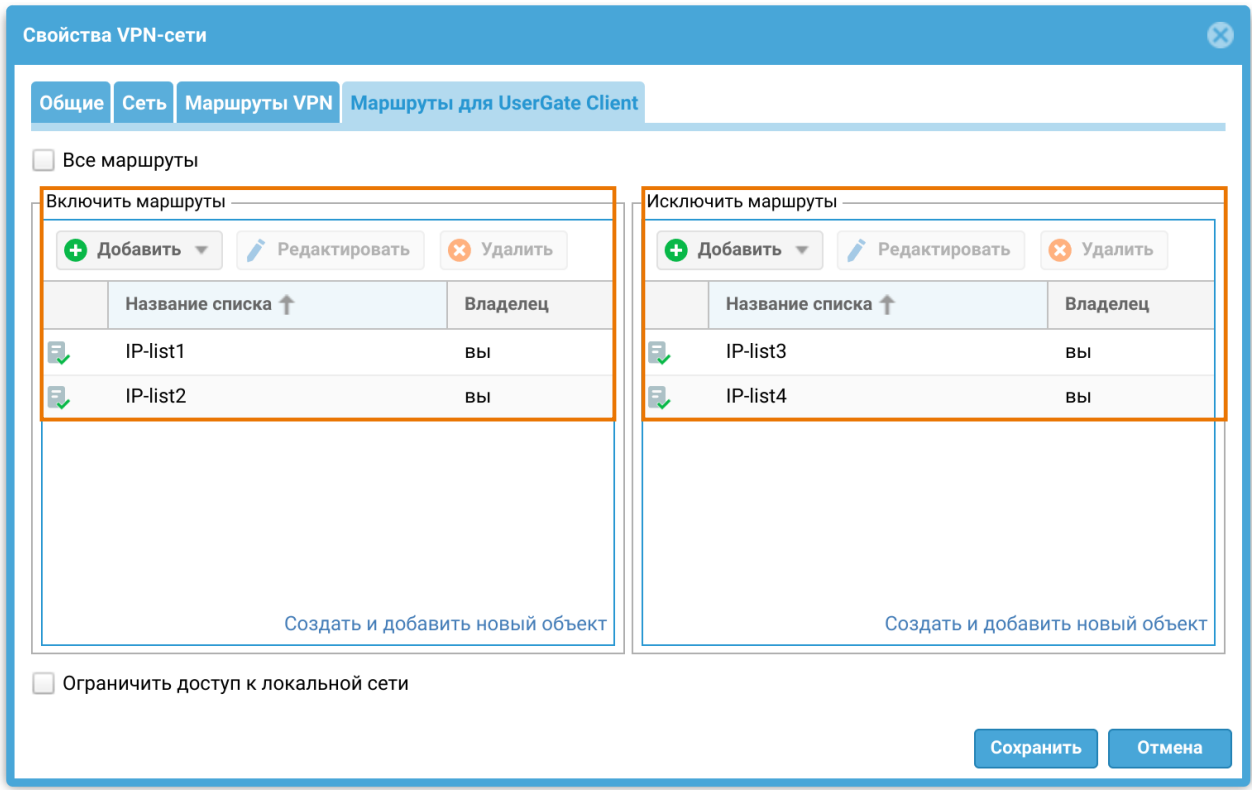
b) Если в поле **Включить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида *n.n.n.n/c* ➜ *VPN-шлюз* с гарантированно минимальной метрикой 2.



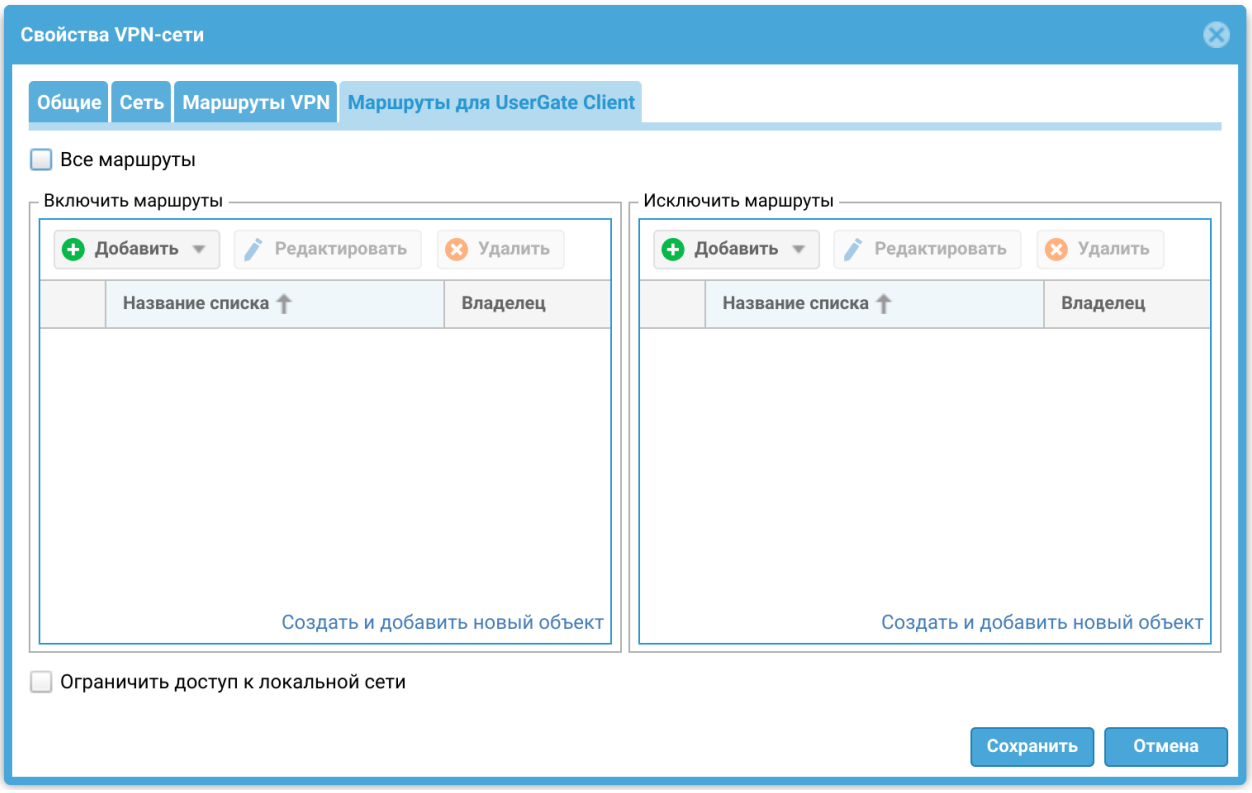
c) Если в поле **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то в таблицу маршрутизации клиента будет добавлен маршрут по умолчанию вида *0.0.0.0/0* ➜ *VPN-шлюз*. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.



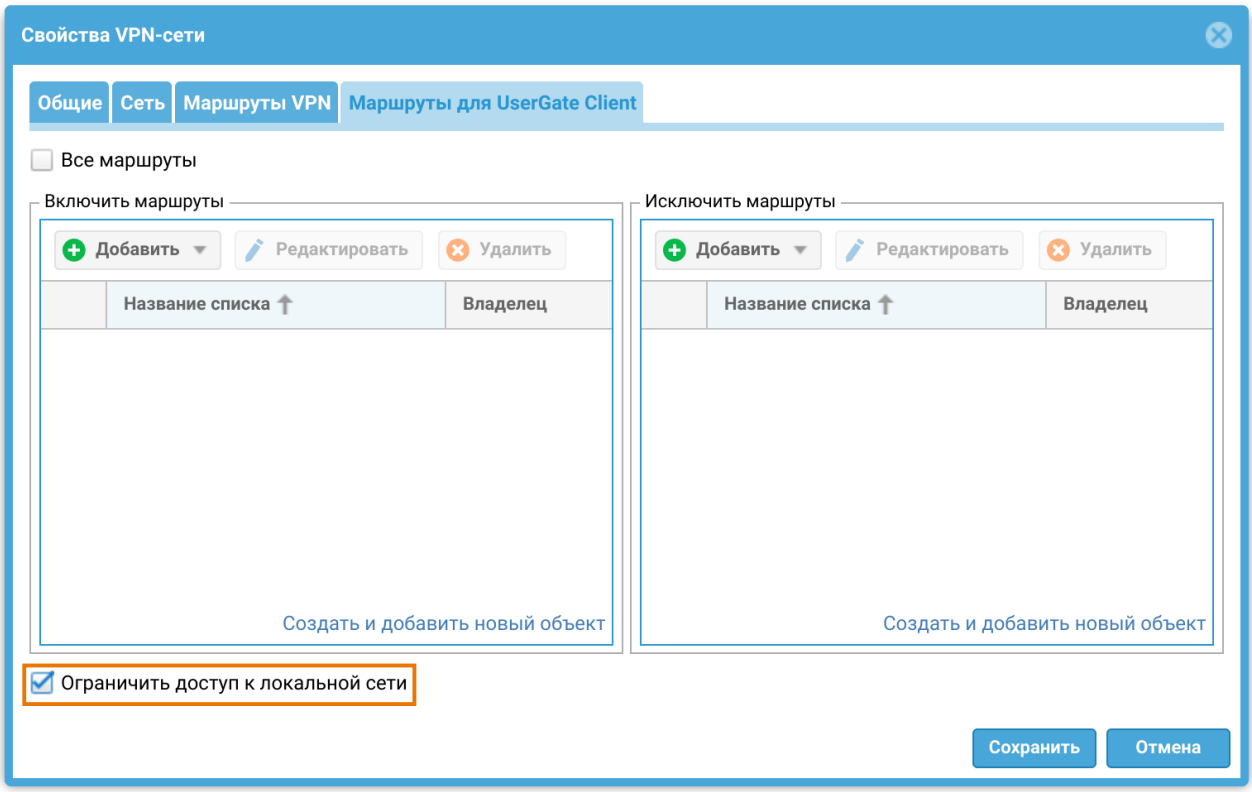
d) Если в обоих полях **Включить маршруты** и **Исключить маршруты** добавлены IP-адреса или списки IP-адресов, то для каждого включенного адреса добавляется маршрут вида *n.n.n.n/c* ➜ *VPN-шлюз* с гарантированно минимальной метрикой 2. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN.



e) Если во 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 MC/NGFW/VPN-сервера не создаются.



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*.



В зависимости от сценариев настроек метрики для VPN-маршрутов broadcast- и multicast-адресов получают следующие значения:

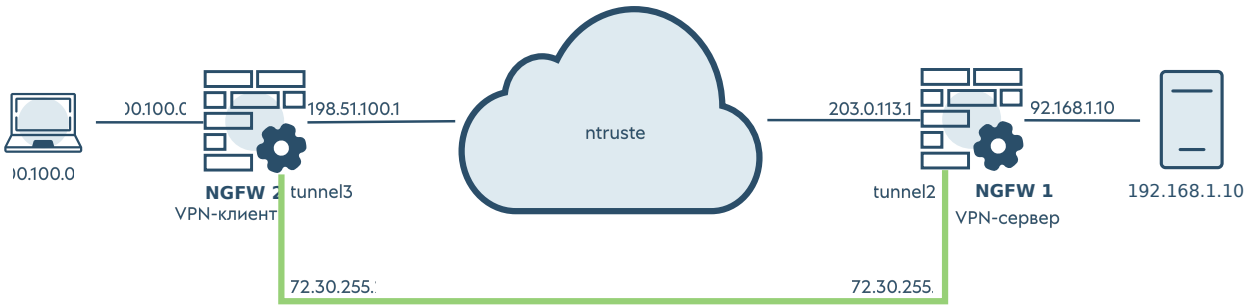
- Лучшая метрика среди соответствующих адресов — для сценариев a) и c);
- Гарантированно худшая метрика 10000 — для сценариев b) и d).

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

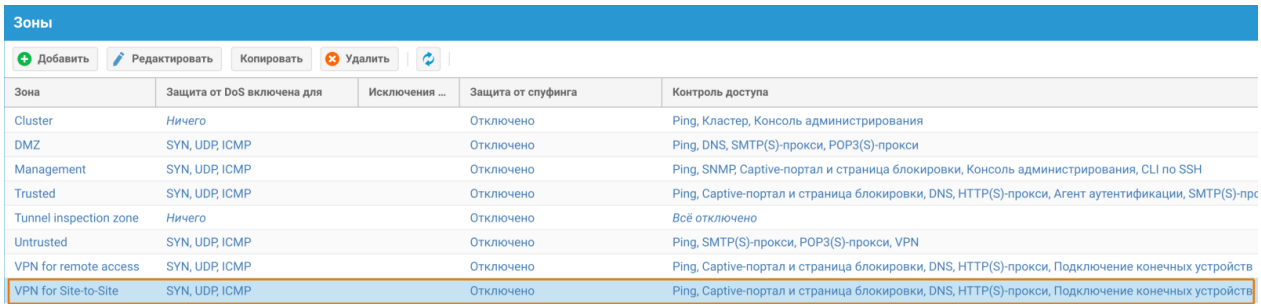
Для настройки узла **NGFW 1** в качестве VPN-сервера необходимо выполнить следующие шаги:

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 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.



Шаг 3. Настроить параметры аутентификации.

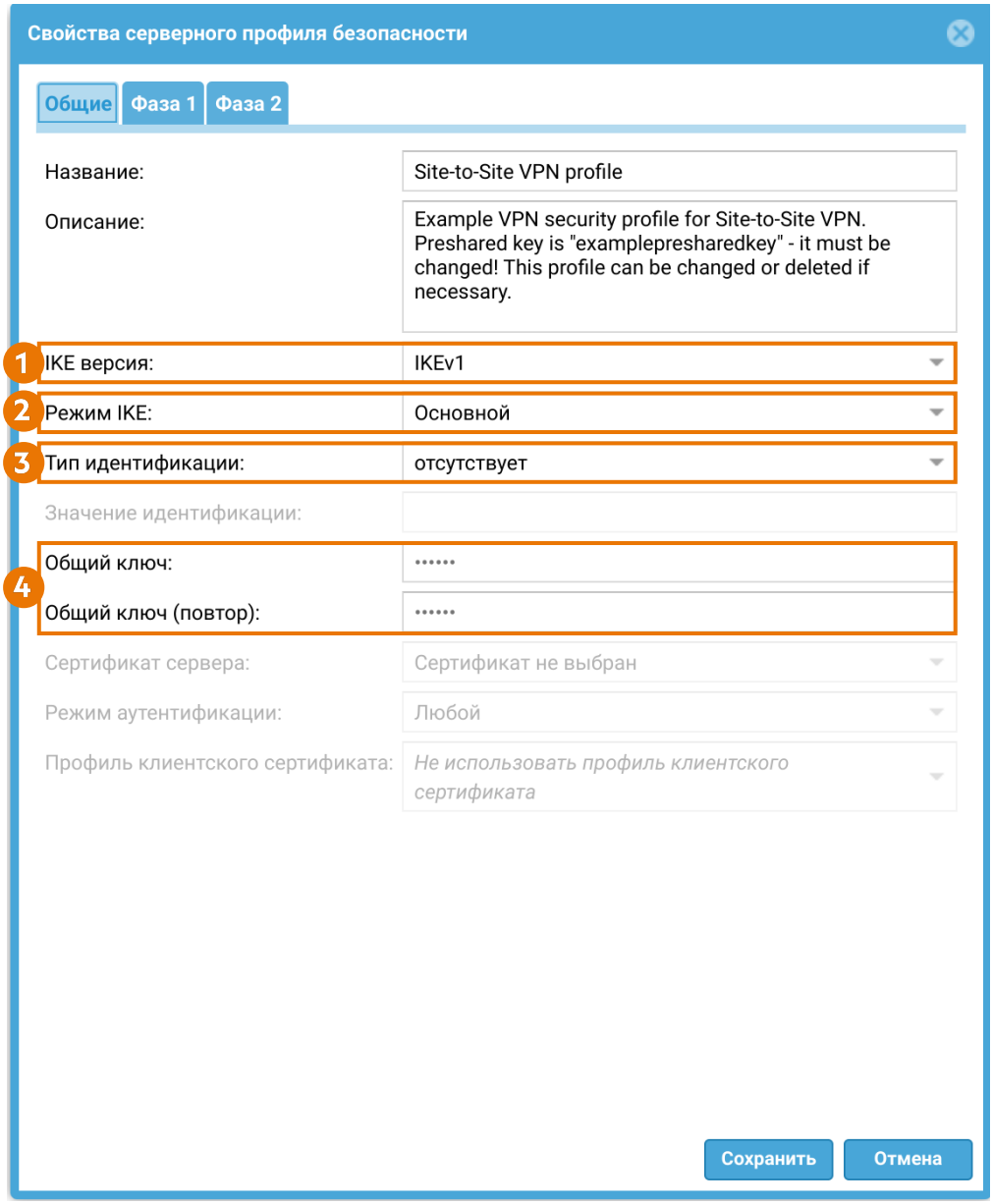
1. Создадим локальную учетную запись, которая будет использоваться для аутентификации узла, выступающего в роли VPN-клиента при установлении L2TP туннеля. В веб-консоли NGFW 1 в разделе **Пользователи и устройства → Пользователи** создадим локальную учетную запись *vpn client 1* (логин: *vpnclnt1)* для 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:



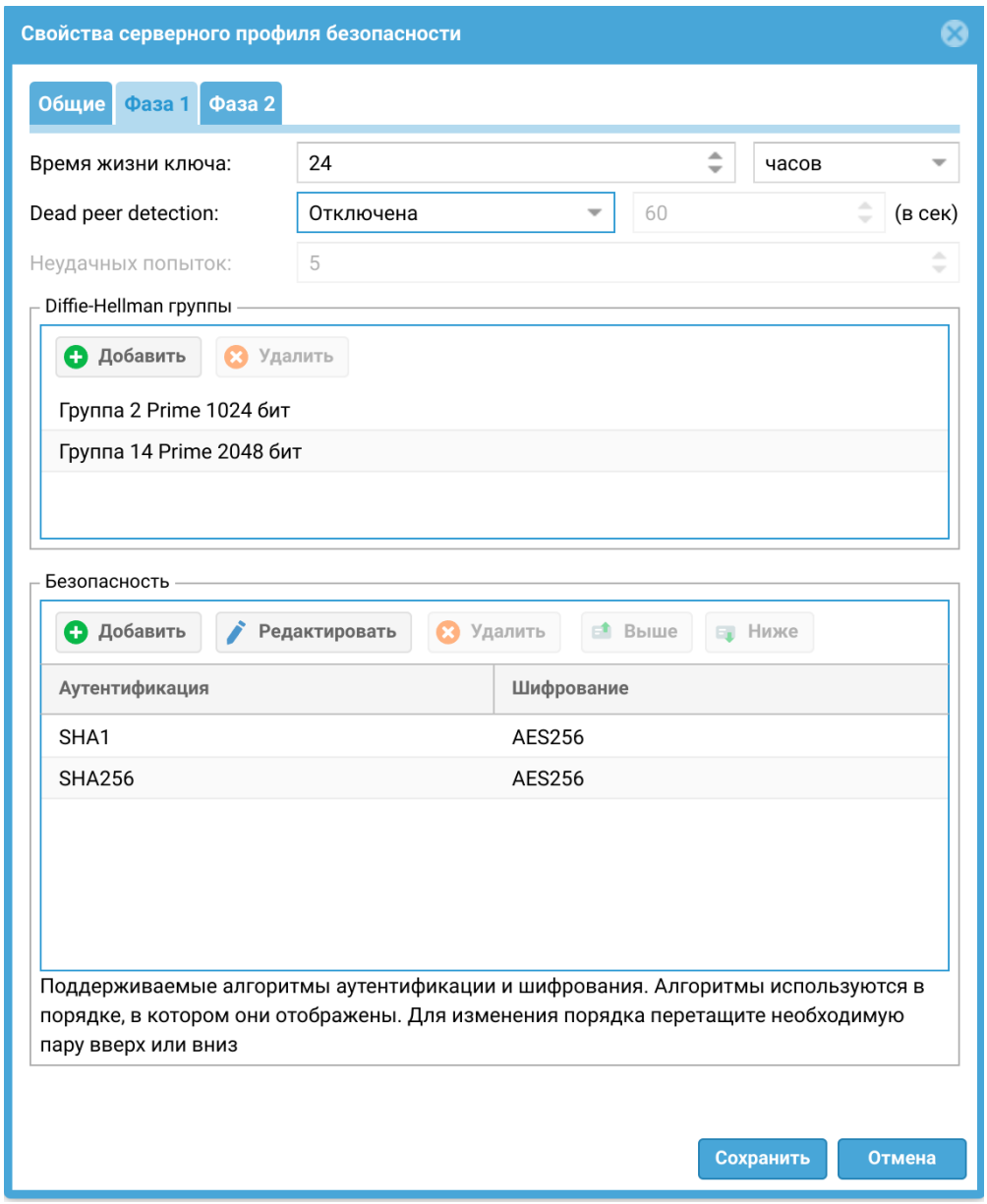
1. **Версия** протокола **IKE** (Internet Key Exchange). В рассматриваемом примере для создания защищенного канала будет использоваться протокол IKEv1.

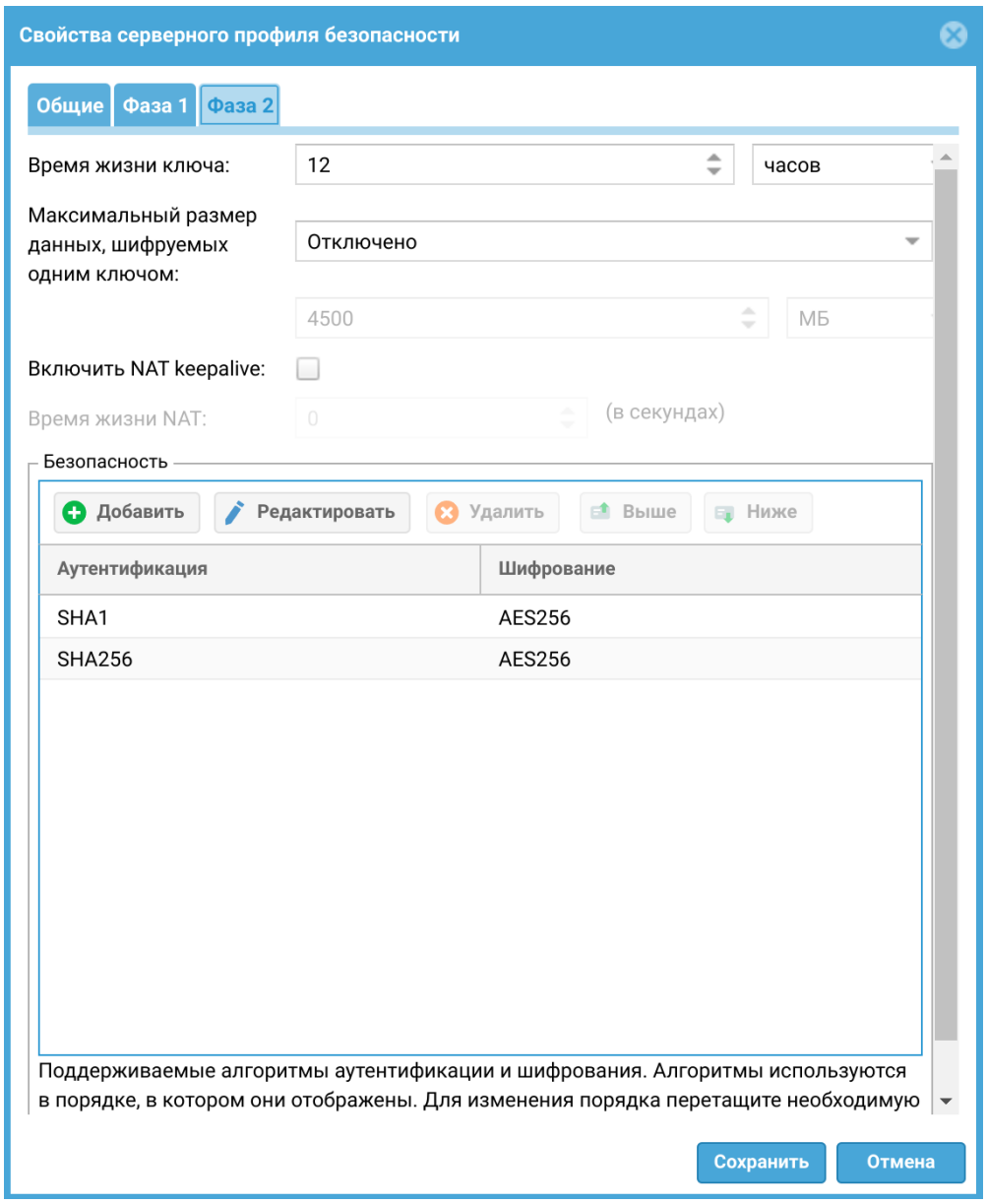
2. **Режим** работы **IKE**. В рассматриваемом примере используется Основной режим работы IKEv1.

3. **Тип идентификации** (параметр IKE local ID). 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 на VPN-сервере и VPN-клиенте для успешного подключения.

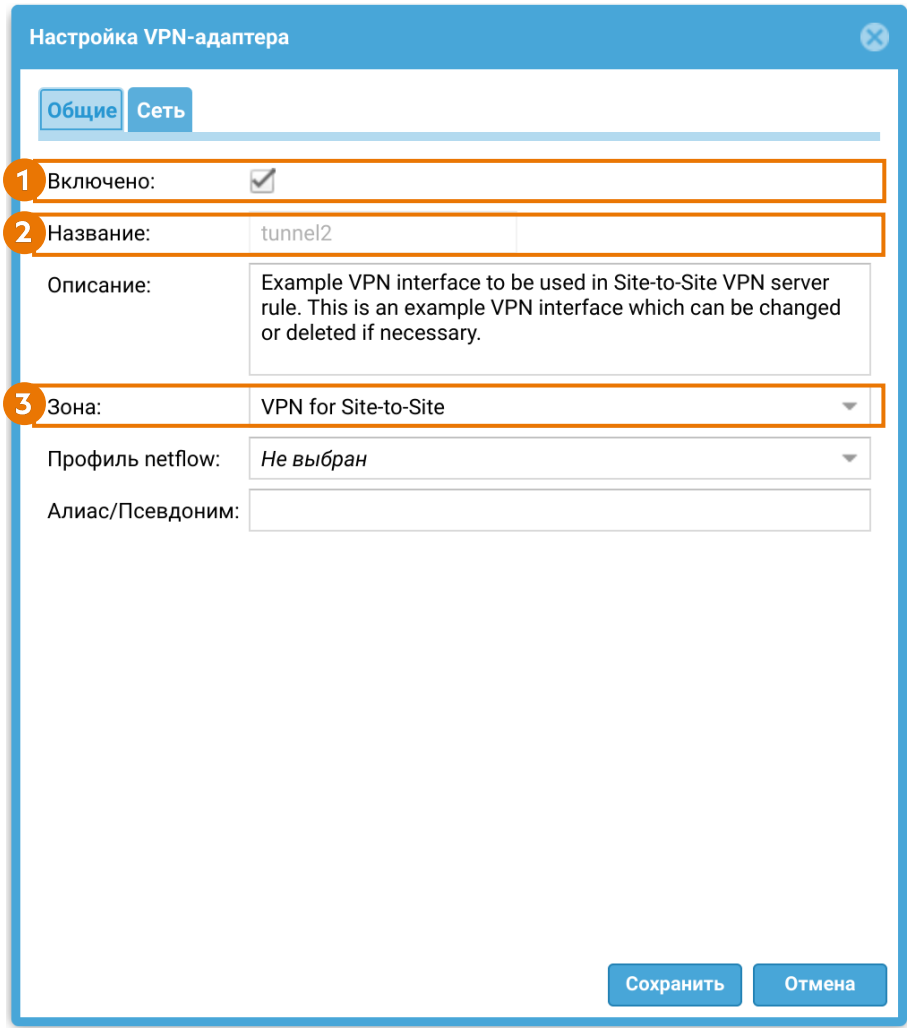
Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:


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
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



Шаг 5. Создать VPN-интерфейс.

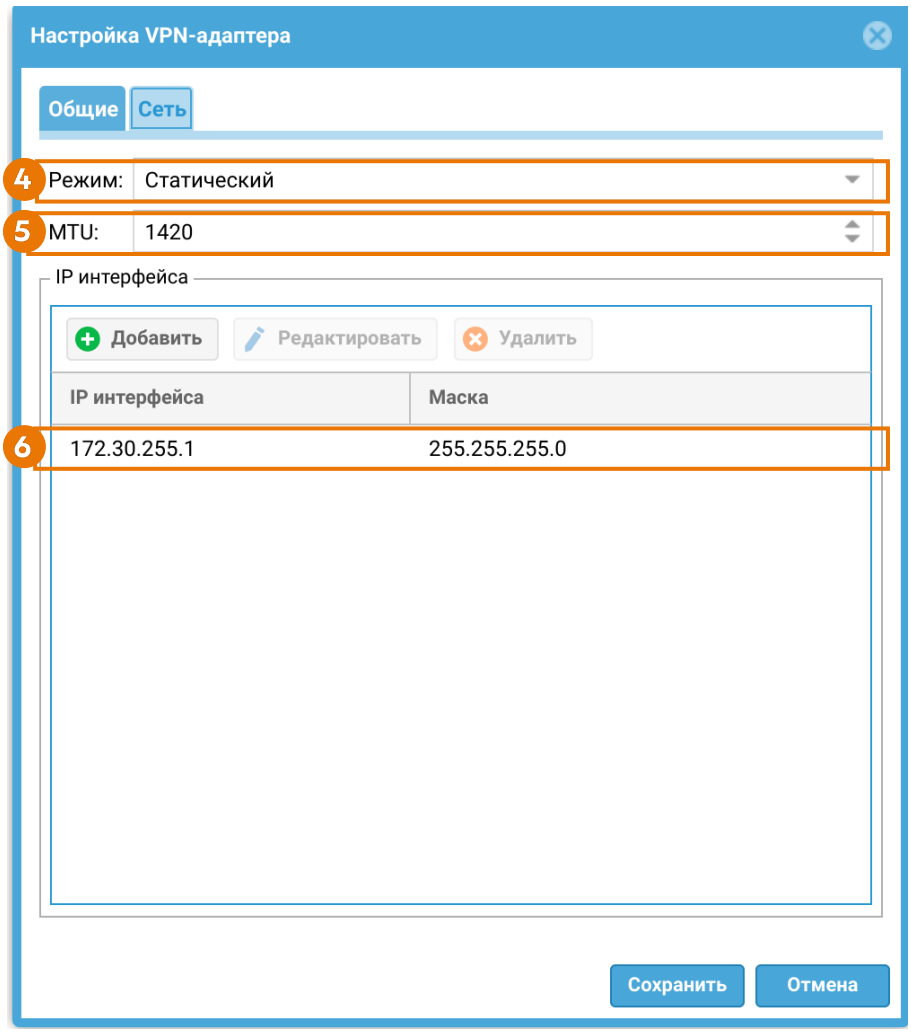
Для примера на узле создан VPN-интерфейс **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера.



1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel2).

3. **Зона**, к которой будет относится 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.



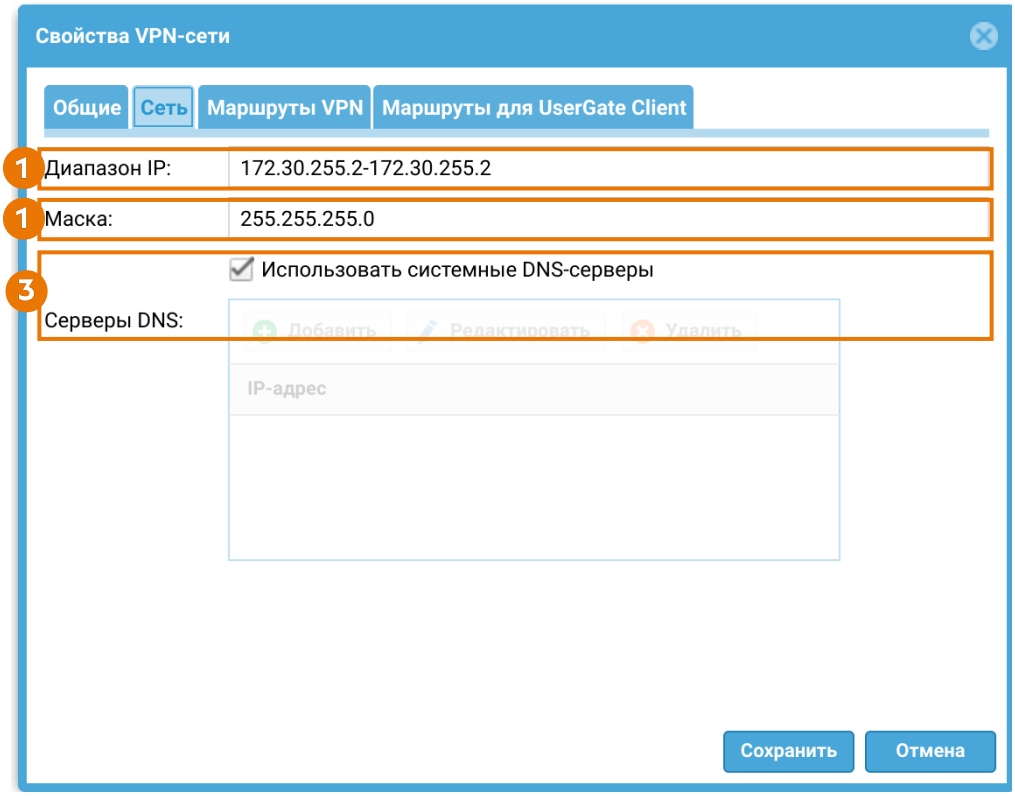
4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес.

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.

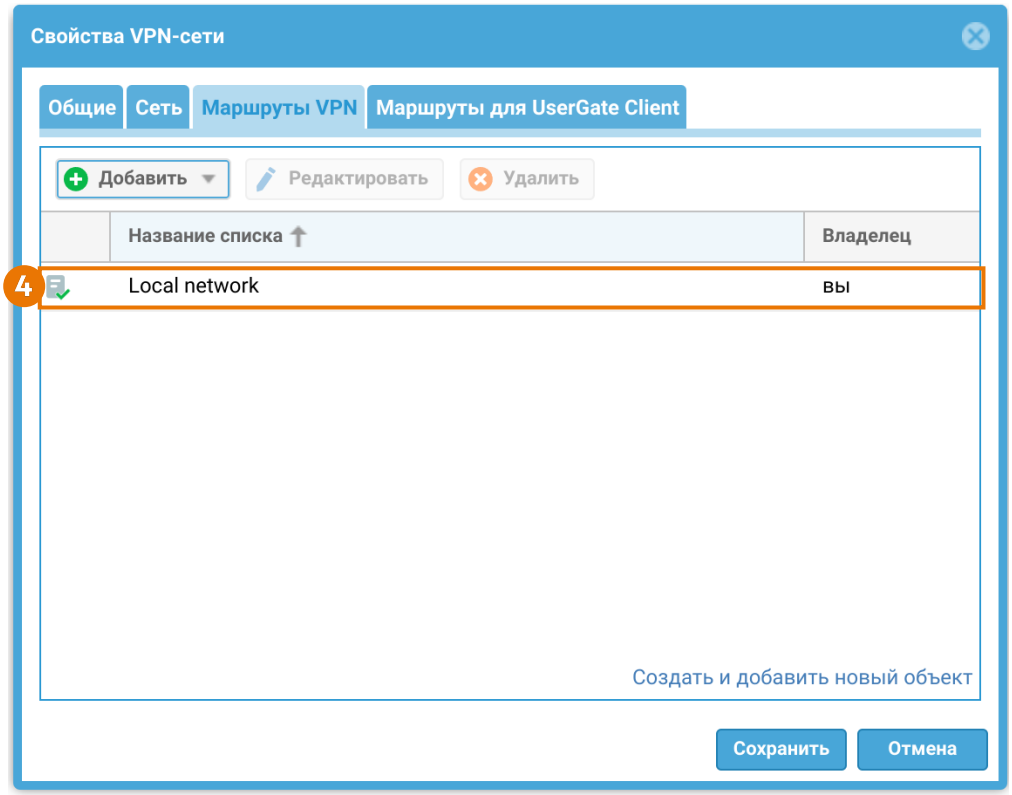
Для примера на узле создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:



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.

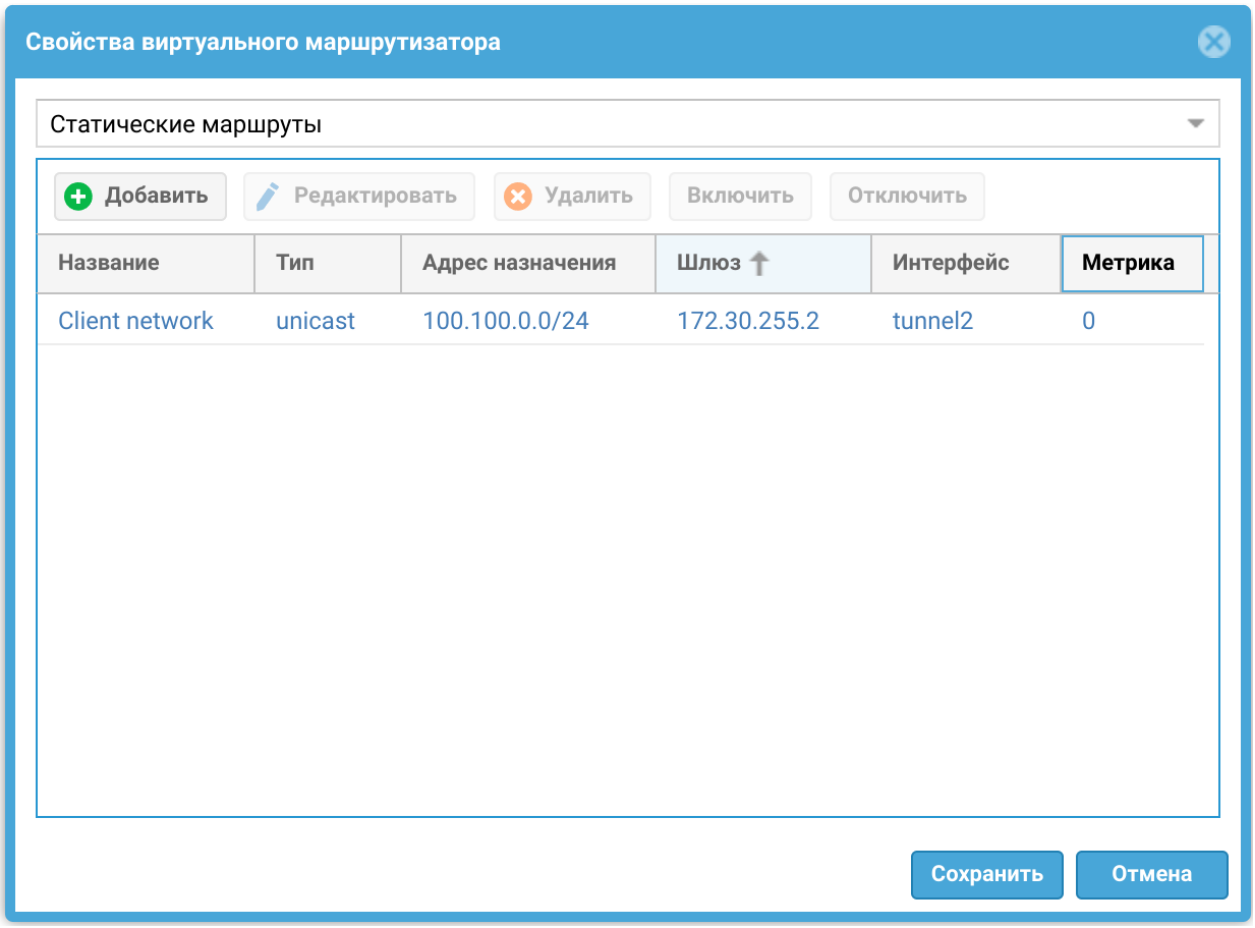
2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

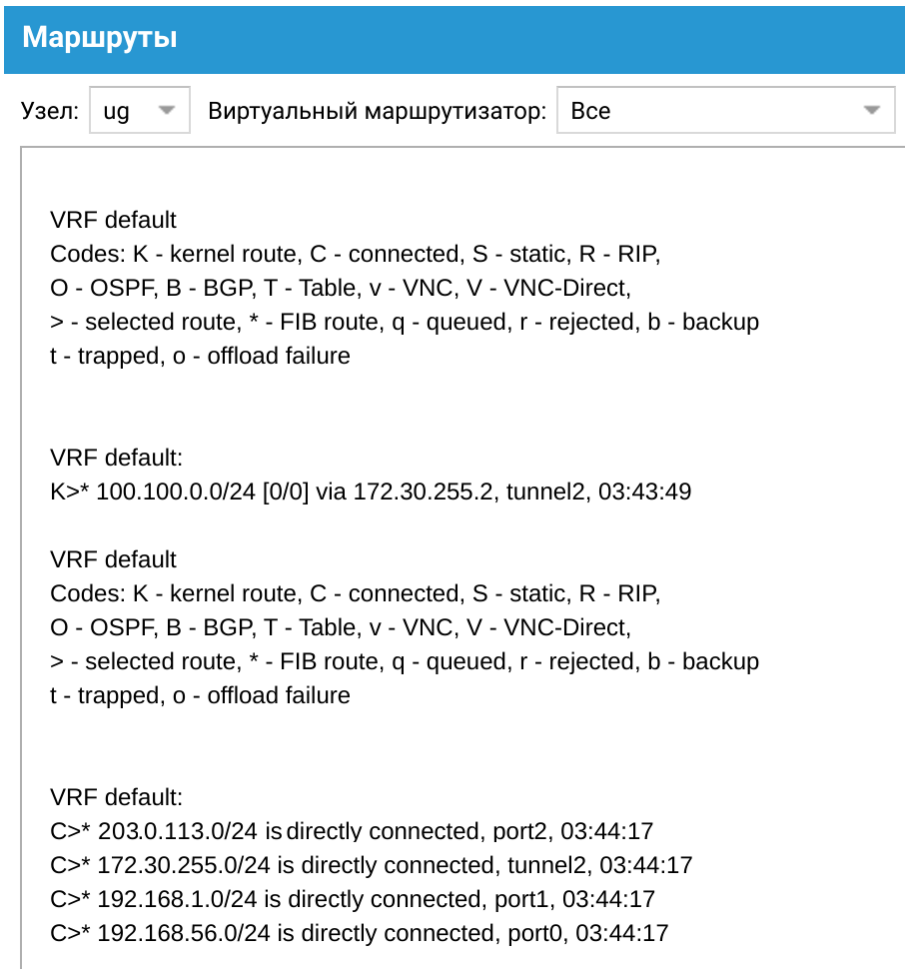


4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

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:

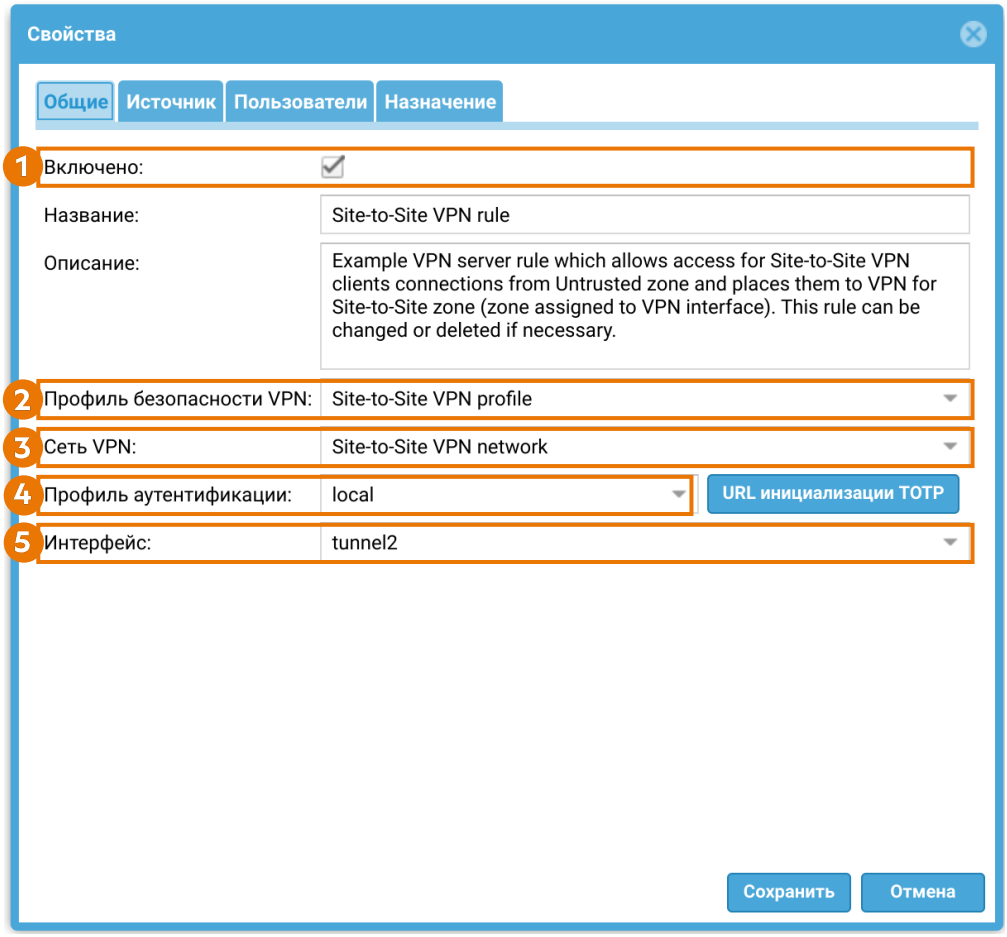


В разделе **Журналы и отчеты → Мониторинг → Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:



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:



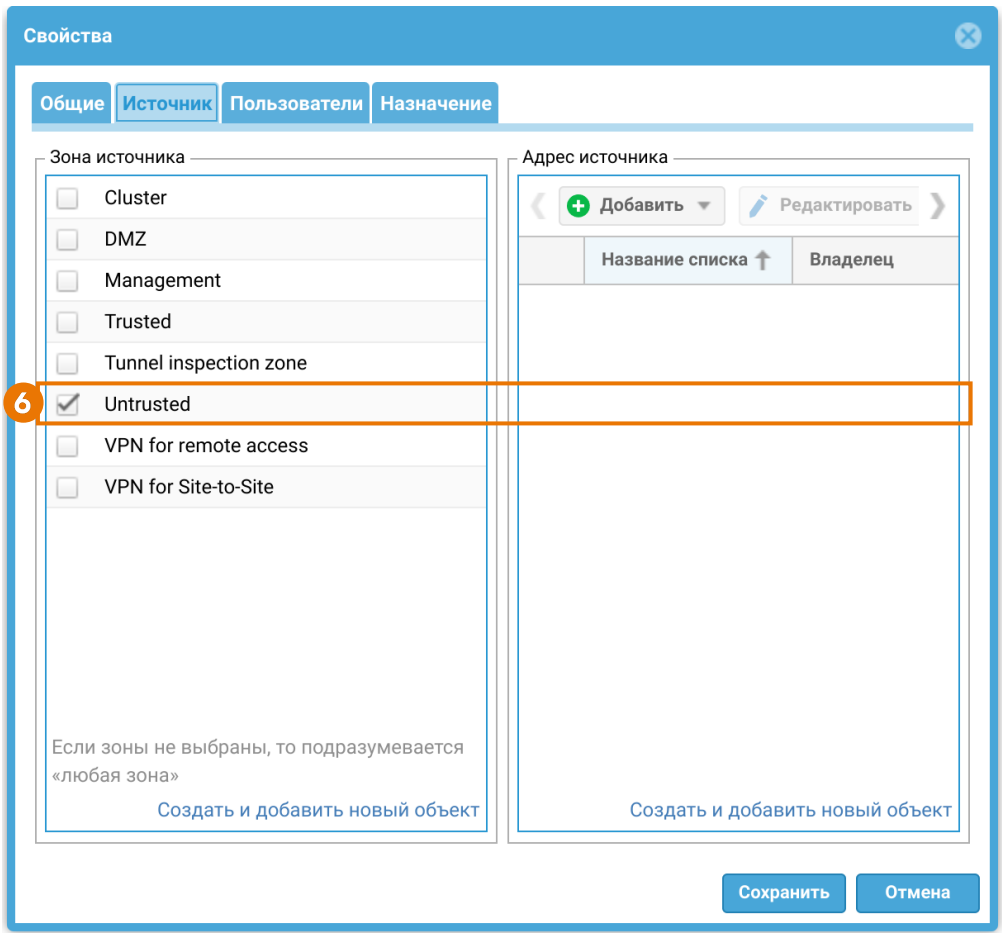
1. **Включено** — включить правило VPN.

2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на Шаге 4 (Site-to-Site VPN profile).

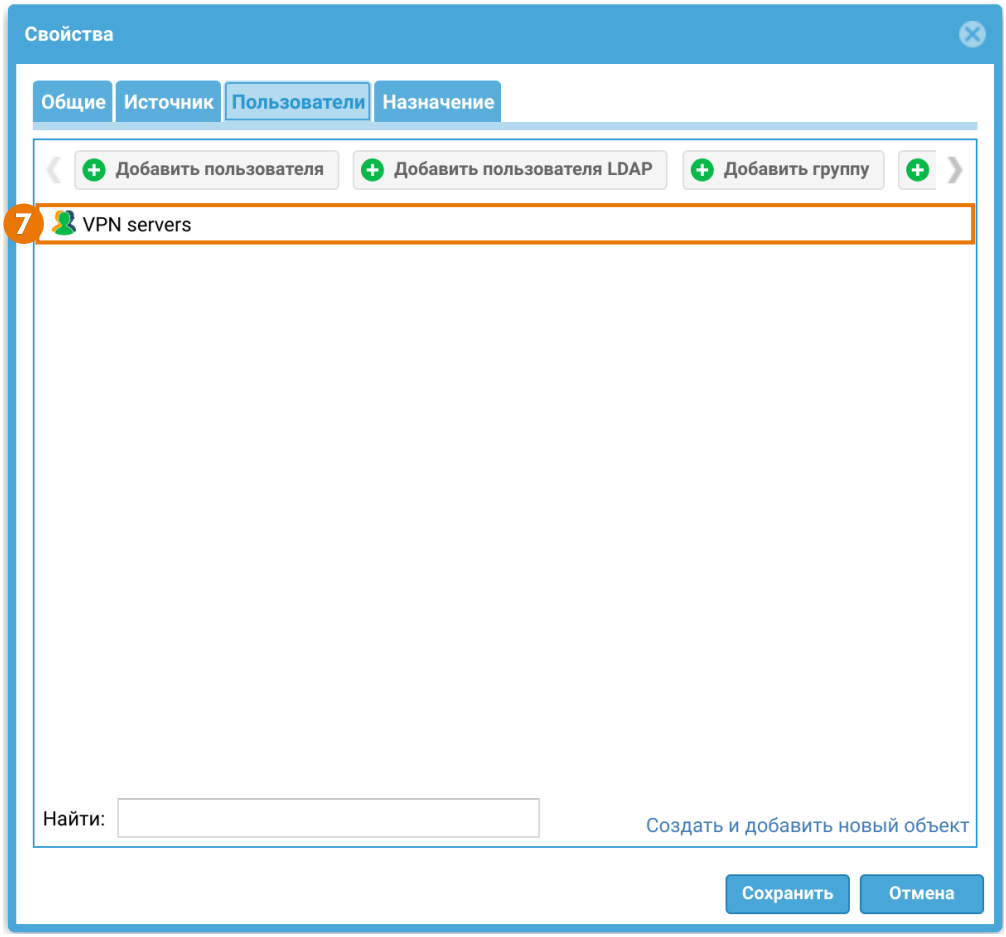
3. **Сеть VPN** — сеть VPN, созданная ранее на Шаге 6 (Site-toSite VPN network).

4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. Шаг 3).

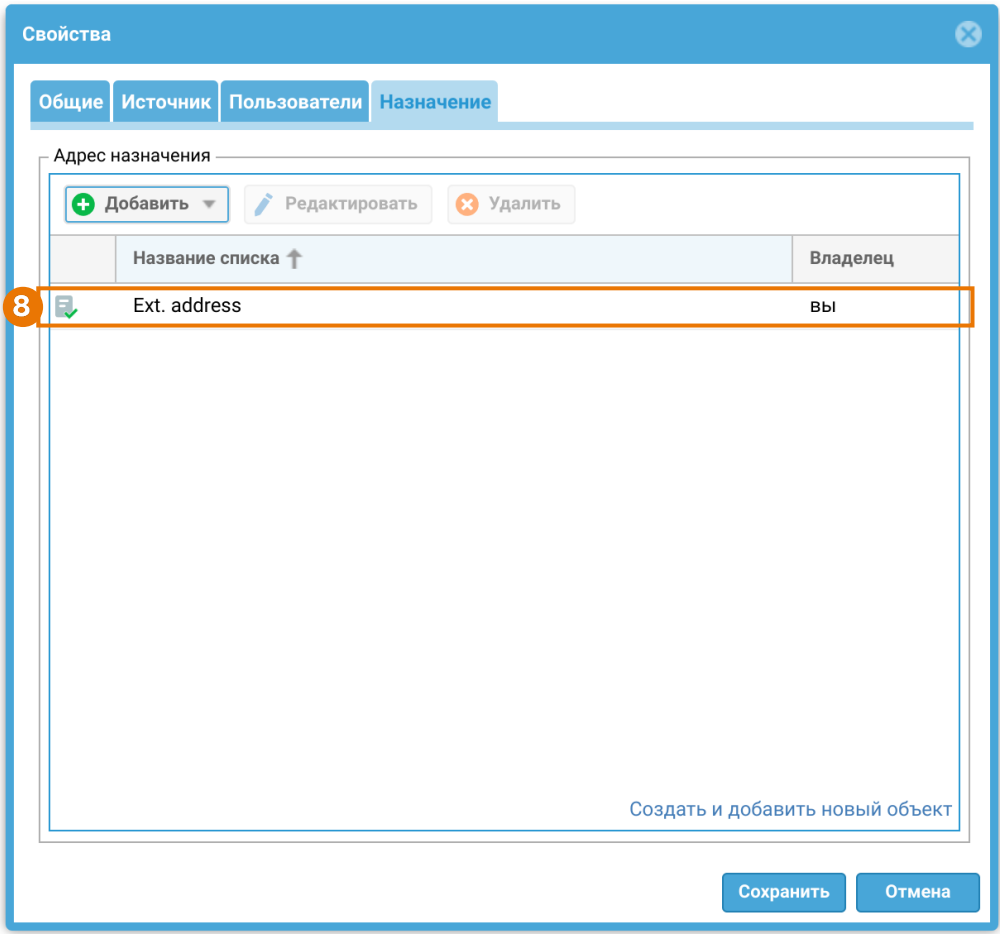
5. **Интерфейс** — созданный ранее на Шаге 5 интерфейс VPN (tunnel2).



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 Шаге 3 учетную запись *vpn client 1*.



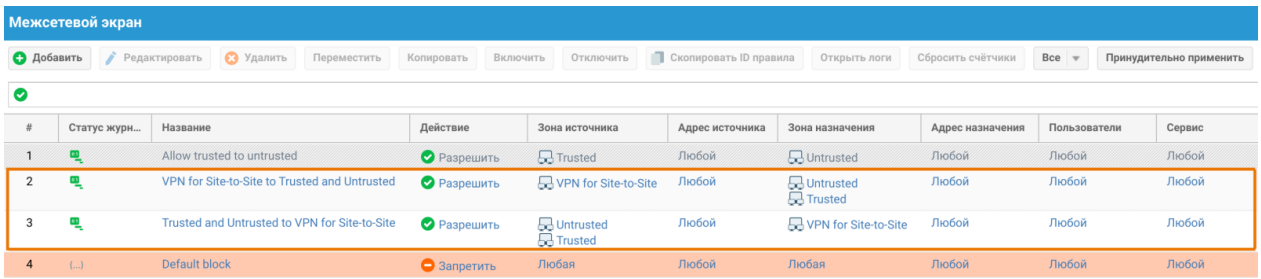
8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1.

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**.



Настройка VPN-клиента

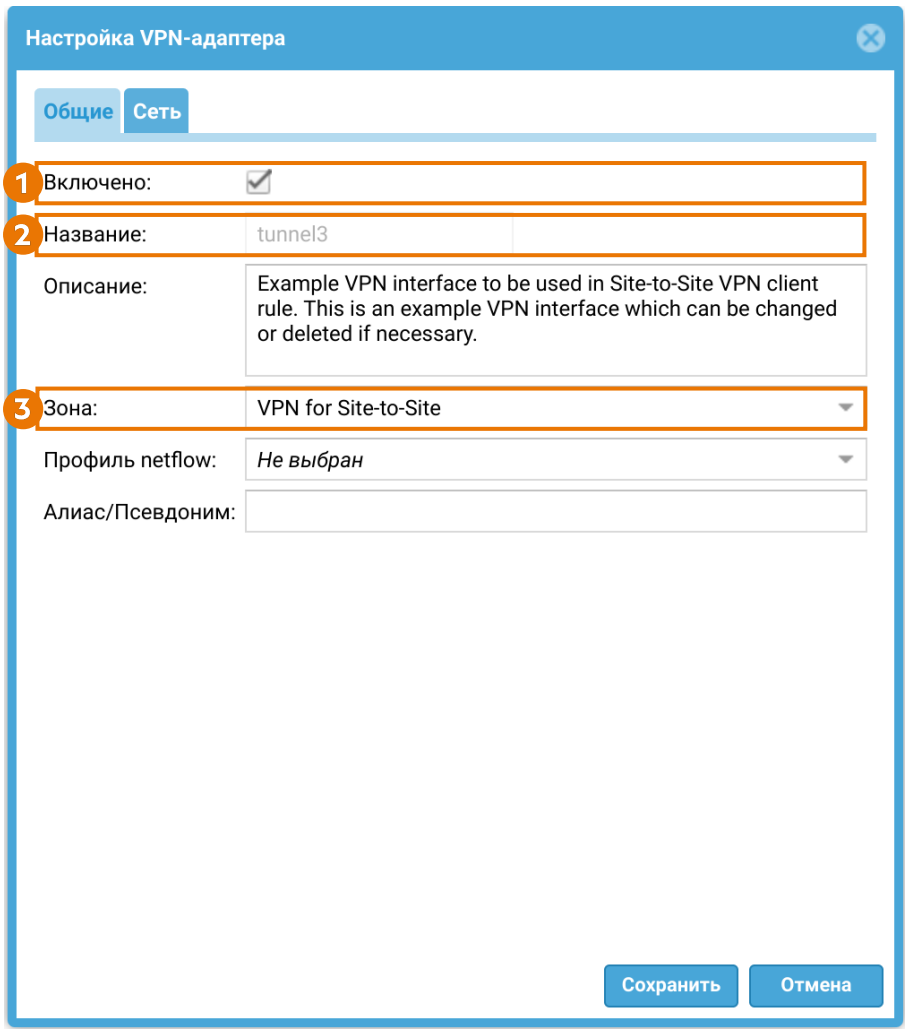
Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

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.

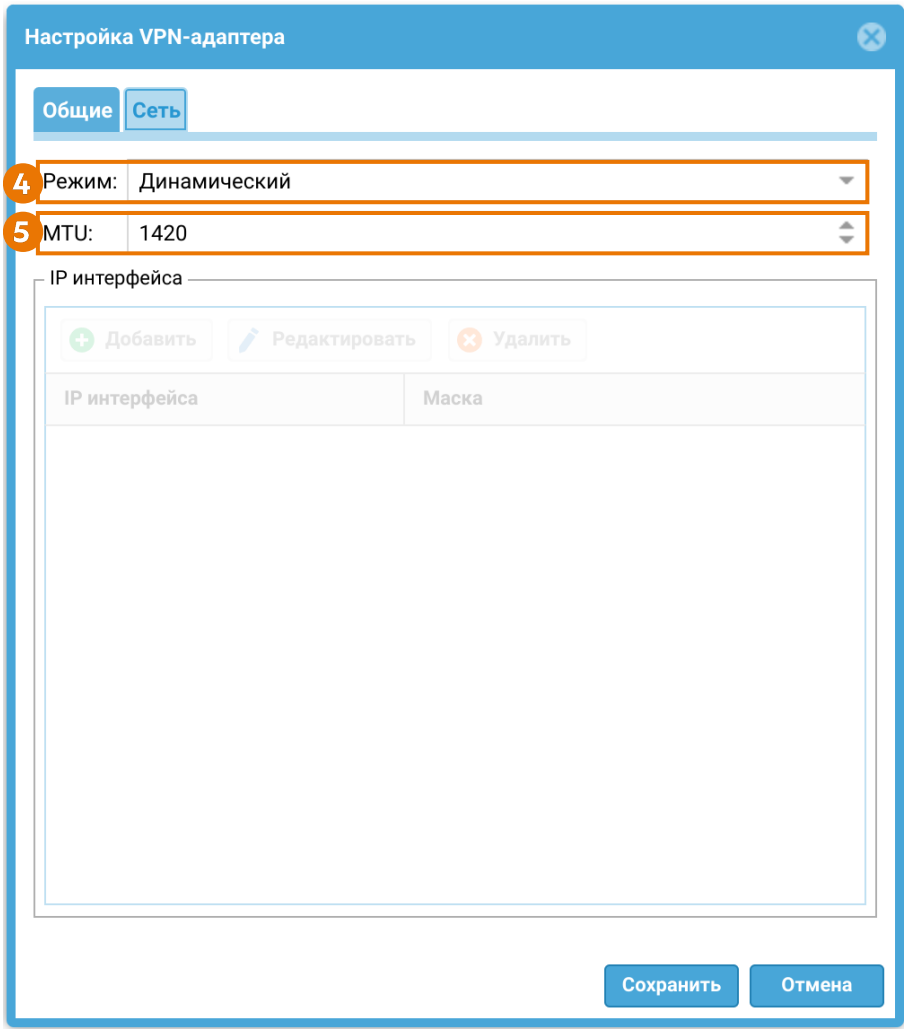
Для примера на узле создан VPN-интерфейс **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера создания защищенного VPN-соединения:



1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel3).

3. **Зона**, к которой будет относится данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на Шаге 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.

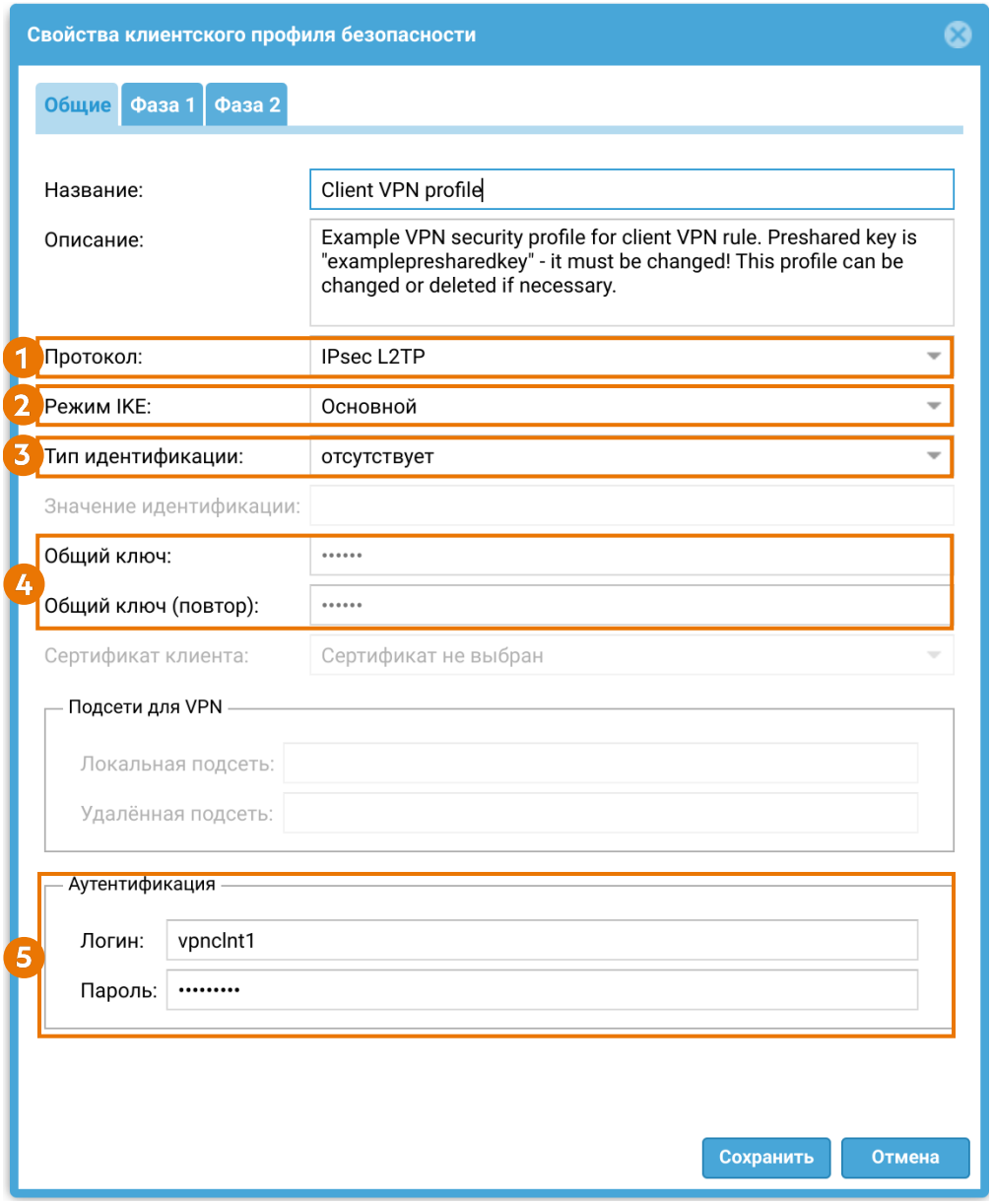
Шаг 3. Контроль доступа к ресурсам.

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:



1. **Протокол**. В рассматриваемом примере для создания защищенного канала будет использоваться **IPsec L2TP**.

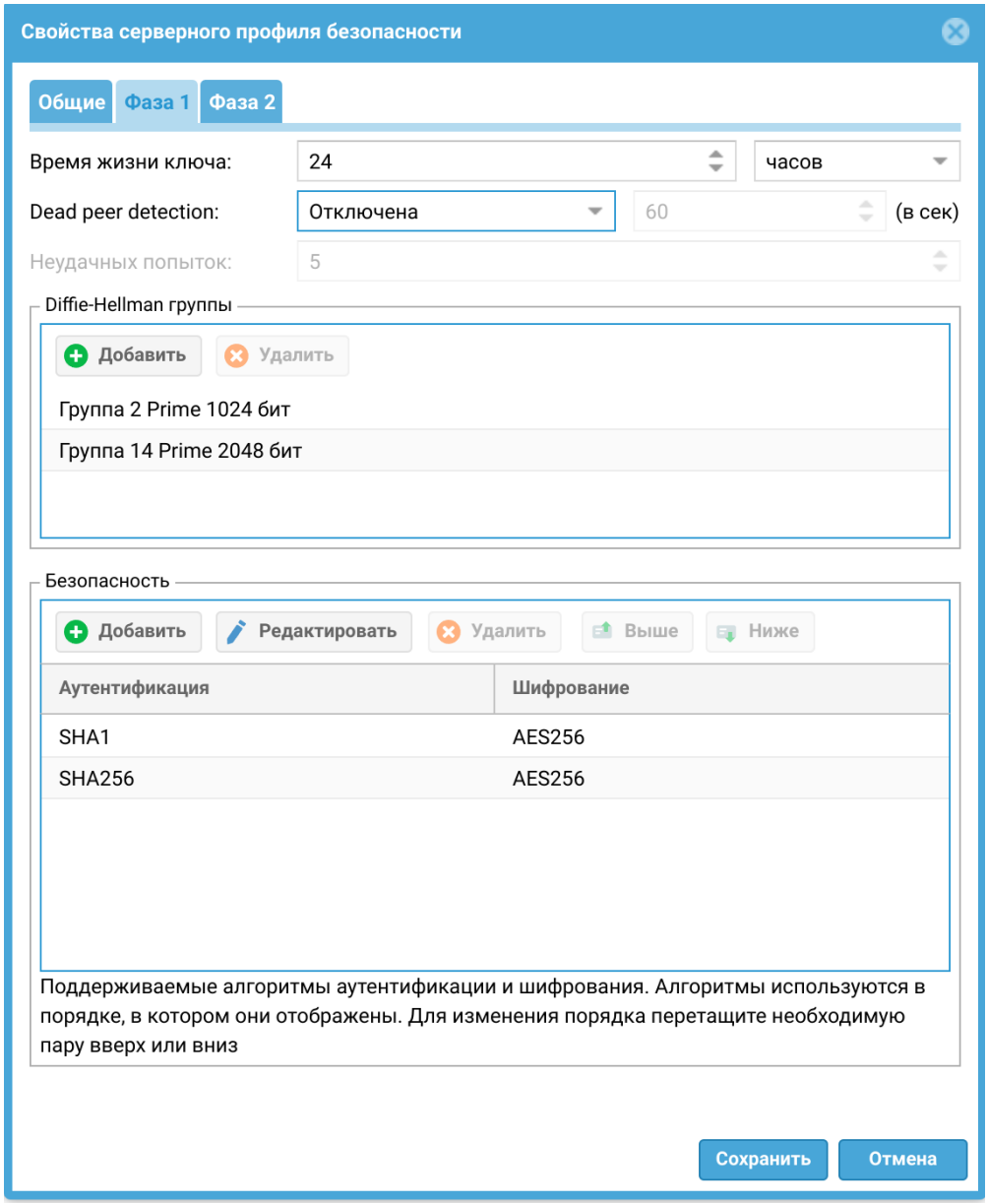
2. **Режим** работы **IKE**. В рассматриваемом примере используется **Основной** режим работы IKEv1.

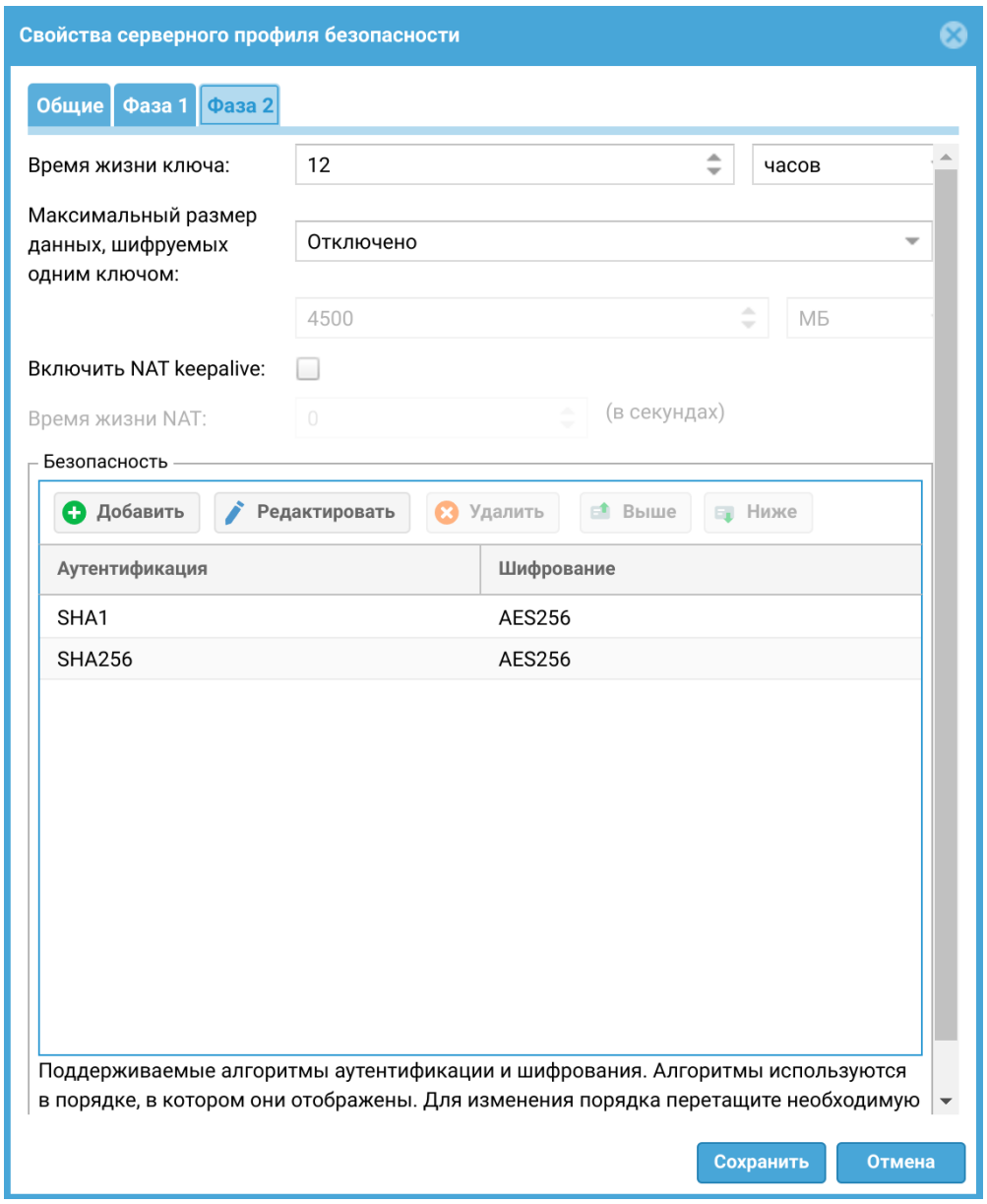
3. Тип идентификации (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

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 (vpnclnt1).

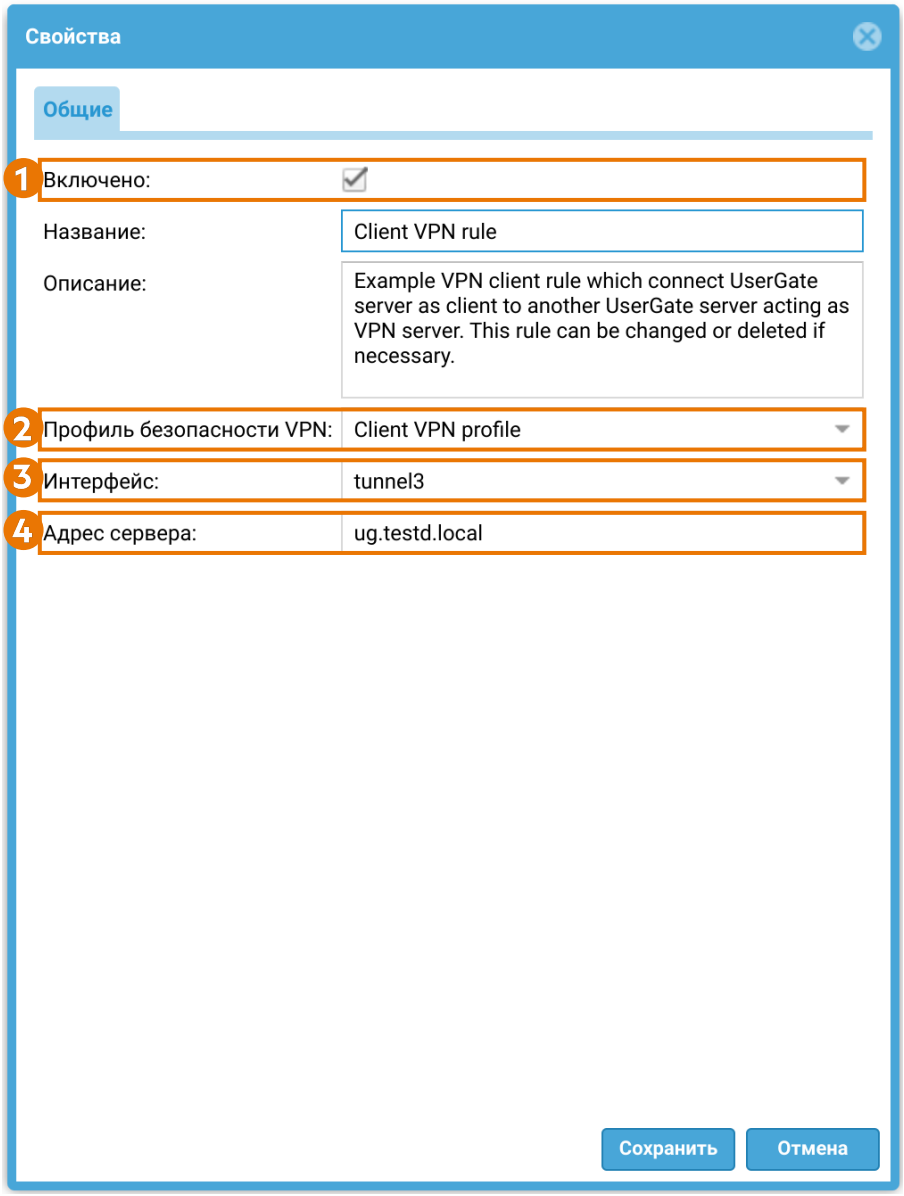
Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:





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:



1. **Включено** — включить правило.

2. **Профиль безопасности VPN** — созданный на Шаге 4 клиентский профиль безопасности VPN.

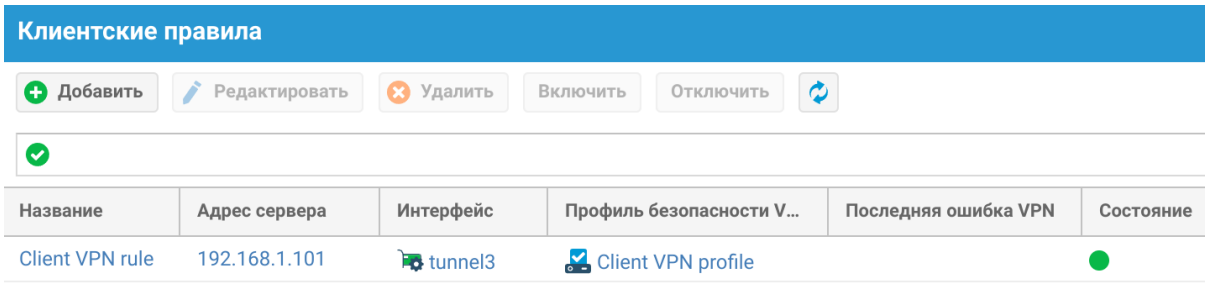
3. **Интерфейс** — созданный на Шаге 2 VPN-интерфейс.

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.

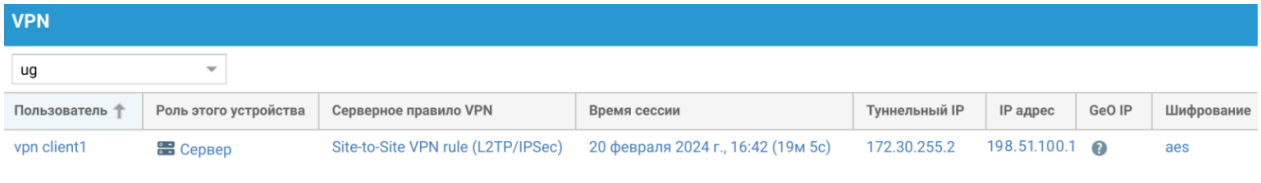
Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узле NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля:

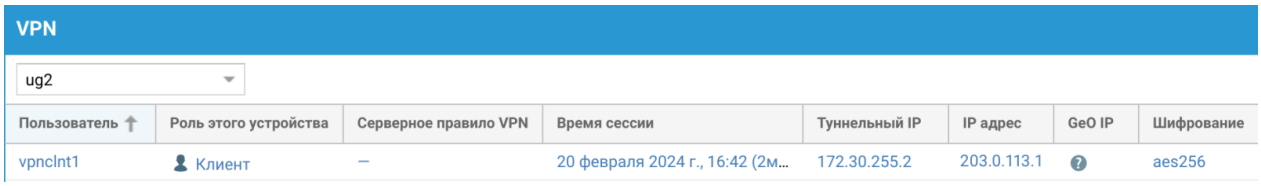


На узлах NGFW 1 и NGFW 2 в разделе **Журналы и отчеты → Мониторинг → VPN** появится информация о новом туннеле.

На NGFW 1:



На NGFW 2:



В разделе **Журналы и отчеты → 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 172.30.255.1, 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>* 198.51.100.0.0/24 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 172.30.255.2 TTL 30 Интерфейс 172.30.255.1 (tunnel2)

Счётчик 6 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 172.30.255.1 TTL 30 Интерфейс 172.30.255.2 (tunnel3)

Счётчик 6 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
```

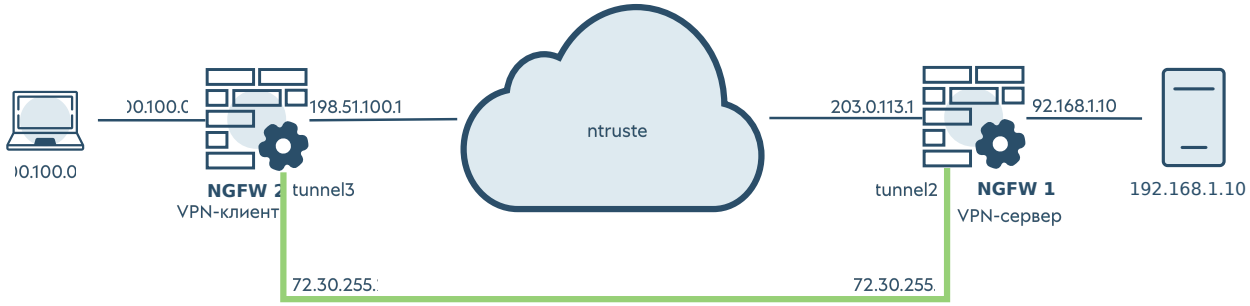
Хосты в сетях обоих офисов доступны друг для друга:

```
        :~$ 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 ***vpnclnt1***, входящего в группу **VPN servers**:

```
Admin@ug# create users user name "vpn client 1" login vpnclnt1 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-lifesize-enabled    : off
    key-lifesize            : 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-lifesize-enabled    : off
    key-lifesize            : 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 vpnclnt1
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
```

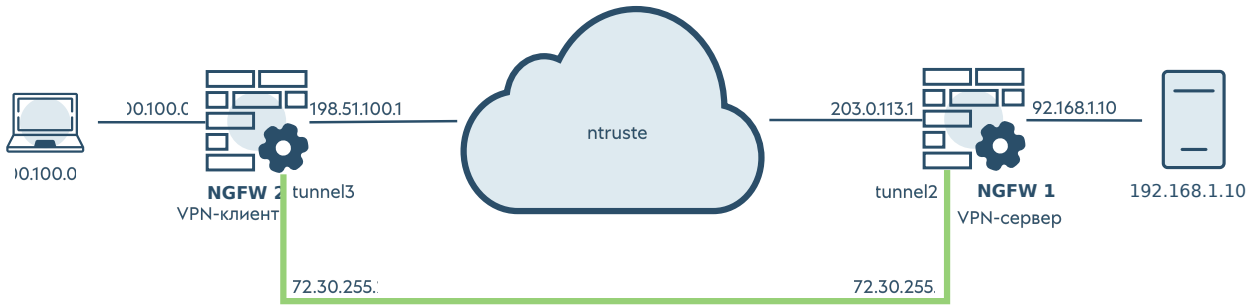
```
Admin@ug> ping host 172.30.255.2

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

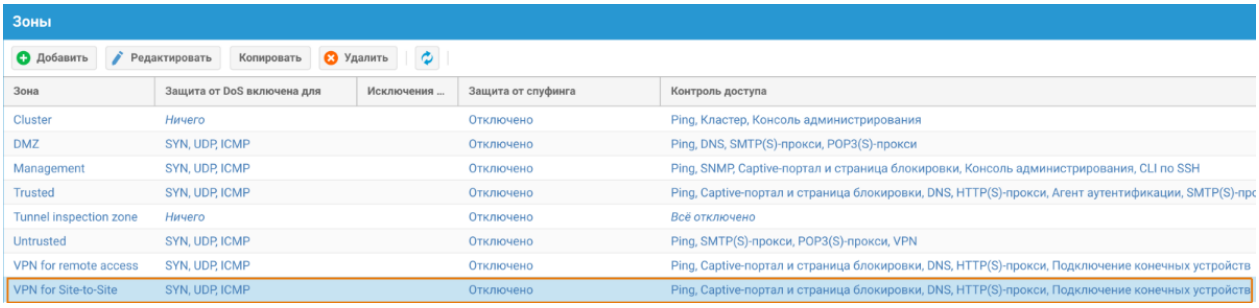
Для настройки узла **NGFW 1** в качестве VPN-сервера необходимо выполнить следующие шаги:

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 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.

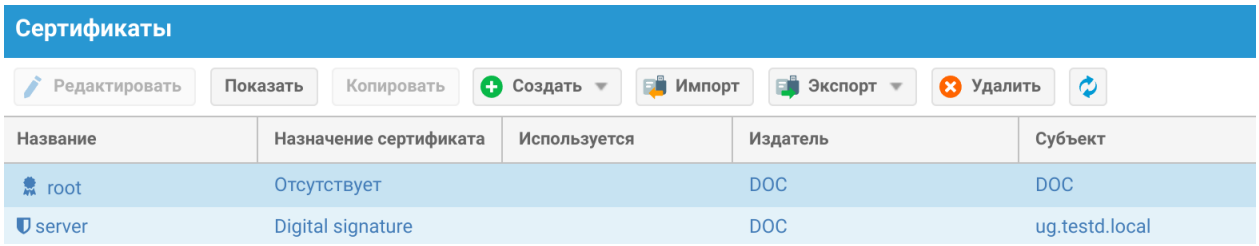
В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье Настройка зон.



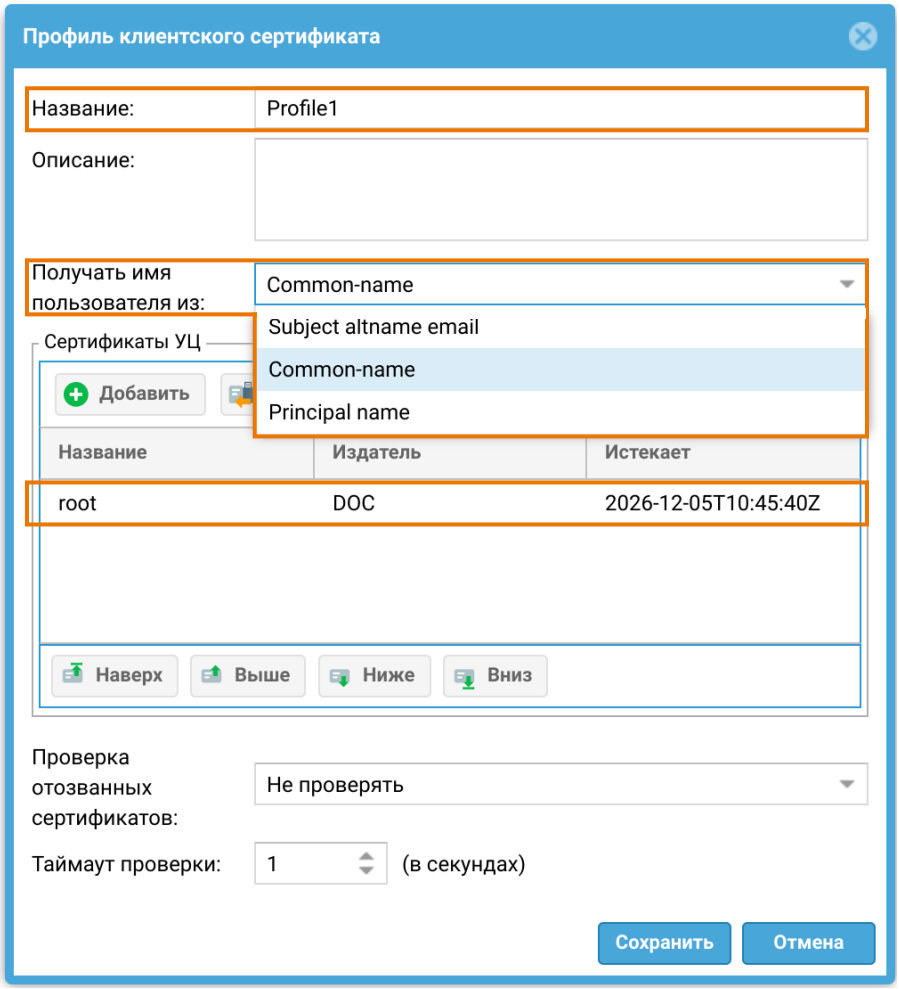
Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в Приложении. Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

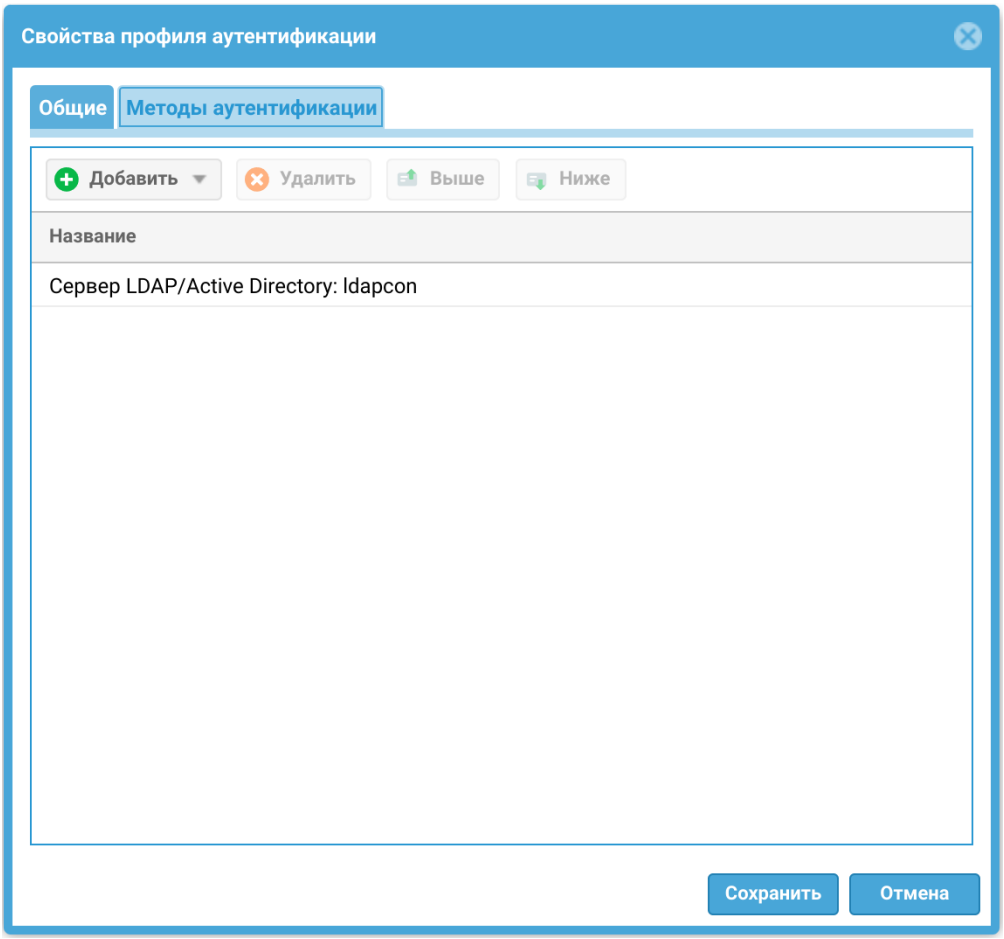
В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать.** В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

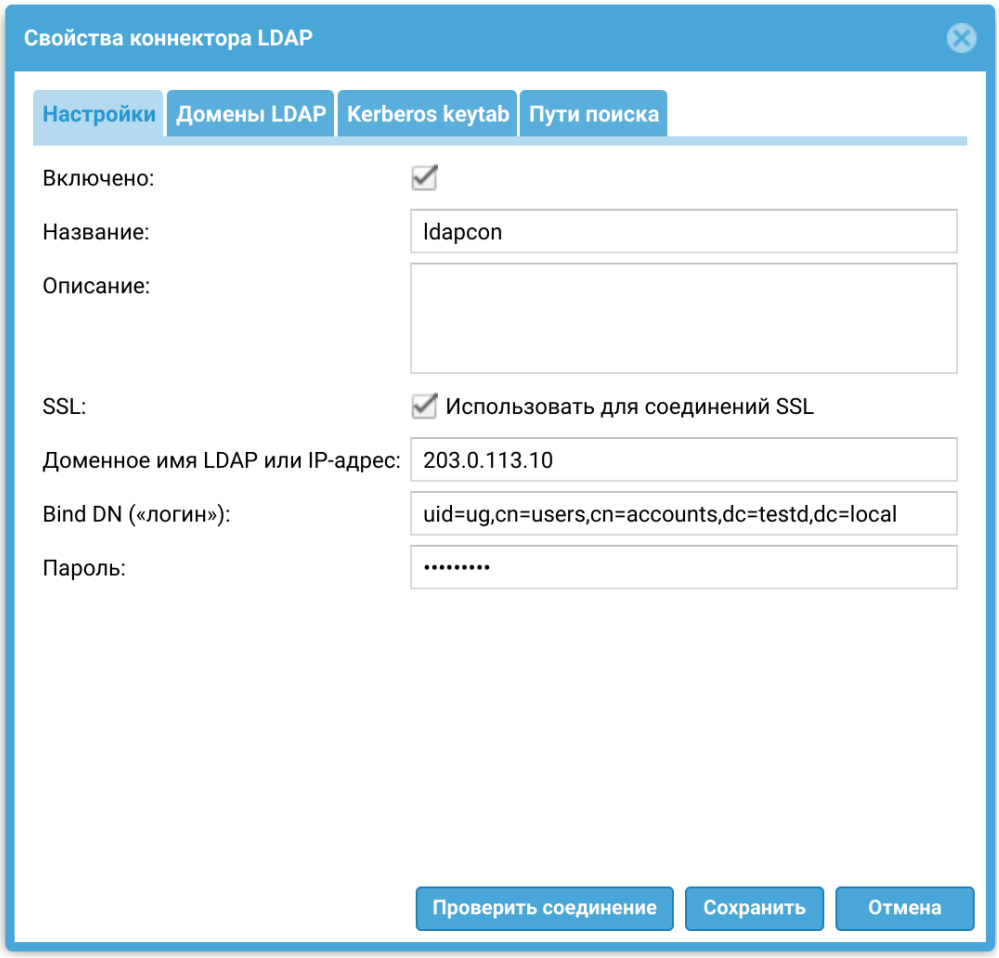


Создадим профиль клиентских сертификатов в веб-консоли администратора NGFW 1, исполняющего роль VPN-сервера. Для этого необходимо перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя:



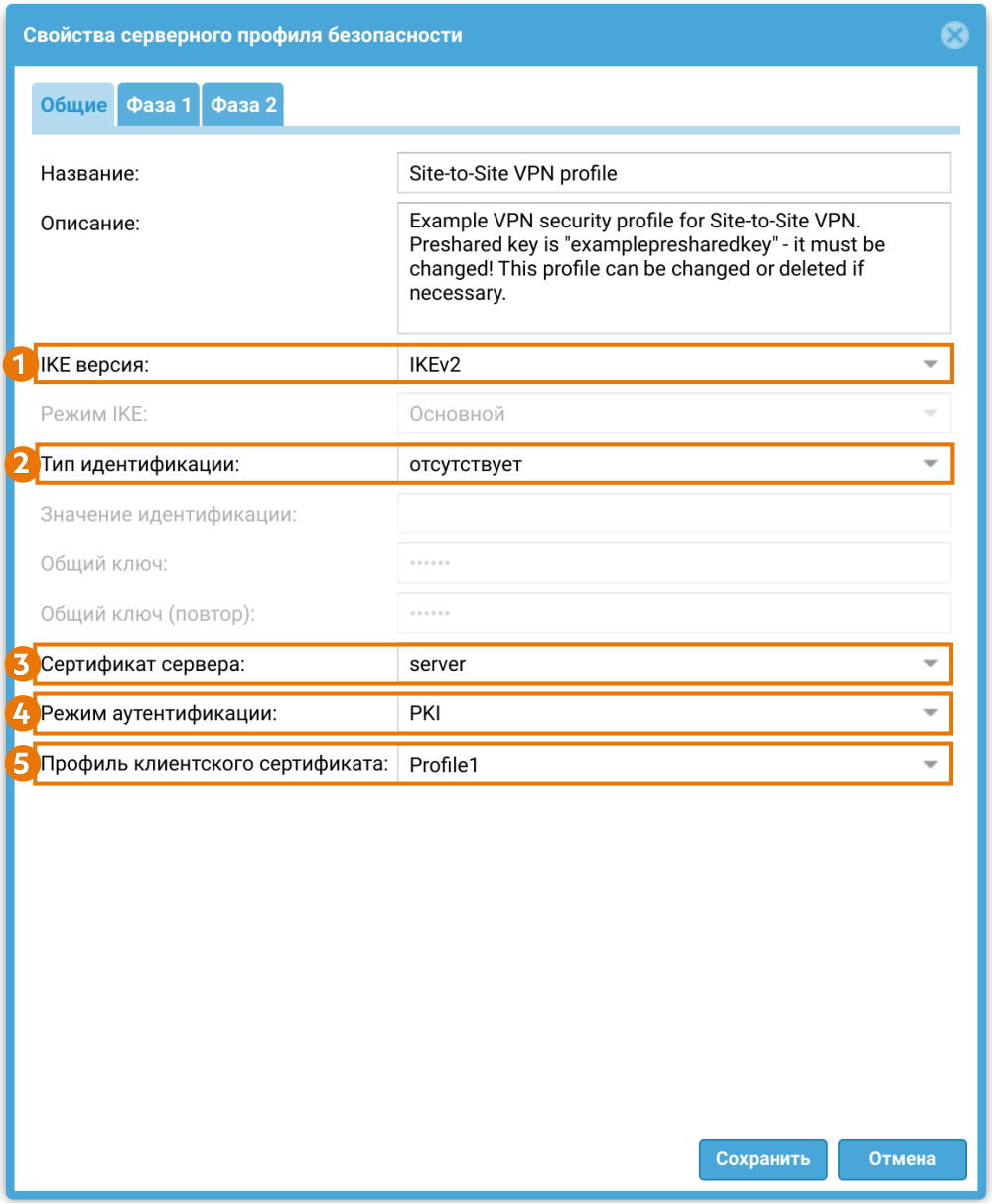
2. Создадим профиль аутентификации для VPN пользователей. Подробно о профилях аутентификации смотрите в разделе данного руководства Профили аутентификации. Для данного примера был создан профиль аутентификации в домене testd.local через LDAP-коннектор:


Свойства профиля аутентификации
Общие
Методы аутентификации
Добавить
Удалить
Выше
Ниже
Название
Сервер LDAP/Active Directory: ldapcon
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:



1. **Версия** протокола **IKE** (Internet Key Exchange). В данном примере для создания защищенного канала будет использоваться протокол IKEv2.

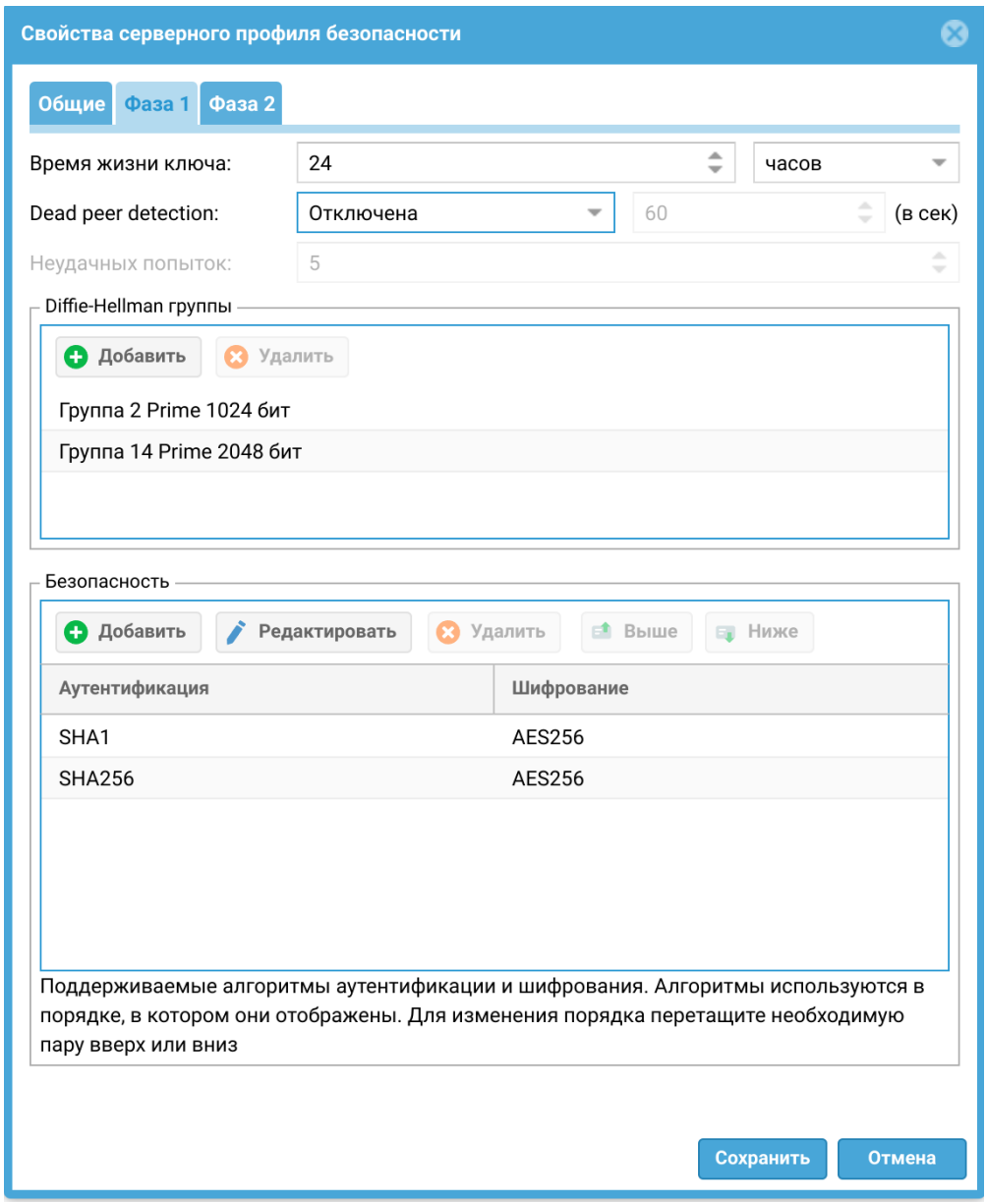
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

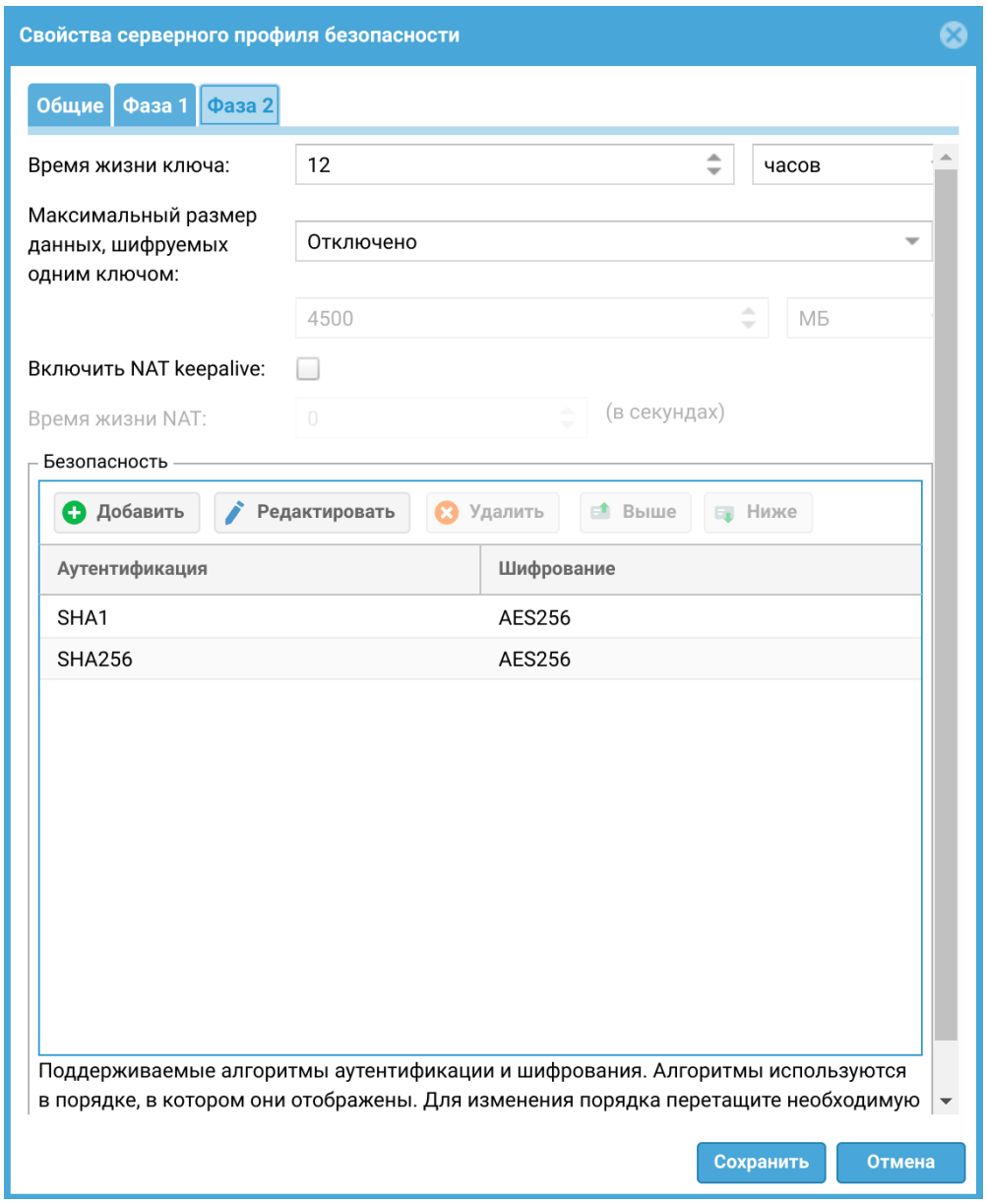
3. Указать **сертификат сервера**, импортированный ранее на Шаге 3.

4. В качестве **режима аутентификации** выберем PKI.

5. Выберем профиль клиентского сертификата, созданный ранее на Шаге 3.

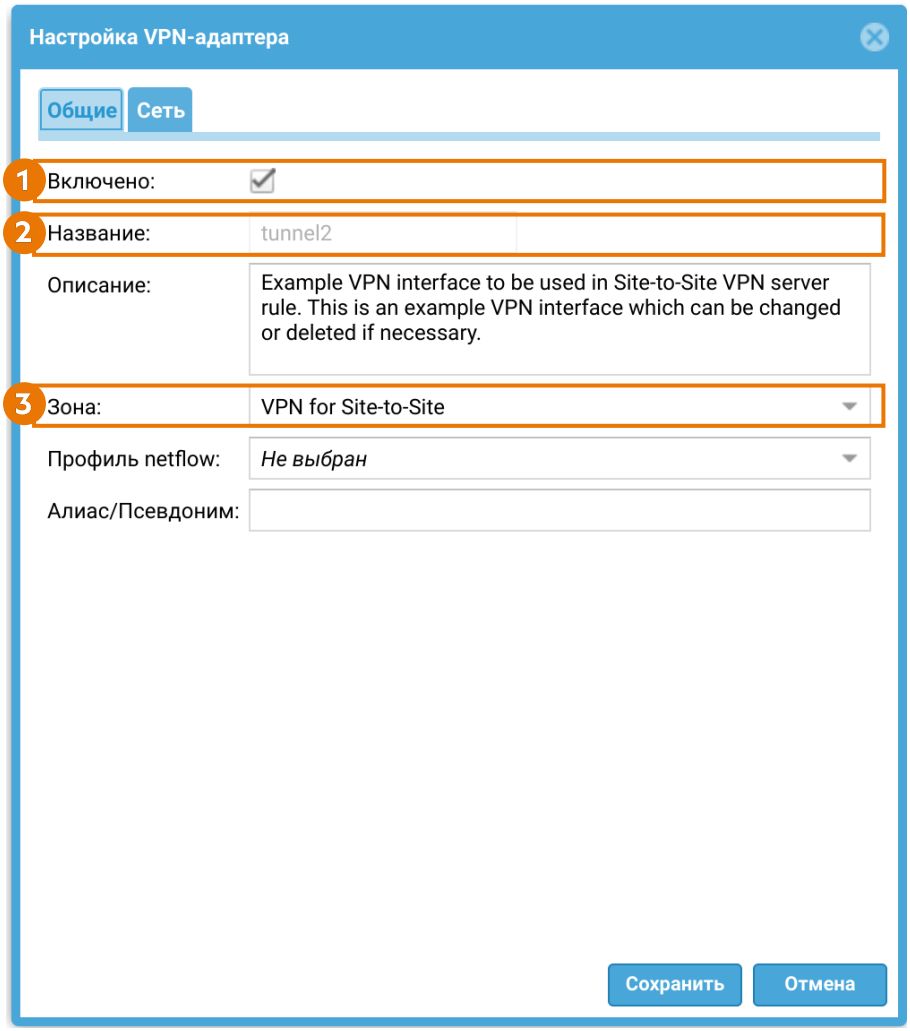
Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:


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



Шаг 5. Создать VPN-интерфейс.

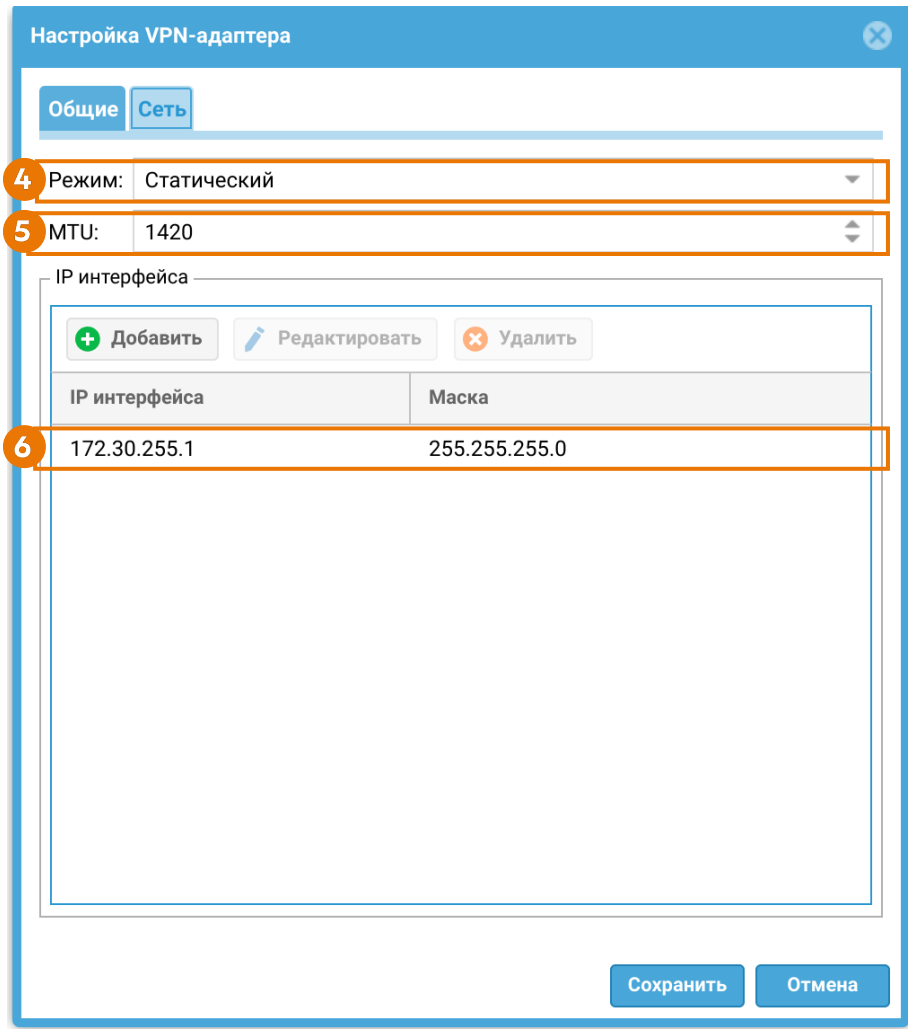
В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:



1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel2).

3. **Зона**, к которой будет относится 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.



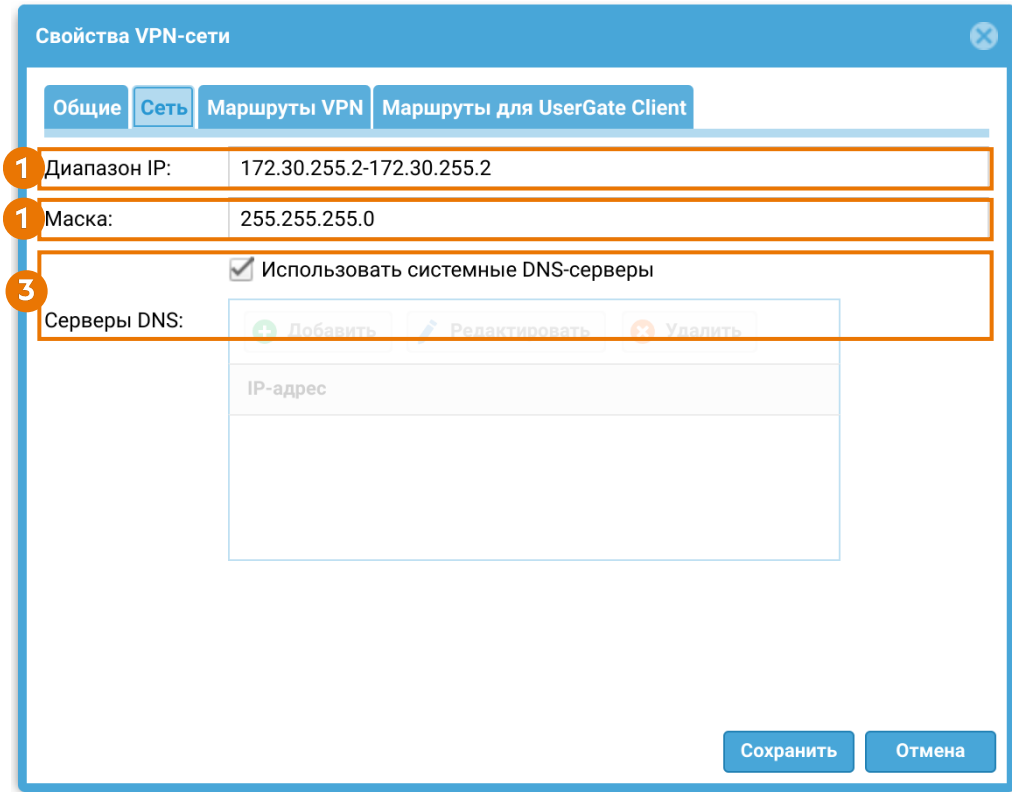
4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.255.1, который задается в поле **6**.

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.

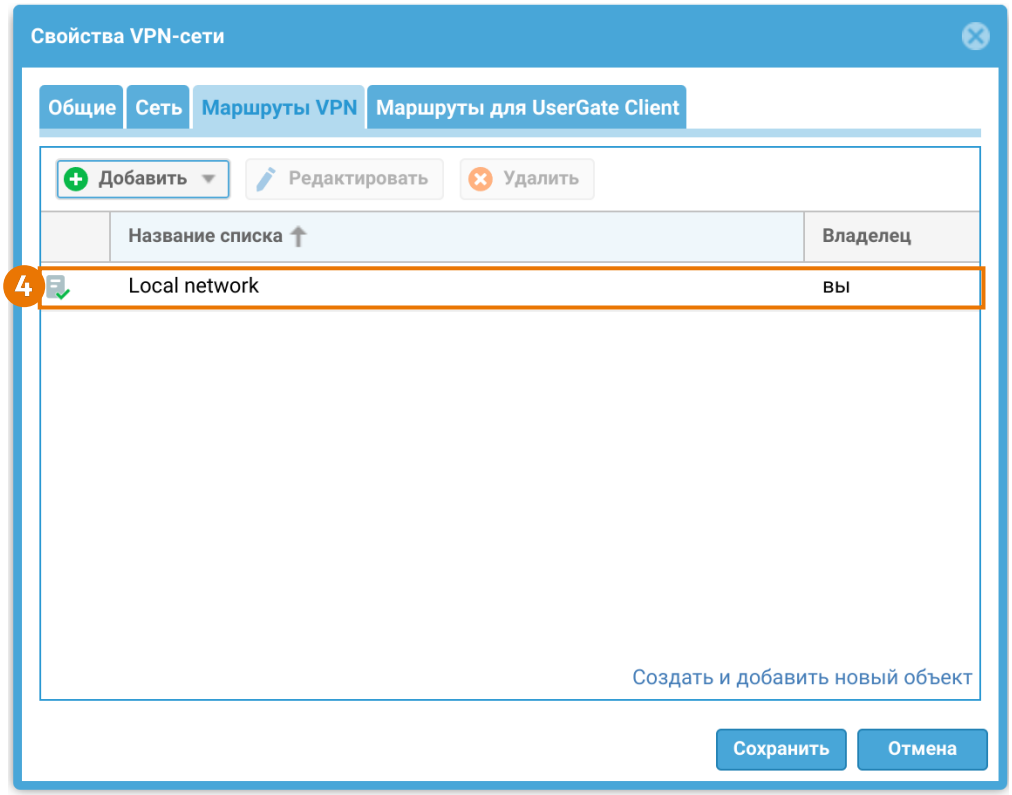
В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Site-to-Site VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:



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.

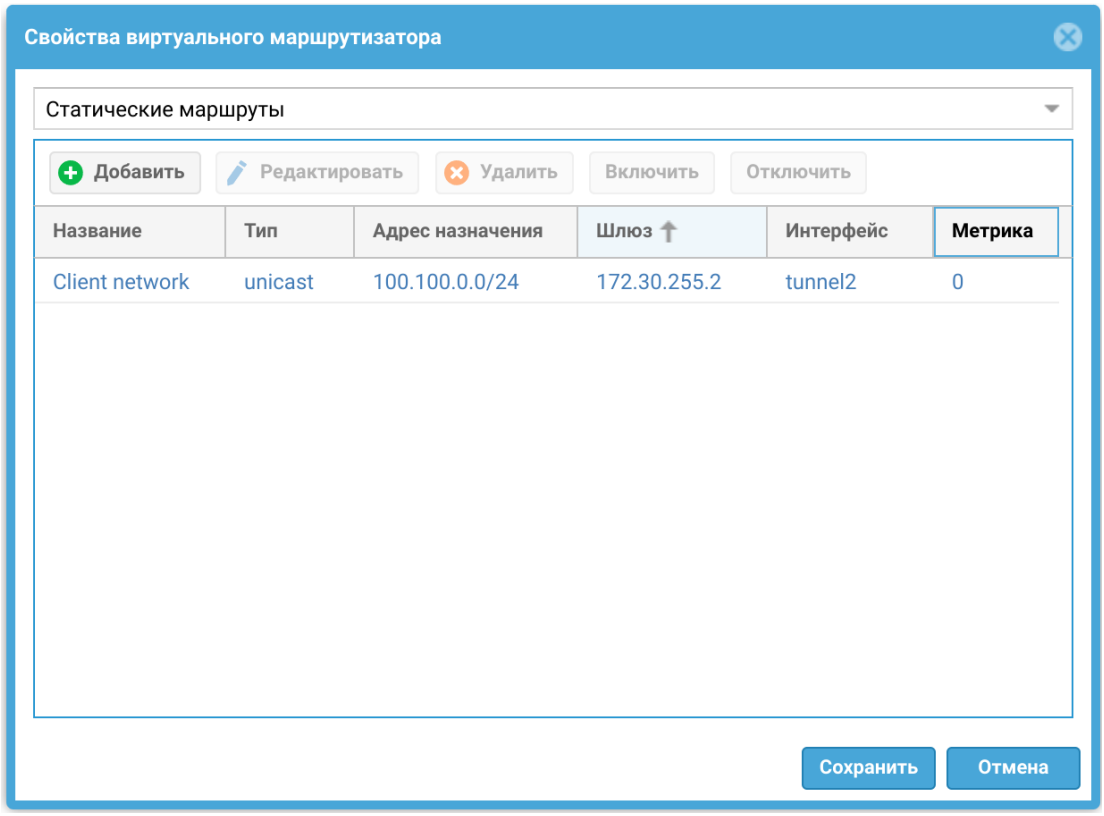
2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

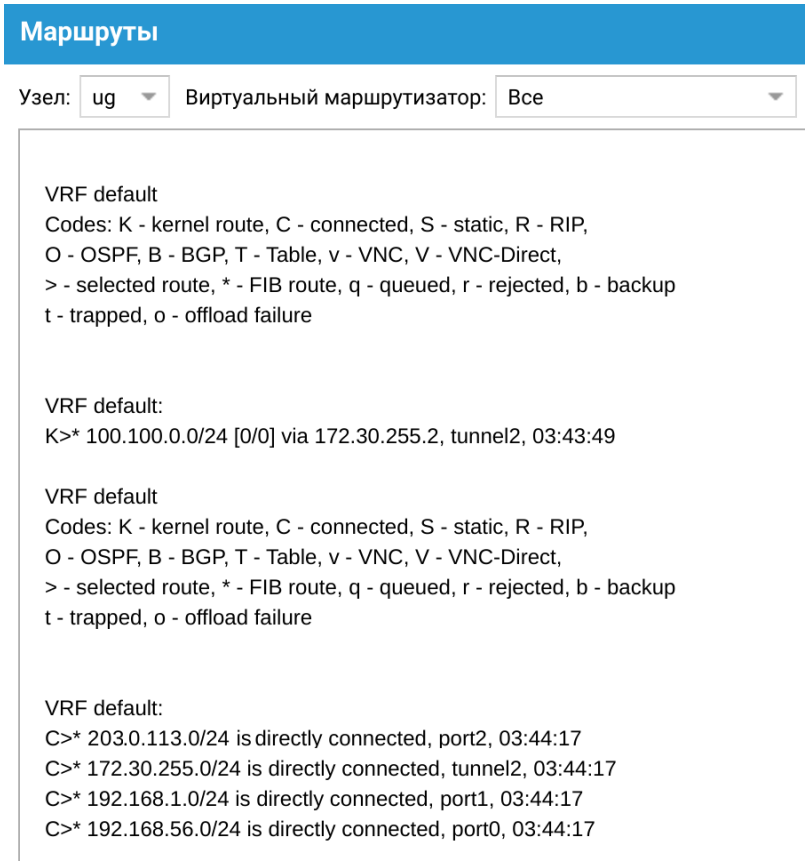


4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

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:

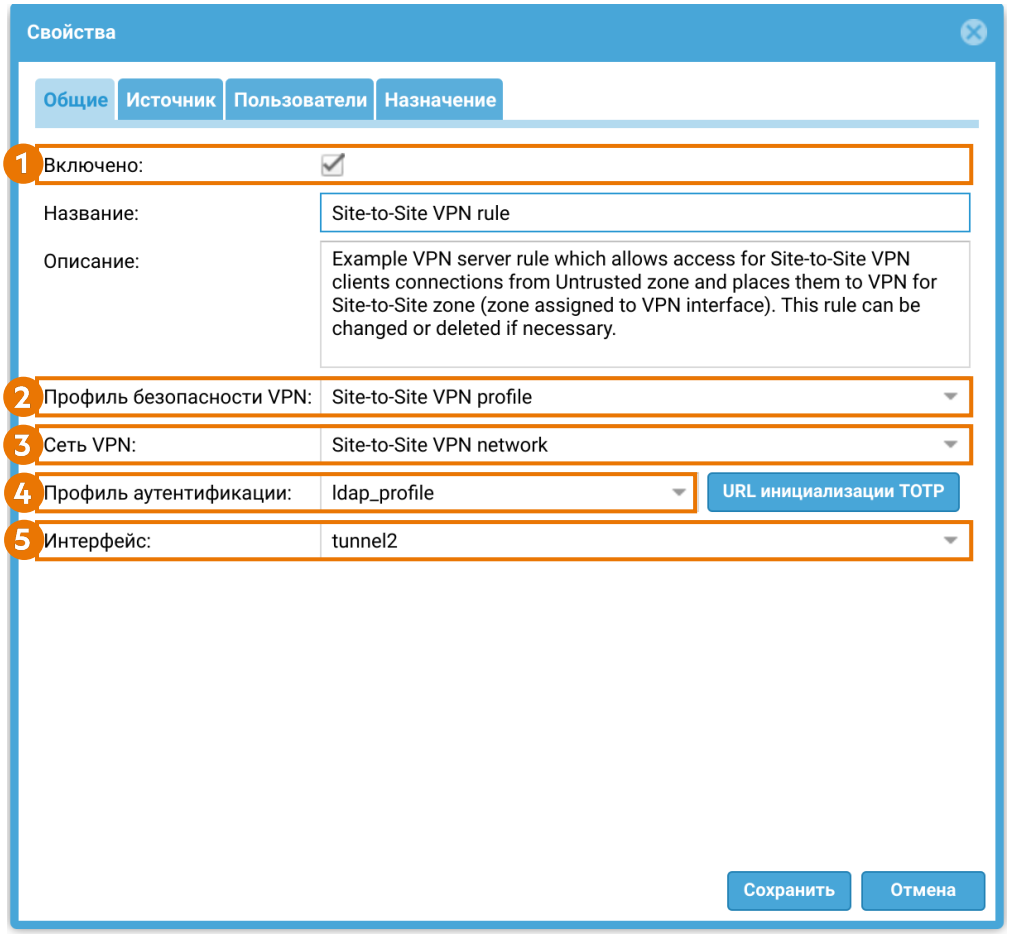


В разделе **Журналы и отчеты → Мониторинг → Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:



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:



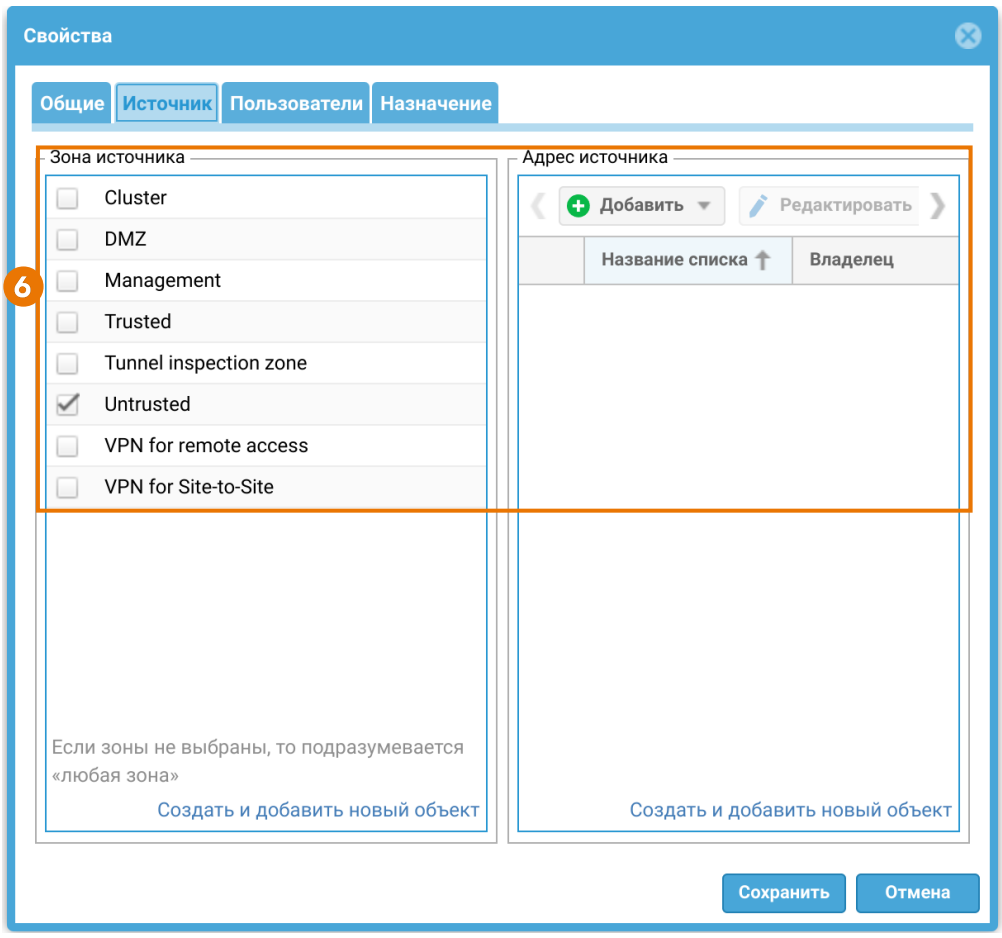
1. **Включено** — включить правило VPN.

2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на Шаге 4 (Site-to-Site VPN profile).

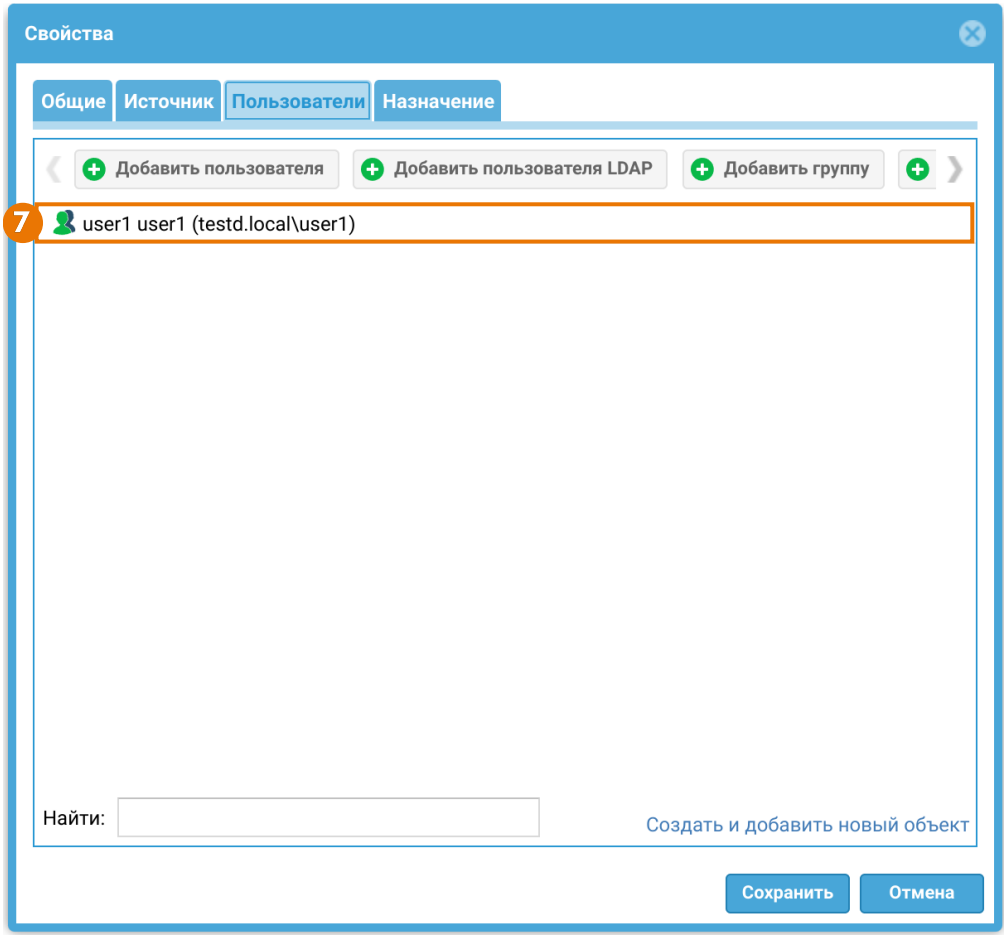
3. **Сеть VPN** — сеть VPN, созданная ранее на Шаге 6 (Site-toSite VPN network).

4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. Шаг 3).

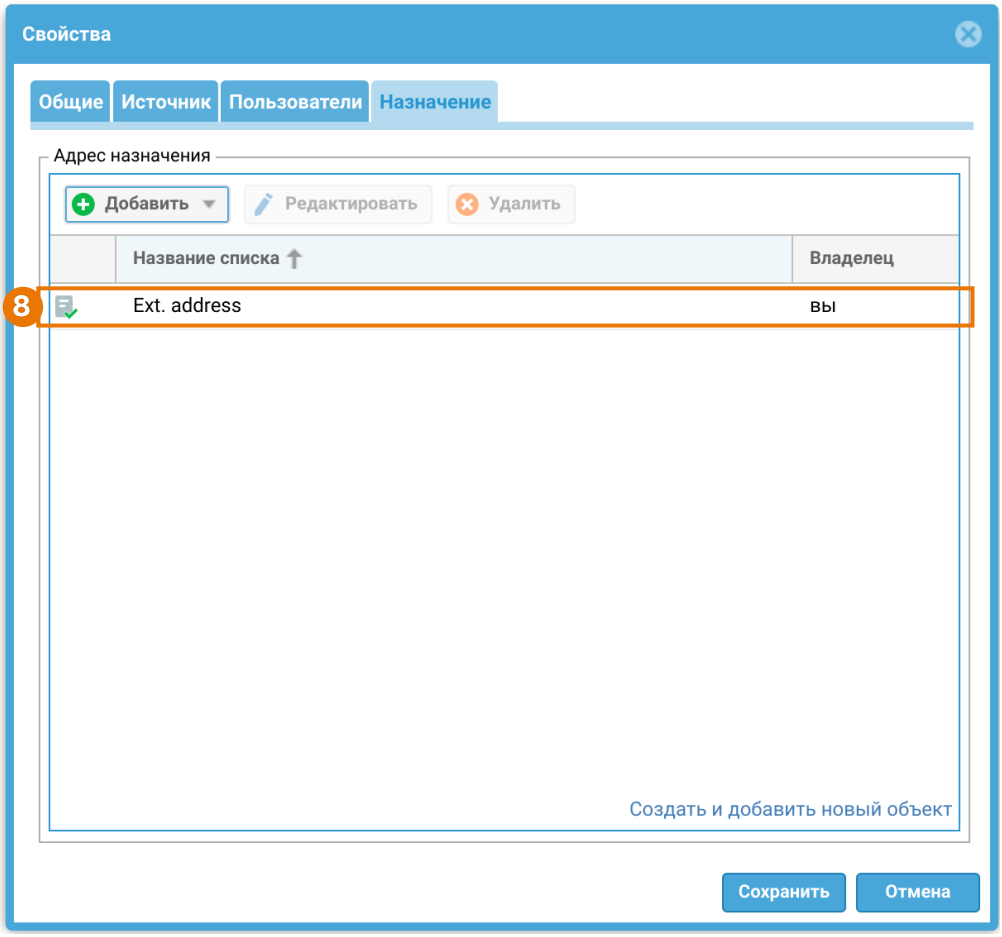
5. **Интерфейс** — созданный ранее на Шаге 5 интерфейс VPN (tunnel2).



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.



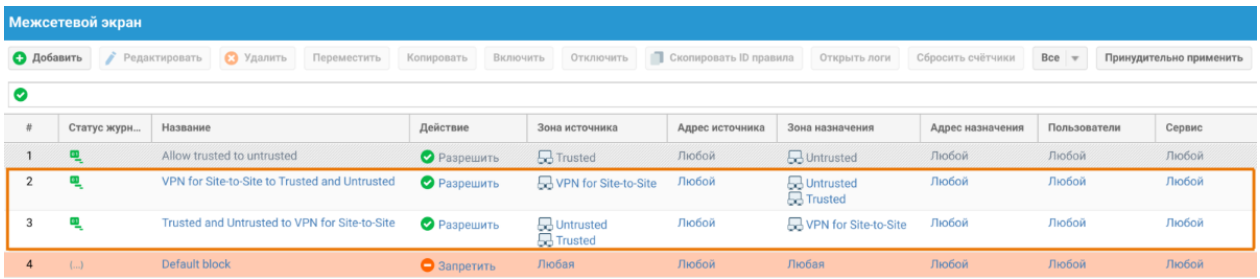
8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1

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**.



Настройка VPN-клиента

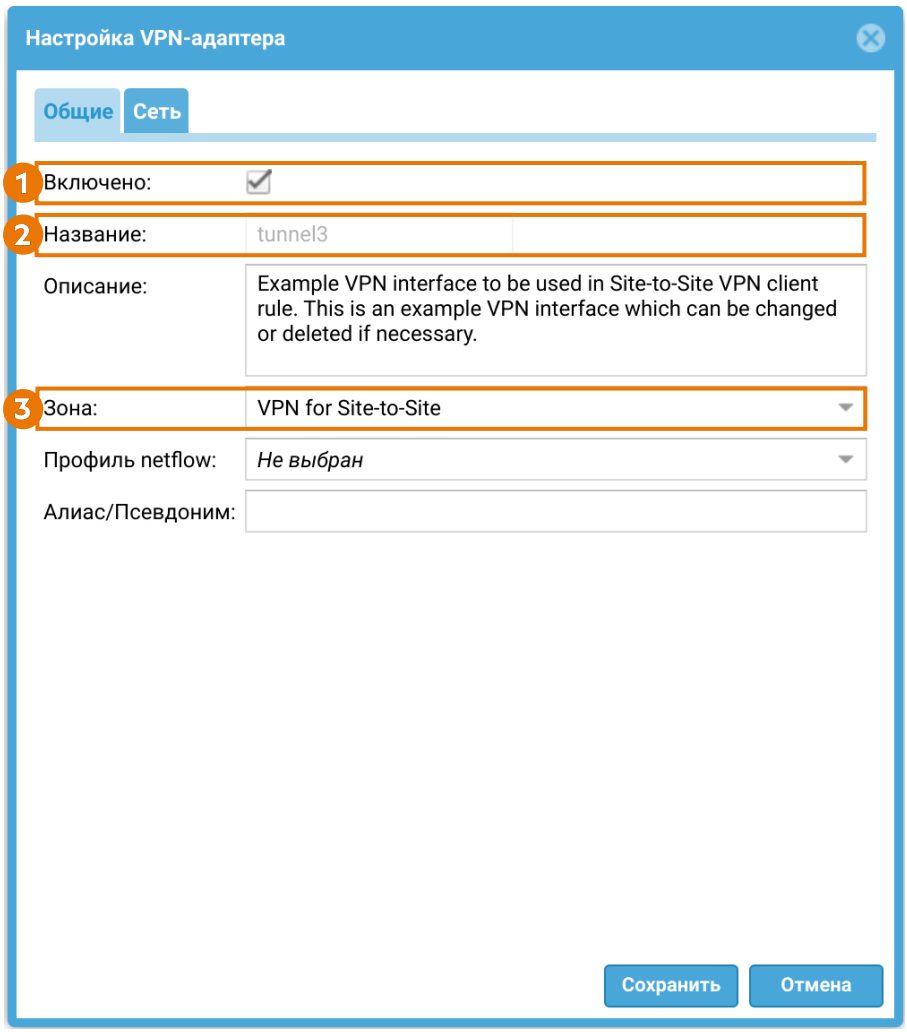
Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

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.

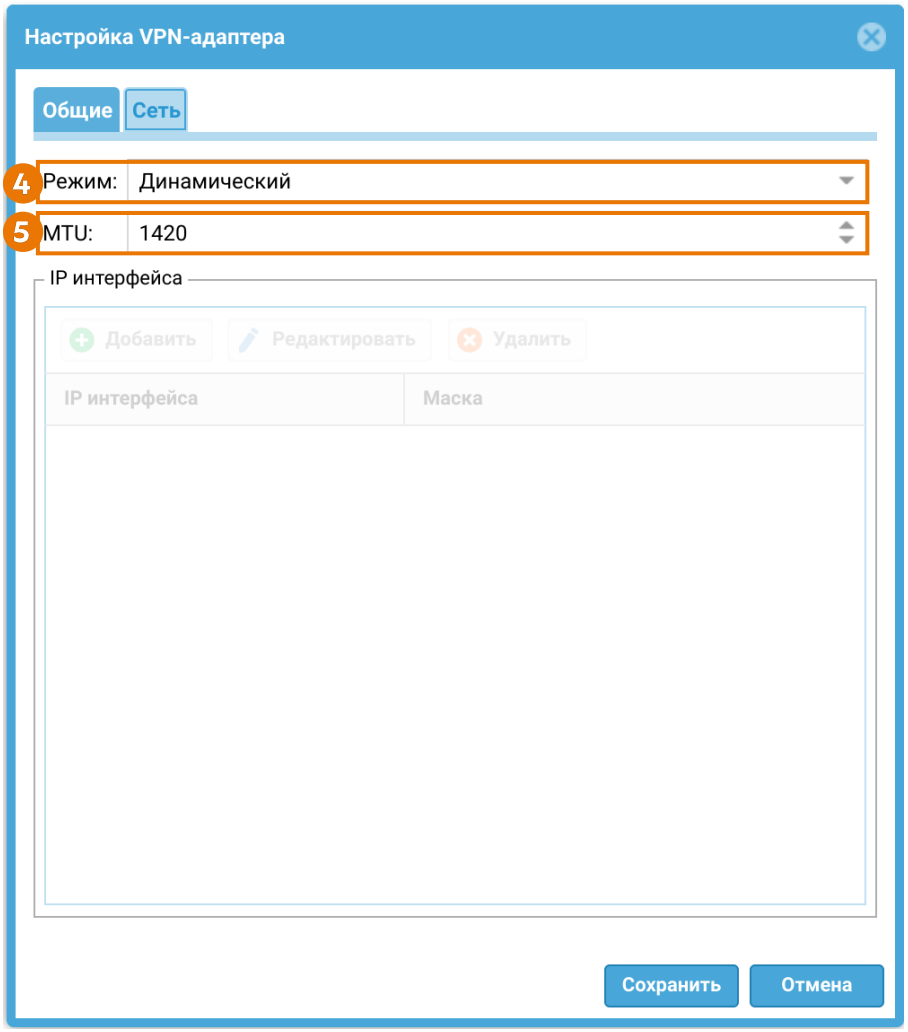
В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для примера создания защищенного VPN-соединения в этой статье:



1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel3).

3. **Зона**, к которой будет относится данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на Шаге 1.



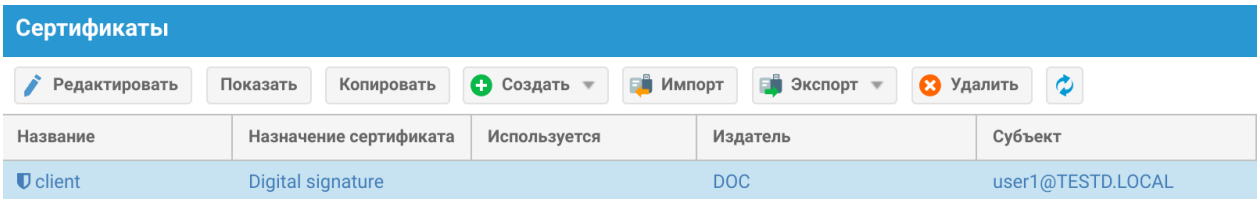
4. **Режим**. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, созданной на Шаге 6 настроек VPN-сервера.

5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

Шаг 3. Настроить параметры аутентификации.

Импортируем созданный ранее сертификат VPN-клиента. Примеры создания самоподписанных сертификатов приведены в Приложении.

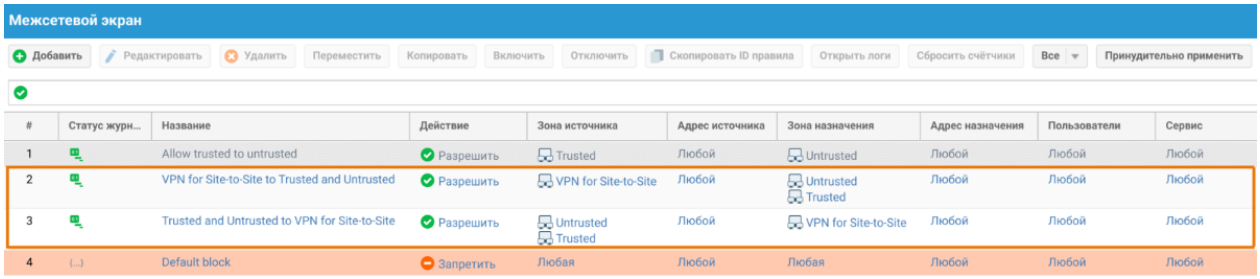
В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать.** В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-клиента и приватного ключа.



Шаг 4. Контроль доступа к ресурсам.

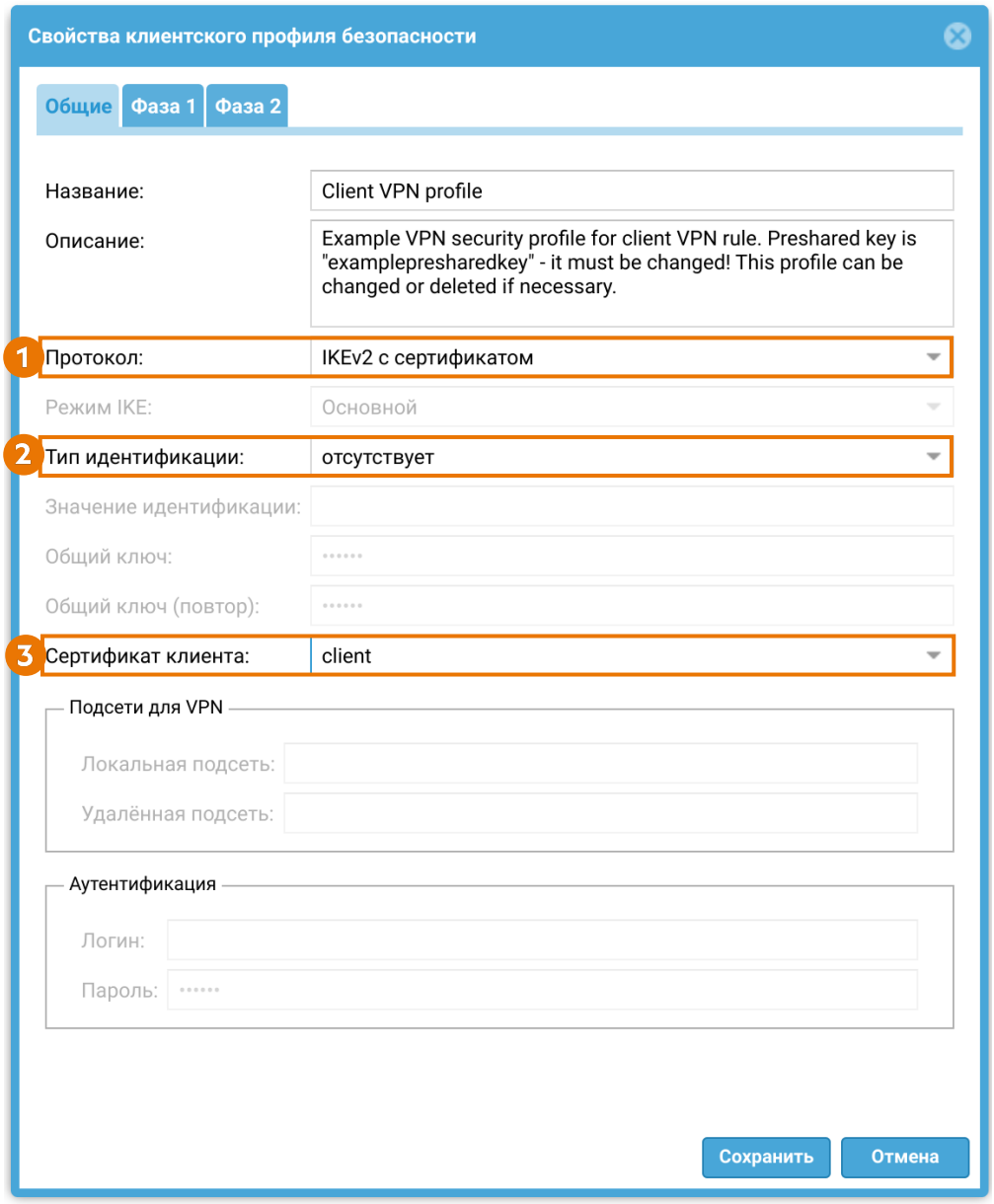
Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site**, **Trusted** и **Untrusted**.

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.**



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.

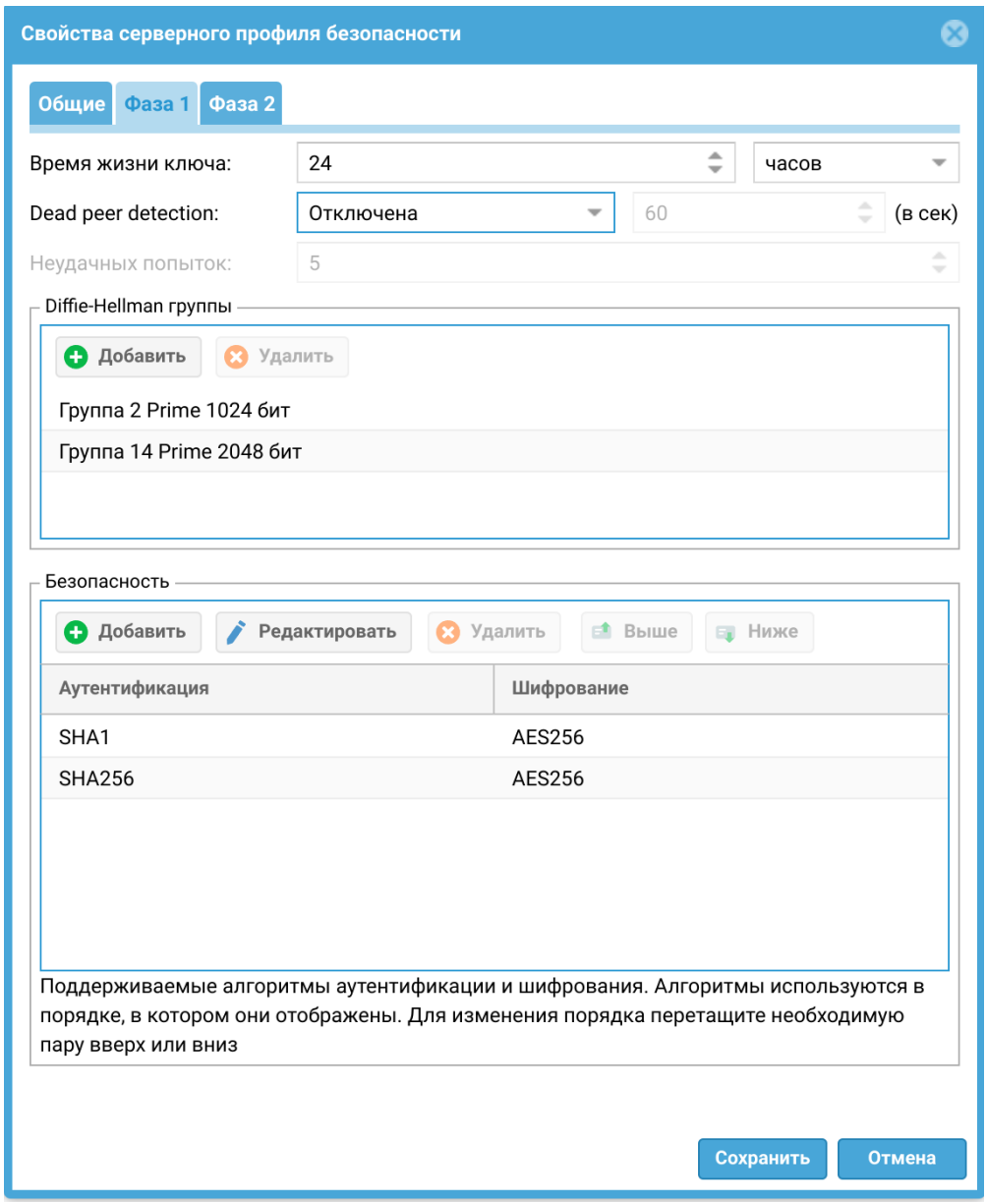


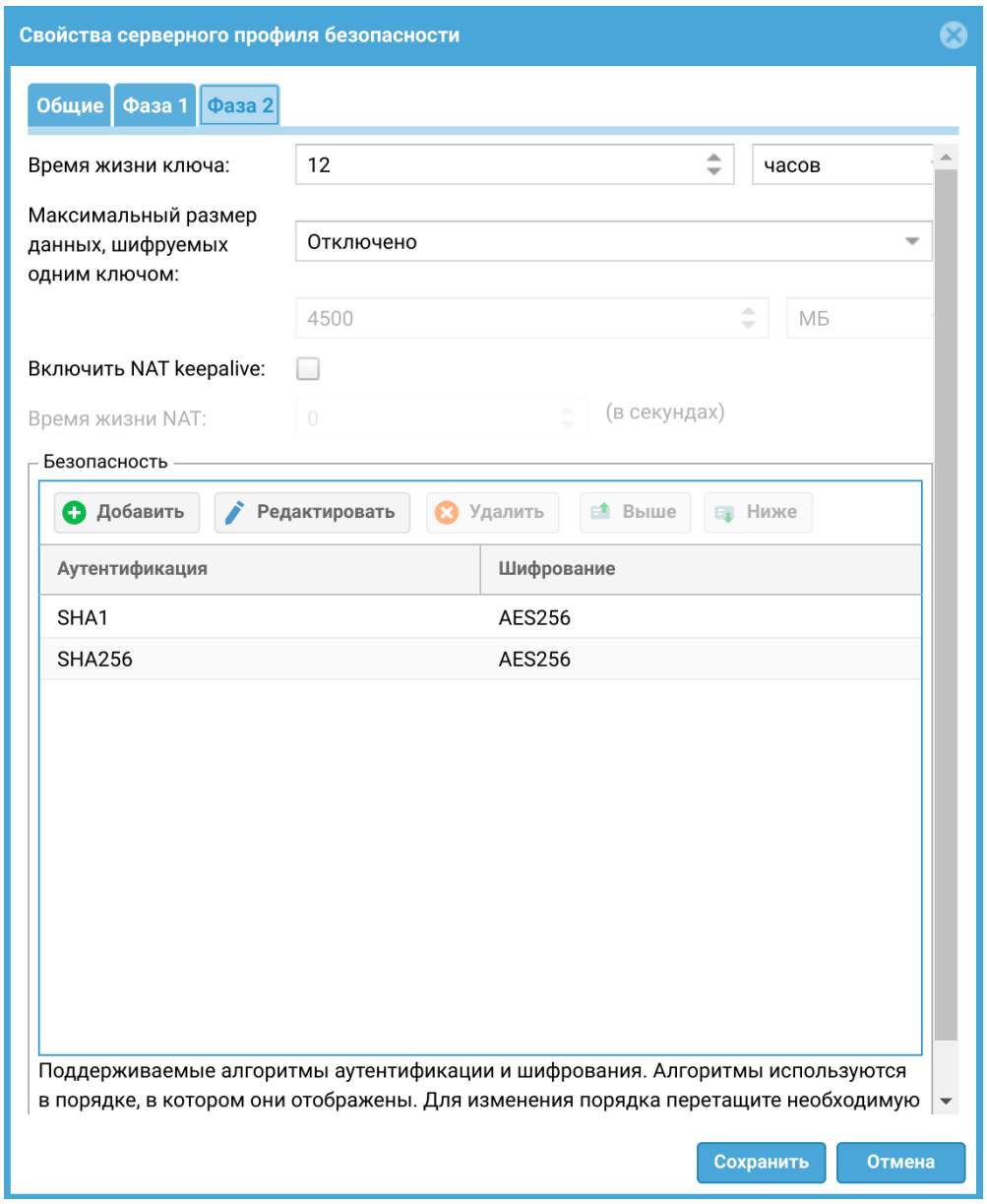
1. **Протокол**. В рассматриваемом примере для создания защищенного канала будет использоваться **IKEv2 с сертификатом**.

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 Шаге 3.

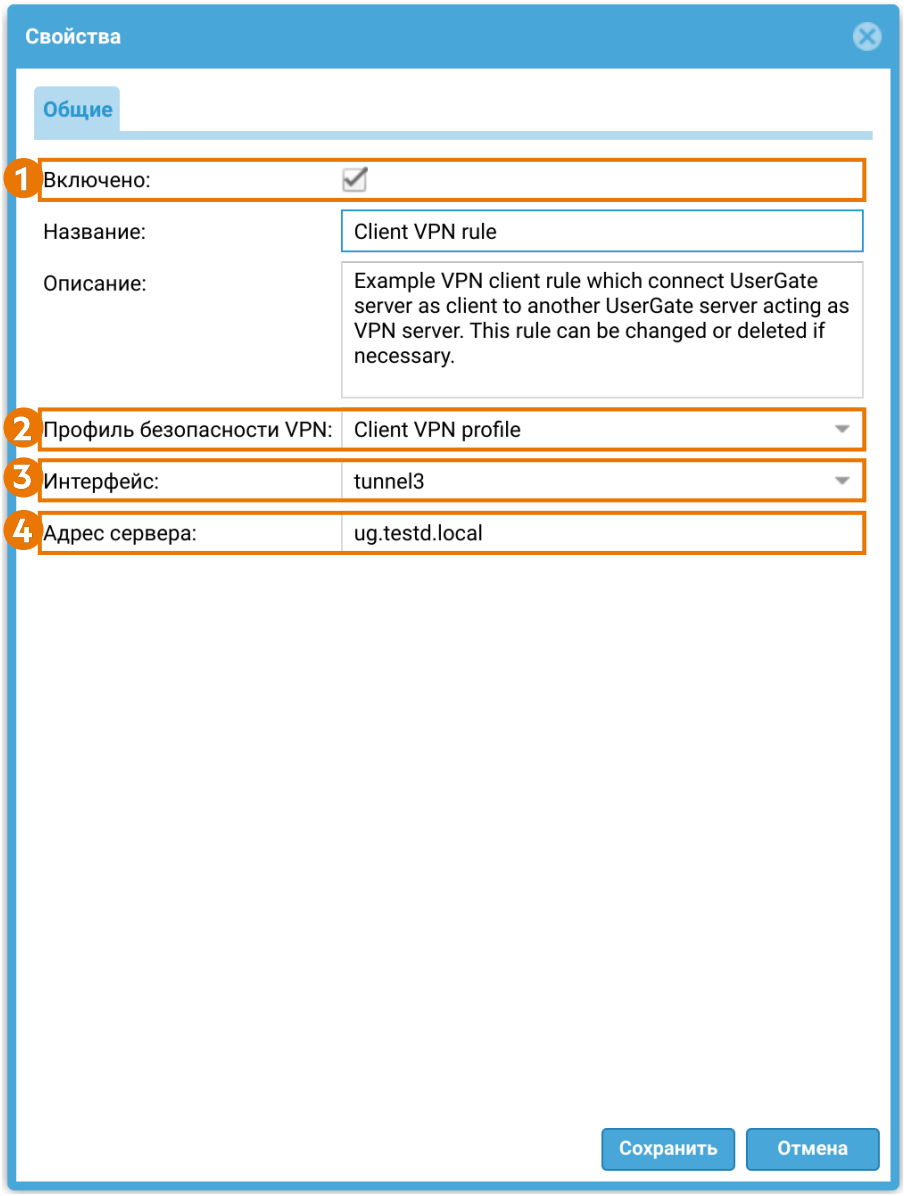
Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:


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



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.



1. **Включено** — включить правило.

2. **Профиль безопасности VPN** — созданный на Шаге 5 клиентский профиль безопасности VPN.

3. **Интерфейс** — созданный на Шаге 2 VPN-интерфейс.

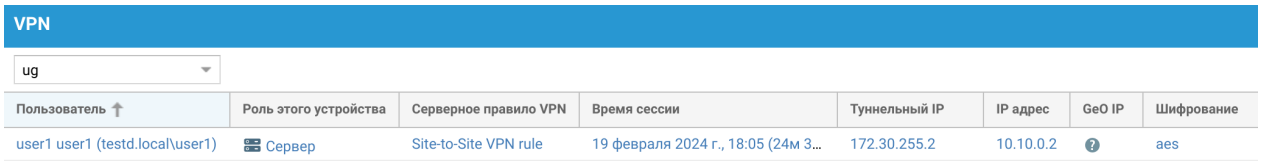
4. **Адрес сервера**.В рассматриваемом примере это доменное имя NGFW 1 (ug.testd.local), выполняющего роль VPN-сервера.

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.

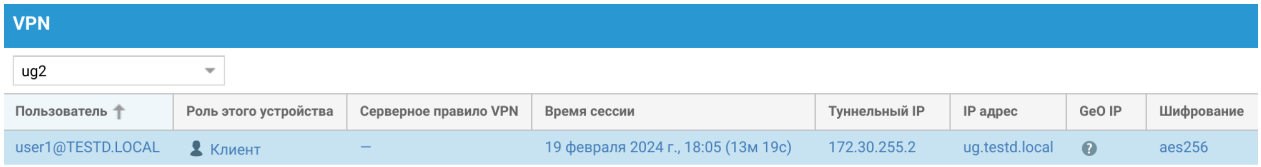
Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узлах NGFW 1 и NGFW 2 в разделе **Журналы и отчеты → Мониторинг → VPN** появится информация о новом туннеле.

На NGFW 1:



На NGFW 2:



В разделе **Журналы и отчеты → Мониторинг → Маршруты** на узле NGFW 2 добавится маршрут в сеть удаленного офиса 192.168.1.0/24 через туннельный интерфейс tunnel3:

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW 1:

Ping

Настройка ping

Ping host 172.30.255.2 TTL 30 Интерфейс 172.30.255.1 (tunnel2)

Счётчик 6 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 172.30.255.1 TTL 30 Интерфейс 172.30.255.2 (tunnel3)

Счётчик 6 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:

```
[redacted]:~$ 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
[redacted]:~$ 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
```

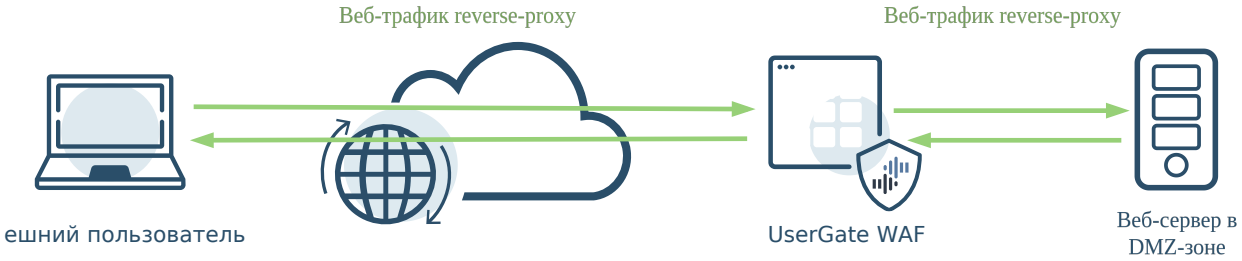
```
[redacted]:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft 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
[redacted]:~$ 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
```

WAF

WAF (Описание)

WAF (Web Application Firewall) — система безопасности, предназначенная для защиты веб-приложений от известных уязвимостей и угроз. WAF в UserGate используется для фильтрации трафика приложений на прикладном уровне модели OSI. Пропуская трафик через обратный прокси-сервер и анализируя входящий и исходящий HTTP/HTTPS трафик, WAF блокирует потенциально вредоносные запросы и обеспечивает повышенный уровень безопасности веб-приложений.

Если UserGate WAF находит в трафике примеры вредоносного кода или другие особенности, отмеченные в сигнатурах безопасности, прохождение трафика может быть заблокировано, событие сохраняется в журнал.



Для настройки UserGate WAF необходимо выполнить следующие шаги:

- Лицензировать WAF.
- Создать профиль. Профили отвечают за создание и редактирование наборов слоев с UPL правилами. В профиле могут использоваться как персональные слои с пользовательскими правилами, так и системные слои, содержащие системные правила.
- В созданном профиле включить слои с необходимыми UPL-правилами.
- Подключить профиль в правило reverse-прокси.

Лицензирование UserGate WAF

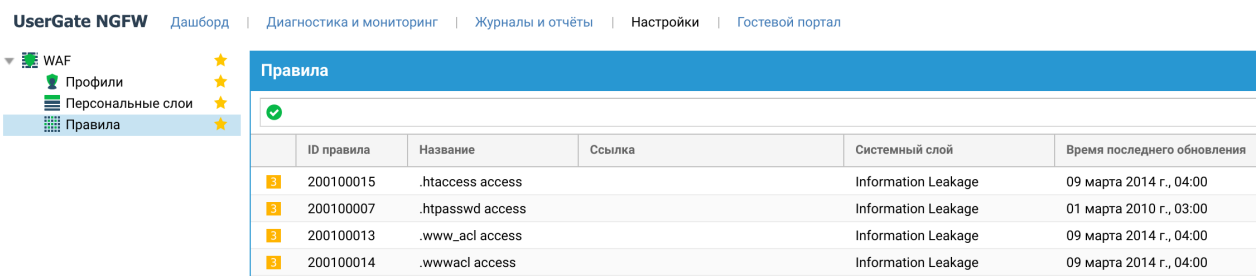
Для работы с функциональностью WAF на межсетевом экране UserGate необходимо запросить лицензию, содержащую соответствующий модуль. Без необходимой лицензии функциональность WAF скрыта из графического интерфейса, соответствующие методы API тоже недоступны.

После активации лицензии необходимо выйти из веб-консоли и заново авторизоваться. После нового входа в GUI все страницы и окна WAF будут доступны, можно совершать операции обновления правил, удаления, добавления, просмотра и т.д.

При отсутствии лицензии функциональность WAF отключается, все параметры становятся недоступны, однако пользовательские правила сохраняются в памяти устройства. Если снова активировать модуль, то старые правила отобразятся в списках.

Системные правила

Системные правила — это правила, загружаемые с серверов UserGate автоматически после активации лицензии. Системные правила отображаются в разделе веб-интерфейса **WAF → Правила** только для просмотра и не редактируются:



Для быстрого поиска предусмотрен фильтр и сортировка по полям в таблице правил.

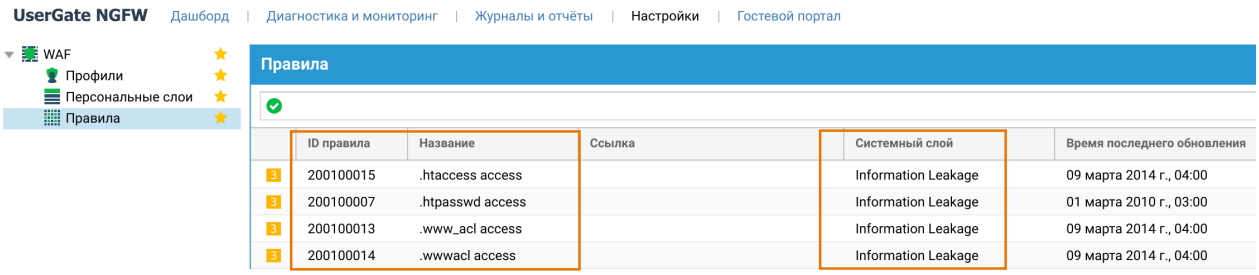
В структуре системных правил используются следующие поля:

Слои

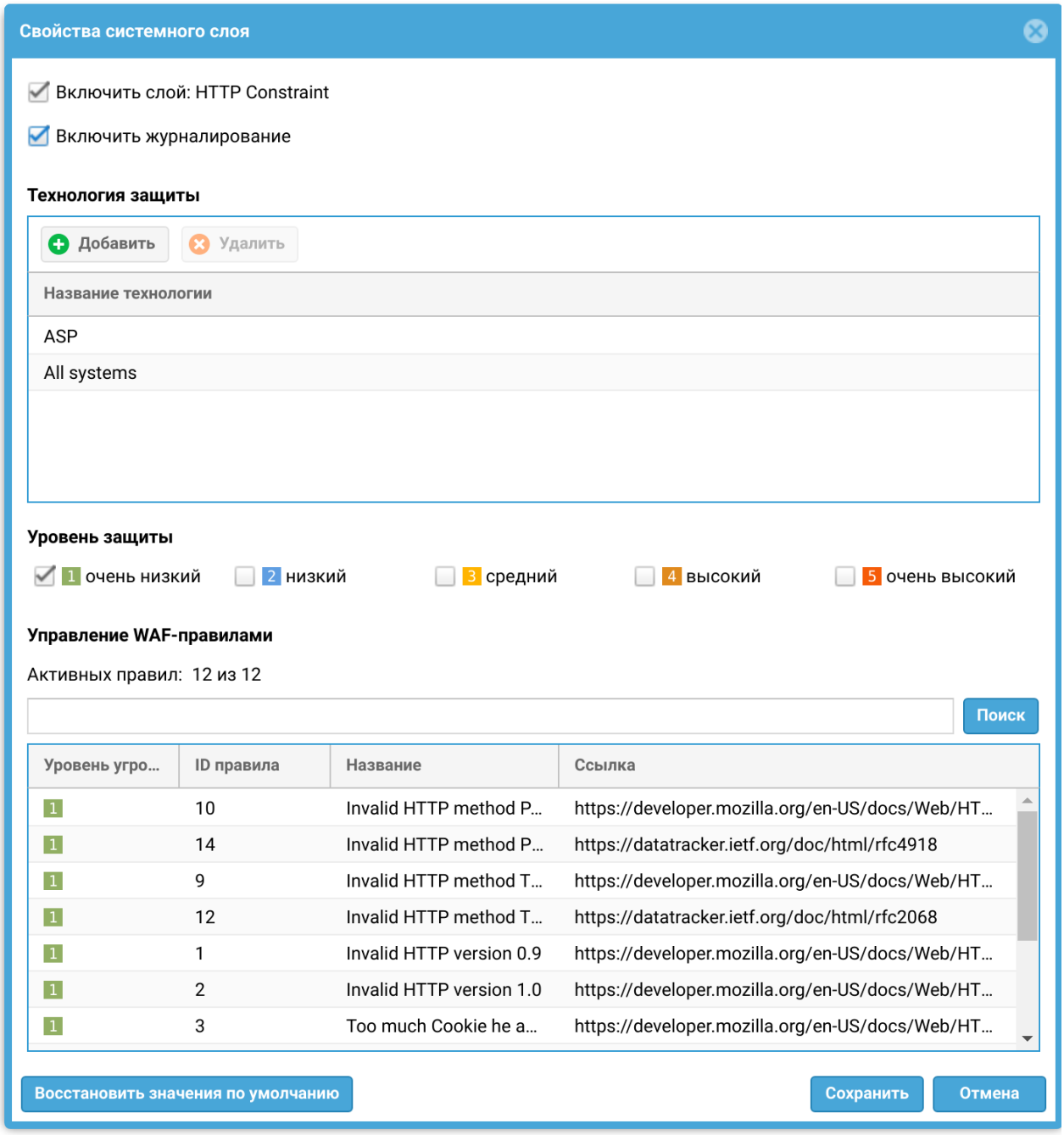
Слой — это конструкция, используемая для группировки правил и принятия одного решения. Существуют системные и персональные слои.

Системные слои создаются компанией UserGate, они содержат правила, сгруппированные по типам атак.

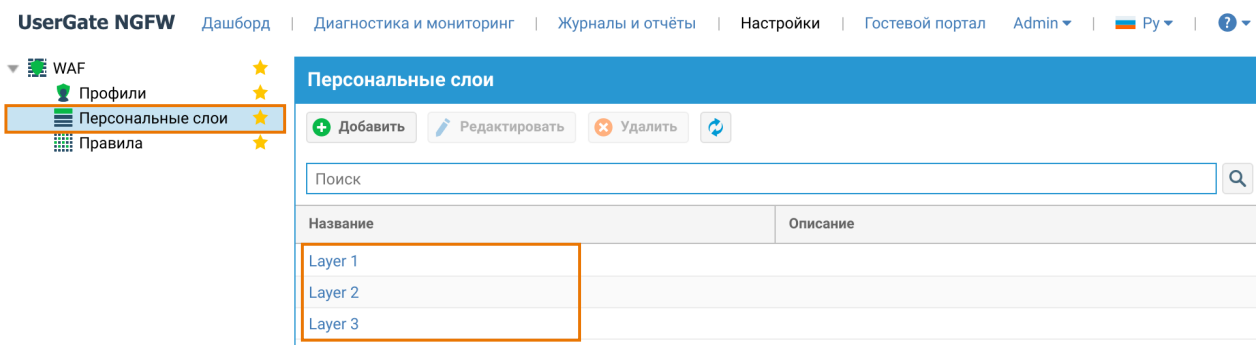
Принадлежность правил системным слоям можно посмотреть в разделе **WAF → Правила**:



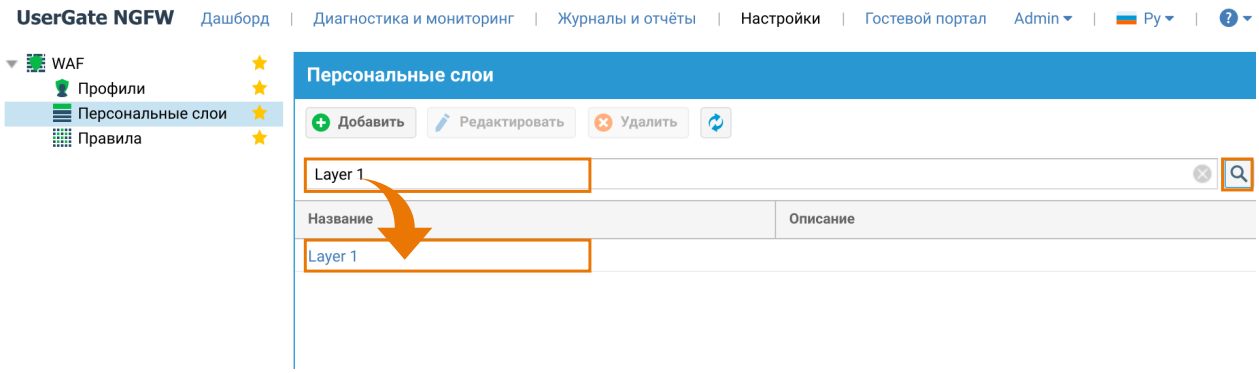
Также состав системного слоя можно посмотреть в свойствах системного слоя. Свойства системного слоя вызываются из профиля WAF. Предусмотрена возможность фильтрации правил в системном слое (Подробнее читайте ниже).



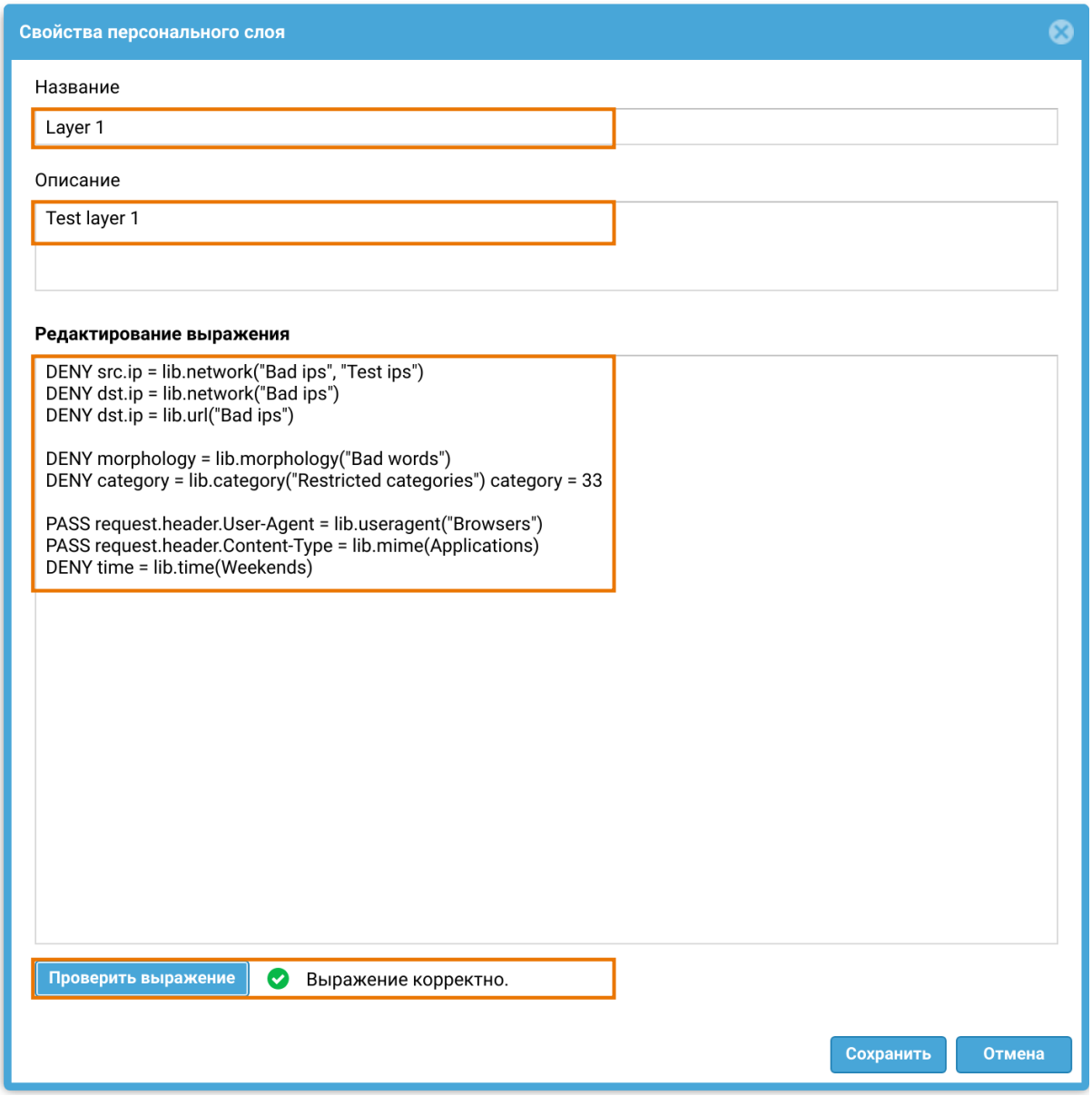
Персональные слои — это наборы UPL-правил, созданные администратором межсетевого экрана. Раздел **WAF → Персональные слои** в веб-консоли позволяет управлять персональными слоями: создавать, удалять, обновлять и просматривать:



Так как количество слоев может быть большим, в верхней части раздела **Персональные слои** есть фильтр для поиска слоев по имени:

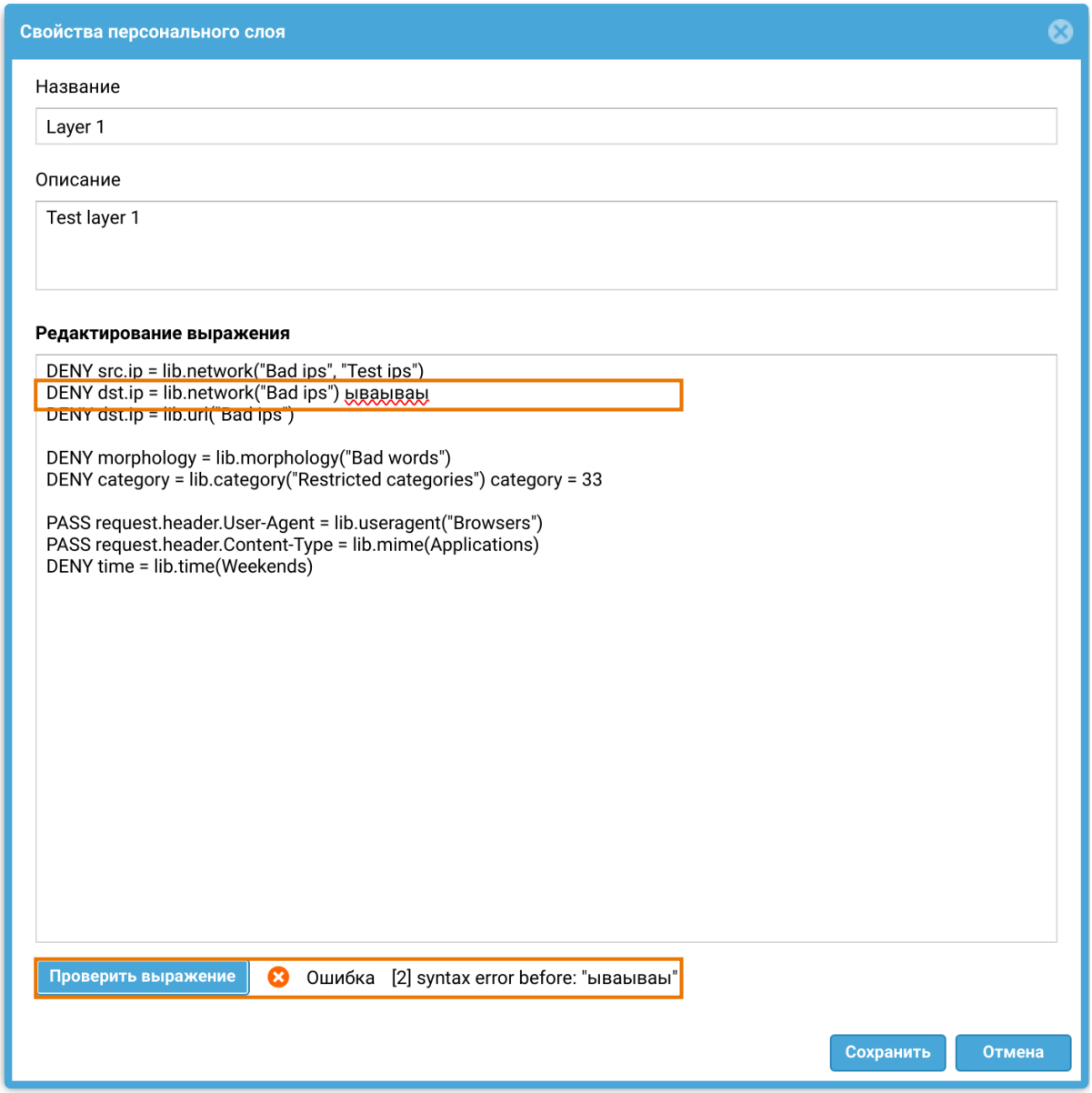


Для создания персонального слоя необходимо нажать на кнопку **Добавить**, в свойствах персонального слоя указать следующие параметры:



- **Название** — название персонального слоя.
- **Описание** — опциональное описание персонального слоя.
- **Редактирование выражения** — поле для записи/редактирования UPL-выражения, содержащего правила фильтрации трафика.
- **Проверить выражение** — проверка UPL-выражения.

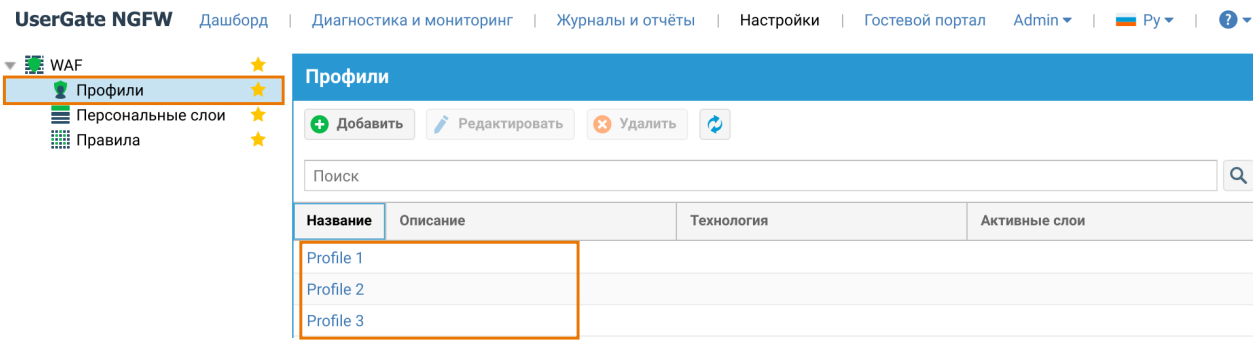
В случае неверного синтаксиса в выражении после проверки будут отображены подсказки и номер строки, где была допущена ошибка:



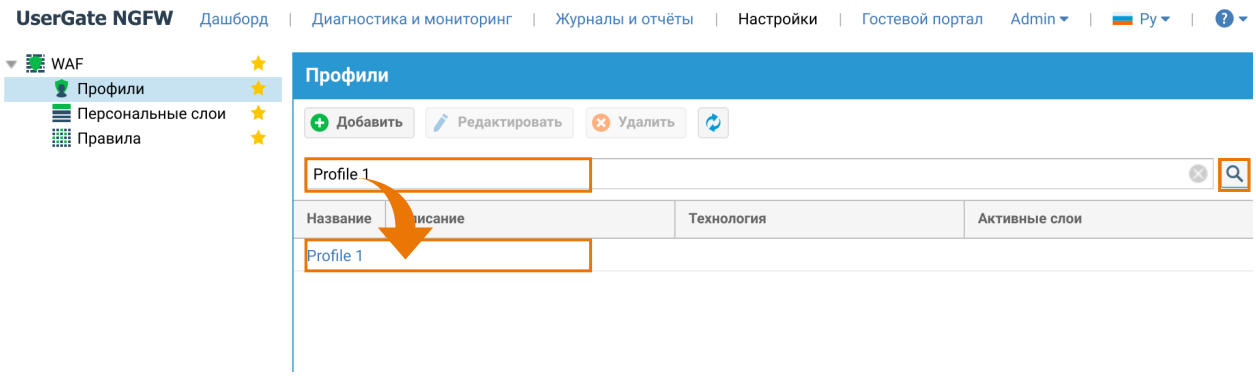
Подробнее о синтаксисе написания UPL-правил смотрите в разделе Настройка правил с использованием UPL - UserGate.

Профили

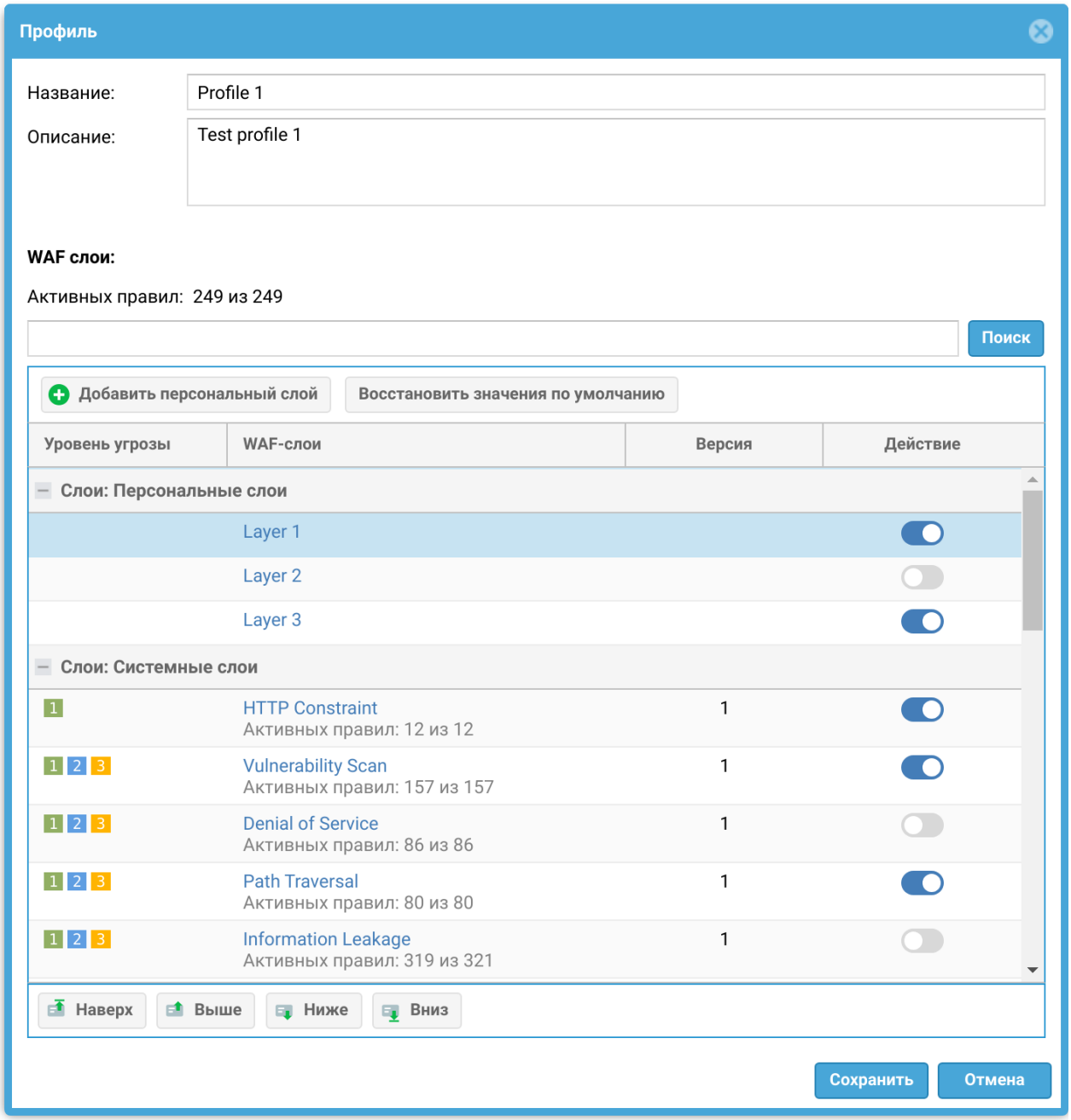
Профиль — это набор персональных и/или системных слоев. В разделе веб-интерфейса **WAF → Профили** можно управлять профилями: создавать, удалять, обновлять и просматривать.



В верхней части страницы **Профили** есть фильтр для поиска профилей по имени:



Для создания профиля необходимо нажать на кнопку **Добавить**, в свойствах указать следующие параметры:

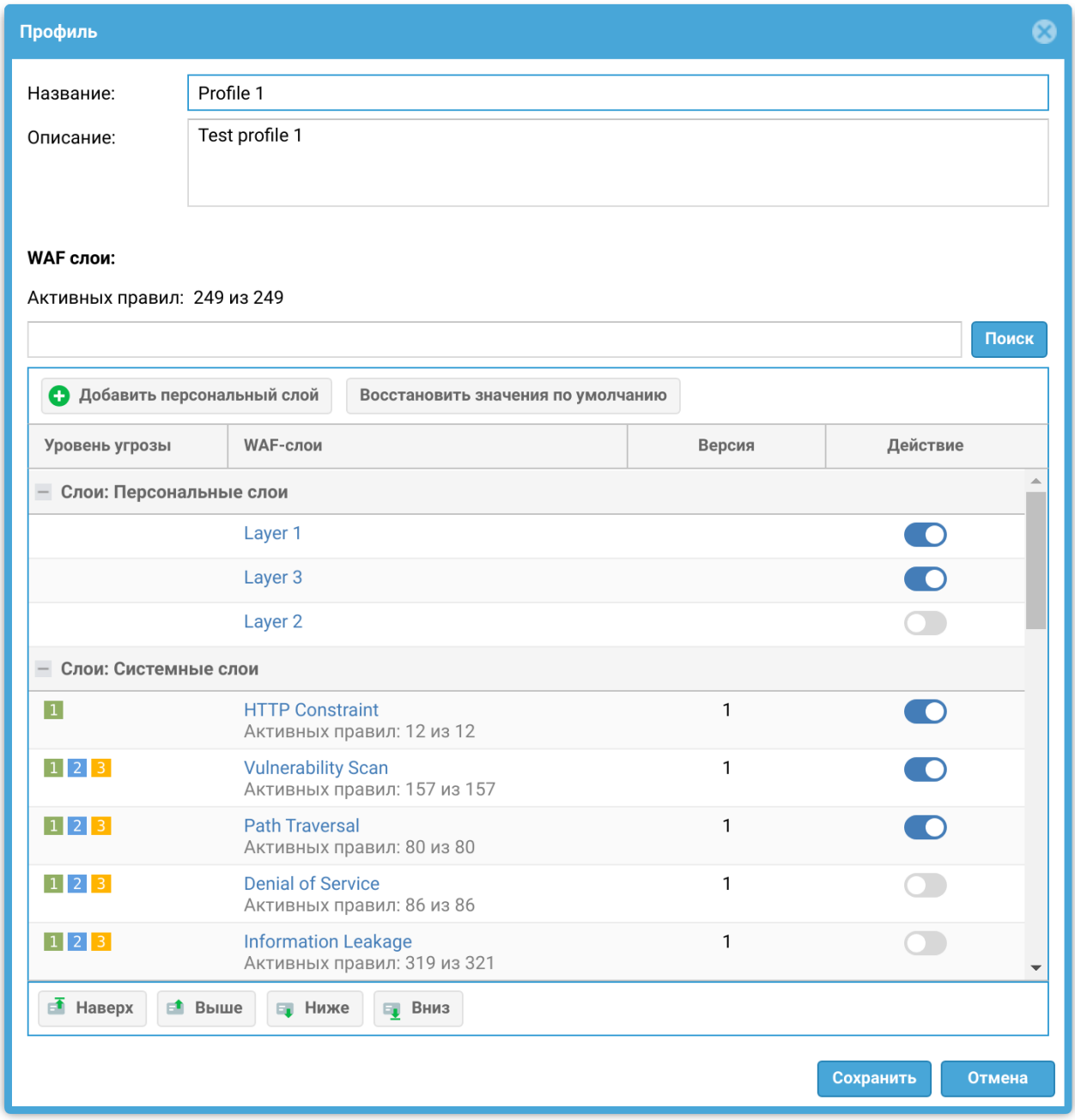


- **Название** — название профиля
- **Описание** — опциональное описание профиля.
- **WAF слои** — наборы UPL-правил (персональные слои, системные слои). Для включения слоя в редактируемый профиль его нужно включить в колонке **Действие**.
- **Активных правил** — отображает количество активированных правил.

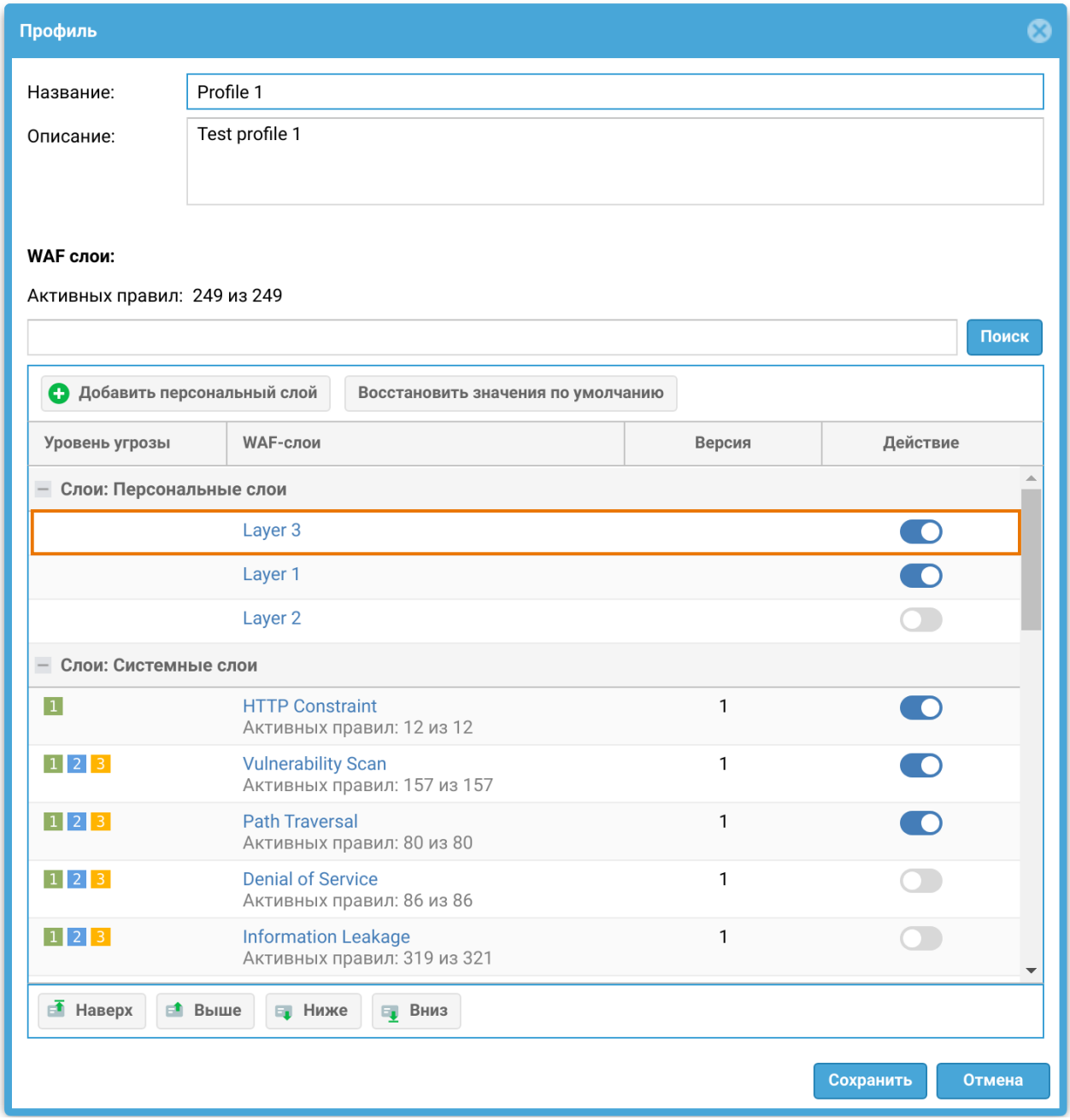
После сохранения профиля включенные слои автоматически поднимаются наверх в своих группах. Порядок в таком случается определяется так: первый в списке включенный слой поднимается на первое место, после чего ищется

следующий включенный слой, который поднимается на второе место и так далее.

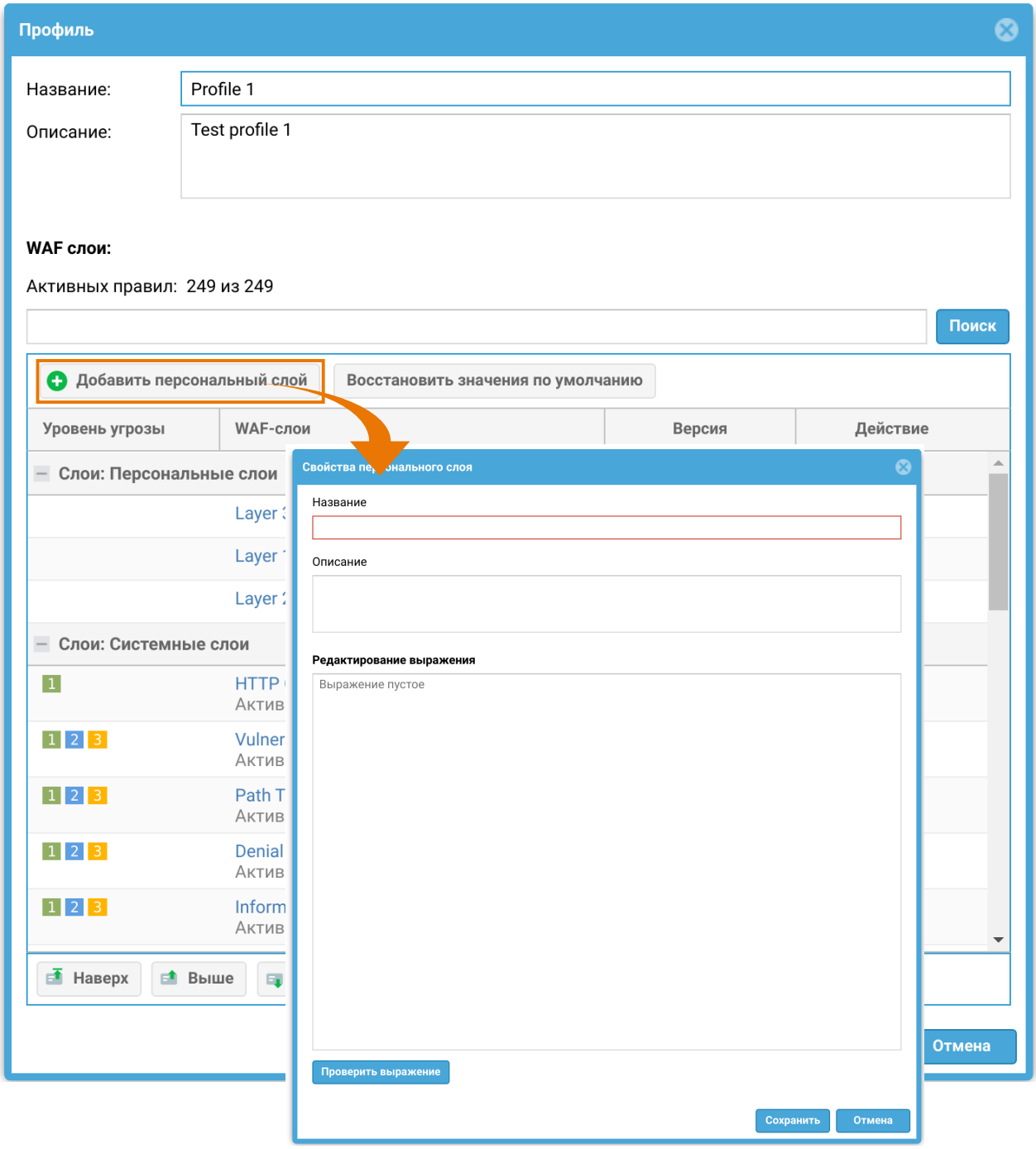
Важно: Слои можно перемещать только в рамках своих групп, первым идут персональные слои, затем системные.



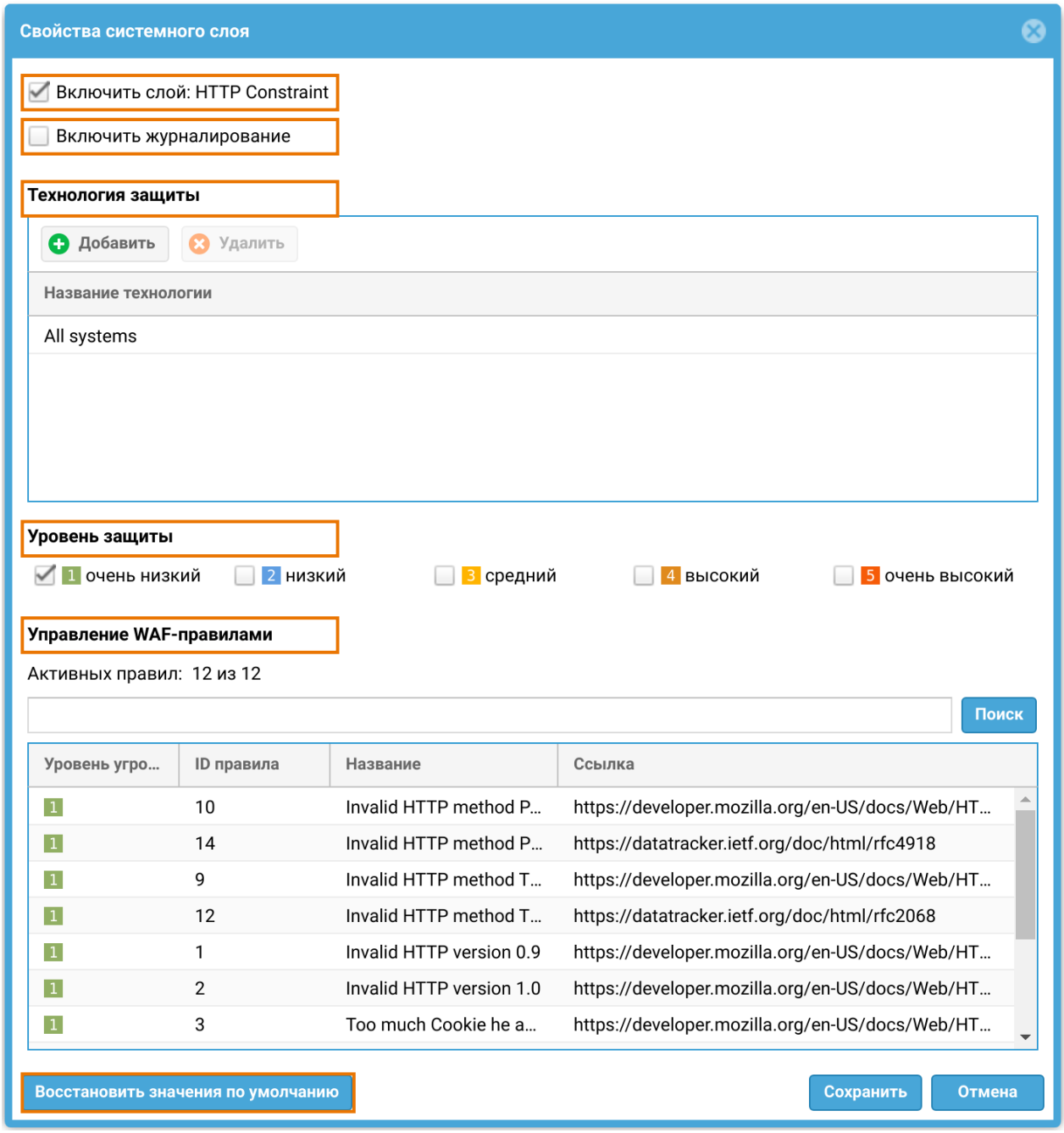
Включенные слои автоматически поднялись на самый верх списка в своих группах. Можно поменять включенные слои местами (например, передвинуть слой "Layer 3" на самых верх) и после повторного открытия профиля, порядок изменится:



Непосредственно из окна профиля можно создать новый персональный слой. При нажатии кнопки **Добавить персональный слой** откроется диалоговое окно создания персонального слоя:



Предусмотрена возможность фильтровать системные правила в выбранном системном слое, который будет подключен в редактируемый профиль. Для редактирования нужно нажать на системный слой в окне профиля, появится диалоговое окно:



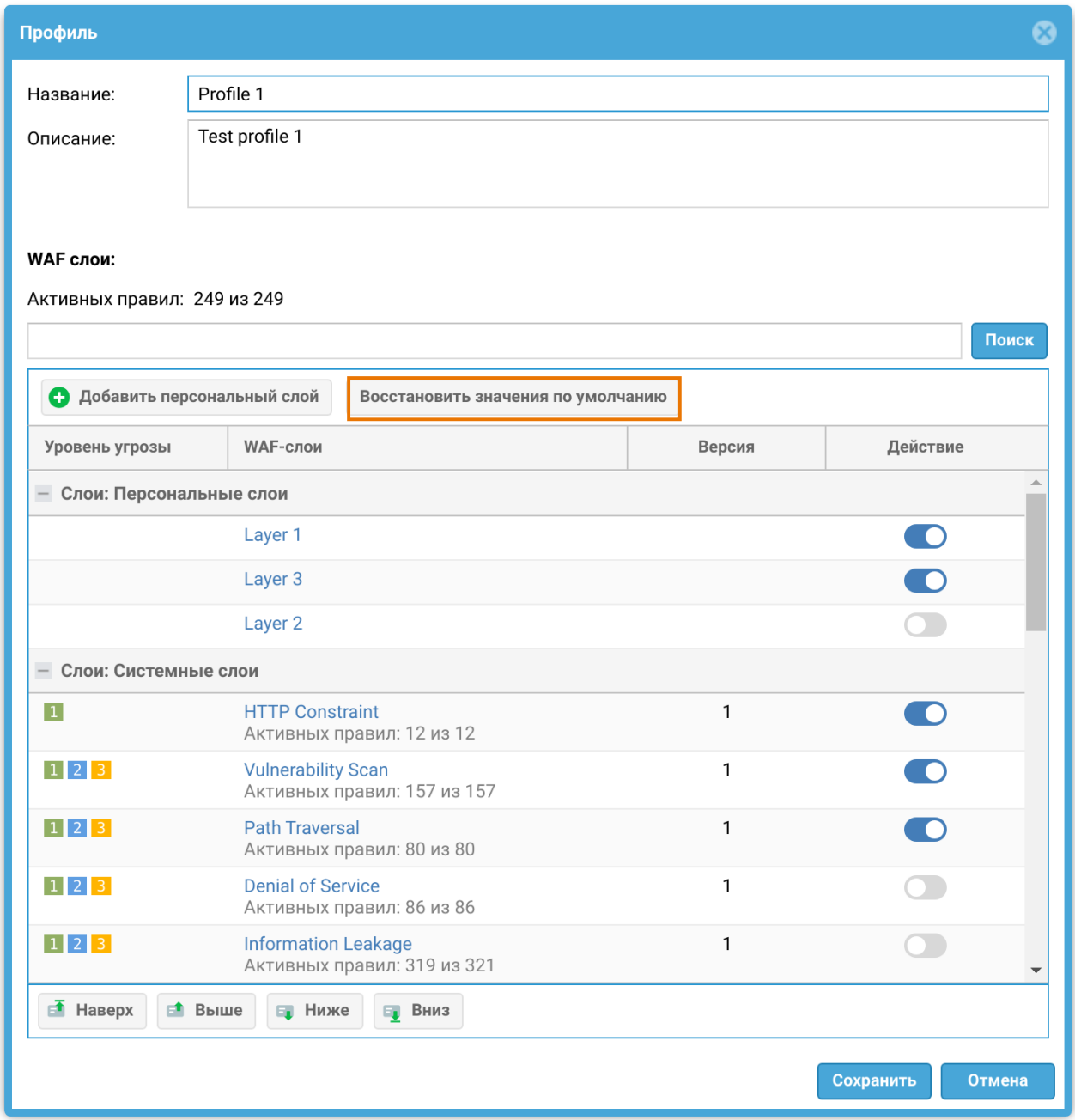
В открывшемся окне предоставлены:

- Флажок для включения/отключения данного системного слоя.
- Флажок для включения/отключения журналирования правил.
- Технология защиты — фильтр технологий для правил из выбранного системного слоя. В профиль будут подключены правила только с выбранными технологиями.
- Уровень защиты — фильтр правил по уровню защиты. В профиль будут подключены правила только с выбранными уровнями защиты.

- Управление WAF-правилами — таблица, отображающая все отфильтрованные правила, которые будут подключены к редактируемому профилю.

Администратор может сбросить в первоначальное состояние выставленные технологии и уровни защиты данного системного слоя, нажав кнопку **Восстановить значения по умолчанию**.

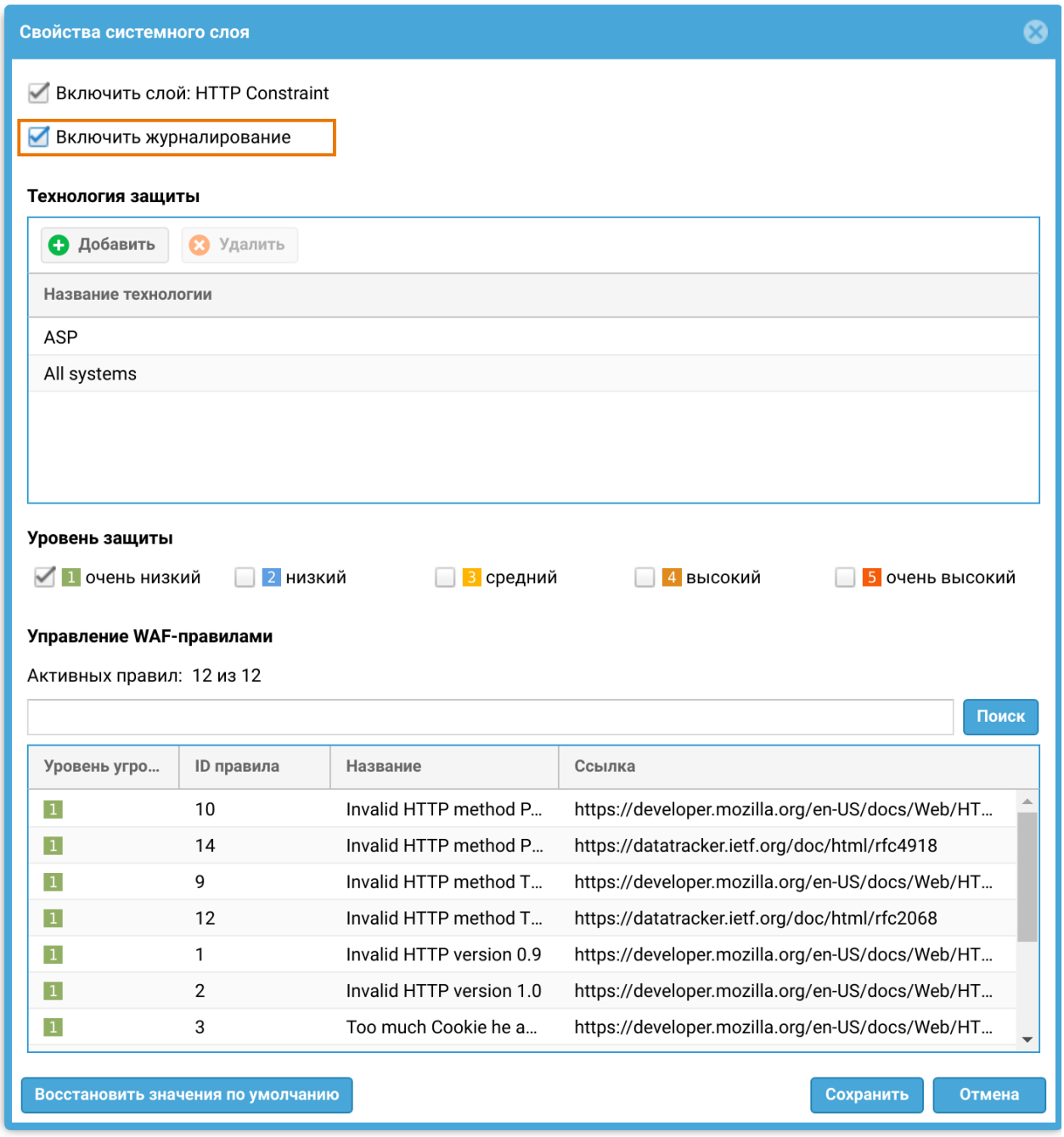
Для восстановления в исходное состояние всех системных слоев профиля одновременно, необходимо нажать кнопку **Восстановить значения по умолчанию** в окне профиля:



Журналирование правил

Для того чтобы информации о срабатывании правила отображалась в журнале веб-доступа, нужно включить опцию журналирования.

1. Для системного слоя эта опция включается с помощью флажка **Включить журналирование** в свойствах системного слоя. В этом случае будут журналироваться все правила в этом слое:



2. Для персонального слоя журналирование включается для каждого правила отдельно. Для этого необходимо добавить в UPL-правило свойство "*rule_log(true)*". После этого требуется включить эти слои и сохранить профиль.

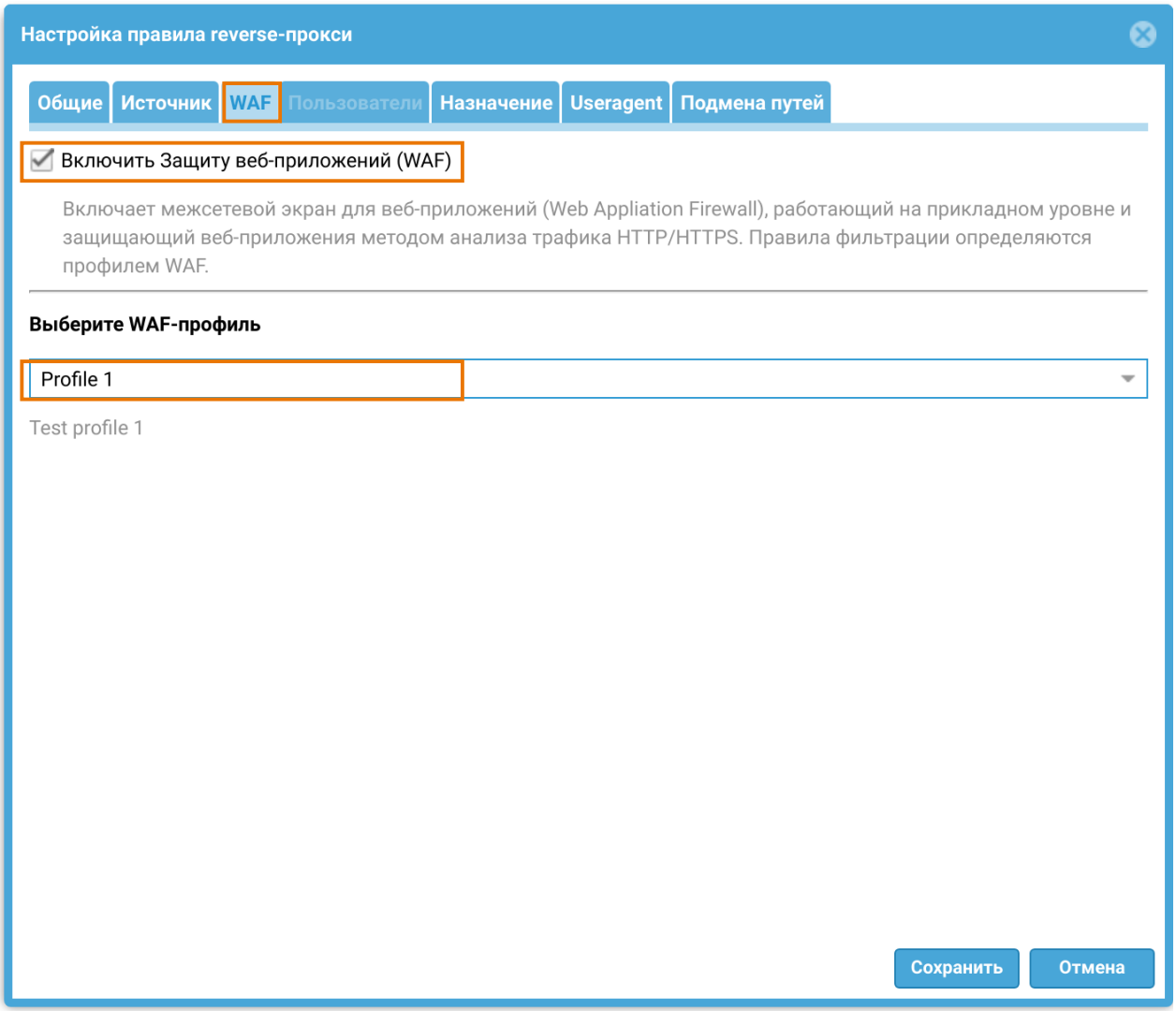
Подключение WAF-профиля в правила reverse-прокси

Для активации созданного WAF-профиля необходимо указать его в правилах reverse-прокси. Порядок подключения следующий:

1. Перейти в раздел **Глобальный портал**, выбрать **Правила** reverse-прокси.

2. Нажать кнопку **Добавить**, в появившемся диалоговом окне редактируемого правила выбрать вкладку **WAF**.

3. Поставить флажок **Включить защиту веб-приложений (WAF)**, выбрать необходимый WAF-профиль и сохранить внесенные изменения.

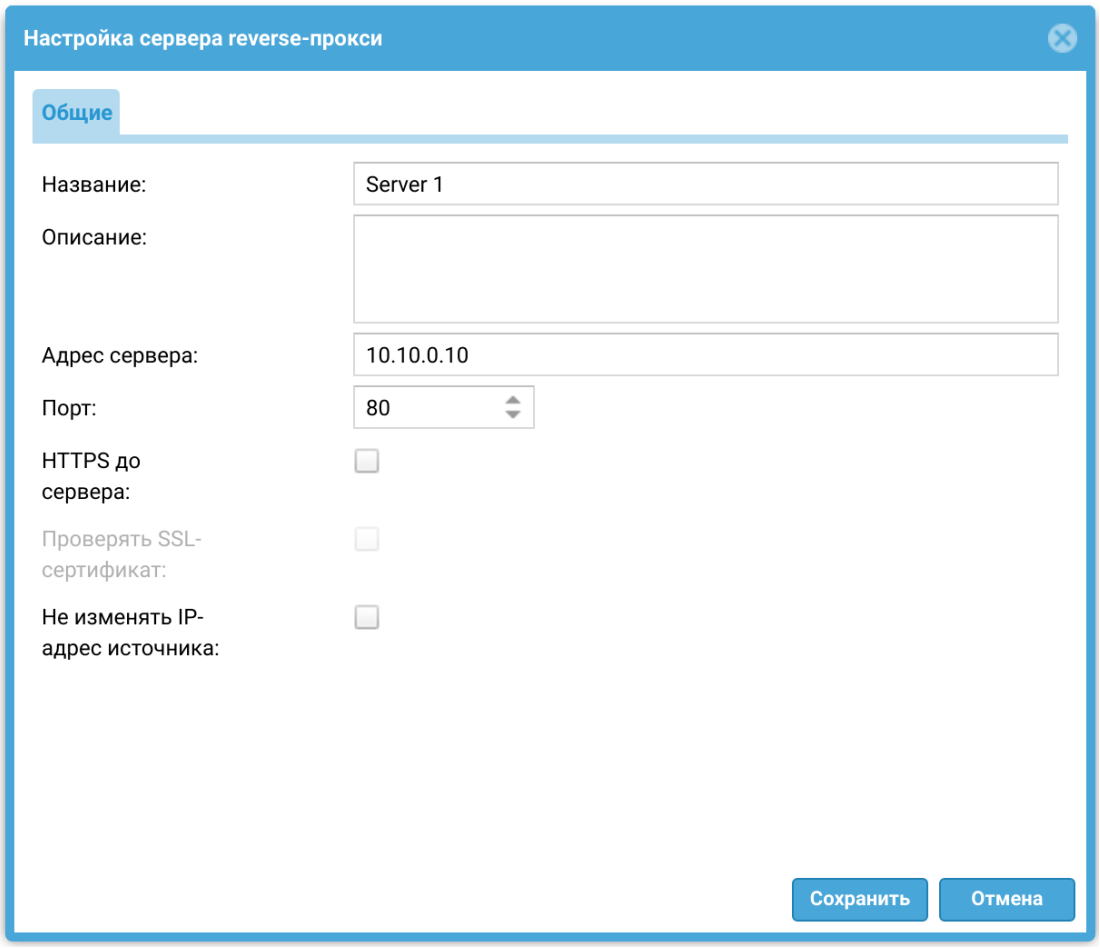


Пример использования WAF-профиля в правилах reverse-прокси

В качестве примера использования профиля WAF в правилах reverse-прокси рассмотрим настройку редиректа HTTP —> HTTPS.

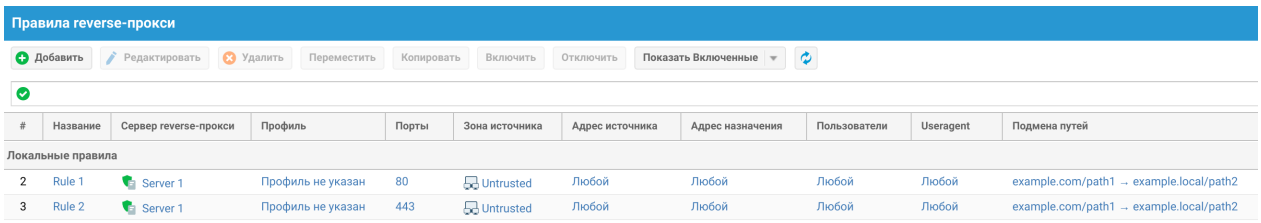
1. Создадим сервер для публикации через reverse-прокси.

В разделе веб-консоли **Глобальный портал → Серверы reverse-прокси** создадим профиль сервера Server 1:



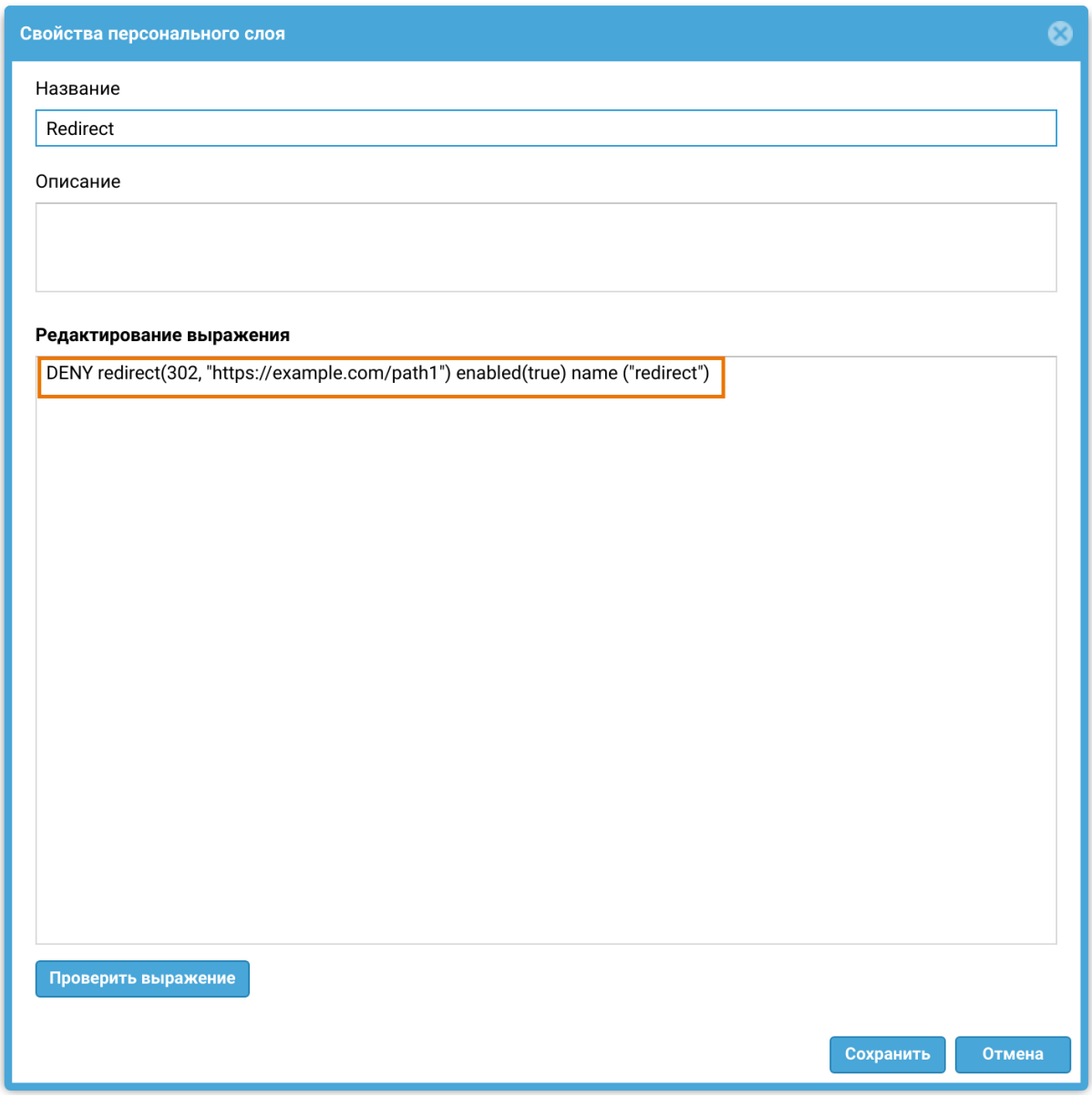
2. Создадим правила reverse-прокси для публикации сервера.

В разделе веб-консоли **Глобальный портал → Правила reverse-прокси** создадим два правила публикации сервера Server 1: одно — через порт 80, другое — через порт 443.



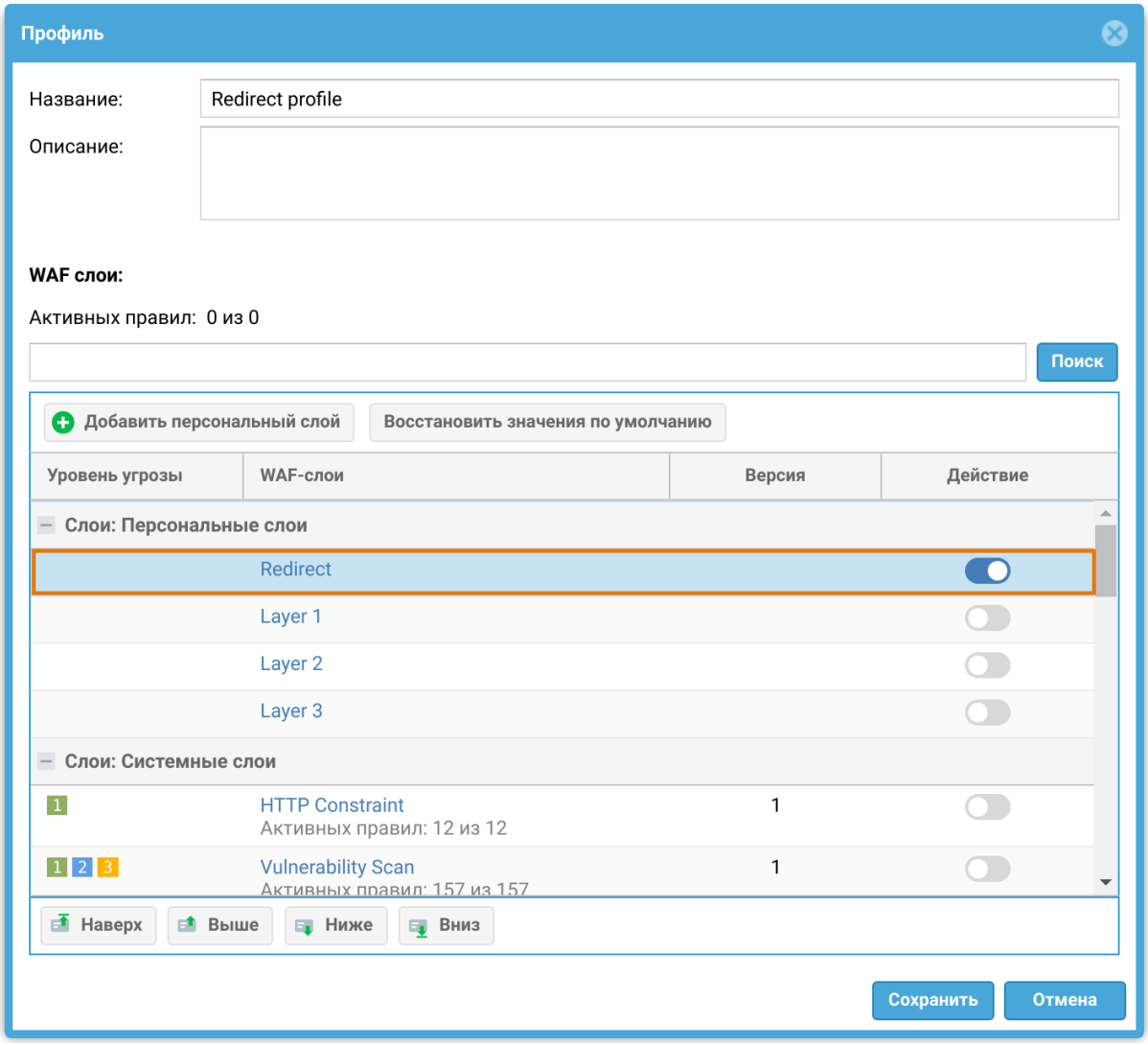
3. Создадим персональный слой WAF.

В разделе веб-консоли **WAF → Персональные слои** создадим слой Redirect со следующим UPL-выражением:

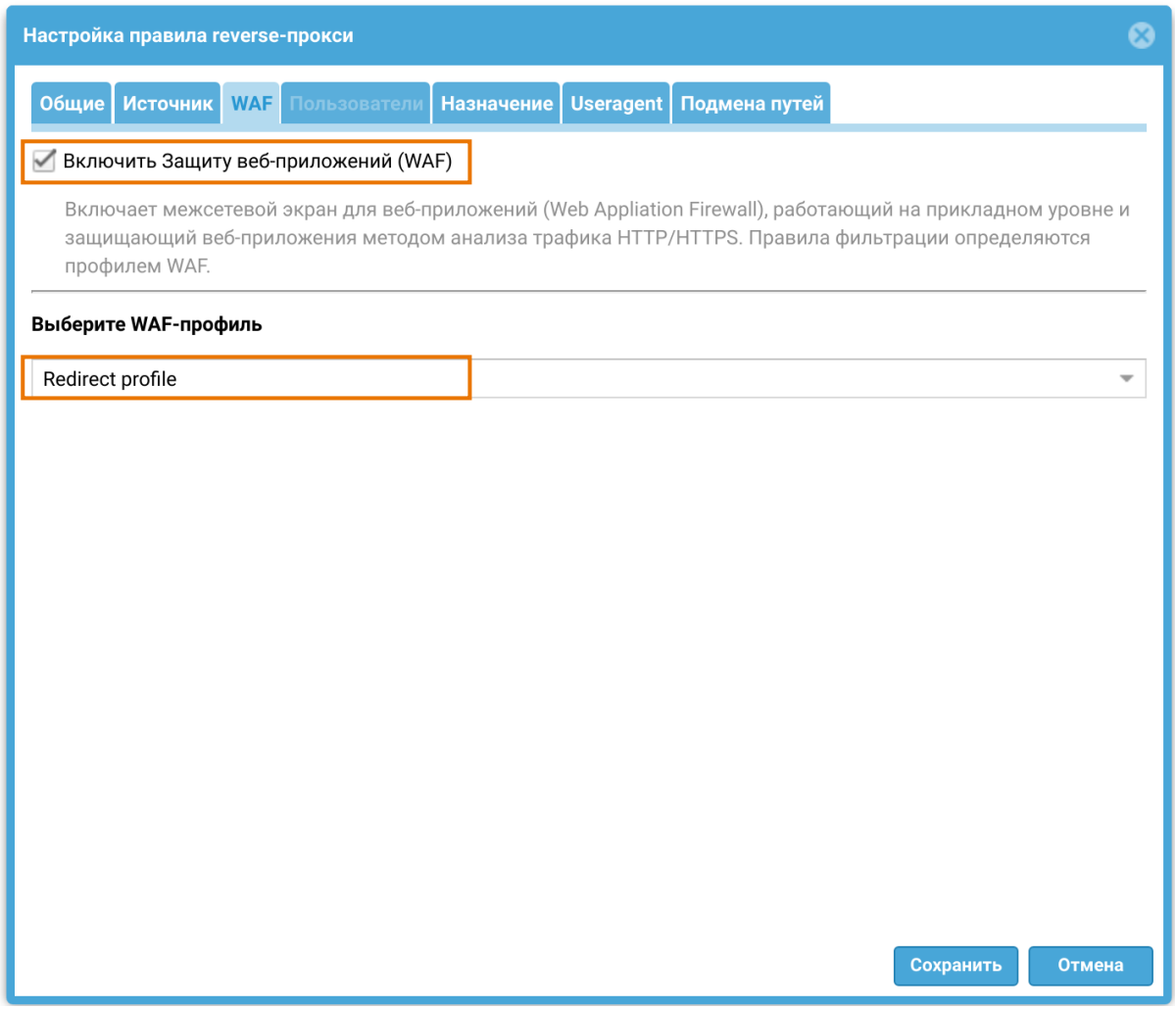


4. Создадим профиль WAF.

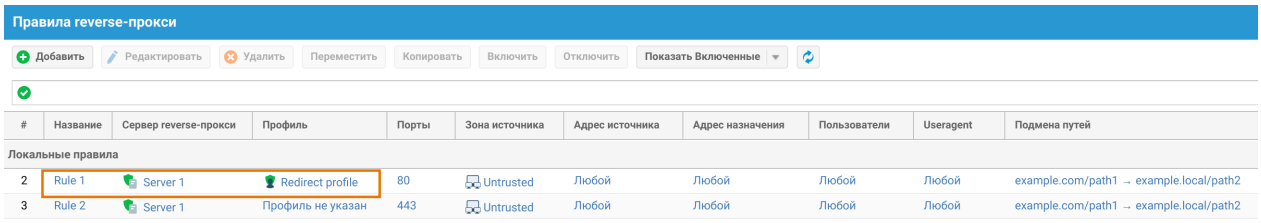
В разделе веб-консоли **WAF → Профили** создадим профиль Redirect profile, содержащий созданный ранее персональный слой Redirect:



5. Добавим созданный профиль WAF в правило reverse-прокси Rule 1 (с портом 80):



Настройка завершена:



БИБЛИОТЕКИ ЭЛЕМЕНТОВ

Описание

Данный большой раздел содержит в себе все записи, адреса-сайтов, IP-адреса, шаблоны 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, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Более подробно о лицензии на продукт вы можете прочитать в главе Лицензирование.

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.

Наименование	Описание
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.
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.

Наименование	Описание
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

Наименование	Описание
	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".

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.

Сервисы

Раздел сервисы содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил NGFW. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервис.	Нажать на кнопку **Добавить**, дать сервису название, ввести комментарий.
Шаг 2. Указать протокол и порт.	Нажать на кнопку **Добавить**, выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. Для указания диапазона портов можно использовать — (тире), например, 33333—33355.

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.
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.
Шаг 2. Указать адрес обновления списка (не обязательно).	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

Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл **list.txt** со списком адресов.
	Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например:
	`x.x.x.x`
	`y.y.y.y`
	`z.z.z.z`

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/ или ftp://x.x.x.x/.** 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".

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. • 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.

Наименование	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".

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.**
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.

Наименование	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".

Списки URL

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет собственные обновляемые списки. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе Лицензирование.

Наименование	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	Данный 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	Данный список содержит URL фишинговых сайтов.
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru.

Наименование	Описание
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru.

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В разделе **Библиотеки → Списки URL** нажать на кнопку **Добавить**, задать название нового списка. Выбрать **Тип** списка — **Локальный** или **Обновляемый**. Для обновляемого списка указать **URL обновления** и настроить **Расписание скачивания обновлений**. Установить 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 для использования в правилах DNS-фильтрации. Категория списка задается при его создании. Изменить категорию после создания списка нельзя.
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «$» и «*»: «*» — любое количество любых символов «^» — начало строки «$» — конец строки Символы «?» и «#» не могут быть использованы.
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Фильтрация контента.

Если URL-запись начинается с http://, «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S)

фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Внимание!

Спецсимволы не работают в списках-исключениях для блокировки рекламы. В этих списках применение спецсимволов не рекомендуется.

Если вы хотите заблокировать точный адрес, используйте символы «^» и «$»:

^http://domain.com/exacturl$

Для блокирования точного URL всех дочерних папок используйте символ «^»:

^http://domain.com/exacturl/

Для блокирования домена со всеми возможными URL используйте запись такого вида:

domain.com

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
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://qwertyahoo.com/
^mail.yahoo.com$	Заблокирован только mail.yahoo.com	Заблокированы только: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/$	Ничего не заблокировано	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
^http://finance.yahoo.com/personal-finance/$	Ничего не заблокировано	Заблокирован только: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не заблокировано	Заблокированы: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все межсетевые экраны UserGate. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл **list.txt** со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
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 и указать URL для обновления.	На каждом NGFW создать список URL. 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/ или ftp://x.x.x.x/.**

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".

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.

Наименование	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 DCSP для QoS.	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

Шаблоны страниц

С помощью шаблонов страниц администратор может управлять видом страницы блокировки и страницы авторизации Captive-портала. Администратор может использовать разные шаблоны для разных правил фильтрации контента и правил Captive-портала.

NGFW поставляется с различными типами шаблонов — шаблоны страниц блокировки, Captive-портала, веб-портала, инициализации TOTP и др. Они могут использованы как образцы для создания пользовательских шаблонов, например, в фирменном стиле компании или на необходимом языке.

Наименование	Описание
Шаблоны **Blockpage (EN)** и **Blockpage (RU)**	Стандартные шаблоны блокировки на английском и русском языках.
Шаблоны **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.
Шаблоны **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 принятия пользователем правил политики доступа. При успешной авторизации пользователь получает доступ в Интернет.
Шаблоны **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 с подтверждением пользователя письмом по email. Для корректной работы данных шаблонов необходимо настроить раздел **Оповещения** в Captive-профиле.
Шаблон **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 данных шаблонов необходимо настроить раздел **Оповещения** в Captive-профиле.
Шаблон **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 принятия пользователем правил политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы данного шаблона требуется установить метод **Принять политику** в качестве метода аутентификации в Captive-профиле.
Шаблоны **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.

Наименование	Описание
Шаблоны **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.**
Шаблоны **FTP client (EN)** и **FTP client (RU)**	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP.
Шаблоны **SSL VPN (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы веб-портала.
Шаблоны **SSL VPN RDP (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал.
Шаблоны **SSL VPN SSH (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал.
Шаблоны **TOTP INIT PAGE (EN)** и **TOTP INIT PAGE (RU)**	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей.

Для создания собственного шаблона необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Экспортировать существующий шаблон, поставляемый по умолчанию.	Выбрать один из существующих шаблонов, нажать на кнопку **Экспорт** и сохранить шаблон в файле.
Шаг 2. Изменить экспортированный шаблон.	Используя редактор, изменить содержание шаблона. Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут испортить внутреннюю структуру шаблона. Используйте простые редакторы текста.
Шаг 3. Создать новый шаблон.	Нажать на кнопку **Добавить**, выбрать соответствующий тип шаблона, задать название шаблону и сохранить его.
Шаг 4. Импортировать измененный на шаге 2 шаблон.	Выделить вновь созданный шаблон, нажать на кнопку **Импорт** и выбрать файл с измененным шаблоном.

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.

Наименование	Описание
Шаг 2. Добавить категории.	Выделить созданную группу и в панели **Категории**, нажать на кнопку **Добавить** и выбрать необходимые категории из списка.

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. Они используются в межсетевом экране для анализа трафика на 7 уровне модели OSI для контроля сетевого трафика.

Типы сигнатур приложений

В UserGate могут использоваться два типа сигнатур приложений:

- Проприетарные сигнатуры приложений.
- Кастомизированные сигнатуры приложений.

Проприетарные сигнатуры приложений создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В списке сигнатур в библиотеке такие сигнатуры помечаются в колонке **Владелец** как: @UserGate.

Кастомизированные сигнатуры приложений создаются самим пользователем. Для создания пользовательской сигнатуры приложений в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Приложения** и нажать на кнопку **Добавить**. Далее заполняются поля с параметрами сигнатуры, описываются признаки сигнатуры с помощью синтаксиса UASL.

Необходимо заполнить следующие поля:

Наименование	Описание
Тип	Тип сигнатуры; • Приложение. • Протокол. • Поддержка — вспомогательная сигнатура.
Id	ИИдентификатор сигнатуры. Если поле оставить пустым, то будет выдан свободный id из пользовательского пула.
Название	Название сигнатуры.
Описание	Описание сигнатуры.
Уровень угрозы	

Наименование	Описание
	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • **1** — очень низкий. • **2** — низкий. • **3** — средний. • **4** — высокий. • **5** — очень высокий.
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

Наименование	Описание
UASL	Описание признаков сигнатуры с помощью синтаксиса UASL.

Сигнатуры приложений, зависимые от типа протокола

Некоторые сигнатуры приложений для своей работы в профилях приложений требуют наличия 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,

Сигнатура протокола	ID зависимых сигнатур
	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, 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

Некоторые сигнатуры зависят не только от сигнатуры протокола, но и от 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 тол ько

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
				сигнатуру протокола (id=19).
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

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
				необходимо добавить сигнатуру протокола (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).

Профили приложений

Назначение профиля приложений

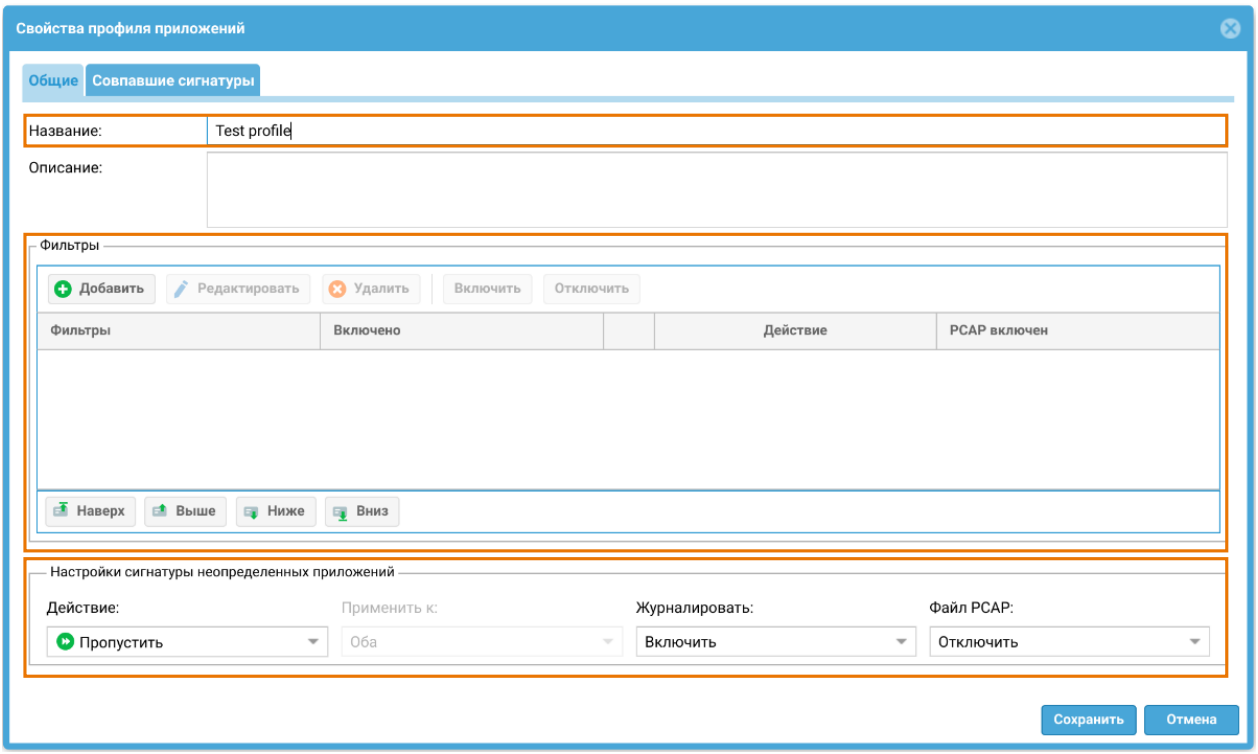
Профиль приложений позволяет создавать динамический набор сигнатур приложений, предназначенный для анализа трафика на 7 уровне модели OSI. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. При изменении библиотеки сигнатур приложений профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определятся 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**.

Необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля приложений:



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.

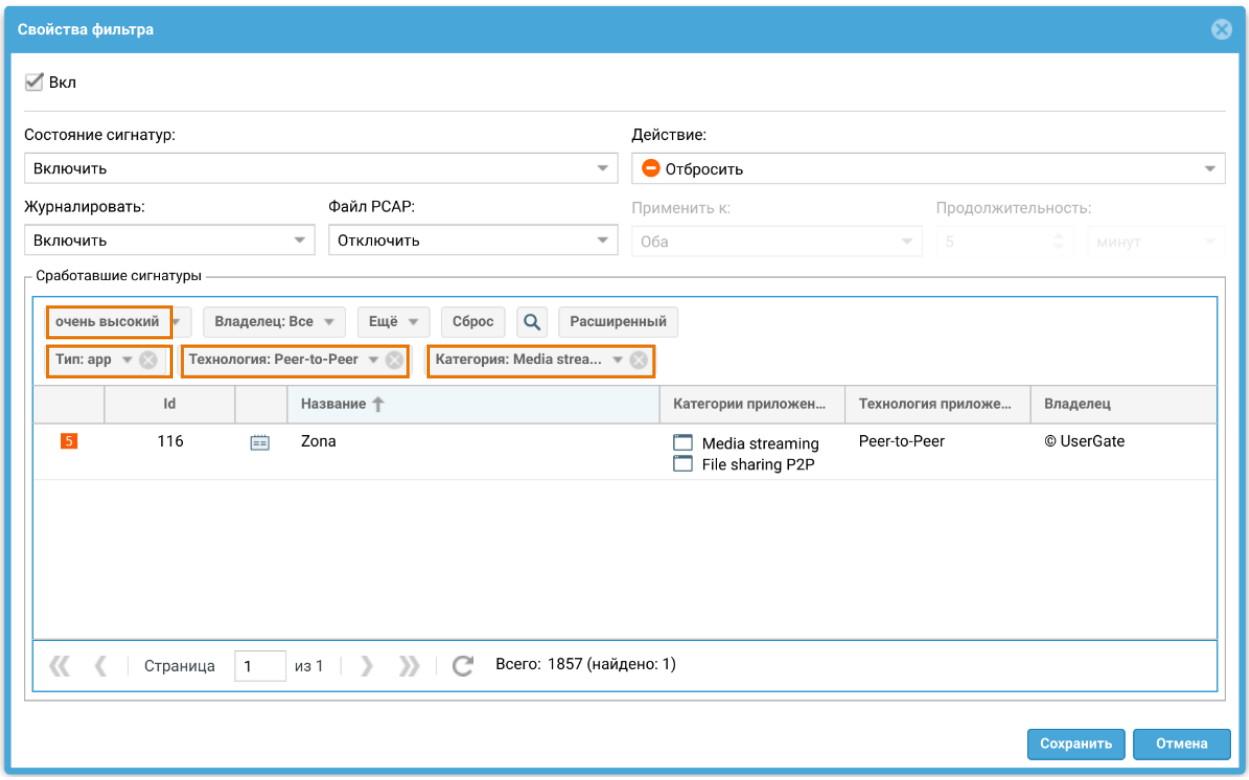
4. В области **Настройки сигнатуры неопределенных приложений** определяются действия с трафиком, который не был определен сигнатурами данного профиля.

5. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур приложений, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над приложениями, отфильтрованными этими сигнатурами.

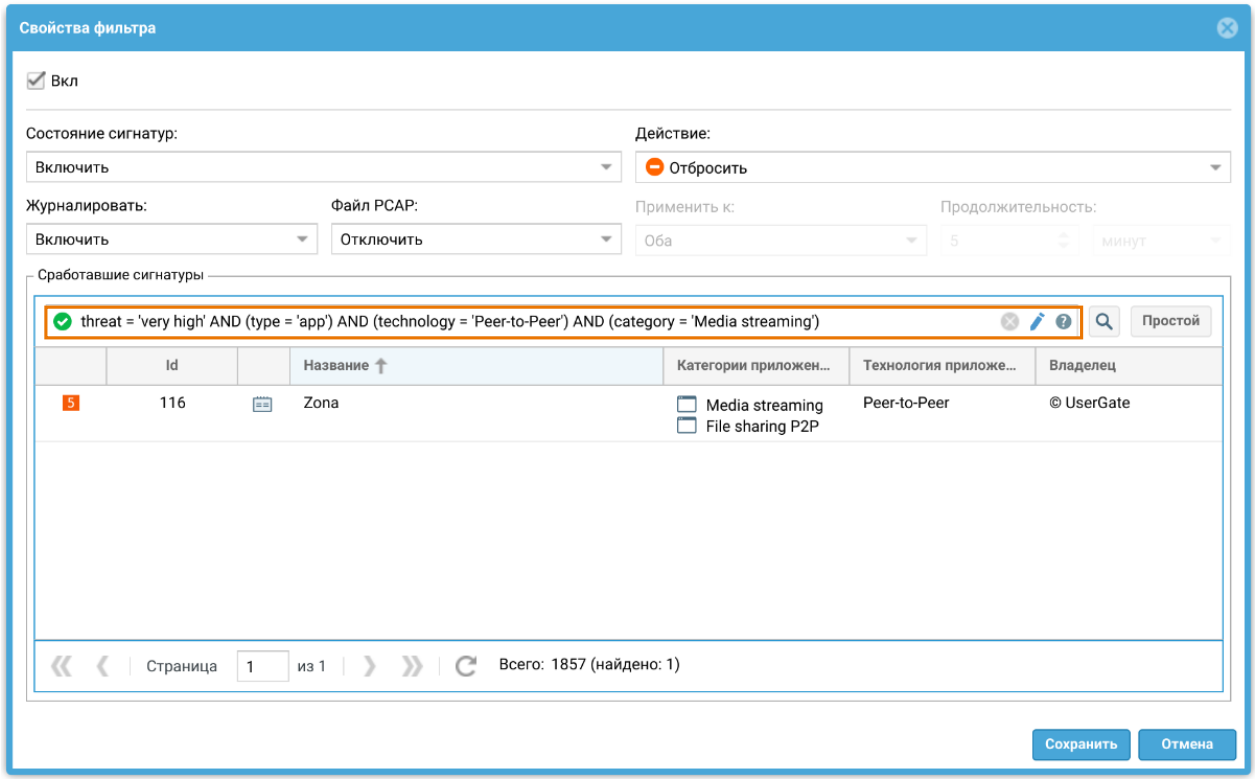
Настройка фильтров сигнатур в профиле приложений

Для создания фильтра сигнатур приложений необходимо в области **Фильтры** нажать кнопку **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:

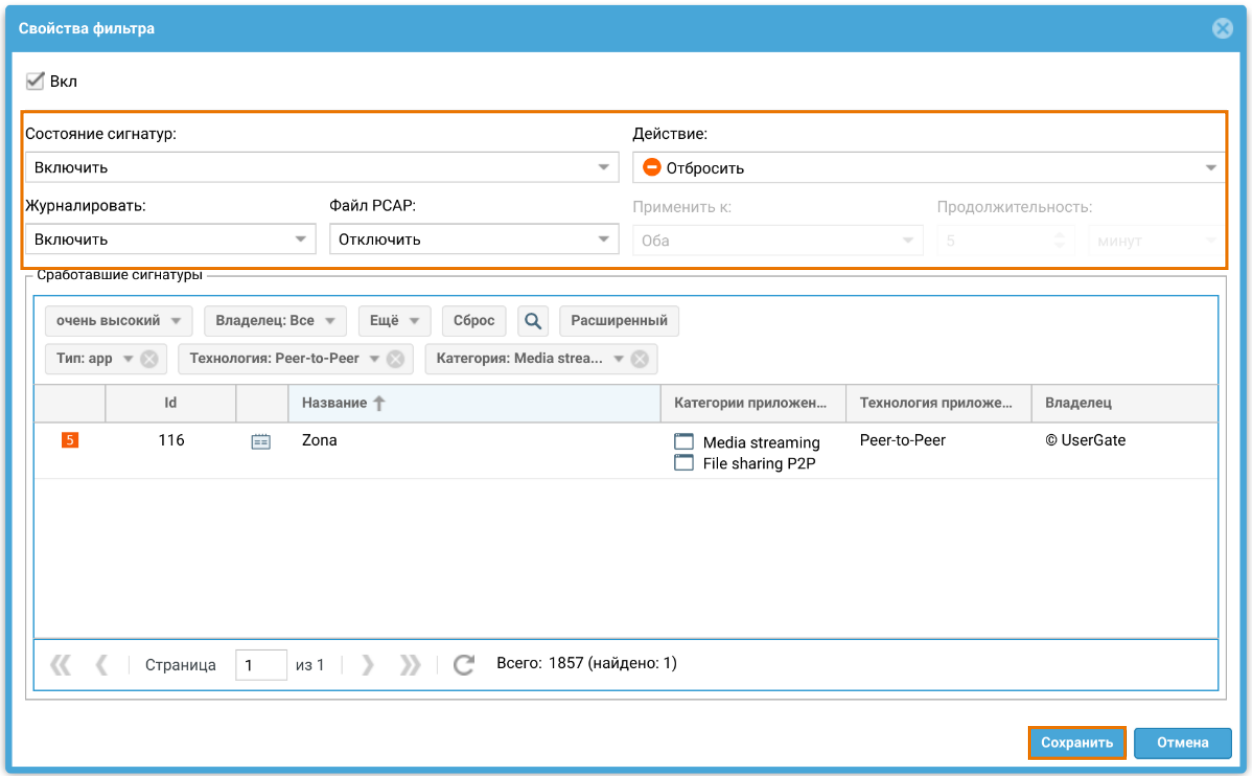


Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого необходимо нажать кнопку **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:



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 pcap-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.



Для сохранения созданного фильтра необходимо нажать кнопку **Сохранить**.

В одном профиле может быть создано сразу несколько фильтров.

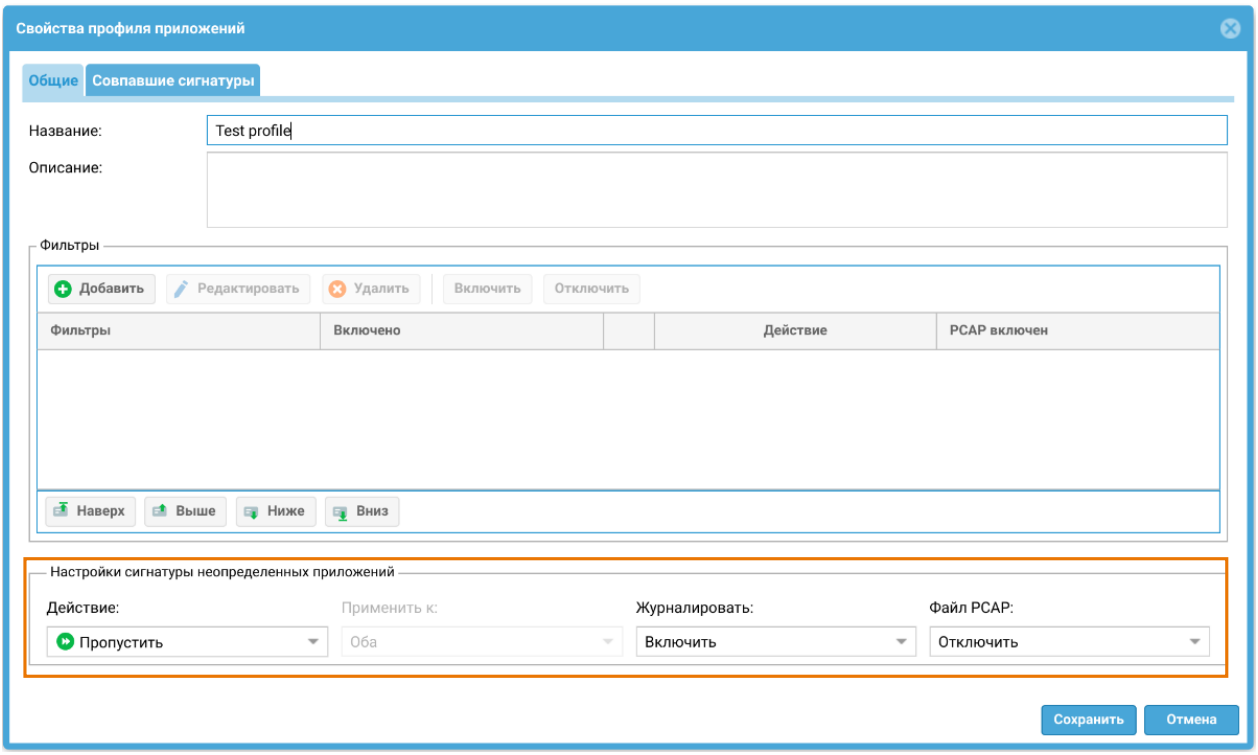
Фильтры в профиле работают по правилу логического ИЛИ.

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.



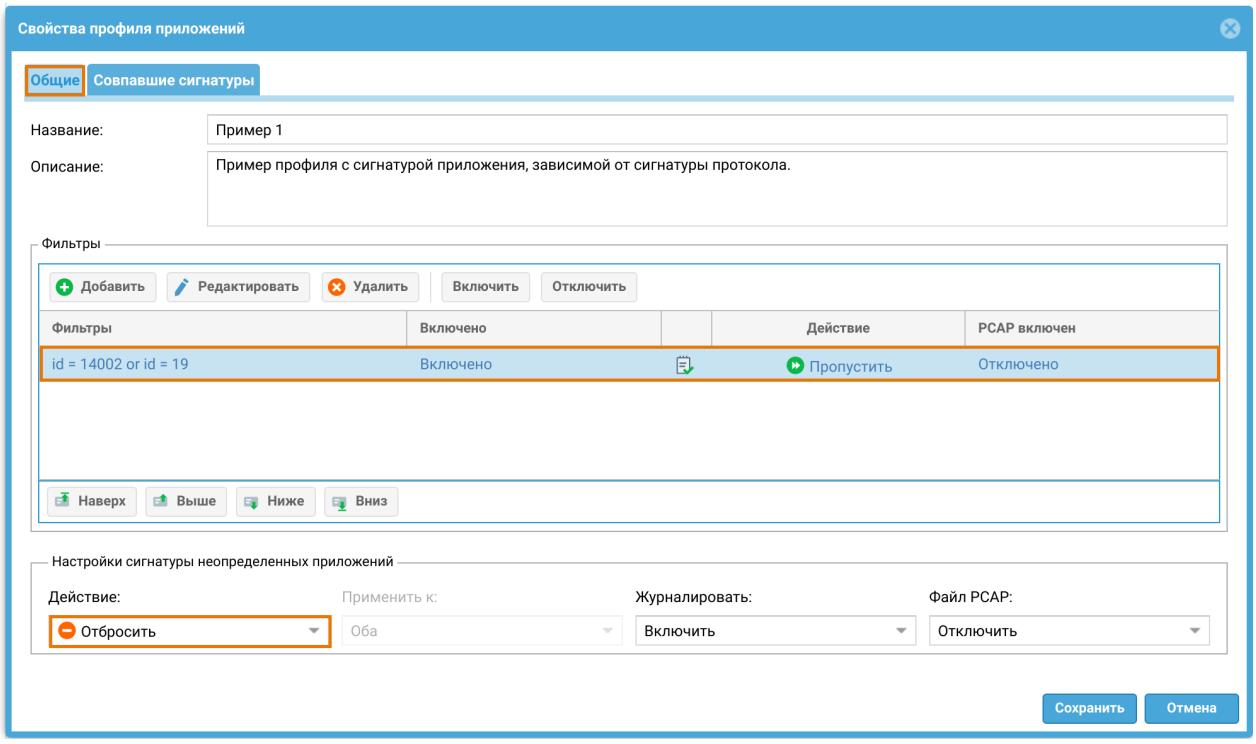
Действия могут быть следующие: пропустить, отбросить, отбросить с разрывом TCP соединения.

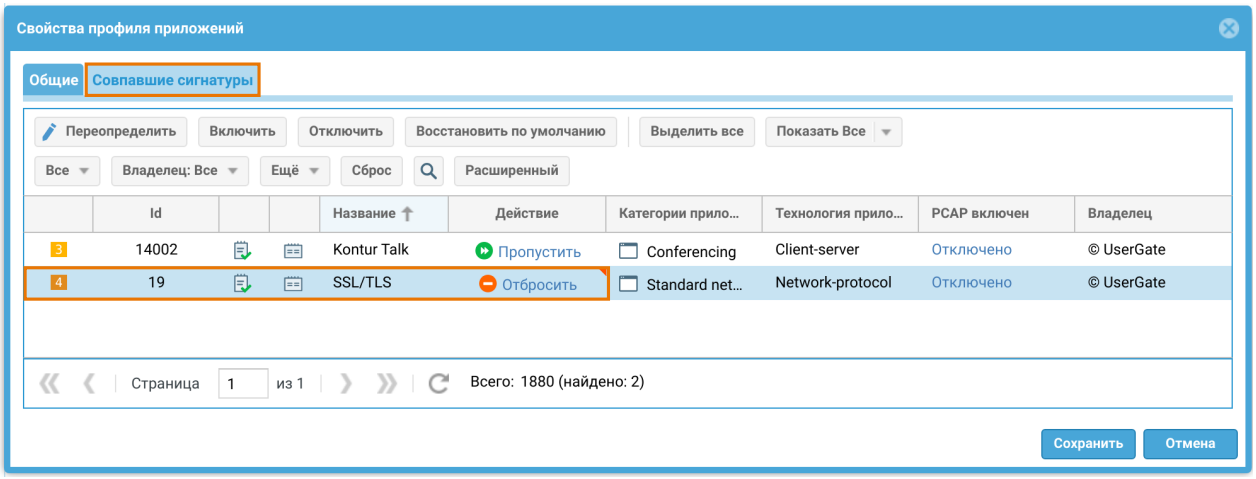
Примеры настроек профилей приложений

Пример 1. Профиль приложения с сигнатурой, зависимой от сигнатуры протокола

Списки сигнатур, зависимых 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:





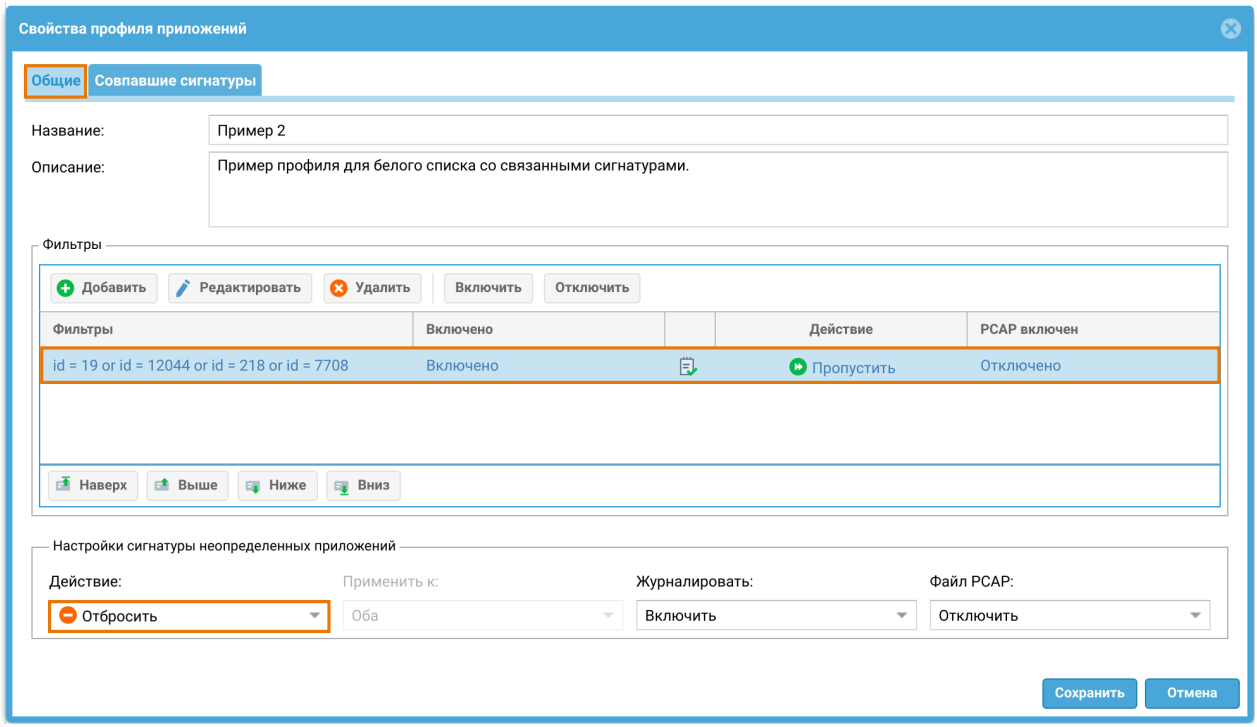
Сигнатура SSL/TLS (id=19) необходима для работы сигнатуры Kontur Talk, поэтому она добавляется в профиль, но для нее выставляется действие **Отбросить**, чтобы не пропускать посторонний трафик по протоколам SSL/TLS. Для неидентифицированного трафика также устанавливается действие **Отбросить**.

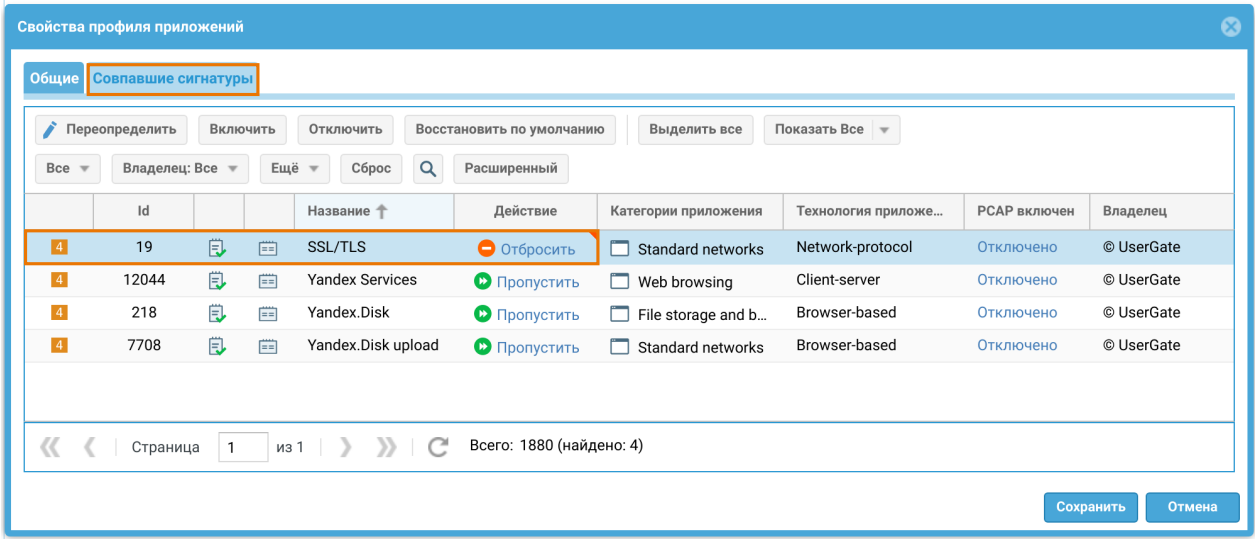
Пример 2. Профиль для белого списка со связанными сигнатурами

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:



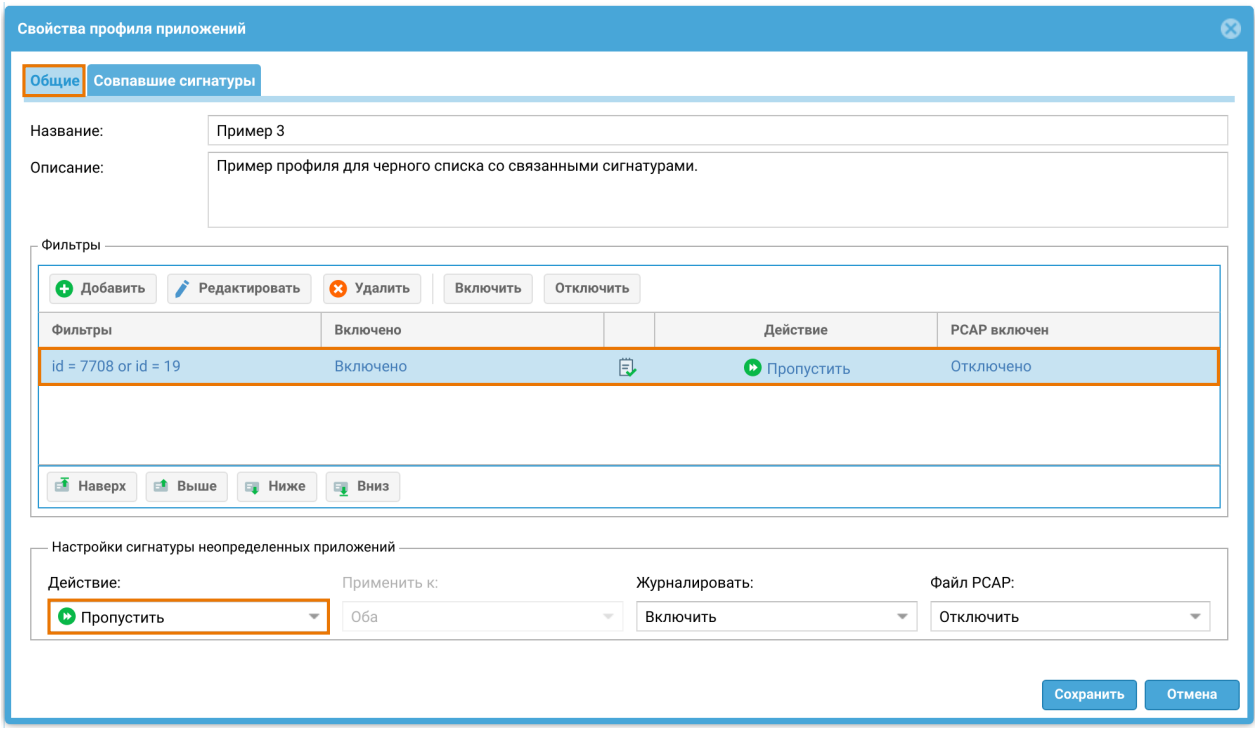


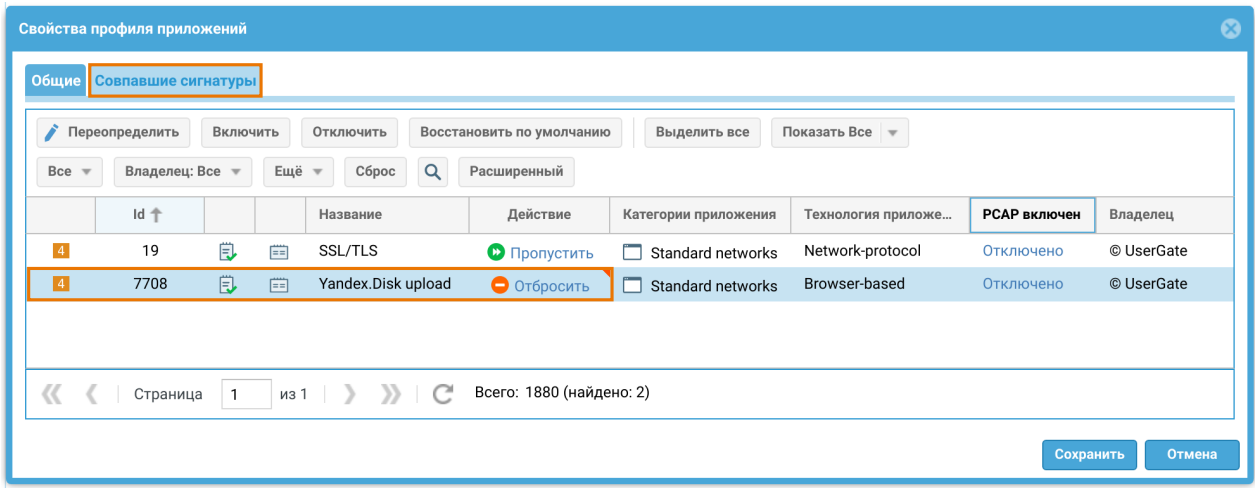
Таким образом разрешается доступ и загрузка файлов на Yandex Disk, а весь остальной трафик помечается как неидентифицированный и отбрасываться либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

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:





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.

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 неидентифицированного трафика.

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 СОВ/L7 IP-адреса** (подробнее читайте в разделе Заблокированные СОВ/L7 IP-адреса).

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.

Наименование	Описание
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.

Наименование	Описание
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. 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".

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. 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

Наименование	Описание
	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".

Сигнатуры СОВ

Сигнатуры СОВ представляют собой некоторую совокупность строк (паттернов) и семантических выражений (фильтров, модификаторов, иных конструкций), которые позволяют идентифицировать/пометить сетевую атаку и предпринять определенные действия. Сигнатуры добавляются в профили СОВ и используются в правилах межсетевого экрана для обнаружения вторжений и защиты сети.

В UserGate могут использоваться два типа сигнатур СОВ:

- Проприетарные сигнатуры.
- Кастомизированные пользовательские сигнатуры.

Проприетарные сигнатуры СОВ создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В списке сигнатур в библиотеке такие сигнатуры помечаются в колонке **Владелец** как: @UserGate. В проприетарных сигнатурах пользователь может перенастроить следующие параметры:

- Включение/отключение сигнатуры..
- Журналирование сигнатуры.
- Запись в pcap-файл, если сигнатура сработала.

- Предпринимаемое действие, если сигнатура сработала, т.е. была найдена в трафике. Действия могут быть следующие: пропустить пакет, отбросить пакет, отбросить пакет с разрывом TCP соединения, блокировать IP-адрес источника и/или назначения.

После изменения настроек параметров по умолчанию у проприетарных сигнатур в колонке **Статус** будет указано: **Изменено.** Измененные пользователем настройки проприетарных сигнатур СОВ можно вернуть в первоначальное состояние, для этого в веб-консоли администратора в разделе **Библиотеки → Сигнатуры СОВ** нужно выделить сигнатуру в списке и нажать кнопку **Восстановить по умолчанию**.

Кастомизированные сигнатуры СОВ создаются самим пользователем.

Для создания кастомизированной сигнатуры СОВ в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Сигнатуры СОВ** и нажать на кнопку **Добавить**. Далее заполняются поля с параметрами сигнатуры. Признаки сетевых уязвимостей описываются с помощью синтаксиса языка UASL (UserGate Application and Security Language).

При создании кастомизированной сигнатуры необходимо заполнить следующие поля:

Наименование	Описание
Включено	Индикатор включения/выключения сигнатуры.
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.
Класс	Класс сигнатуры определяет тип атаки, которая описывается данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например,

Наименование	Описание
	обнаружение установления сессии TCP. Список классов может быть пополнен. • **arbitrary-code-execution** – попытка запуска произвольного кода. • **attempted-admin** – попытка получения административных привилегий. • **attempted-dos** – попытка совершения атаки Denial of Service. • **attempted-recon** – попытка атаки, направленной на утечку данных. • **attempted-user** – попытка получения пользовательских привилегий. • **bad-unknown** – потенциально плохой трафик. • **buffer overflow** – попытка атаки, использующей принцип перепонения буфера. • **command-and-control** – попытка общения с C&C центром • **default-login-attempt** – попытка логина с именем/паролем по умолчанию. • **denial-of-service** – обнаружена атака Denial of Service. • **exploit-kit** – обнаружен exploit kit • **information disclosure** – утечка данных. • **memory corruption** – попытка атаки, использующей принцип повреждения памяти. • **misc-activity** – прочая активность. • **misc-attack** – обнаружена атака. • **network-scan** – сканирование сети. • **path traversal** – попытка атаки, использующей принцип обхода пути к файлам на сервере, на котором работает приложение. • **policy-violation** – нарушение сетевых политик. • **protocol-command-decode** – обнаружение необычной команды протокола. • **shellcode-detect** – обнаружен исполняемый код. • **string-detect** – обнаружена подозрительная строка. • **successful-recon-limited** – утечка информации • **suspicious-login** – попытка логина с использованием подозрительного имени пользователя. • **system-call-detect** – попытка использования системных вызовов. • **targeted-activity** – обнаружение направленной активности.

Наименование	Описание
	• **trojan-activity** – обнаружен сетевой троян. • **uncaught exception** – необрабатываемое приложением исключение.
Категория	Категория сигнатуры - группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • **adware pup** – нежелательное рекламное ПО. • **attack_response** – сигнатуры, определяющие ответы на известные сетевые атаки. • **bruteforce** – атака типа brutr force. • **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. • **icmp** – известные уязвимости протокола icmp. • **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. • **p2p** – идентификация трафика точка-точка (peer-to-peer). • **phishing** – сигнатуры известных phishing атак. • **policy** – нарушение информационной безопасности. • **pop3** – известные уязвимости протокола POP3. • **rpc** – известные уязвимости протокола RPC. • **scada** – известные уязвимости протокола SCADA. • **scan** – сигнатуры, определяющие попытки сканирования сети на известные приложения. • **shellcode** – сигнатуры, определяющие известные попытки запуска программных оболочек. • **sip** – известные уязвимости протокола SIP. • **smb** – известные уязвимости протокола SMB. • **smtp** – известные уязвимости протокола SMTP. • **snmp** – известные уязвимости протокола SNMP.

Наименование	Описание
	• **sql** – известные уязвимости SQL. • **telnet** – известные попытки взлома по протоколу telnet. • **tftp** – известные уязвимости протокола TFTP. • **user_agents** – сигнатуры подозрительных Useragent. • **voip** – известные уязвимости протокола VoIP. • **web_client** – сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • **web_server** – сигнатуры, определяющие известные попытки взлома различных веб-серверов. • **web_specific_apps** – сигнатуры, определяющие известные попытки взлома различных веб приложений. • **worm** – сигнатуры, определяющие сетевую активность известных сетевых червей.
Операционная система сигнатуры	Операционная система, для которой разработана данная сигнатура. • **Windows** • **Linux** • **BSD** • **Mac OS** • **Solaris** • **Cisco** • **IOS** • **Android** • **Other**
CVE	Идентификатор уязвимоси по реестру CVE.
BDU	Идентификатор уязвимости по реестру BDU.
URL	Опциональная ссылка на ресурс с описанием уязвимости.
UASL	Описание признаков сигнатуры с помощью синтаксиса UASL.
Настройки	• **Действие** – реакция на срабатывание сигнатуры. Определены следующие значения:: ◦ **Нет** – действие не определено.

Наименование	Описание
	◦ **Пропустить** – пропустить пакет. ◦ **Отбросить** – отбросить пакет. ◦ **Сбросить** – отбросить пакет с разрывом TCP соединения (отправка TCP reset). ◦ **Блокировать IP** – блокировать IP-адрес источника и/или назначения. • **Журналировать**: ◦ **Включить** – включить запись событий в журнал. ◦ **Отключить** – отключить запись событий в журнал. • **Файл pcap** – трассировка срабатывания сигнатуры с записью в файл формата pcap. ◦ **Включить** – включить трассировку. ◦ **Отключить** – отключить трассировку. • **Применить к** – применимость действий типа **Ресет** или **Блокировать IP** на срабатыване сигнатуры: ◦ **Источник** – действия **Ресет** или **Блокировать IP** применяются к адресу источника отправления пакетов. ◦ **Назначание** – действия **Ресет** или **Блокировать IP** применяются к адресу назначения отправления пакетов. ◦ **Оба** – действия **Ресет** или **Блокировать IP** применяются и к источнику, и к назначению. • **Продолжительность** – длительность блокировки для действия **Блокировать IP**.

Профили СОВ

Назначение профиля СОВ

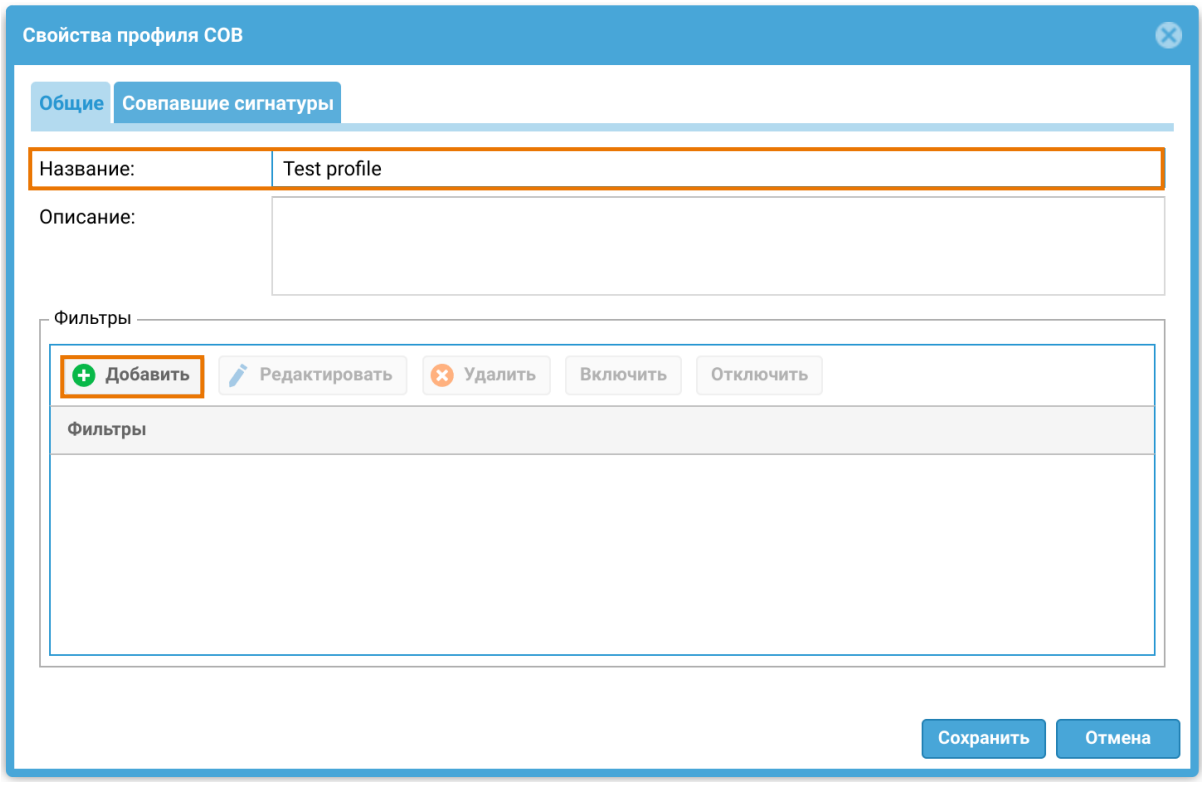
Профиль СОВ позволяет создавать динамический набор сигнатур СОВ, предназначенный для обнаружения вторжений и защиты определенных сервисов. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. Для фильтрации используются как описательные поля сигнатур, так и настройки. В итоге получается, что при изменении библиотеки сигнатур профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определяться действия, которые будут выполняться над трафиком, отфильтрованным сигнатурами.

Создание профиля СОВ в веб-консоли администратора

В веб-консоли администратора профили СОВ создаются в разделе **Библиотеки → Профили СОВ**.

Необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля:



1. В поле **Название** указать название создаваемого профиля.

2. В поле **Описание** опционально указать назначение профиля.

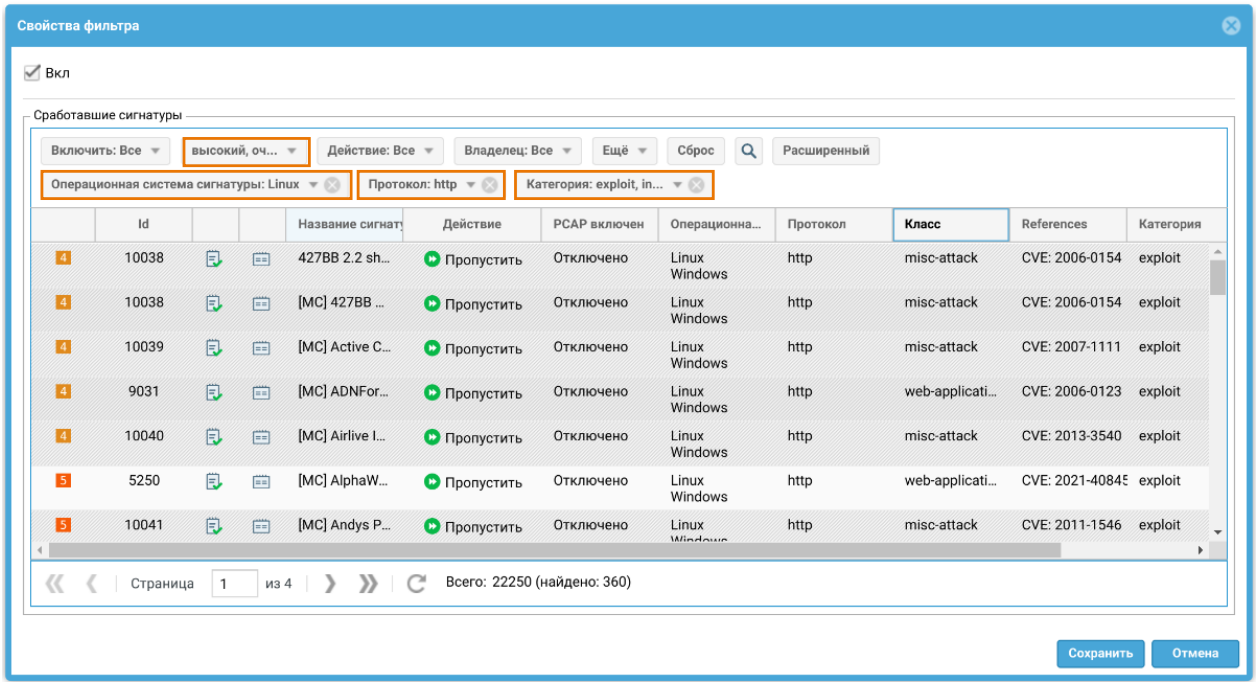
3. В области **Фильтры** добавляются фильтры для выбора необходимых сигнатур из библиотеки.

4. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур СОВ, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над трафиком, отфильтрованным этими сигнатурами.

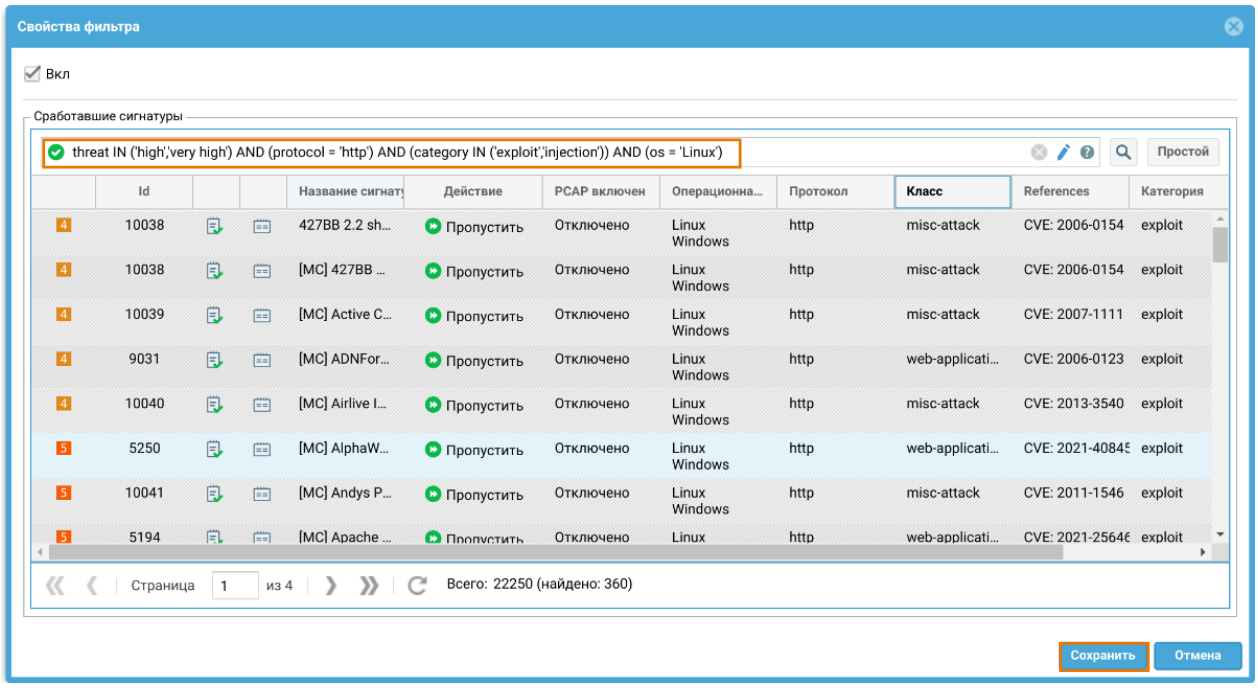
Настройка фильтров сигнатур в профиле СОВ

Для создания фильтра сигнатур необходимо в области **Фильтры** нажать кнопку **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции 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 необходимо нажать кнопку **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:



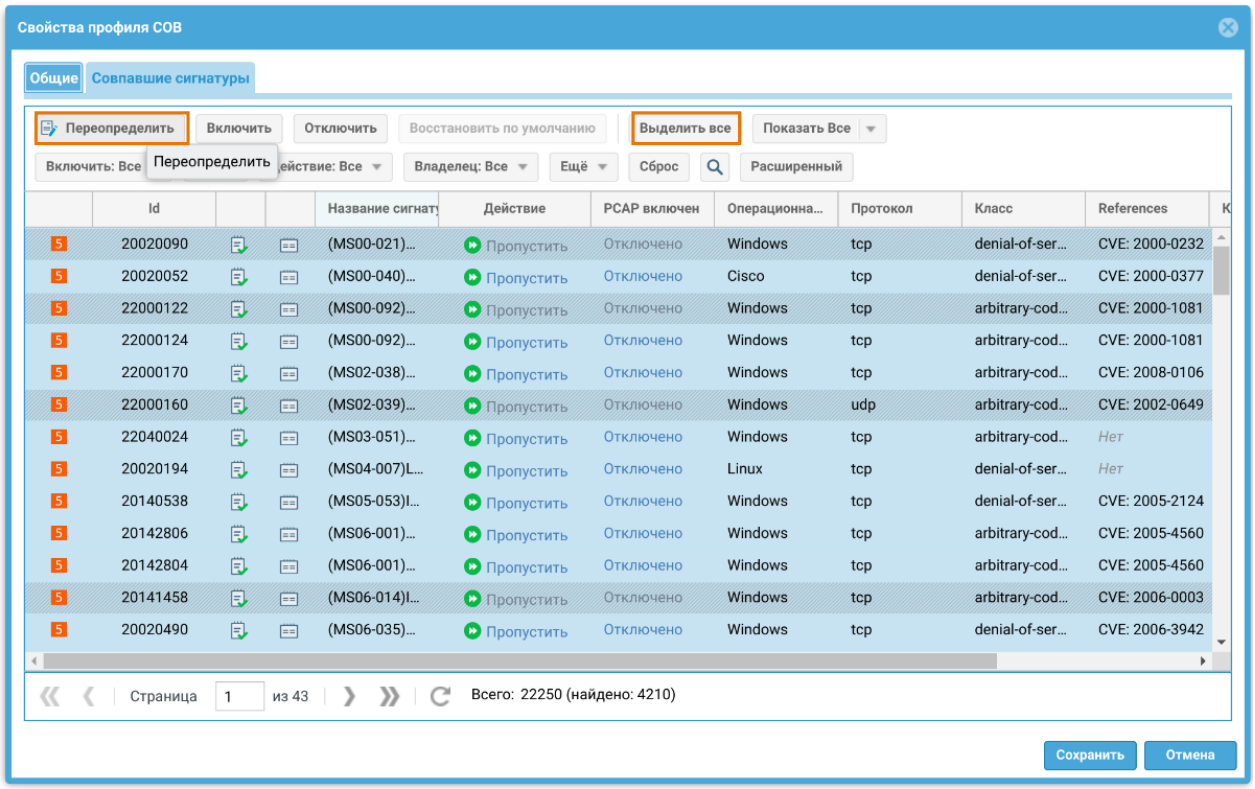
Для сохранения созданного фильтра необходимо нажать кнопку **Сохранить**.

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`.

Настройка параметров сигнатур в профиле СОВ

В рамках профиля можно переопределить параметры сигнатур, такие как действие, журналирование, запись в файл pcap, включение/отключение сигнатуры. Для этого необходимо выбрать нужные сигнатуры в списке совпавших сигнатур и нажать кнопку **Переопределить** в панели инструментов.



Изменение настроек сигнатур в профиле СОВ имеет более высокий приоритет, чем настройки этих же сигнатур на странице сигнатур СОВ. Измененные настройки сигнатур СОВ можно вернуть в первоначальное состояние, для этого нужно выделить сигнатуру в списке сигнатур профиля и нажать кнопку **Восстановить по умолчанию** в панели инструментов профиля.

Применение профилей СОВ

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 СОВ 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 СОВ, 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 СОВ, если была включена опция

журналирования. Если ни одна из сигнатур профиля не была найдена, то трафик пропускается дальше.

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 СОВ/L7 IP-адреса** (подробнее читайте в разделе Заблокированные СОВ/L7 IP-адреса).

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.

Наименование	Описание
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.
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.

Наименование	Описание
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** — NGFWe 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.
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 CHACHA20 POLY1305 SHA256 • 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

Наименование	Описание
	• 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 DHE RSA with CHACHA20 POLY1305 SHA256 • TLS DHE RSA with DES CBC SHA • 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 ECDSA with CHACHA20 POLY1305 SHA256 • TLS ECDHE ECDSA with RC4 128 SHA • 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 ECDHE RSA with CHACHA20 POLY1305 SHA256 • TLS ECDHE RSA with RC4 128 SHA • 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 • TLS ECDH ECDSA with AES 256 GCM SHA384 • TLS ECDH ECDSA with RC4 128 SHA • 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

Наименование	Описание
	• 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 ECDH RSA with RC4 128 SHA • TLS GOST2012256 with 28147 CNT IMIT • TLS GOSTR341001 with 28147 CNT IMIT • TLS RSA PSK with 3DES EDE CBC SHA • TLS RSA PSK with AES 128 CBC SHA • TLS RSA PSK with AES 128 CBC SHA256 • TLS RSA PSK with AES 128 GCM SHA256 • TLS RSA PSK with AES 256 CBC SHA • TLS RSA PSK with AES 256 CBC SHA384 • TLS RSA PSK with AES 256 GCM SHA384 • TLS RSA PSK with RC4 128 SHA • 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 • TLS RSA with DES CBC SHA • TLS RSA with RC4 128 MD5 • TLS RSA with RC4 128 SHA • TLS SRP DSS with 3DES EDE CBC SHA • TLS SRP DSS with AES 128 CBC SHA • TLS SRP DSS with AES 256 CBC SHA • TLS SRP RSA with 3DES EDE CBC SHA • TLS SRP RSA with AES 128 CBC SHA • TLS SRP RSA with AES 256 CBC SHA
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 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.

HIP объекты

Объекты HIP позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

Примечание

После подключения к NGFW конечное устройство будет отсылать телеметрию с периодичностью в 1 минуту.

> **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; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта.

Наименование	Описание
	• **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	Ключ реестра Microsoft Windows - каталог, в котором хранятся настройки и параметры операционной системы.

Наименование	Описание
	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 → Bfd profiles** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Задать имя профиля BFD.
Detect multiplier	Определить множитель времени обнаружения. Локальная система рассчитывает время обнаружения неисправностей соединения как произведение множителя времени обнаружения, полученного от удаленной 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 приема пакетов.
Receive interval	Настроить интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами). Интервал не согласовывается между узлами. Для определения интервала каждый из узлов сравнивает свой интервал передачи с интервалом приема соседа — большее из двух значений принимается в качестве интервала передачи для этого узла.

Наименование	Описание
	Значение по умолчанию — 50 мс.
Transmit Interval	Указать интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами. Значение по умолчанию — 50 мс.
Echo receive Interval	Настроить минимальный интервал, через который данная система способна принимать echo-пакеты. Значение по умолчанию — 50 мс.
Echo transmit interval	Настроить минимальный интервал передачи, через который эта система будет способна отправлять echo-пакетов BFD. Значение по умолчанию — 50 мс.
Echo mode	Включить или выключить режим передачи **Echo mode**. По умолчанию этот режим отключен. 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 эхо-потока данных не получено, сессия объявляется нерабочей. Преимущество **Echo mode** состоит в том, что она тестирует только путь пересылки на удаленной системе. Это позволяет уменьшить задержку при прохождении маршрута и уменьшить время, затрачиваемое на обнаружения сбоев. Эхо-режим не поддерживается в многоуровневых сетях (см. RFC-5883).
Passive mode	Включить или выключить режим **Passive**. При работе в режиме **Passive** система ждет 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 вы хотите избежать отправки ненужных управляющих пакетов BFD. По умолчанию используется режим **Active**. В случае работы в режиме **Active** — узел отправляет управляющие пакеты соседнему узлу. **Важно!** Оба узла не могут работать в режиме Passive; хотя бы один из них (или оба) должен работать в режиме Active.
Minimum-ttl	Только для сеансов с несколькими переходами: настроить минимальное значение 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.

Наименование	Описание
	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 мы ожидаем только один прыжок 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 два 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.

> **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 сценариея может быть задача по ограничению на определенное время пропускной спообности для пользователя, который выбрал установленный лимит трафика.

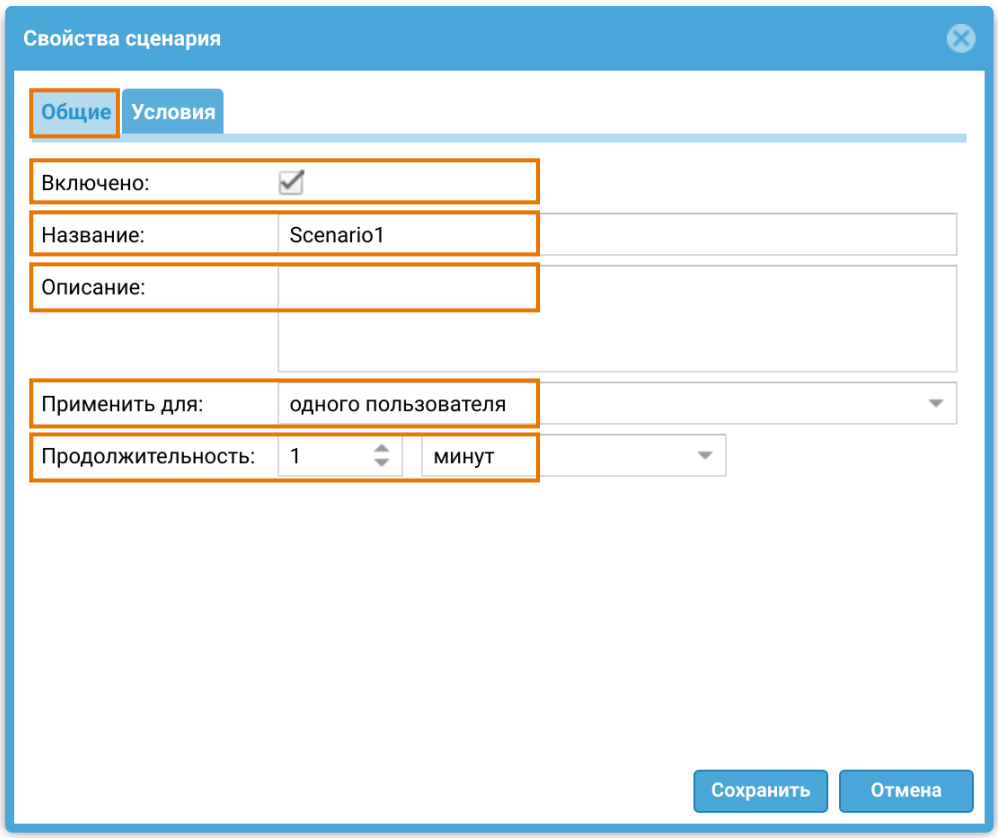
Настройка сценариев

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.

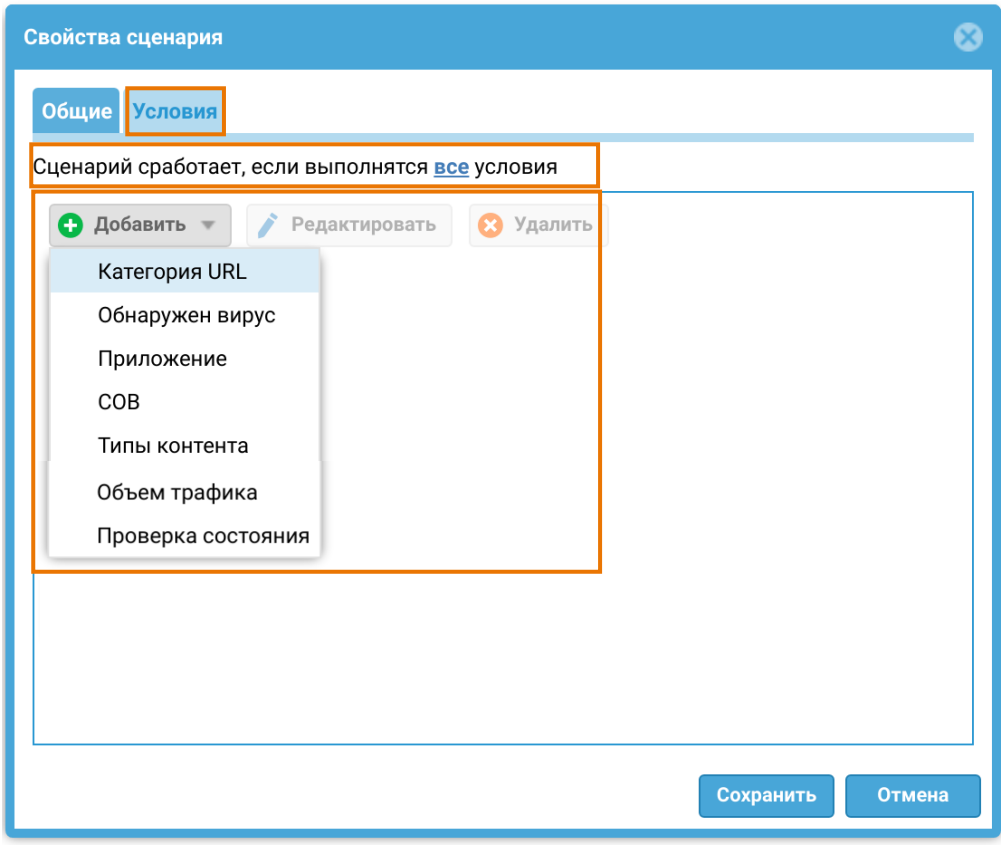
В веб-консоли администратора сценарии создаются в разделе **Библиотеки элементов → Сценарии**.

При создании сценария необходимо указать следующие параметры:



- **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.



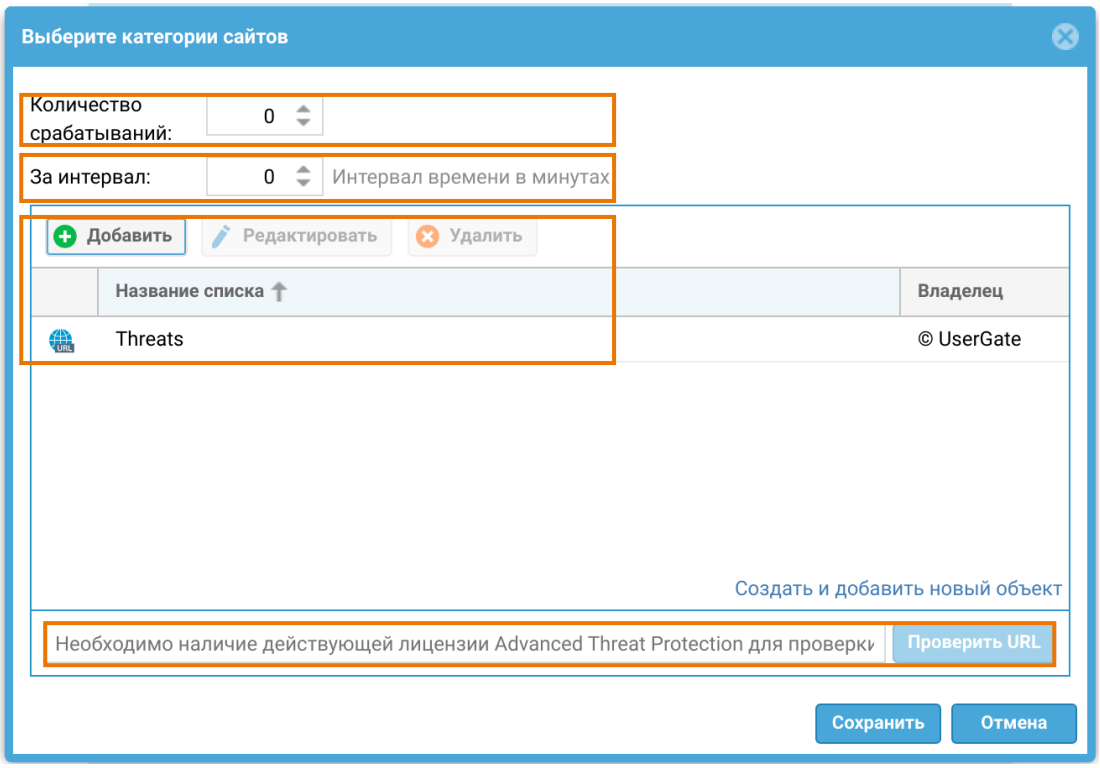
Настройка условий срабатывания сценариев

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

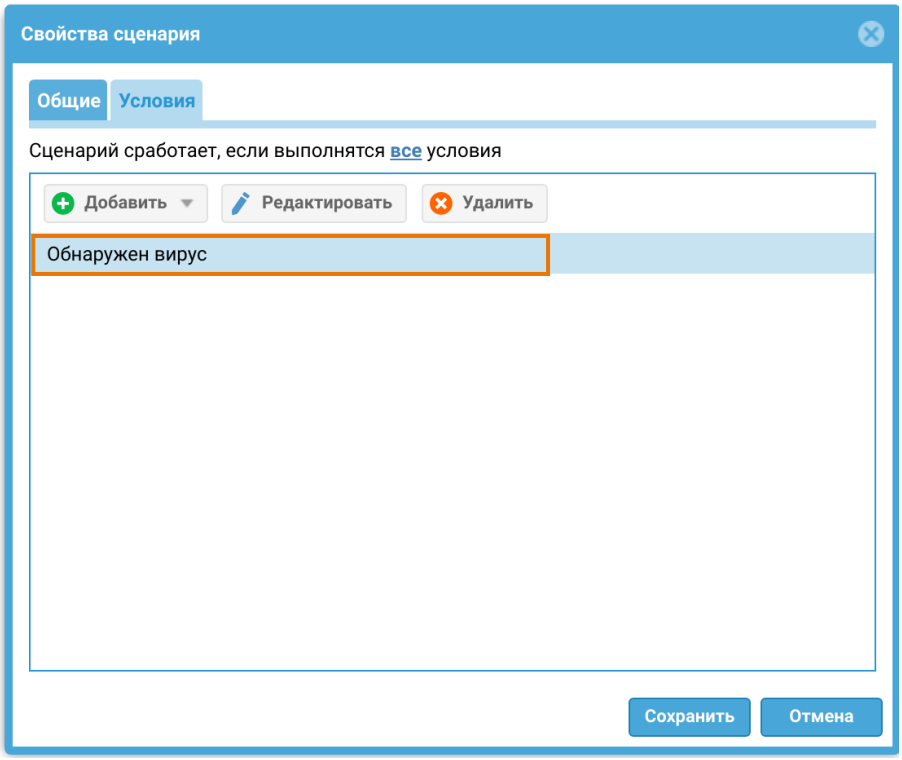
Условием срабатывания в данном случае является совпадения указанных категорий UserGate URL в трафике пользователя.



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.

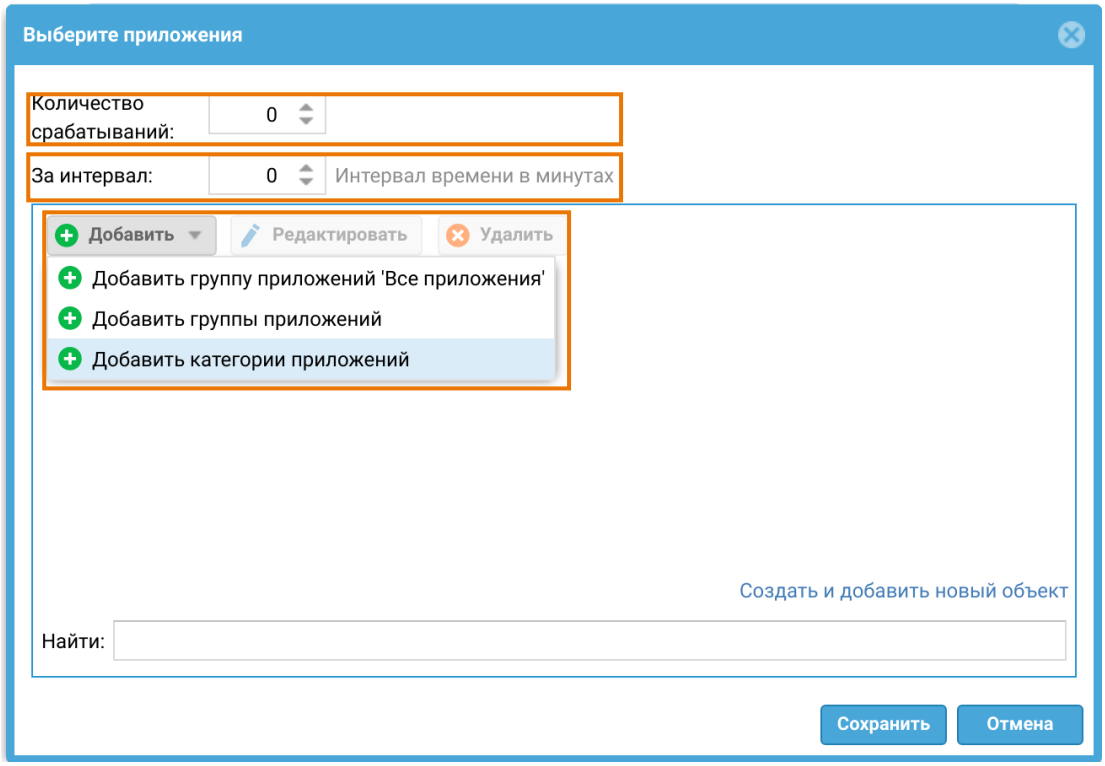
Обнаружен вирус



Условием срабатывания в данном случае является обнаружение вируса в трафике пользователя.

Приложение

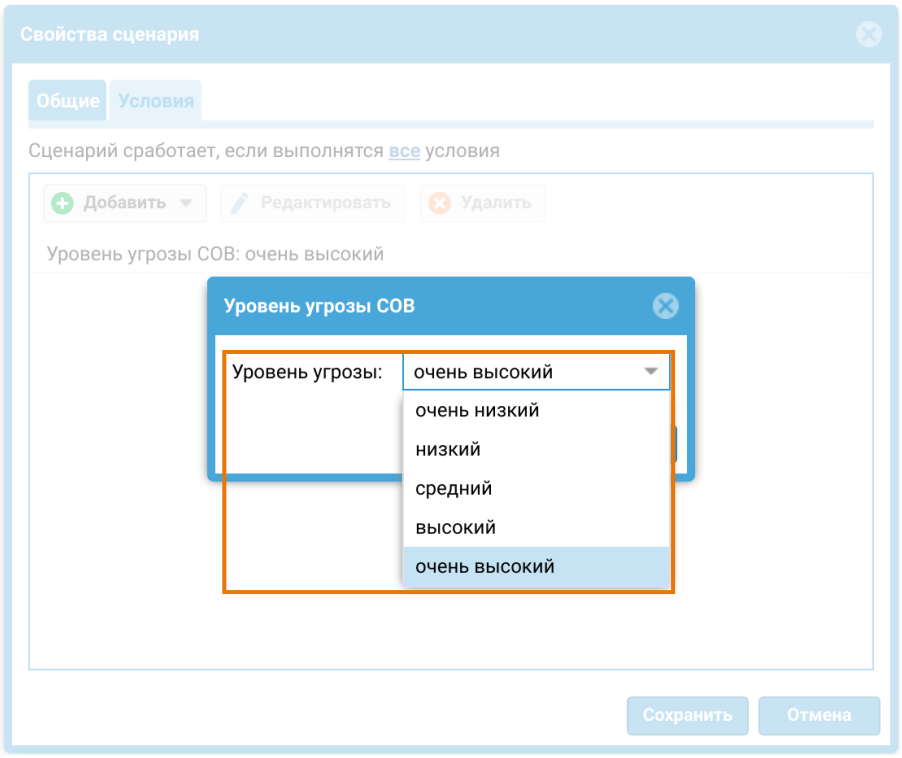
Условием срабатывания в данном случае является обнаружение определенных приложений в трафике пользователя.



В данном условии настраиваются следующие параметры:

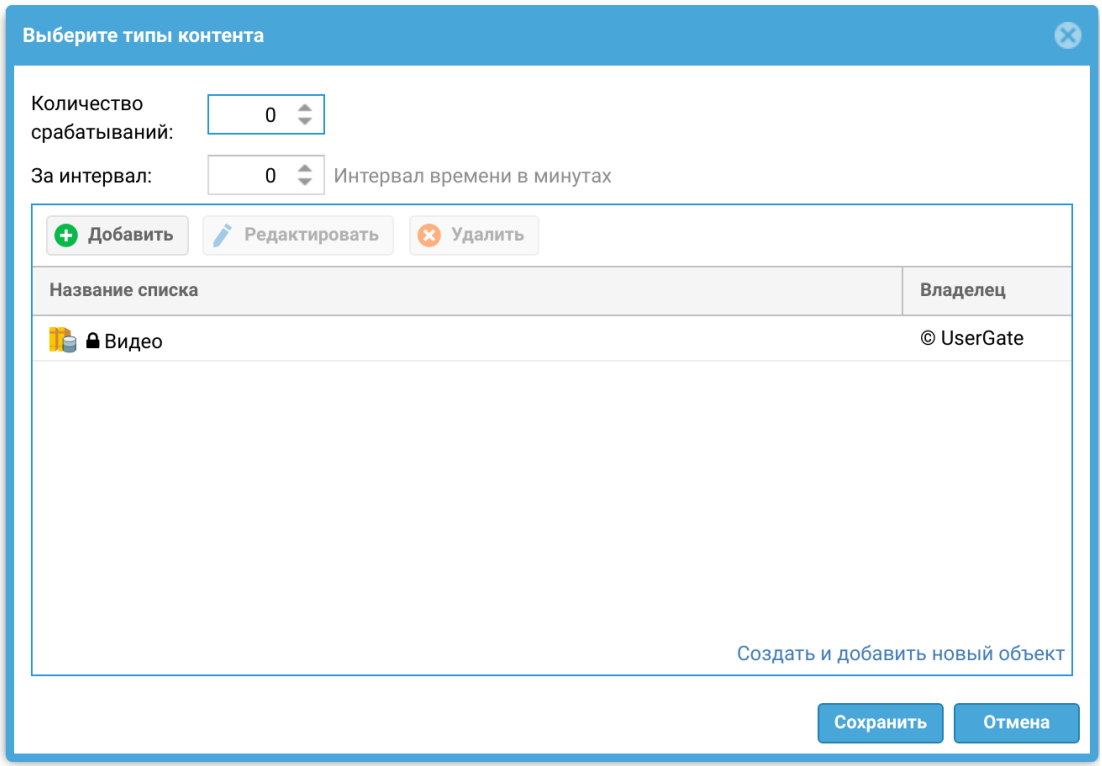
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выбор групп или категорий приложений из библиотеки элементов.

СОВ



Условием срабатывания в данном случае является детектирование системой СОВ угрозы определенного уровня.

Типы контента

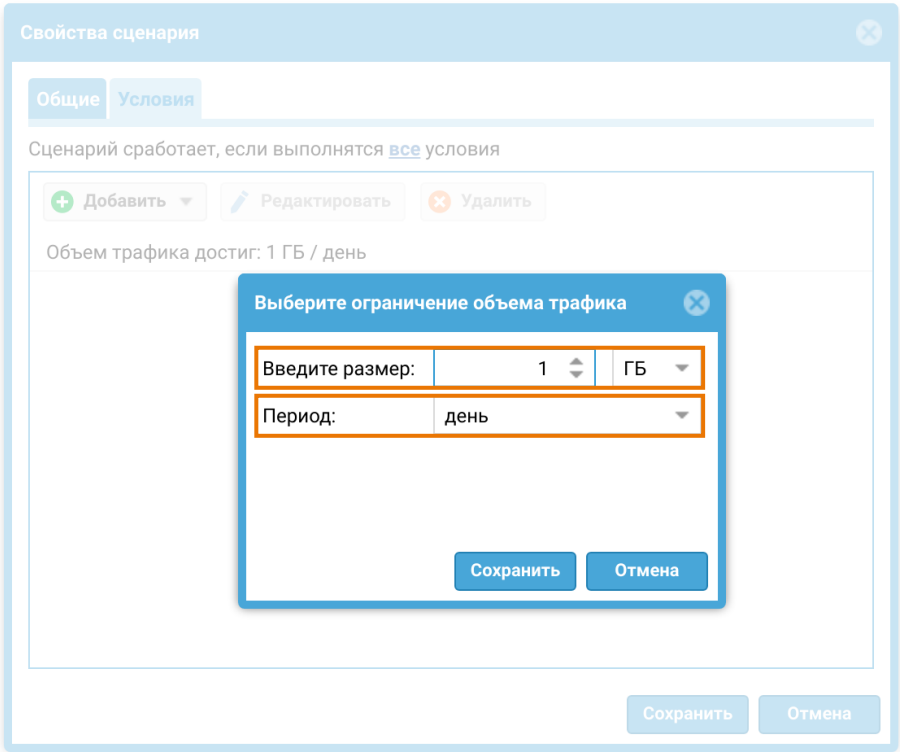


В данном условии настраиваются следующие параметры:

- **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.



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.

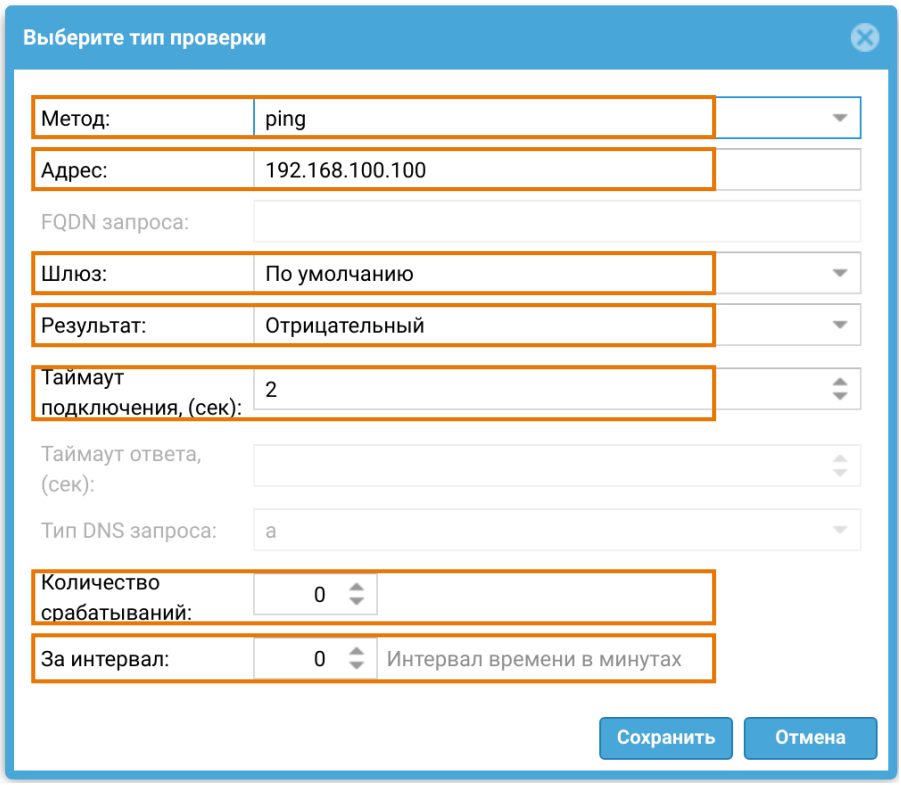
Проверка состояния

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**.

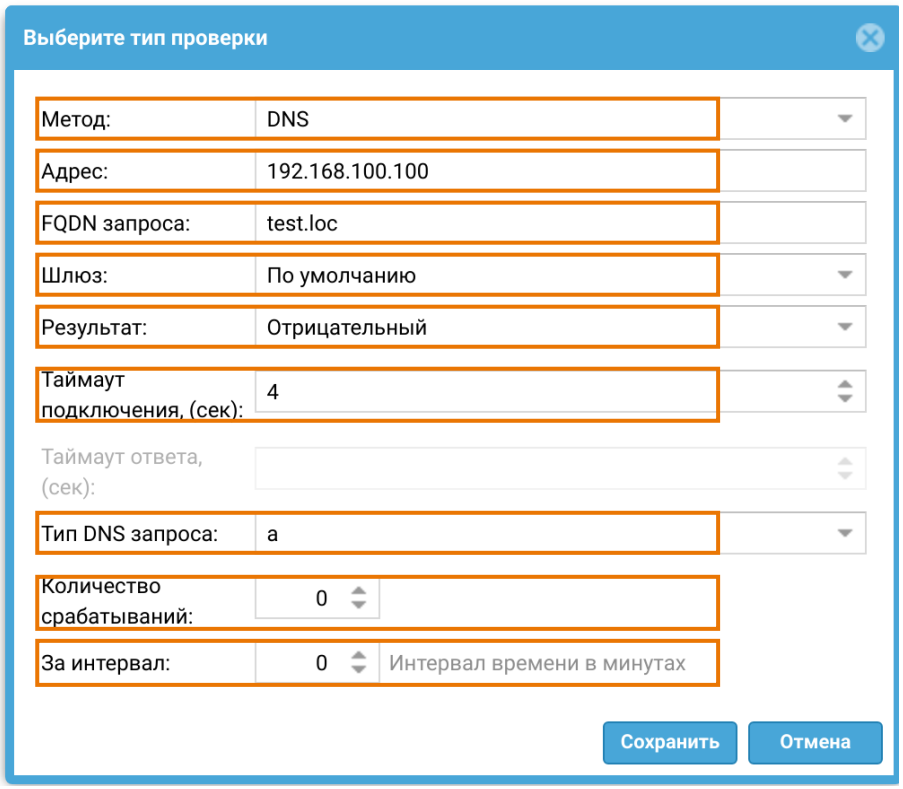


В данном условии настраиваются следующие параметры:

- **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**.

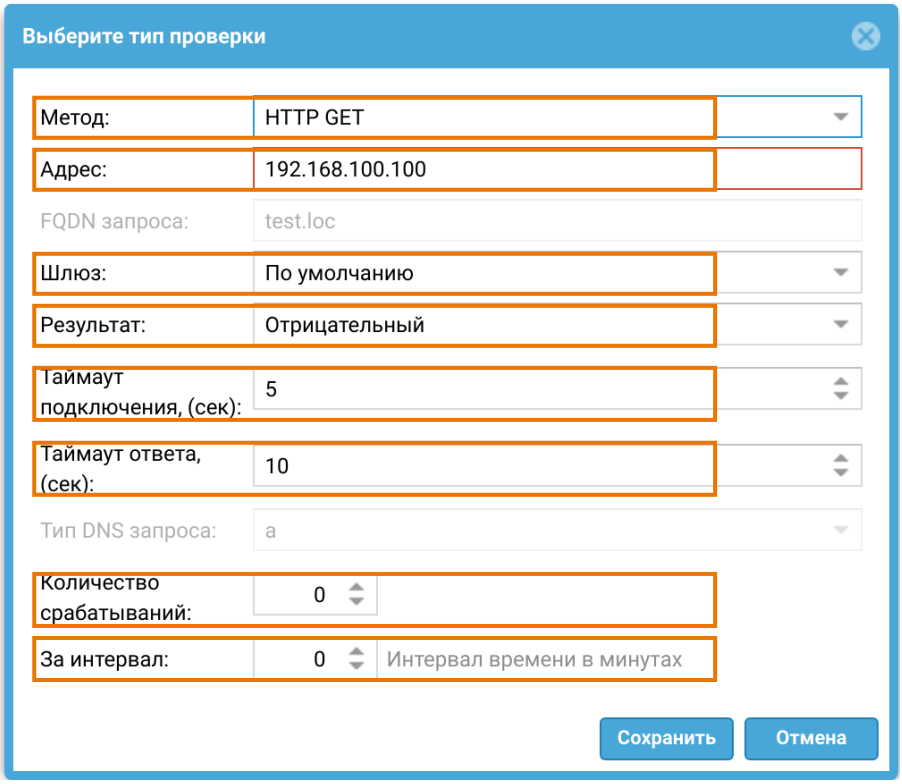


В данном условии настраиваются следующие параметры:

- **Адрес** — IP-адрес для выполнения запроса DNS с NGFW.
- **FQDN запроса** — доменное имя сервера, по которому будет производится обращение.
- **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**



В данном условии настраиваются следующие параметры:

- **Адрес** — домен для выполнения HTTP GET с NGFW.
- **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.
- **Тайм-аут ответа** — тайм-аут ответа для проверки выполнением HTTP GET.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.

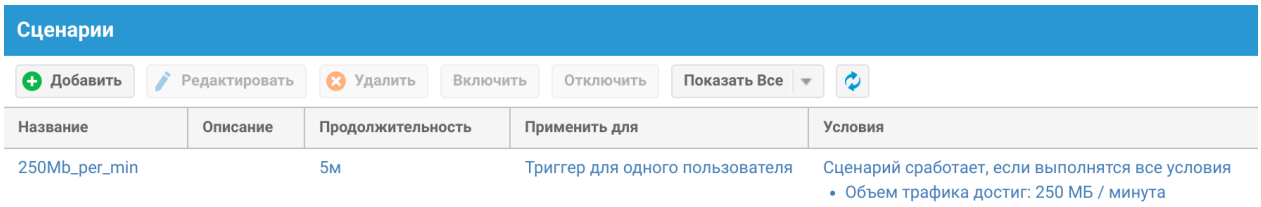
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.

Пример использования сценариев

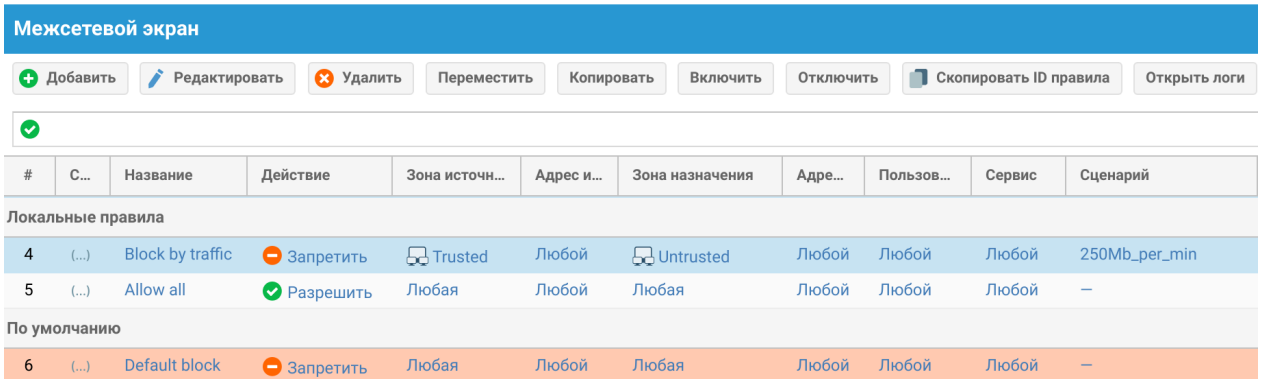
Как пример, сценарии могут использоваться в правилах межсетевого экрана для ограничения доступа в сеть, если происходит какое-либо событие, описанное в сценарии.

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:



В межсетевом экране создано блокирующее правило, в которое добавлен созданный сценарий:



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**.

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 **C** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **S** в списке маршрутов.

- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **O** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **B** 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 **Закрыть** сессию.

Заблокированные СОВ/L7 IP-адреса

СОВ отслеживает и блокирует атаки в режиме реального времени. Мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал мониторинга.

Раздел **Заблокированные СОВ/L7 IP-адреса** отображает список всех заблокированных IP-адресов. Кластерные узлы имеют одну общую таблицу **Заблокированных СОВ/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 http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.
- **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 pcap-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.
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 крайне полезно при определении проблем с доступом к определенным сайтам. Для трассировки правил необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать необходимый фильтр.	Нажать на кнопку **Настроить** в разделе **Диагностика и мониторинг → Трассировка правил** и указать параметры фильтра: • **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 осуществляет запрос. Фильтр необходим для ограничения вывода диагностической информации. Если его не задать, то могут быть также отображены результаты обработки запросов других пользователей.
Шаг 2. Запустить трассировку.	Нажать на кнопку **Начать.**
Шаг 3. Открыть проблемный сайт.	Попросить пользователя открыть проблемный сайт и наблюдать, какие правила срабатывают при открытии сайта. Будут указаны все правила, которые выполняются во время обработки пользовательского запроса.

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

Данный раздел отображает список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP.

Наименование	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.
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.

Наименование	Описание
	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 интерфейсе.
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.
Deleted	Количество удалений записей о соседях LLDP.

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 SMNP-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.
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.

Наименование	Описание
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.

Наименование	Описание
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	Стутус файловой системы. Состояние файловой системы изменилось на "not_clean".
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружение атаки системой СОВ.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора.
trapLowMemory	Высокая загрузка памяти.
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 загруженности >=95% за 5 минут хотя бы на одном из дисковых устройств.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.

Наименование	Описание
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	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmDataPartionFSStatus	integer	Состояние файловой системы. • **0** — clean. • **1** — not clean.
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • **0** — master-узел. • **1** — slave-узел. • **3** — fault.
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • **1** — связь с узлом потеряна. • **2** — HTTP прокси-сервер недоступен. • **3** — ни один из шлюзов недоступен.

Наименование	Тип данных	Описание
		• **4** — DNS-сервер недоступен. • **5** — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора (%).
utmMemory	integer	Использование оперативной памяти (%).
utmLogdiskSpace	integer	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.

Наименование	Тип данных	Описание
		• **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. • **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.

Наименование	Тип данных	Описание
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 в %.
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 UPD 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. (*)

Наименование	Тип данных	Описание
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 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. (*)

Наименование	Тип данных	Описание
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	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**.

Наименование	Тип данных	Описание
		• **on**. • **off**.
raidType	string	Тип RAID массива.
raidStatus	string	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.

Наименование	Тип данных	Описание
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Описание 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.
fInNUcastPkts	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 передачи. 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.
ifHCOutOctets	counter64	Смысл одинаков со смыслом объекта **ifOutOctets** — количество байтов, переданное данным

Наименование	Тип данных	Описание
		интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutUcastPkts** — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutMulticastPkts** — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutBroadcastPkts	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.
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).
thermEntry	sequence	

Наименование	Тип данных	Описание
		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 производиться 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). • С аутентификацией, без шифрования (authNoPriv).

Наименование	Описание
	• 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.

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.
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.

ЖУРНАЛЫ И ОТЧЕТЫ

ЖУРНАЛЫ

Описание

UserGate NGFW журналирует все события, которые происходят во время его работы, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением настроек NGFW, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных NGFW.
- **Журнал DNS** — содержит события, связанные с DNS трафиком.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- **Журнал СОВ** — события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — события, регистрируемые правилами контроля систем АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — поисковые запросы пользователей в популярных поисковых системах.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование.
- **Агент UserID** — содержит описание событий отражающие 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 будут отображены в журнале событий. В случае, если подключен LogAn, то запись будет отображена в журнале событий LogAn.

Ротация записей журнала событий никогда не производится.

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.
- Референер (при наличии).
- Операционная система.
- User-agent браузер.

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.

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 АСУ ТП

Журнал АСУ ТП отображает срабатывания правил автоматизированной системы управления технологическим процессом, для которых включена функция журналирования. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.
- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

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.

Агент UserID

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные агентом UserID 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.

Наименование	Описание
Конечное устройство\сенсор	UserID конектор.
Уровень лога	Поле «Keywords» из журнала AD.
Данные	Содержание события из журнала AD.
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 агентом UserID с серверов Syslog. 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.
Запись журнала syslog	Ссылка на событие.
Правило	Правило под которое попало Syslog сообщение.

Наименование	Описание
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.
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.

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 СОВ.
- Журнал трафика.
- Журнал АСУ ТП. (в версиях 6+)
- Журнал инспектирования SSH. (в версиях 6+)

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**.

> **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	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал СОВ. • Журнал трафика. • Журнал АСУ ТП. • Журнал инспектирования SSH.

Наименование	Описание
	Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • 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.
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	

Наименование	Описание
	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**. • **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.

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.
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. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 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, ip!=172.16.31 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 равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date<='2019-03-28T20:59:59' AND statusCode=303
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть

Наименование	Описание
	применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date>="2019-03-13T21:00:00" AND statusCode=200
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404)
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, несодержащие 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\"'

Наименование	Описание
	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.

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.

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.

- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **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.

Наименование	Описание
	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	Задает 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.
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).

Наименование	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.
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**.

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.

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

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.

Наименование	Описание
	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.
	  • 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 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.

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI) V7.1

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения (Описание)

UserGate NGFW позволяет производить настройки устройства с помощью интерфейса командной строки, или CLI (Command Line Interface). С помощью CLI администратор может выполнить ряд диагностических команд, таких, как ping, nslookup, traceroute, произвести сетевые настройки устройства, настройки политик безопасности, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании NGFW), через последовательный порт или с помощью SSH по сети.

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

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к NGFW.	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin).

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к NGFW.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к NGFW.

Наименование	Описание
Шаг 2. Запустить терминал.	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin).

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны.	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал.	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес NGFW, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: ssh *Admin@IPNGFW* -p *2200*
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге.

После успешной авторизации в CLI появится строка, ожидающая ввода команды (режим диагностики и мониторинга). Для просмотра текущих возможных значений или автодополнения необходимо использовать **Tab** или **?**. Доступны:

- **traceroute** — трассировка соединения до определённого хоста.
- **shutdown** — выключение NGFW.
- **show** — просмотр сетевых настроек, мониторинг трафика, LLDP.
- **clear** — обновление информации OSPF и BGP.
- **check-geoip** — проверка принадлежности IP-адреса по текущей базе GeoIP.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка NGFW.

- **date** — просмотр текущих даты и времени на сервере.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **configure** — переход в режим конфигурации.
- **dig** — проверка записи DNS-домена.

Данные команды доступны в режиме конфигурации; подробнее читайте в разделах Команды execute и Команды диагностики и мониторинга.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

CLI поддерживает ввод команды в несколько строк (многострочный ввод). Для перехода на новую строку необходимо добавить "\" в конце строки. Начиная со второй строки ввод "\" необязателен; чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@nodename# set users user example \
... name username1
... enabled on
... groups [ "Default Group" ]
...
Admin@nodename#
```

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВИЧНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла (Описание)

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу radmin-emergency.

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация (Описание)

Первоначальная инициализацию NGFW с использованием интерфейса командной строки можно произвести несколькими способами.

Установка как главного узла.

Для настройки NGFW в качестве главного узла используется команда:

```
Admin@nodename# execute install master
```

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора.

Параметр	Описание
	Указание пароля также доступно при нажатии **Enter** после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Установка как дополнительного узла кластера.

Для настройки NGFW в качестве дополнительного узла кластера используется команда:

```
Admin@nodename# execute install slave
```

Необходимо указать параметры:

Параметр	Описание
interface	Интерфейс для подключения к кластеру.
slave-ip	IP-адрес, который будет назначен на интерфейс, использующийся для подключения к кластеру.
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 NGFW.
password	Пароль учётной записи администратора.

Настройка через UserGate Management Center.

Для настройки NGFW через UGMC используется команда:

```
Admin@nodename# execute install mc
```

Необходимо указать параметры:

Параметр	Описание
login	Логин администратора NGFW.
password	Пароль учётной записи администратора.
mc-ip	IP-адрес сервера UGMC.
device-code	Уникальный код устройства, использующийся для подключения узла к UGMC.

После первичной инициализации будет доступно полное управление из CLI.

КОМАНДЫ ДИАГНОСТИКИ И МОНИТОРИНГА

Команды диагностики и мониторинга (Описание)

Команды диагностики позволяют просмотреть следующее:

- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.
- Мониторинг состояния кластера.
- Мониторинг заблокированных СОВ IP-адресов.
- Отображение системной информации.
- Диагностику работы протоколов динамической маршрутизации.
- Информацию об авторизованных пользователях.

Статистика интерфейсов

Для отображения информации об интерфейсах используется следующая команда:

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

Для отображения статистики определенного интерфейса и информации о нём используется следующая команда:

```
Admin@nodename> show network interface <interface-name>
```

Также доступно отображение только информации или только статистики интерфейса:

```
Admin@nodename> show network interface <interface-name> type info
Admin@nodename> show network interface <interface-name> type statistics
```

ARP-записи

Для просмотра информации о записях ARP:

```
Admin@nodename> show network arp
```

При просмотре записей доступно использование фильтров. Параметры фильтрации:

Параметр	Описание
node-name	Название узла кластера, ARP-записи которого необходимо отобразить. Далее необходимо указать интерфейс или IP-адрес хоста: `Admin@nodename> show network arp node-name <node-name> interface <iface-name>`

Параметр	Описание
	`Admin@nodename> show network arp node-name <node-name> host <ip>`
interface	Название интерфейса 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>
```

Просмотр записей ARP также доступен в режиме конфигурации; команды идентичны командам в режиме диагностики и мониторинга.

> **Примечание**
> **В режиме диагностики и мониторинга действия производятся с системными записями; в режиме конфигурации – со статическими записями ARP.**

Добавление статических ARP-записей доступно в режиме конфигурации с использованием следующей команды:

```
Admin@nodename# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

Параметры команды:

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 NGFW.
host	IP-адрес устройства.

Параметр	Описание
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 и мониторинга;
- **delete**: удаление статических записей в режиме конфигурации.

Далее будет представлен формат команд удаления на примере команд режима диагностики и мониторинга.

Для удаления системной записи:

```
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>
```

Следующая команда позволяет удалить все системные записи на заданном интерфейсе (можно указать несколько интерфейсов):

```
 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>
```

Отслеживание пакетов

Чтобы произвести отслеживание пакетов, используется следующая команда:

```
Admin@nodename> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия портов источника и назначения UserGate, номера TCP/UDP портов источника и назначения. Команда также доступна в режиме конфигурации.

Чтобы выйти из режима отслеживания пакетов - **Ctrl+C**.

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации на уровне **network**. Для создания правила используется следующая команда:

```
Admin@nodename# create network trace-rules
```

Далее указываются следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила отслеживания пакетов: • **on**. • **off**.
name	Название правила. Если название правила не было задано, то оно задаётся автоматически в формате: trace_rule_N (где N — порядковый номер создаваемого правила отслеживания пакетов).
zones-in	Список зон источников трафика.
source-ip-lists	Список групп IP-адресов источника пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов.
source-ip-addresses	Список IP-адресов источника пакета.
dest-ip-lists	Список групп IP-адресов назначения пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов.
dest-ip-addresses	Список IP-адресов назначения пакета.
services	Тип сервиса. Подробнее читайте в разделе Настройка сервисов.

Пример команды создания правила:

```
Admin@nodename# create network trace-rules enabled on name "Test trace"
source-ip-addresses [ 192.168.0.100 ]
```

Для редактирования правила:

```
Admin@nodename# set network trace-rules <trace-rule-name>

Admin@nodename# set network trace-rules "Test trace" services
[ "[SYSTEM] Any ICMP" ]
```

Для изменения доступны параметры, представленные в таблице выше.

Чтобы просмотреть существующие правила отслеживания пакетов:

```
Admin@nodename# show network trace-rules
```

Для удаления правила отслеживания пакетов используется следующая команда:

```
Admin@nodename# delete network trace-rules <trace-rule-name>
```

Также доступно удаление значений отдельных параметров правил. Для удаления доступны:

- **zones-in**.
- **source-ip-lists**.
- **source-ip-addresses**.
- **dest-ip-lists**.
- **dest-ip-addresses**.
- **services**.

Мониторинг трафика

Следующая команда используется для мониторинга трафика:

```
Admin@nodename> show traffic
```

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Доступна фильтрация по: • **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.). Фильтрация доступна по: • **protocol** — протокол. • **source-ip** — IP-адрес источника. • **dest-ip** — IP-адрес назначения. • **node-name** — название узла. • **expect** — отображение неустановленных соединений: ◦ **on**. ◦ **off**.
capture	Отображение захвата пакетов. Доступна фильтрация по следующим параметрам: • **destination** — IP-адрес назначения • **destination-port** — порт назначения. • **ipv4-protocol** — номер протокола IPv4 (0-255). • **interfaces** — название интерфейса. • **protocol** — выбор протокола.

Параметр	Описание
	• **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
```

LLDP

Просмотр информации, полученной по LLDP (Link Layer Discovery Protocol), доступен с использованием команд:

```
Admin@nodename> show lldp
Admin@nodename> show lldp neighbors
Admin@nodename> show lldp statistics
```

Параметры команды:

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.

Параметр	Описание
	• **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 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. • **Deleted** — количество удалений записей о соседях LLDP.

Примечание

Для просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на NGFW (профили LLDP настроены в библиотеке элементов и активированы в настройках интерфейсов).

Маршруты

Данный раздел необходим для проведения диагностики и мониторинга маршрутной информации на NGFW.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

```
Admin@nodename> show network route
```

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить.
node-name	**Выбор узла кластера.**
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам NGFW. Данные маршруты помечены символом **C** в списке маршрутов.
kernel	Отображение маршрутов, добавленных администратором; маршруты помечены символом **K** 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 **O** в списке маршрутов.
bgp	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации BGP; маршруты помечены символом **B** 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 производится с использованием команд, представленных ниже. Отображение информации OSPF:

```
Admin@nodename> show network ospf
...
Admin@nodename> show network ospf <parameter>
```

Параметр	Описание
node-name	**Выбор узла кластера.**
virtual-router	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF: (<vrf-name> | **all**).

Параметр	Описание
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, находящихся 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, подключённых 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). • 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.

Параметр	Описание
	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@nodename> clear network ospf <parameter>
```

Параметр	Описание
interface-name	Название интерфейса.
node-name	**Выбор узла кластера.**
virtual-router	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<vrf-name> | **all**).
interface	Интерфейс, на котором необходимо перезапустить процесс OSPF (<interface-name>).
neighbor	Выбор соседей в отношении которых будет перезапущен процесс

Мониторинг BGP

В данном разделе представлены команды диагностики и мониторинга BGP.

Для отображения таблиц BGP маршрутизатора:

```
Admin@nodename> show network bgp
...
Admin@nodename> show network bgp <parameter>
```

Параметр	Описание
node-name	**Выбор узла кластера.**
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> | **all**).
ip	IP-адрес, маршрут до которого необходимо отобразить.
statistics	Отображение статистики BGP.
neighbors	Отображение информации о BGP-соседях (доступно отображение информации об определённом 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.
summary	Просмотр краткой информации о соседях.

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии):

```
Admin@nodename> clear network bgp
```

Далее доступно указание параметров:

Параметр	Описание
ip	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации.
node-name	**Выбор узла кластера.**

Параметр	Описание
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@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

В данном разделе представлены команды диагностики и мониторинга 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 нём не была получена):

```
Admin@nodename> show network rip
...
Admin@nodename> show network rip <parameter>
```

Доступно использование следующих параметров:

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:

```
Admin@nodename> show network mroute
...
Admin@nodename> show network mroute <parameter>
```

Доступно использование следующих параметров:

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. Доступно указание параметра: • **ip** — отображение записи для определённого IP-адреса; далее необходимо указать IP-адрес.
ip	Отображение записи для определённого 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). Для отображения информации для маршрутизатора по умолчанию:

```
Admin@nodename> show network igmp <parameters>
```

Далее необходимо указать параметры:

Параметр	Описание
node-name	Выбор узла кластера.
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). • Таймер, который обнуляется каждый раз, как приходит сообщение Query с меньшим IP-адресом.

Параметр	Описание
	Доступно указание: • **interface-name** — название интерфейса. • **detail** — подробная информация об интерфейсе.

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды (указание параметров является обязательным). Для отображения информации для маршрутизатора по умолчанию:

```
Admin@ndename> show network pim <parameter>
```

Далее необходимо указать параметры:

Параметр	Описание
node-name	Выбор узла кластера, для которого необходимо отобразить информацию.
virtual-router	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию.
vxlan-groups	Информация о группах VXLAN, использующихся в мультивещании.
statistics	Статистика протокола.
join	Отображение информации о группах PIM протокола.
neighbor	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.
next-hop	Записи о адресах next-hop.
state	

Параметр	Описание
	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List).
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешённые 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 разрешённых групповых адресов для SSM (Source Specific Multicast).
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса.

Мониторинг состояния кластера

Команды мониторинга состояния кластера могут быть запущены на любом из узлов, входящих в кластер. Они позволяют получить информацию о текущем состоянии кластера, его узлов, режиме работы кластера и истории переключения состояний кластера.

Для мониторинга состояния кластера используется следующая команда:

```
Admin@nodename> show ha-cluster state
```

Для мониторинга состояния узлов кластера используется команда:

```
Admin@nodename> show ha-cluster tablestat
```

Для отображения информации об истории переключения состояния кластера используется команда:

```
Admin@nodename> show ha-cluster failover
```

Мониторинг заблокированных СОВ IP-адресов

Для просмотра таблицы с заблокированными системой СОВ IP-адресами используется команда:

```
Admin@nodename> show blocked-ip
```

Для разблокирования отдельных IP-адресов используется команда:

```
Admin@nodename> clear blocked-ip ips [ ip-address ip-address ... ]
```

Отображение системной информации

Для просмотра версии ПО системы используется команда:

```
Admin@nodename> show system version
```

Для отображения информации о количестве активных TCP/UDP/ICMP сессий на системе используется команда:

```
Admin@nodename> show system sessions
```

Для отображения информации о количестве активных сессий по отдельным протоколам или временным интервалам используется команда:

```
Admin@nodename> show system sessions counters [ parameters ]
```

Очистить статистику:

```
Admin@nodename> 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 производится командой debug в режиме конфигурации (подробнее читайте в разделе Режим конфигурации).

Для просмотра записей debug-лога используется команда:

```
Admin@nodename> show 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:

```
Admin@nodename> show log tail on routing <parameters>
```

Далее необходимо указать один из параметров из таблицы команды просмотра записей debug-лога, размещенной выше.

Для отключения вывода событий debug-лога в консоль в реальном времени по отдельным протоколам используется команда:

```
Admin@nodename> show log tail off routing <parameters>
```

Параметры команды аналогичны параметрам, указанным ранее.

Просмотр информации об авторизованных пользователях

Для просмотра информации об авторизованных пользователях используется следующая команда интерфейса командной строки:

```
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.

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации используется команда:

```
Admin@nodename> configure
```

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

```
Admin@nodename#
```

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin@nodename# set network virtual-router default
* name                 Name
+ description          Description
+ interfaces           List of network interfaces attached to this
virtual router
> bgp                  BGP router
> multicast-router     Multicast router
> ospf                 OSPF router
> rip                  RIP router
> routes               List of static network routes
```

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 конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **execute** — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • **set** — редактирование всех объектов, а также включение различных параметров, например, radmin. • **end** — переход на один уровень выше. • **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • **top** — возврат на самый верхний уровень конфигурации. • **exit** — выход из режима конфигурации. • **export** — экспорт конфигурации. • **import** — импорт конфигурации. • **create** — создание новых объектов. • **delete** — удаление объекта или параметра из списка параметров. • **debug** — включение журналирования событий протоколов динамической маршрутизации. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: `Admin@nodename# show network interface` С использованием следующей команды производится переход на уровень **network interface.** Текущий уровень будет отображён над командной строкой:

Наименование	Описание

```
Admin@nodename# edit network interface
[ network interface ]
Admin@nodename#
```

После перехода на уровень **network interface** для отображения всех интерфейсов используется команда show без указания уровня:

```
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
...
...
...
```

Для возвращения с уровня **network interface** обратно на общий уровень режима конфигурации необходимо набрать команду **end** 2 раза:

```
[ network interface ]
Admin@nodename# end
[ network ]
Admin@nodename# end
Admin@nodename#
```

Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду **top**:

Наименование	Описание

	`[ network interface ]`
	`Admin@nodename# top`
	`Admin@nodename#`

<level>	Уровни в командной строке повторяют веб-интерфейс UserGate NGFW: • **security-policy** — соответствует разделу веб-интерфейса **Политики безопасности**. • **network** — соответствует разделу веб-интерфейса **Сеть**. • **settings** — соответствует разделу веб-интерфейса **UserGate**. • **global-portal** — соответствует разделу веб-интерфейса **Глобальный портал**. • **network-policy** — соответствует разделу веб-интерфейса **Политики сети**. • **vpn** — соответствует разделу веб-интерфейса **VPN**. • **users** — соответствует разделу веб-интерфейса **Пользователи и устройства**. • **libraries** — соответствует разделу веб-интерфейса **Библиотеки**. • **monitoring** — соответствует разделу веб-интерфейса **Диагностика и мониторинг**. • **waf** — соответствует разделу веб-интерфейса **WAF**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info> (рассмотрено далее в разделе). 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: `Admin@nodename# show network interface adapter port0`

Наименование	Описание
	то будет отображена информация об интерфейсе port0 текущего узла UserGate. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла: `Admin@nodename# show network interface adapter ( node-name another_nodename interface port0 )` **Важно!** Круглые скобки должны быть отделены пробелами с обеих сторон.

<configuration_info>	Набор пар: параметр-аргумент. 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:
	`Admin@nodename# create users group "VPN users"`
	Множественные аргументы используются для установки множества значений какого-либо параметра; 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]:
	`Admin@nodename# set users group "VPN users" users [ user1 user2 ]`
	Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

```
Admin@nodename# execute <command-name>
```

Доступны следующие команды:

Параметр	Описание
update	Обновление: • **software-updates** — обновление программного обеспечения. • **libraries-updates** — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • **hostname <ip-or-domain>** — IP-адрс 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. `Admin@nodename# execute traceroute hostname <hostname>`
license	Команда регистрации продукта имеет следующую структуру: `Admin@nodename# execute license activate <pin-code>` Укажите код активации продукта вместо <pin-code>.
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Настройка сессий администраторов.
cache	Очистка кэша LDAP-записей: • **ldap-clear**.
check-geoip	Проверка принадлежности IP-адреса по текущей базе GeoIP.

Параметр	Описание
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • **hostname** — IP-адрес или доменное имя хоста. • **count** — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • **numeric** — не резолвить 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** — размер mtu отправляемых пакетов. • **virtual-router** — имя виртуального маршрутизатора. `Admin@nodename# execute ping hostname <hostname> count <number>`
reboot	Перезагрузка сервера UserGate.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение сервера UserGate.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • **address** — доменное имя хоста 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).

Параметр	Описание

	• **data** — запрос содержимого сайта. По умолчанию запрашиваются только заголовки.
	• **timeout** — максимальный таймаут ожидания ответа от веб-сервера.
	• **user-agent** — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin@nodename# execute netcheck type tcp address <host-domain-name> data on`
	`Admin@nodename# execute netcheck address <host-domain-name>`

dig	Проверка записи DNS домена.
	• **hostname** — доменное имя хоста или IP-адрес для реверсивного поиска.
	• **reverse-lookup** — получение хоста по IP-адресу.
	• **dns** — указание IP-адреса DNS-сервера.
	• **tcp** — использование протокола TCP вместо UDP.
	
	`Admin@nodename# execute dig hostname <host-domain-name>`
	`Admin@nodename# execute dig hostname <IP-address> reverse-lookup on`

configurate-cluster	Генерирование секретного кода, необходимого для добавления нового узла в кластер конфигурации: `Admin@nodename# execute configurate-cluster generate-secret-key <parameter>` • **secret** — ключ для генерации секретного кола 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.

Параметр	Описание
	Важно! Для использования данной команды необходимо наличие лицензии на модуль **Cluster**, иначе будет отображена ошибка.

mc-force-disconnect	Команда аварийного отключения узла от МС, с которым он был интегрирован. В зависимости от выбранного аргумента импортированные из МС объекты сохраняются локально или удаляются:
	• **keep** — отключение от МС с сохранением всех импортированных из МС объектов (библиотеки, правила итд.). Импортированные из МС объекты конвертируются в локальные.
	• **delete** — отключение от МС с удалением всех импортированных из МС объектов (библиотеки, правила итд.). Импортированные объекты, которые в настоящий момент используются, конвертируются в локальные.
	`Admin@nodename# execute mc-force-disconnect keep`
	`Admin@nodename# execute mc-force-disconnect delete`

firewall	Операции с межсетевым экраном: • **force-changes** — применение всех правил межсетевого экрана заново с обрывом текущих сессий.
restore-mac	Восстановление mac-адреса интерфейса.

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, WAF**.

В разделе настроек UserGate доступен импорт сертификатов. Подробнее читайте в разделе Настройка сертификатов.

В разделах **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN, WAF** доступен импорт правил, написанных на UPL. При использовании импорта, все существующие правила будут заменены на указанные; можно указать сразу несколько правил.

В разделе **Пользователи** доступен импорт правил Captive-портала. Подробнее о добавлении правил читайте в соответствующем разделе Настройка Captive-портала.

В разделе **Сеть** доступен импорт правил DNS. Подробнее читайте в разделе Настройка правил DNS.

В разделе **Политики сети** доступен импорт правил межсетевого экрана, NAT и маршрутизации, пропускной способности, балансировки нагрузки. Подробнее читайте в соответствующих разделах Настройка правил межсетевого экрана, Настройка правил NAT и маршрутизации, Настройка правил пропускной способности. Настройка балансировки нагрузки.

В разделе **Политики безопасности** доступен импорт правил 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** доступен импорт правил веб-портала и reverse-прокси. Подробнее о создании правил читайте в разделах Настройка веб-портала и Настройка правил reverse-прокси.

В разделе **VPN** доступен импорт серверных и клиентских правил, о добавлении которых написано в разделах Настройка серверных правил и Настройка клиентских правил.

Команды export

Доступен экспорт сертификатов и элементов библиотек.

Подробнее об экспорте сертификатов смотрите в разделе Настройка сертификатов.

Для экспорта доступны следующие элементы библиотек: IP-адреса, Useragent браузеров, списки URL, категории URL, изменённые категории URL, типы контента, морфология, почтовые адреса и номера телефонов. Для экспорта элемента библиотеки используется команда:

```
Admin@nodename# export libraries <library-name> <list-name>
```

где:

<library-name> — название библиотеки элементов (IP-адреса, Списки URL и т.д.).

<list-name> — название элемента библиотеки.

Команда debug

Команда debug позволяет включать журналирование событий протоколов маршрутизации. 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:

Параметр	Описание
rip	Протокол RIP.
bgp	Протокол BGP.
igmp	Протокол IGMP
pim	Протокол PIM.

Параметр	Описание
ospf	Протокол OSPF.
bfd	Протокол BFD.
msdp	Протокол MSDP.
mroute	Таблица мультикаст-маршрутизации mroute.
ssmpingd	Инструмент тестирования мультикаст-вещания ssmpingd.

НАСТРОЙКА УСТРОЙСТВА

Настройка устройства (Описание)

Настройка CLI

Настройка интерфейса командной строки производится на уровне **settings cli**. Чтобы задать уровень детализации диагностики используется следующая команда:

```
Admin@nodename# set settings cli log-level <off | error | debug |
warning | info>
```

Уровни детализации:

- **off** — отключить журналирование.
- **error** — только ошибки.
- **debug** — максимальная детализация.
- **warning** — ошибки и предупреждения.
- **info** — ошибки, предупреждения и дополнительная информация.

Для отображения настроек CLI:

```
Admin@nodename# show settings cli
```

Для настройки системного приглашения (prompt) консоли CLI используется команда:

```
Admin@nodename# set settings cli custom-prompt <new-custom-prompt>
```

Для возвращения системного приглашения в первоначальное состояние используется команда:

```
Admin@nodename# set settings cli custom-prompt default
```

Общие настройки UserGate

Общие настройки сервера UserGate задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

```
Admin@nodename# set settings general <settings-module>
```

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень **settings general admin-console**): • **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. • **webaccess**: режим аутентификации веб-консоли: ◦ **password**: аутентификация по имени и паролю. ◦ **cert**: аутентификация по X.509-сертификату.

Параметр	Описание
	• **uc-profile**: выбор профиля пользовательских сертификатов. • **web-ssl-profile**: выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL смотрите 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 смотрите в разделе Настройка профилей SSL. • **api-session-lifetime**: время ожидания сеанса администратора в секундах.
server-time	Настройка параметров установки точного времени (уровень **settings general server-time**): • **ntp-enabled**: включение/отключение использования NTP-серверов: ◦ **on**. ◦ **off**. • **primary-ntp-server**: указание основного ntp-сервера. • **second-ntp-server**: указание запасного ntp-сервера. • **time**: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
modules	Настройка модулей UserGate (уровень **settings general modules**): • **proxy-port**: указать нестандартный номер порта, который будет использоваться для подключения к встроенному прокси-серверу. • **auth-captive**: указать служебный домен, который используется UserGate при авторизации пользователей через Captive-портал. • **logout-captive**: указать служебный домен, который используется пользователями UserGate для окончания сессии (logout). • **block-page-domain**: указать служебный домен, который используется для отображения страницы блокировки пользователям. • **ftp-enabled**: включить/отключить модуль, позволяющий получать доступ к содержимому FTP-серверов из пользовательского браузера.

Параметр	Описание
	• **ftp-domain**: указать служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. • **tunnel-inspection-zone**: выбрать зону для инспектируемых туннелей. Необходимо указать: ◦ **enabled** — включить/выключить зону. ◦ **name** — указать название зоны. • **snmp-engine-id**: настроить SNMP Engine ID: ◦ **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 SNMP Engine ID (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ **value** — значение идентификатора. • **terminal-sever-agent**: настроить пароль агентов терминального сервиса. • **lldp**: настроить использование протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своём 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, изменение имени хоста или адреса управления. Может принимать значения от 1 до 3600; задаётся 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	Настройка кэша прокси-сервера (уровень **settings general cache**): • **caching-mode**: включение или отключение кэширования. ◦ **on**. ◦ **off**.

Параметр	Описание
	• **exclusions**: список URL, которые не будут кэшироваться. Для удаления исключений: `Admin@nodename# delete settings general cache exclusions [ <URL> ]` • **max-cacheable-size**: максимальный размер объектов, которые будут кэшироваться (указывается в Мбайт). • **ram-size**: размер оперативной памяти, отведенный под кэширование (указывается в Мбайт).
log-analyzer	Настройки модуля Log Analyzer (уровень **settings general log-analyzer**): • **use-local-stat-server** — использование локального Log Analyzer: ◦ **on**. ◦ **off**.
proxy-portal	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (уровень **settings general proxy-portal**): • **enabled**: включение/отключение использования веб-портала: ◦ **on**. ◦ **off**. • **hostname**: имя хоста. • **port**: порт. • **auth-profile**: выбор профиля аутентификации. Подробнее о настройке профилей авторизации с использованием CLI читайте в разделе Настройка профилей аутентификации. • **auth-template**: выбор шаблона страницы авторизации. • **portal-template**: выбор шаблона портала. • **enable-ldap**: выбор домена AD/LDAP на странице авторизации: ◦ **on**. ◦ **off**. • **use-captcha**: показ CAPTCHA: ◦ **on**. ◦ **off**.

Параметр	Описание
	• **ssl-profile**: выбор профиля SSL. Подробнее о настройке профилей аутентификации с использованием CLI читайте в разделе Настройка профилей SSL. • **certificate**: выбор сертификата. • **auth-mode**: выбор метода аутентификации. Доступны следующие методы: ◦ **aaa** — аутентификация через логин/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	`Admin@nodename# set settings general pcap packet-capture-mode <parameter>` Настройка захвата пакетов (уровень **settings general pcap**): • **no-capture**: без захвата. • **one-packet**: один пакет. • **previous**: предшествующие пакеты. • **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 учёта изменений (уровень **settings general change-tracker**): • **enabled**: включение/отключение учёта изменений. ◦ **on**. ◦ **off**. • **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда:

Параметр	Описание
	`Admin@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ]`
management-center	`Admin@nodename# set settings general management-center <parameters>` Настройка агента UserGate Management Center (уровень **settings general management-center**): • **enabled**: включение/отключение агента UserGate Management Center. ◦ **on**. ◦ **off**. • **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 (уровень **settings general updates-schedule**).
	
	Для расписания обновления программного обеспечения UserGate:
	
	`Admin@nodename# set settings general updates-schedule software schedule <schedule/disabled>`
	
	Расписание скачивания обновлений библиотек может быть единым:
	
	`Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>`
	
	или может быть настроено отдельно для каждого элемента:

Параметр	Описание

	`Admin@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled>`
	
	Время задаётся в crontab-формате: (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".
	
	Команда для просмотра расписания обновлений:
	
	`Admin@nodename# show settings general updates-schedule`

upstream-proxy	Настройка перенаправления HTTP трафика на вышестоящий прокси-сервер: • **enabled** — включение/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. • **auth** — аутентификация на вышестоящем прокси-сервере (on/off). • **name** — логин на вышестоящем прокси-сервере. • **password** — пароль на вышестоящем прокси-сервере.

Настройка управления устройством

Настройка диагностики

На уровне **settings radmin** можно включить или отключить удалённый доступ к серверу для технической поддержки UserGate (**Radmin**). Команда включения/отключения Radmin:

```
Admin@nodename# set settings radmin enabled <on | off>
```

Для просмотра состояния Radmin:

```
 Admin@nodename# show settings radmin
```

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, задаются на уровне **settings loglevel**. С помощью следующей команды можно установить необходимы уровень детализации диагностики (отключено; только ошибки; ошибки и предупреждения; ошибки, предупреждения и дополнительная информация; максимум детализации):

```
 Admin@nodename# set settings loglevel value <off | error | warning |
info | debug>
```

Для просмотра состояния уровня детализации диагностики:

```
Admin@nodename# show settings loglevel

value    : error
```

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром узла администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации UserGate. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора. Команда включения/отключения удалённого доступа к серверу для технической поддержки в таких случаях:

```
Admin@nodename# set radmin-emergency enabled <on | off>
```

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

```
Admin@nodename# set settings device-mgmt updates-channel <stable |
beta>
```

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

```
 Admin@nodename# show settings device-mgmt updates-channel
```

Управление резервным копированием

Создание резервной копии устройства осуществляется на уровне **settings device-mgmt**. 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>
```

Для настройки доступны следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила создания резервной копии устройства.
name	Название правила резервного копирования.

Параметр	Описание
description	Описание правила резервного копирования.
type	Выбор удалённого сервера для экспорта файлов: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены файлы.
schedule	Расписание экспорта файлов резервных копий. Время задаётся в Crontab-формате: (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".

Редактирование существующего правила резервного копирования устройства UserGate производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-
name>
```

Команда для отображения правила резервного копирования:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Также, для команд редактирования, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек сервера UserGate.
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.

Параметр	Описание
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (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".

Обновление существующего правила экспорта настроек сервера UserGate производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-
name>
```

Команда для отображения правила экспорта настроек:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации (настроек) продукта 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.

- **log** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания изменений конфигурации. Требует указания пароля, который был задан при активации режима отслеживания конфигурации.
- **block** — активирует режим отслеживания изменений конфигурации. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate.

Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего "замораживает" настройки (режим **log** или **block**). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений:

```
Admin@nodename# show settings change-control config
```

Настройка защиты исполняемых файлов от изменения

Чтобы настроить защиту параметры защиты исполняемого кода продукта от потенциального несанкционированного изменения:

```
Admin@nodename# set settings change-control code <off | log | block>
```

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate

- **log** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания несанкционированных изменений исполняемого кода. Требует указания пароля, который был задан при активации режима отслеживания исполняемого кода.
- **block** — активирует режим отслеживания несанкционированных изменений исполняемого кода. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов:

```
Admin@nodename# show settings change-control code
```

Настройка режима ускоренной обработки сетевого трафика

Для включения/отключения режима ускоренной обработки трафика используется команда:

```
Admin@nodename# set settings fastpath enabled <on/off>
```

Для просмотра настройки 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 обновления существующего узла кластера:

```
Admin@nodename# set settings device-mgmt configuration-cluster <node-
name>
```

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера.
description	Обновить описание узла кластера.
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения настроек 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

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.

Параметр	Описание
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, 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: `Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>` Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера.

Параметр	Описание
	• <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.

Параметр	Описание
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 (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: `Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>`

Параметр	Описание
	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 редактироания 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 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.

Параметр	Описание
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).
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.

Параметр	Описание
	• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `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`
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. `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`
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.

Параметр	Описание
	• **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: `Admin@nodename# create settings administrators profiles ... api-permissions <permission> all` или

Параметр	Описание
	`Admin@nodename# create settings administrators profiles ... api-permissions <permission> [ object ... ]`

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:
	`Admin@nodename# create settings administrators profiles ... webui-permissions <permission> all`
	или
	`Admin@nodename# create settings administrators profiles ... webui-permissions <permission> [ object ... ]`

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:
	`Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all`
	или
	`Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [ object ... ]`

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.

Параметр	Описание
	• **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 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.
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.

Параметр	Описание
	• **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-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 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/отключение загрузки модуля L7: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate.
sip	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен. **Важно!** После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (кнопка **Принудительно применить** в разделе **Политики сети → Межсетевой экран**).

Параметр	Описание
h323	Включение/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/отключение загрузки модуля IDPS: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate.
sunrpc	Включение/отключение загрузки модуля SunRPC: • **on**. • **off** По умолчанию модуль выгружен.
ftp-alg	Включение/отключение загрузки модуля FTP; модуль необходимо включать для сопоставления 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/отключение блокировки пакетов с невалидным набором параметров в полях заголовка: • **on**.

Параметр	Описание
	• **off** По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной.
fw-established	Включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • **on**. • **off** По умолчанию настройка выключена.
bypass-optimization	Включение/отключение оптимизации инспектирования SSL: • **on**. • **off** 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**. 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.

Параметр	Описание
	• **strict** — соблюдать RFC. Данный режим используется по умолчанию.

Для просмотра текущих настроек используйте команду:

```
Admin@nodename# show settings proxy
```

Настройка Upstream Proxy

В интерфейсе командной строки (CLI) настройка функциональности Upstream Proxy доступна на уровне **settings general**. 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/выключение перенаправления трафика на вышестоящий прокси-сервер: • **on** — включено. • **off** — выключено.
mode	Тип вышестоящего прокси-сервера: • **HTTP(S)**. • **SOCKS5**.
ip	IP-адрес вышестоящего прокси-сервера.
port	Порт вышестоящего прокси-сервера.
auth	Аутентификация на вышестоящем прокси-сервере: • **on** — включена. • **off** — выключена.

Параметр	Описание
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/выключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • **on** — включено. • **off** — выключено.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: • **on** — включена. • **off** — выключена.
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 смотрите в статье 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 smnp-parameter**:

```
Admin@nodename# edit monitoring snmp-parameter <parameters>
```

Для редактирования доступны следующие параметры:

Наименование	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.
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**.

Наименование	Описание
	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 smnp**:

```
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. 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	

Наименование	Описание
	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 ля аутентификации SNMP-менеджеров используются команды на уровне **monitoring smnp-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

Наименование	Описание
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.

Наименование	Описание
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.

Pcap-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 pcap-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>
```

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.

Параметр	Описание
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. ◦ **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	

Параметр	Описание
	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. • **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).

Параметр	Описание
	• **"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. • **"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

Параметр	Описание
	аутентификации используются журналы ActiveDirectory и Syslog. • **BFD**: сервис Bidirectonal Forwarding Detection для быстрого обнаружения сетевых ошибок.
service-addresses	Указание разрешённых IP-адресов для сервисов: • **service**: выбор сервисов (список соответствует **enabled-services**). • **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

Параметр	Описание
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

Список упорядоченных имён сетевых интерфейсов и соответствующие им физические адреса доступен для отображения при выполнении команды (команда доступна и в режиме диагностики и мониторинга и в режиме конфигурации):

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

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

Упорядочивание интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующие команды в режиме диагностики и мониторинга и в режиме конфигурации соответственно:

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

Admin@nodename# delete network interface-mapping
```

После перезагрузки сервера UserGate список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate.

Далее будет рассмотрена настройка интерфейсов, которая производится на уровне **network interface**.

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

```
Admin@nodename# set network interface adapter <adapter_name>
```

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: 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). • **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.
zone	Зона, которой будет принадлежать интерфейс.
link-info	

Параметр	Описание
	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей читайте в разделе Настройка профилей LLDP.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся 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 задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.

Параметр	Описание
mtu	Указание размера MTU.
rx-ring	Размер буфера RX ring интерфейса типа adapter.
tx-ring	Размер буфера TX ring интерфейса типа adapter.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip | none>). • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

```
Admin@nodename# delete network interface adapter <adapter-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

```
Admin@nodename# show network interface adapter
```

Для отображения информации об адаптере:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

```
Admin@nodename# create network interface vlan
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: Layer 3 (можно 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 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.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.

Параметр	Описание
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся 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 задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **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:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

```
Admin@nodename# show network interface vlan
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

```
Admin@nodename# create network interface bond
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]`

Параметр	Описание
	где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
bonding	Дополнительные параметры бонд-интерфейса: • **aggr-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 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).

Параметр	Описание
	◦ **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, 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.

Параметр	Описание
	• **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. • **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

Параметр	Описание
	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. • **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.
iface-type	Тип создаваемого интерфейса: • **l3** — Layer 3 интерфейс. • **mirror** — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся 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 задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего бонд-интерфейса:

```
Admin@nodename# set network interface bond <bond-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

```
Admin@nodename# 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, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Настройка bridge-интерфейса

Настройка моста производится на уровне **network interface bridge**.

Чтобы добавить новый bridge-интерфейс:

```
Admin@nodename# create network interface bridge
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).
description	Описание bridge-интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.

Параметр	Описание
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
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: ◦ **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. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
ip-addresses	Назначение интерфейсу IP-адреса.

Параметр	Описание
	Адрес задаётся 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 задаётся 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-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего bridge-интерфейса:

```
Admin@nodename# set network interface bridge <bridge-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления bridge-интерфейса или его параметров:

```
Admin@nodename# 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.

Чтобы отобразить информацию о всех bridge-интерфейсах:

```
Admin@nodename# show network interface bridge
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bridge <bridge-name>
```

Настройка PPPoE

Настройка интерфейса PPPoE производится на уровне **network interface PPPoE**.

Для создания интерфейса PPPoE:

```
Admin@nodename# create network interface pppoe
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса PPPoE: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет ppp1).
description	Описание интерфейса PPPoE.
alias	Алиас/псевдоним интерфейса.
node-name	Имя узла кластера, на котором создаётся интерфейс.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.

Параметр	Описание
	• **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.

config	Дополнительные параметры PPPoE интерфейса:
	
	• **interface**: интерфейс, на котором будет создаваться интерфейс PPPoE.
	• **login**: имя пользователя для соединения PPPoE.
	• **password**: пароль пользователя для соединения PPPoE.
	• **persist-connection**: автоматическое переподключение при обрыве связи:
	  ◦ **on**.
	  ◦ **off**.
	• **auth-type**: тип авторизации:
	  ◦ **CHAP**.
	  ◦ **PAP**.
	• **holdoff**: интервал времени в секундах после разрыва соединения перед повторным запуском.

Параметр	Описание

	• **default-route**: интерфейс PPPoE в качестве маршрута по умолчанию:
	  ◦ **on**.
	  ◦ **off**.
	• **echo-interval**: интервал проверки соединения.
	• **echo-failure**: количество неуспешных проверок соединения, после которого UserGate считает, что соединение отсутствует и разрывает его.
	• **providers-dns**: использование DNS-серверов, выданных провайдером:
	  ◦ **on**.
	  ◦ **off**.
	• **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.

Обновление существующего интерфейса PPPoE:

```
Admin@nodename# set network interface pppoe <pppoe-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Команда удаления интерфейса PPPoE:

```
Admin@nodename# delete network interface pppoe <pppoe-name>
```

Чтобы отобразить информацию о всех интерфейсах PPPoE:

```
Admin@nodename# show network interface pppoe
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface pppoe <pppoe-name>
```

Настройка VPN-адаптера

VPN-адаптеры настраиваются на уровне **network interface vpn**.

Чтобы создать VPN-адаптер:

```
Admin@nodename# create network interface vpn
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VPN-интерфейса: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет tunnel1).
description	Описание VPN-интерфейса.
alias	Алиас/псевдоним 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_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]`

Параметр	Описание
	где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN), то необходимо использовать статический IP-адрес. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. Для использования интерфейса, используемого в роли клиента, необходимо выбрать динамический режим.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся 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 задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mtu	Указание размера MTU для выбранного интерфейса.

Обновление существующего интерфейса VPN:

```
Admin@nodename# set network interface vpn <vpn-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Команда для удаления интерфейса VPN или его параметров:

```
Admin@nodename# delete network interface vpn <vpn-name>
```

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех интерфейсах VPN:

```
Admin@nodename# show network interface vpn
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface vpn <vpn-name>
```

Настройка туннелей

Создание и настройка туннелей производится на уровне **network interface tunnel**.

Для создания туннелей используется команда:

```
Admin@nodename# create network interface tunnel
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение туннеля: • **on**. • **off**.
interface-number	Необходимо ввести номер, который будет отображён в названии туннеля (например 1, тогда название созданного интерфейса будет gre1).

Параметр	Описание
description	Описание туннеля.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан туннель.
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_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
mtu	Размер MTU для выбранного интерфейса.

Параметр	Описание
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. Адрес задаётся 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 задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
local-ip	Локальный адрес Point-to-Point интерфейса.
remote-ip	Удалённый адрес Point-to-Point интерфейса.
mode	Режим работы туннеля: • **gre**: GRE (протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47). • **ipip**: 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 Source IP — точкой входа в туннель, и Destination — точкой выхода из туннеля). • **vxlan**: VXLAN (протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789).
vxlan-id	Идентификатор VXLAN. Только для типа туннеля VXLAN.

Редактирование параметров существующего туннеля:

```
Admin@nodename# set network interface tunnel <tunnel-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-number**, **node-name** (изменение значений этих параметров недоступно).

Команда для удаления интерфейса туннель или его параметров:

```
Admin@nodename# delete network interface tunnel <tunnel-name>
```

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех туннелях:

```
Admin@nodename# show network interface tunnel
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface tunnel <tunnel-name>
```

Настройка loopback-интерфейса

Создание и настройка loopback-интерфейса производится на уровне **network interface loopback**.

Для создания интерфейса используется команда:

```
Admin@nodename# create network interface loopback
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.
interface-name	Название интерфейса.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]**, маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP.

Параметр	Описание
	• **manual**: без адреса. 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 читайте в разделе Настройка профилей LLDP.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
node-name	Узел кластера, на котором будет создан интерфейс.
mac	MAC-адрес интерфейса.

Параметр	Описание
mtu	Указание размера MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip | none>). • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего интерфейса:

```
Admin@nodename# set network interface loopback <interface-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания loopback-интерфейса, кроме **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления loopback-интерфейса или его параметров:

```
Admin@nodename# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех loopback-интерфейсах:

```
Admin@nodename# show network interface loopback
```

или об определённом интерфейсе:

```
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.
interface	Интерфейс, использующийся для выхода в Интернет.
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**.

Параметр	Описание
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.
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**.

Параметр	Описание
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**.
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

Правила DNS настраиваются на уровне **network dns rules** с использованием UPL. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

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")**.
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.
dns-a-records	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 dns-a-records [ 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
    dns-a-records    : 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"
dns-a-records [ 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
```

```
dns-a-records    : 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 **dns-a-records**.

Пример удаления значения параметра **dns-a-records** в ранее созданной записи и удаления всей статической записи DNS.

```
Admin@nodename# delete network dns static-records "Test DNS static
record" dns-a-records [ 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
dns-a-records    : 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
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	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**.
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:
	`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>`
	Далее указываются следующие параметры:
	• **enabled <on | off>**: включение/отключение использования интерфейса.
	• **interface**: название интерфейса, входящего в данный виртуальный маршрутизатор.
	• **description**: описание интерфейса.

Параметр	Описание
	• **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 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.

Параметр	Описание
	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** (использование MD5-хеша 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:
	`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>`
	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.

Параметр	Описание
	◦ **digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне зоны. • **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 инжекции 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	

Параметр	Описание
	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**).

Параметр	Описание
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**.
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:
	`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>`
	Параметры routemap:
	• **name** — название routemap.
	• **description** — описание routemap.

Параметр	Описание
	• **action** — действие: ◦ **allow** — разрешить прохождение данных, попадающих под условия routemap. ◦ **block** — запретить прохождение данных, попадающих под условия routemap. • **match-by** — условие применения routemap. Сравнивать по: ◦ **ip** — сравнение по IP-адресу. ◦ **aspath** — сравнение по AS пути. ◦ **community** — сравнение по Community. • **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. • **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 (_), 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.

Параметр	Описание

filters	Фильтр позволяет фильтровать маршруты при перераспределении.
	Для создания фильтра или изменения параметров созданного ранее фильтра используются следующие команды:
	`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>`
	Параметры:
	• **name** — название фильтра.
	• **description** — описание фильтра.
	• **action** — действие:
	◦ **allow** — разрешить прохождение данных, попадающих под условия routemap.
	◦ **block** — запретить прохождение данных, попадающих под условия routemap.
	• **filter-by** — условия применения фильтра. Доступно:
	◦ **ip** — фильтровать по IP-адресу.
	◦ **aspath** — фильтровать по AS пути.
	• **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.

neighbors	BGP-соседи. Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды:

Параметр	Описание

	`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>`
	
	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.
	• **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 непрямое соединение (более одного хопа):
	◦ **on**.
	◦ **off**.

Параметр	Описание
	• **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-соседям: ◦ **on**. ◦ **off**. • **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. • **routemap-in** — ограничение маршрутизирующей информации, которую BGP получает от соседей. • **routemap-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**. • **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	

Параметр	Описание
	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**. • **bgp** — распространение другим RIP-роутерам маршрутов, полученных по BGP: ◦ <metric> — 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:
	`Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces new`
	`Admin@UGOS# set network virtual-router`

Параметр	Описание
	`<virtual-router-name> rip interfaces <interface-name>` Параметры: • **interface** — выбор интерфейса. • **send-version** — версия протокола RIP, которую маршрутизатор будет отсылать. 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 посылаться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль. • **split-horizone** — метод предотвращения петель маршрутизации, при котором маршрутизатор не 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 отсылает его соседу, от которого его получил. ◦ **on**. ◦ **off**. • **passive-mode** — режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает 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.
register-suppress	Интервал, после которого маршрутизатор отсылает сообщение register suppress.
keep-alive	Интервал, через который маршрутизатор будет посылать сообщения keepalive 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:

Параметр	Описание

	`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>`
	
	Далее необходимо указать параметры:
	• **interface** — выбор интерфейса для работы мультикаст. 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.
	• **use-igmpv2** — использование версии IGMP v2, по умолчанию используется IGMP v3.

rendevouz-points	При настройке Rendevouz 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.

Параметр	Описание
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

    rendevouz-points      : []
...
```

Команда для удаления параметров мультикаст-маршрутизатора:

```
 Admin@nodename# delete network virtual-router <virtual-router-name>
multicast-router
```

Для удаления доступны следующие параметры:

- Интерфейсы, использующиеся для работы мультикаста: **interfaces**.
- Rendevouz 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**.

Параметр	Описание
	• **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). • **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.

Параметр	Описание
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	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.

Параметр	Описание
	◦ **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 ПРАВИЛ С ИСПОЛЬЗОВАНИЕМ UPL

Настройка правил с использованием UPL (Описание)

UPL — UserGate Policy Language — язык описания политик (конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента) UserGate.

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**). 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.**

UPL используется для настройки правил в следующих разделах:

- 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**).
- СОВ (уровень: **security-policy intrusion-prevention**).
- 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 (уровень: **vpn server-rules**).
- Клиентские правила (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.

В качестве примера рассмотрим создание правила межсетевого экрана (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 отобразиться 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.

Синтаксис UPL-правил WAF

Правила WAF в межсетевом экране UserGate описываются с помощью языка UPL.

Прежде всего, UPL контролирует следующее:

- требования к аутентификации пользователя;
- доступ к веб-ресурсам;
- различные аспекты обработки запросов и ответов;
- журналирование.

Правила обычно пишутся в одной строке, но могут быть разбиты на строки с помощью специального символа обратного слеша.

Любая строка, начинающаяся с символа %, является комментарием. Символ процента после пробела или табуляции определяет комментарий, который продолжается до конца строки (кроме случаев, когда символ процента отображается внутри кавычек – это часть выражения).

```
% Это комментарий
DENY("Too many Host headers") request.header.Host.count = 2..  % и это
тоже
```

Правило состоит из условий (conditions) и некоторого количества действий (actions), записанных в любом порядке. Есть еще свойства (properties), которые синтаксически выглядят как действие, но при этом активных действий не производят. Например, свойство name просто ставит атрибут имя на 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 (actions) и текущий слой (layer) 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 (actions) 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'. Если все условия выполняются, то к трафику применяются все перечисленные в правиле действия.

В свою очередь, условие является логической комбинацией триггеров (triggers). Триггеры — это отдельные тесты, которые можно сделать над компонентами запроса (url=), ответа (response.Header.Content-Type=), связанным пользователем (user=, group=) или состоянием системы (time=).

Действия — это настройки, которые управляют обработкой транзакции. Например, запретить (deny) или обработать объект, к примеру изменить заголовок (rewrite).

```
Rule ::= (PASS|FORCE_PASS|DENY|(DENY '(' string ')')|FORCE_DENY|
FORCE_DENY'(' string ')'|WARNING|OK)? Conditions '\'? Actions
Conditions ::= condition '\'? Conditions
Actions ::= action '\'? Actions
```

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

Параметр	Описание
	адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>.
ip-mac	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 ля 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 учетной 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.
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.
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.

Параметр	Описание
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	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 MFA.
description	Описание профиля MFA.
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).
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	

Параметр	Описание
	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 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

Параметр	Описание
	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**. • **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	

Параметр	Описание
	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: yyyy-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. • pki – аутентификация посредством X.509 сертификатов.
uc-profile	Выбор профиля пользовательского сертификата при аутентификации методом pki.

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 Настройка правил с использованием UPL.

Параметры правил captive-портала:

Параметр	Описание
OK **PASS**	Действия правила Captive-портала: • **OK** – использовать аутентификацию. • **PASS** – не использовать аутентификацию.

Параметр	Описание
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.
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	

Параметр	Описание
	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. 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.

Параметр	Описание
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 содания 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.

Параметр	Описание
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 будут 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 будут 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.

Параметр	Описание
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут 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 РАЗДЕЛА ПОЛИТИКИ СЕТИ

Настройка правил межсетевого экрана

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

```
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 СОВ. Подробнее о создании и настройке профилей СОВ с использованием интерфейса командной строки читайте в разделе Настройка профилей СОВ. Например: **ips_profile("Test ips profile")**.

Параметр	Описание
l7_profile	Профиль приложений. Подробнее о создании и настройке профилей приложений с использованием интерфейса командной строки читайте в разделе Настройка профилей приложений. Например: **l7_profile("Test application-profile")**.
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 (подробнее о добавлении и настройке сервисов читайте в разделе ов). • **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 Нас тройка 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.
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).

Параметр	Описание

	Примеры добавления пользователей в правило:
	
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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.

Параметр	Описание
	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

Настройка правил NAT и маршрутизации происходит на уровне **network-policy nat-routing**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

```
Admin@nodename# create network-policy nat-routing 1 upl-rule
<parameters>
```

Настройка правил типа NAT

При настройке правил типа NAT, необходимо указать следующие параметры:

Параметр	Описание
PASS **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 NAT. Например: **name("NAT rule example")**.
desc	Описание правила. Например: **desc("NAT rule example set via CLI")**.
nat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника при наттировании пакетов. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.
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(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, MAC-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.

Параметр	Описание
	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. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
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.

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 типа DNAT

При настройке правил типа **DNAT** необходимо указать следующие параметры.

Параметр	Описание
PASS **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 DNAT. Например: **name("DNAT rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("DNAT rule example created via CLI")**.
dnat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника при наттировании пакетов. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.

Параметр	Описание
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(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Чтобы указать зону источника трафика, например Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-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. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
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, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о

Параметр	Описание
	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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
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.
target_ip	Адрес назначения DNAT. Для указания адреса назначения: **target_ip("1.1.1.1")**.
target_snat	Изменение IP-адреса источника на адрес UserGate: • **target_snat(yes)** или **target_snat(true)**. • **target_snat(no)** или **target_snat(false)**.

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 типа Порт-форвардинг

При настройке правил типа **Порт-форвардинг** необходимо указать:

Параметр	Описание
PASS **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 Порт-форвардинга. Например: **name("Port forwarding rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Port forwarding rule example created via CLI")**.
port_mapping	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника при наттировании пакетов. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.
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(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**.

Параметр	Описание
	Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-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. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
port_map	Переопределение портов публикуемых сервисов: Для переопределения необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, **port_map(tcp, 2000, 2100)**. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.

Параметр	Описание
target_ip	Адрес назначения DNAT. Для указания адреса назначения: **target_ip("1.1.1.1")**.
target_snat	Изменение IP-адреса источника на адрес UserGate: • **target_snat(yes)** или **target_snat(true)**. • **target_snat(no)** или **target_snat(false)**.

Пример создания правила порт-форвардинг 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("1af47c3f-96a3-4e65-90e3-debf169bb745") \
    name(port_fw1)\
    port_mapping
```

Настройка правил типа Policy-based routing

Для настройки правил типа **Policy-based routing** нужно указать:

Параметр	Описание
PASS **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 типа Policy-based routing. Например: **name("Policy-based routing rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Policy-based routing rule example set via CLI")**.
route	Тип правила (указывается в свойствах правила).
gateway	Выбор одного из существующих шлюзов: **gateway("1.1.1.1")**. О добавлении шлюзов через CLI читайте в разделе Настройка шлюзов.
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(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о

Параметр	Описание
	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. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
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

user	Пользователи или группы пользователей, для которых применяется правило (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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

Пример создания и редактирования правила policy-based routing 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 типа Network mapping

При настройке правил типа Network mapping необходимо указать следующие параметры:

Параметр	Описание
PASS **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 типа Network mapping. Например: **name("Network mapping rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Network mapping rule example set via CLI")**.
netmap	Тип правила (указывается в свойствах правила).
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(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о

Параметр	Описание
	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. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
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
target_ip	Параметр подмены сетей; адрес сети, на которую будет производится замена, например: **target_ip("1.1.1.0")**.
direction	Параметр подмены сетей. Направление: • **direction(input)** — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении **target_ip**. • **direction(output)** — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении **target_ip**.

Пример создания правила network mapping 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 Настройка правил с использованием UPL.

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
PASS **OK**	Действие для создания правила с помощью UPL.
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.

Параметр	Описание
	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**.
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.

Параметр	Описание
	• **wlc — leighted 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. • **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.

Параметр	Описание
	Например: **ipvs_fallback(masq, 10.10.100.100:1812)**.

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:
	`monitor_kind(ping) \`
	`monitor_interval(60) \`
	`monitor_timeout(60) \`
	`monitor_failurecount(10) \`

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 **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 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.

Параметр	Описание
	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 Настройка правил с использованием UPL.

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
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.

Параметр	Описание
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; 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

Параметр	Описание
	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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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

Параметр	Описание
	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.
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. 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 Настройка правил с использованием UPL.

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** — блокировать 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)**.

Параметр	Описание
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.
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")**.

Параметр	Описание
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).
	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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

dst.zone	Зона назначения трафика, например, **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.

Параметр	Описание
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.
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.

Параметр	Описание
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 морфологи`_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.
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 Настройка правил с использованием UPL.

Для создания правила веб-безопасности используется команда:

```
Admin@nodename# create security-policy safe-browsing <position> upl-
rule
```

Параметры правил веб-безопасности:

Параметр	Описание
PASS **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	

Параметр	Описание
	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)**.
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.

Параметр	Описание
cocial_sites_block	Блокировка приложений социальных сетей: • **cocial_sites_block(yes)** или **cocial_sites_block(true)**. • **cocial_sites_block(no)** или **cocial_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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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 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 Настройка правил с использованием UPL.

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. • **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")**.

Параметр	Описание
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.
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.

Параметр	Описание
	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 nunnel-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 nunnel-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 Настройка правил с использованием UPL.

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.

Параметр	Описание
	Подробнее о создании и настройке с использованием CLI профилей пересылки читайте в разделе Настройка 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_forward_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 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.

Параметр	Описание
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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

Параметр	Описание
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.
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.

Параметр	Описание
	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 испоьзуется 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 Настройка правил с использованием UPL.

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.
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

Параметр	Описание
	ssh user@host 'command' 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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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

Параметр	Описание
	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. 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 СОВ

Настройка параметров системы обнаружения и предотвращения вторжений производится на уровне **security-policy intrusion-prevention**.

```
Admin@nodename# set security-policy intrusion-prevention <parameter>
```

Доступны параметры:

Параметр	Описание
mode	Включение/отключение режима умного сканирования (сканирование только первых байт каждой сессии): • **on**. • **off**.
limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Для просмотра состояния режима:

```
Admin@nodename# show security-policy intrusion-prevention
```

По умолчанию режим умного сканирования включен; проверяются первые 200 КБ каждой сессии.

Профили СОВ создаются в библиотеке элементов и добавляются в правила межсетевого экрана для активации системы обнаружения и предотвращения вторжений.

Настройка сценариев

Общие правила создания сценариев

Настройка сценариев происходит на уровне **security-policy scenarios** с использованием UPL (подробнее об UserGate Policy Language читайте в разделе Настройка правил с использованием UPL).

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")**.

Наименование	Описание
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 security-policy 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 security-policy 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)**.
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 СОВ

Параметры условия типа **СОВ**:

Наименование	Описание
scond_type	Тип условия: **scond_type(ips)**.
ips_tl	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)**.

Наименование	Описание
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 Размер пакета

Для создания и настройки условия типа **Размер пакета** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: **scond_type(net_packet_size)**.
packet_size	Размер пакета, при превышении которого выполняется условие; указывается следующим образом: • **packet_size(1)** – размер пакета 1 байт; • **packet_size(1KB)** – размер пакета 1 Кбайт; • **packet_size(1MB)** – размер пакета 1 Мбайт; • **packet_size(1GB)** – размер пакета 1 Гбайт.

Условие типа Сессий с одного IP

При настройке условия типа **Сессий с одного IP** используются:

Наименование	Описание
scond_type	Тип условия: **scond_type(sessions_per_ip)**.
sessions_limit	Максимальное количество сессий, разрешённых с одного IP-адреса: **sessions_limit()**.

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; • **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;

Наименование	Описание
	• **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): **he alth_answer_timeout()**.
health_type_request	Тип DNS-запроса: • **health_type_request(a)**. • **health_type_request(aaaa)**. • **health_type_request(cname)**. • **health_type_request(ns)**. • **health_type_request(ptr)**.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): **count_interval( )**.
max_event_count	Количество срабатываний: **max_event_count()**.

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 Настройка правил с использованием UPL.

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	

Параметр	Описание
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.
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

Параметр	Описание
	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.
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).

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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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"**.

Параметр	Описание
	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.

Параметр	Описание
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 Настройка правил с использованием UPL.

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,

Параметр	Описание
	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.
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.

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.

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 LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора).
	Примеры добавления пользователей в правило:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

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.

Параметр	Описание
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. 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.
port	Задать TCP-порт ICAP-сервера; значение по умолчанию: 1344.
max-msg-size	Определить максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
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 Respmod: • <text> — задать путь на сервере ICAP. • **off** — отключить использование режима Respmod.
user-header	Установить отсылку имени пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер.

Параметр	Описание
	• **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	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	

Параметр	Описание
	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 Настройка правил с использованием UPL.

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. 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;

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 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:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

dst.zone	Зона назначения 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.
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.

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 Настройка правил с использованием UPL.

Структура команды создания страницы web-портала:

```
Admin@nodename# create global-portal web-portal <position> upl-rule
<parameters>
```

Параметры настройки закладок веб-портала:

Параметр	Описание
PASS **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	

Параметр	Описание
	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 предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку. 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:

Параметр	Описание

	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

Для редактирования правила web-портала используется команда:

```
Admin@nodename# set global-portal web-portal <position> upl-rule
<parameters>
```

Для просмотра параметров правил web-портала используется команда:

```
Admin@nodename# show global-portal web-portal <position>
```

Пример создания правила web-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 web-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 Настройка правил с использованием UPL.

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
PASS **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.

Параметр	Описание
	• **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. 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

Параметр	Описание
	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): `user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")` 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	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.

Параметр	Описание
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 http://www.example.com/path1 в http://www.example.loc/path2. 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.

Параметр	Описание
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.

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 УДАЛЁННОГО ДОСТУПА (VPN)

Настройка серверных правил

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе Настройка правил с использованием UPL.

Для создания серверного правила VPN используется команда:

```
Admin@nodename# create vpn server-rules <position> upl-rule
<parameters>
```

При настройке необходимо указать:

Параметр	Описание
PASS **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.
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

Параметр	Описание
	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.
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.
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.

Параметр	Описание
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 локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): `user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc")` 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 Настройка правил с использованием UPL.

Команда для создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules <position> upl-rule
<parameters>
```

При настройке правил необходимо указать:

Параметр	Описание
PASS **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")**.

Параметр	Описание
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, статус подключения и время соединения.

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.
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".

Параметр	Описание
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 зарыт 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 парамеров 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 <parameter>
```

Настраиваемые параметры серверного профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
ike-version	Версия протокола IKE (Internet Key Exchange), использующегося для создания защищённого канала связи между двумя сетями. В NGFW поддерерживаются версии IKEv1 и IKEv2. Возможны следующие варианты конфигурации: • **IKEv1** — для создания защищенного канала будет использоваться IKEv1. • **IKEv2** — для создания защищенного канала будет использоваться 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)

Параметр	Описание
	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.
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	

Параметр	Описание
	Метод аутентификации. Возможна аутентификация с помощью логина и пароля через RADIUS сервер (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. 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.).

Параметр	Описание
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 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: `Admin@nodename# create vpn server-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>` Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**. • **encrypt-alg**: выбор алгоритма шифрования. ◦ **DES**. ◦ **3DES**. ◦ **AES128**. ◦ **AES192**.

Параметр	Описание
	◦ **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-lifesize-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifesize	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-lifesize**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: **off**.
nat-keepalive	Период отправки пакетов NAT kepalive 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 keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону peer-узла для поддержания сесси NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: `Admin@nodename# create vpn server-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>` Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**.

Параметр	Описание
	• **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** — установление L2TP/IPsec VPN. • **IPsec** — Установление IPsec VPN с оборудованием Cisco. • **IKEv2-with-certificate** — установление 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 использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и

Параметр	Описание
	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.
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.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.

Параметр	Описание
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 до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).

Параметр	Описание
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: `Admin@nodename# create vpn client-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>` Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**. • **encrypt-alg**: выбор алгоритма шифрования. ◦ **DES**. ◦ **3DES**. ◦ **AES128**. ◦ **AES192**. ◦ **AES256**.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное

Параметр	Описание
	во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifesize-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifesize	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-lifesize**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: **off**.
nat-keepalive	Период отправки пакетов NAT kepalive 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 keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону peer-узла для поддержания сесси NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: `Admin@nodename# create vpn client-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>` Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**. • **encrypt-alg**: выбор алгоритма шифрования. ◦ **DES**. ◦ **3DES**. ◦ **AES128**. ◦ **AES192**.

Параметр	Описание
	◦ **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 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.

Параметр	Описание
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".
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.

Параметр	Описание
	Для добавления слов и фраз: `Admin@nodename# create libraries morphology ... words new word "word or phrase" weight <weight>`

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). • **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. • **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.

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".
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> [ <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.
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".

Параметр	Описание
	• 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. 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
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. • 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	

Параметр	Описание
	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). ■ **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.

Параметр	Описание
	■ **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 DCSP для 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** — страница блокировки.

- **captiveportal-user-auth** — страница авторизации captive-портала.
- **captiveportal-user-session** — captive-портал, сессия пользователя.
- **content-warning** — содержание страницы предупреждения.
- **ftp-client** — страница отображения FTP поверх HTTP.
- **proxy-portal** — страница веб-портала.
- **pp-login-ssh** — страница SSH-логина веб-портала.
- **pp-login-rdp** — страница RDP-логина веб-портала.
- **totp-init-page** — страница инициализации TOTP.

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.
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.

Параметр	Описание
	• **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-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

Параметр	Описание
	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**. 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.

Параметр	Описание
	• **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.
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>
```

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.
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	

Параметр	Описание
	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • **very-low** — очень низкий. • **low** — низкий. • **medium** — средний. • **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>
```

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.
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 СОВ

На уровне **libraries ips-signature** возможно создание и настройка пользовательских кастомизированных сигнатур системы обнаружения вторжения (СОВ).

Для создания пользовательской сигнатуры СОВ используется команда:

```
Admin@nodename# create libraries ips-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры СОВ. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры СОВ. 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 срабатыване 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
	• shellcode — сигнатуры, определяющие известные попытки запуска программных оболочек. • smtp — известные уязвимости протокола SMTP. • snmp — известные уязвимости протокола SNMP. • sql — известные уязвимости SQL. • telnet — известные попытки взлома по протоколу telnet. • tftp — известные уязвимости протокола TFTP. • user_agents — сигнатуры подозрительных Useragent. • voip — известные уязвимости протокола VoIP. • web_client — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps — сигнатуры, определяющие известные попытки взлома различных веб приложений. • worm — 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. • arbitrary-code-execution — попытка запуска произвольного кода. • attempted-admin — попытка получения административных привилегий. • attempted-dos — попытка совершения атаки Denial of Service. • attempted-recon — попытка атаки, направленной на утечку данных. • attempted-user — попытка получения пользовательских привилегий. • bad-unknown — потенциально плохой трафик. • command-and-control — попытка общения с C&C центром • default-login-attempt — 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 СОВ:

```
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 СОВ:

```
Admin@nodename# show libraries ips-signature
```

или об определенной сигнатуре:

```
Admin@nodename# show libraries ips-signature <ips-signature-name>
```

Пример создания сигнатуры СОВ:

```
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 СОВ используется команда:

```
Admin@nodename# delete libraries ips-signature <ips-signature-name>
```

Настройка профилей СОВ

Настройка профилей СОВ 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 СОВ.
description	Описание профиля СОВ.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур СОВ.

Представленная ниже команда предназначена для редактирования существующего профиля СОВ:

```
 Admin@nodename# set libraries ips-profile <ips-profile-name>
<parameter>
```

С помощью следующей команды можно перенастроить параметры системных сигнатур СОВ, 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 СОВ 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 СОВ:

```
Admin@nodename# show libraries ips-profile
```

или об определенном профиле:

```
Admin@nodename# show libraries ips-profile <ips-profile-name>
```

Пример создания профиля СОВ:

```
Admin@nodename# create libraries ips-profile name testipsprofile1
filters new enabled on value "threat > 2 AND owner = 'UserGate'"
Admin@nodename# show libraries ips-profile testipsprofile1

name           : testipsprofile1
filters        :
```

```
    enabled    : on
    value      : threat > 2 AND owner = 'UserGate'
```

Для удаления профиля СОВ используется команда:

```
Admin@nodename# delete libraries ips-profile <ips-profile-name>
```

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.
connection-security	Варианты безопасности отправки почты; возможны варианты: • **none**. • **starttls**. • **ssl**.
authentication	

Параметр	Описание
	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.
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:

Параметр	Описание
	`Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [ +7¦8 ]`
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. • **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	

Параметр	Описание
	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. • **10** — Netflow версии 10.

Параметр	Описание
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.
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: • **tls1**. • **tls1.1**. • **tls1.2**.
max-tls-version	

Параметр	Описание
	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: • **l2**. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • **l3**. Копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адресы 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).
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.
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.

Параметр	Описание
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. • **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.

Параметр	Описание
	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.

Параметр	Описание
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-пакетов BFD; указывается в миллисекундах.
echo-mode	Включить или выключить режим передачи **Echo mode**.
pessive-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>
```

USERGATE APPLICATION AND SECURITY LANGUAGE (UASL)

UserGate Application and Security Language (UASL)

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 СОВ 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.

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 СОВ; 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>];
```

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).

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; .nopaylo
ad;)
```

> **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";
```

> **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.

Модификаторы области поиска

.no_case

Модификатор **no_case** позволяет осуществлять поиск, заданный параметром позволяет осуществлять поиск, заданный параметром **.pattern**, без учета регистра символов.

.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.
body	Областью поиска является содержимое пакетов HTTP.
file	Областью поиска являются: декодированное http содержимое, вложения в eml, ftp-data сессии.

.service

Данный модификатор области поиска предназначен для выбора диссектора:

```
.service=<MODE>;
```

где <MODE> может принимать следующие значения:

Наименование	Описание
http	Разбор протокола HTTP.

.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

	`.distance=<RANGE> [,<MODE>];`
	
	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:
	
	`.distance=10;`
	
	Пример использования опциональных параметров:
	
	• пропустить 10 байтов от начала:
	
	`.distance=10, start;`
	
	• пропустить 10 байтов от последнего найденного шаблона:
	
	`.distance=10, match;`

.within	Сканировать в заданном интервале (RANGE) от начала или последнего найденного блока (шаблон полностью попадает в заданный интервал).
	
	Задаётся в формате:
	
	`.within=<RANGE> [,<MODE>];`
	
	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:
	
	`.within=10;`
	
	Пример использования опциональных параметров:
	
	• поиск с 1-го (с начала) по 10-й байт:
	
	`.within=10, start;`

Наименование	Описание
	• поиск в диапазоне 10 байтов после последнего найденного шаблона: `.within=10, match;`
.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: `.startin=<RANGE> [,<MODE>];` 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: `.at=<RANGE> [,<MODE>];` 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.

.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.

> **Примечание**
> **Можно задать только один протокол. Если протокол не указан, то сигнатура применяется только к трафику TCP и UDP.**

Частота срабатывания

При задании частоты срабатывание сигнатуры СОВ 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=fr
om_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.

Наименование	Описание
*	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: `.byte_test=1,&,0x80,0;` 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. 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.

Наименование	Описание
<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**.

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: **=**, **!=**.

Наименование	Описание
.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, использующейся 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: `.tcp.seq=<value>,relative;` где <value> - порядковый номер TCP.
.tcp.flags	Проверка TCP-флагов: `.tcp.flags=[<mod>]<tcp_flags>;` где <mod> — модификатор. <tcp_flags> — флаг TCP, который может быть указан как в буквенном, так и в числовом (десятеричной или шестнадцатеричной системах) форматах. 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.

Наименование	Описание
	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 относится к протколам TCP и UDP.

UDP

Для проверки свойств заголовка UDP доступно использование следующих параметров:

Наименование	Описание
.udp.sport	Проверка номера порта или диапазона портов источника. Доступно использование следующих операторов: **=**, **!=**.
.udp.dport	Проверка номера порта или диапазона портов назначения. Доступно использование следующих операторов: **=**, **!=**.
.udp.checksum	Проверка контрольной суммы. Доступно использование следующих операторов: **<**, **>**, **<=**, **>=**, **=**, **!=**.
.udp.data_size	Размер полезной нагрузки пакета UDP (без учета заголовков). Поддерживаются следующие операторы: **<**, **>**, **<=**, **>=**, =, **!=**. Возможно указание как .data_size, тогда параметр будет относится к протколам TCP и UDP.

HTTP

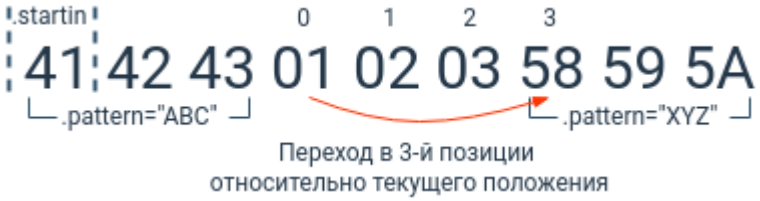
Для проверки свойств заголовка HTTP доступно использование следующих параметров:

Наименование	Описание
.uri	Проверка поля идентификатора ресурса (URI).
.body	Проверка тела содержимого запроса или ответа HTTP.
.host	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 находится 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.

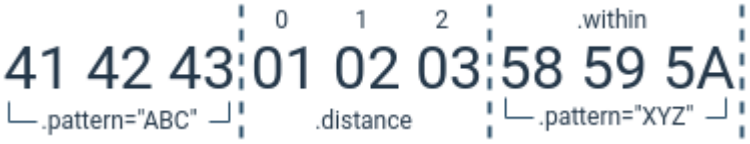
Пример 2


```
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**.

PLATFORM MANAGEMENT CONTROLLER COMMAND LINE INTERFACE

Общие сведения

Для программно-аппаратных комплексов (ПАК) UserGate доступен PMC CLI, предназначенный для мониторинга и управления устройством UserGate.

Структура команд PMC CLI идентична структуре команд CLI основного продукта:

```
<action> <level> <filter> <configuration_info>
```

где:

<action>: действие, которое необходимо выполнить (create, set, show, delete).

<level>: уровень конфигурации (cli, platform, network, factory, users).

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

Также существуют команды, которые позволяют выполнить действия, не относящиеся к конфигурации.

Наименование	Описание

help	Отображение списка доступных команд и краткая информации о них. Помимо **help** возможно использование **?**.
	Для получения подробного описания команды используйте команду типа:
	`PMC> help <command_name>`
	или
	`PMC> ? <command_name>`

Наименование	Описание

	Например:
	
	`PMC> ? ping`
	`ping - send ICMP ECHO_REQUEST to network host`
	`Usage:`
	`ping <Address> [size]`

aux	Переход в интерфейс командной строки (CLI) основного продукта. Для возвращения в PMC CLI используется комбинация клавиш «**CTRL +]**»
autoboot	Запуск команды автозагрузки.
history	Вывод истории команд.
ping	Отправка сообщение ICMP Echo Request к хостам сети; выполняется 5 раз с интервалом в 1 секунду. В качестве опционального параметра можно задать размер данных в пакете.
reset	Перезапуск устройства.
update	Обновление компонентов программного обеспечения (ПО) или вспомогательных элементов. Для обновления доступны: • **pmc** — обновление прошивки Platform Management Controller. • **pmc-backup** — обновление резервного образа PMC. • **boot** — вспомогательное ПО, занимающееся запуском основного образа. • **sys-recovery** — вспомогательная система, позволяющая удалённо в ручном режиме восстановить работоспособность устройства, например, если основной образ был повреждён. Команда имеет следующую структуру: `PMC> update firmware <pmc | pmc-backup | boot | sys-recovery> tftp <address> <filename>` где: <address> - адрес сервера TFTP.

Наименование	Описание

	<filename> - название файла обновления.
	Например, команда обновления прошивки PMC:
	`PMC> update firmware pmc tftp <address> <filename>`
	Обновление приватного ключа SSH:
	`PMC> update key ssh tftp <address> <filename>`
	Важно! Ключ должен быть предварительно сгенерирован и сохранён в формате .der.

version	Отображение текущей версии прошивки PMC.

configure	Вход в режим конфигурирования. После выполнения этой команды меняется промпт в консоли и появляется возможность исполоьзования команд **set**, **delete**, **create**, **diff**, **revert**. Команды непосредственного управлени я платформой (которые не сохраняются в энергонезависимой памяти) отрабатывают сразу при выполнении команды. Настройки требующие сохранения (пока работает только для сетевых настроек) применяются и сохраняются только после команды exit.
	`PMC> configure`
	`PMC#`
	`PMC# exit`
	`PMC>`

exit	Выход из режима конфигурирования и применение настроек. Или logout из терминала.

Управление платформой

Данному разделу соответствует уровень конфигурации **platform**. Команды данного уровня позволяют управлять компонентами устройства UserGate.

Наименование	Описание
bypass	

Наименование	Описание

	Команды управления выполняются на уровне **platform bypass**. В данном разделе реализовано управление состоянием bypass реле сетевых портов и просмотр текущего состояния и мапинга реле.
	Формат команды установки:
	`PMC> set platform bypass <relay-number> <state>`
	`PMC> set platform bypass all <state>`
	где:
	<relay-number> – номер конфигурируемого реле.
	<state> – состояние реле. Возможны следующие значения:
	• **enable** – глобальная настройка; позволяет использовать функционал реле. При отключенном питании реле будут замкнуты. Значение сохраняется в энергонезависимой памяти (если реле выставлено в состояние **enable**, то после перезапуска устройства реле остаются замкнутыми, пока не будет отправлена команда на размыкание).
	• **disable** – глобальная настройка; значение сохраняется в энергонезависимой памяти (если реле выставлено в состояние **disable**, то после перезапуска устройства реле разомкнутся в процессе перезапуска PMC).
	• **on** – замыкание bypass реле (трафик идёт мимо процессора). Состояние сбрасывается после перезапуска.
	• **off** – размыкание bypass реле (трафик идёт через процессор). Состояние сбрасывается после перезапуска.
	Для вывода состояний реле используется следующая команда:
	`PMC> show bypass`

Наименование	Описание
fan	Данный раздел находится на уровне **platform fan**. Команды данного раздела позволяют производить мониторинг работы вентилятора охлаждения. Команда для отображения текущего состояния: `PMC> show platform fan`

soc	Для запуска или остановки процессора необходимо выполнить команду:
	`PMC> set platform soc <start | stop>`
	Для просмотра статуса процессора:
	`PMC> show platform soc`

accelerator	Команда мониторинга работы аппаратного ускорителя (присутствует только на моделях с аппаратным ускорителем). Для просмотра статуса аппаратного ускорителя: `PMC> show platform accelerator`

therm	Мониторинг температуры хост-процессора и платы производится на уровне **platform therm**.
	Для просмотра текущего состояния:
	`PMC> show platform therm`
	Для просмотра только значений температур хост-процессора и платы:
	`PMC> show platform therm value`

power	Раздел мониторинга источников питания производится на уровне **platform power**. Для отображения информации о рабочем состоянии источников питания используется команда: `PMC> show platform power`

Наименование	Описание
	Также доступно указание следующих параметров: • **status** – состояние источников питания. • **measurements** – показания токов и напряжений. Следующая команда предназначена для включения/отключения всего питания, кроме дежурного, т.е. PMC продолжает работу: `PMC> set platform power <on | off>`

Для отображения информации о всех параметрах, доступных на данном уровне конфигурации:

```
PMC> show platform
```

Управление настройками сети

Команды управления настройками сети доступны на уровне **network**. В данном разделе доступна установки и просмотр следующих параметров:

Наименование	Описание

dhcp	Включение выключение DHCP клиента.
	По умолчанию DHCP выключен и используется заданный в настройках IP-адрес.
	Команда включения DHCP:
	`PMC> set network dhcp on`
	Посмотреть пполученные по DHCP настройки можно следующей командой:
	`PMC> show network status`

ip	Статический IP-адрес устройства; значение по умолчанию: 192.168.1.2. Для выставления IP-адреса используется команда:

Наименование	Описание

	`PMC> set network ip <IP_adrress>`
	Чтобы отобразить IP-адрес устройства:
	`PMC> show network ip`
	Также доступен сброс значения параметра до значения по умолчанию:
	`PMC> delete network ip`

netmask	Маска подсети; значение по умолчанию: 255.255.255.0.
	Команда изменения значения маски подсети:
	`PMC> set network netmask <netmask_value>`
	Для отображения текущего значения маски подсети:
	`PMC> show network netmask`
	Также доступен сброс значения параметра до значения по умолчанию:
	`PMC> delete network netmask`

gateway	Шлюз по умолчанию; значение по умолчанию: 192.168.1.1.
	Команда для изменения значения шлюза по умолчанию:
	`PMC> set network gateway <gateway_address>`
	Следующая команда предназначена для отображения текущего адреса шлюза по умолчанию:
	`PMC> show network gateway`
	Чтобы сбросить параметр до значения по умолчанию:
	`PMC> delete network gateway`

vlan	Идентификатор VLAN; значение по умолчанию – 0. Устройство получает все пакеты и при отправке не

Наименование	Описание

	использует VLAN Tag. Если значение отлично от 0, то все пакеты, приходящие с тегом, отличным от выставленного, или без тега, фильтруются. При отправке в Ethernet-заголовок добавляется указанное значение параметра.
	Для изменения значения:
	`PMC> set network vlan <VLANID_value>`
	Для просмотра текущего значения:
	`PMC> show network vlan`
	Для установки значения по умолчанию:
	`PMC> delete network vlan`

arp	Таблица ARP-записей. По умолчанию таблица устройства пустая. При общении с другими узлами сети в таблицу добавляются динамические записи, которые имеют небольшое время жизни и после перезапуска устройства всегда сбрасываются.
	Существует возможность добавления статических ARP-записей. При добавлении необходимо указать IP и MAC. Если IP-адрес назначения присутствует в таблице, то при отправке пакета устройство не делает ARP-запрос, а сразу подставляет в Ethernet-заголовок MAC-адрес из таблицы.
	Для добавления статических ARP-записей:
	`PMC> network arp <IP_address> <HW_address>`
	Чтобы отобразить таблицу ARP:
	`PMC> show network arp`
	Следующая команда позволяет очистить таблицу:
	`PMC> delete network arp`
	Помимо очистки всей таблицы доступно удаление отдельной записи ARP; для удаления необходимо указать IP-адрес:
	`PMC> delete network arp <IP_address>`

Наименование	Описание

ssh-port	Порт, использующийся для входящих подключений PMC SSH. Значение по умолчанию: 22.
	Для изменения порта подключения используется команда:
	`PMC> set network ssh-port <port_number>`
	Чтобы отобразить текущее значение параметра:
	`PMC> show network ssh-port`
	Чтобы вернуть значение параметра по умолчанию:
	`PMC> delete network ssh-port`

nameserver	Адрес DNS сервера.
	По умолчанию адрес DNS сервера не задан и имеет значение 0.0.0.0
	Для изменения значения используется следующая команда:
	`PMC> set network nameserver <IP-address>`
	Для просмотра значения:
	`PMC> show network nameserver`

rule	Правила доступа к MGMT порту. Позволяет составлять белые и черные списки ip адресов для доступа к PMC.
	Примеры добавления правил:
	`PMC> set network rule allow 192.168.1.1 192.168.1.20`
	`Access rule added successfully`
	`PMC> set network rule drop 192.168.1.5 192.168.1.10`
	`Access rule added successfully`
	Прогсмотр правил:
	`PMC> show network rule`

Наименование	Описание
	Удаление правил: `PMC> delete network rule <IP-addresses>`

Чтобы отобразить значения всех параметров уровня **network**

```
PMC> show network
```

После изменения сетевые настройки хранятся в энергонезависимой памяти.

С использованием действия **delete** производится сброс параметров до значений по умолчанию (всех параметров или конкретного):

```
PMC> delete network
```

Работа с заводскими параметрами

Данные параметры устанавливаются один раз —в ходе производственного тестирования. Далее параметры доступны только для чтения.

Для отображения параметров:

```
PMC> show factory
```

Укажите параметр, чтобы посмотреть его значение:

- **sn —серийный номер устройства.**
- **type —тип устройства.**
- **mac — физический адрес (MAC-адрес).**

Управление пользователями

Команды управления пользователями доступны на уровне **users**. В данном разделе доступно создание и удаление пользователей, а также настройка

методов авторизации на SSH-сервере. Устройство позволяет завести до 10 пользователей.

Для создания пользователя используется следующая команда:

```
PMC> create users <username>
```

Далее пользователю необходимо задать метод авторизации и пароль и/или публичный ключ. До задания метода авторизации пользователь не может быть использован.

По умолчанию всегда есть один пользователь **admin** с паролем по умолчанию **password**.

В качестве методов авторизации доступно использовать пароль и публичный ключ ECDSA. Для пользователя может быть задан один или сразу оба метода авторизации.

Чтобы задать авторизацию по паролю:

```
PMC> set users <username> password <password_value>
```

Для задания авторизации по публичному ключу ECDSA:

```
PMC> set users <username> key <public_key_type> <public_key>
```

Чтобы отключить один из способов авторизации, удалите ключ или пароль. Используйте команду с действием **delete**.

```
PMC> delete users <username> <password | key>
```

Для просмотра информации пользователях (всех или определённого); отображаются логин, метод авторизации, публичный ключ:

```
PMC> show users
PMC> show users <username>
```

Работа в режиме загрузчика

Режим загрузчика (PMC-loader) предназначен для обеспечения возможности восстановления работоспособности программно-аппаратного комплекса.

> **Примечание**
> **Режим загрузчика доступен только при подключении через консольный порт.**

Для перехода в данный режим необходимо нажать клавишу **Enter** во время вывода следующей строки:

```
Hit 'Enter' key to stop autoboot: 3
```

Строка приглашения будет выглядеть следующим образом:

```
loader>
```

> **Примечание**
> **В режиме загрузчика работает таймер неактивности. Если в течении 45 секунд выполнение команд не производилось, то устройство будет перезагружено.**

В данном режиме набор доступных команд ограничен. Доступны следующие команды:

- настройка сети без сохранения параметров;
- просмотр версии и factory-параметров;
- отображение уровней напряжений, температуры;
- обновление ПО.

ДАШБОРД

Приборная панель (DashBoard)

Данный раздел позволяет посмотреть текущее состояние NGFW, его загрузку, количество пользователей, объемы трафика, проходящего через NGFW, работу систем фильтрации, статус лицензии и так далее. Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: • Число. • Круговая диаграмма. • Вертикальная гистограмма. • Горизонтальная гистограмма. • Таблица. • График. • Карта мира.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.

> **Примечание**
> **Доступно использование выделения для более подробного ознакомления с определённой частью графика; для возвращения необходимо использовать двойной клик левой кнопкой мыши.**

ПОМОЩЬ

Помощь (Описание)

Раздел предоставляет ссылки на полезные ресурсы портала технической поддержки UserGate:

Наименование	Описание
Помощь	Ссылка на актуальную версию руководства администратора.
Обучающее видео	Ссылка на список видеороликов, объясняющих настройку различных служб UserGate.
Поддержка	Ссылка на портал службы технической поддержки UserGate на сайте компании https://www.usergate.com/ru/support содержит дополнительную информацию по настройке UserGate. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

ADMIN

ADMIN (описание)

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
Сменить пароль	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
Предпочтения	• Количество элементов на странице — устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана. • Ночной режим — устанавливает черный цвет темы графического интерфейса UGOS. • Популярные фильтры — изменение названия или удаление фильтров различных журналов, созданных данным пользователем.
Выход	Завершение сеанса работы в веб-консоли устройства.

ИЗБРАННЫЕ

Избранные

В веб-интерфейсе имеется возможность фильтрации отображаемых разделов путем их добавления в избранное и поиск разделов по их названию. Фильтрация позволяет скрыть неиспользуемые разделы. Отображение только избранных разделов не влияет на функциональность или конфигурацию устройств. Чтобы добавить раздел в избранные, необходимо отметить символ звездочки напротив названия раздела; для настройки отображения используйте переключатель **Только избранные**, расположенный в нижней части панели.

ПРИЛОЖЕНИЯ

Установка сертификата локального удостоверяющего центра

Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика, как это описано в главе Управление сертификатами, и следуйте инструкциям по установке сертификата ниже в этом разделе.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

Откройте папку, куда вы скачали pem-сертификат, переименуйте его в user.der и дважды нажмите на него:

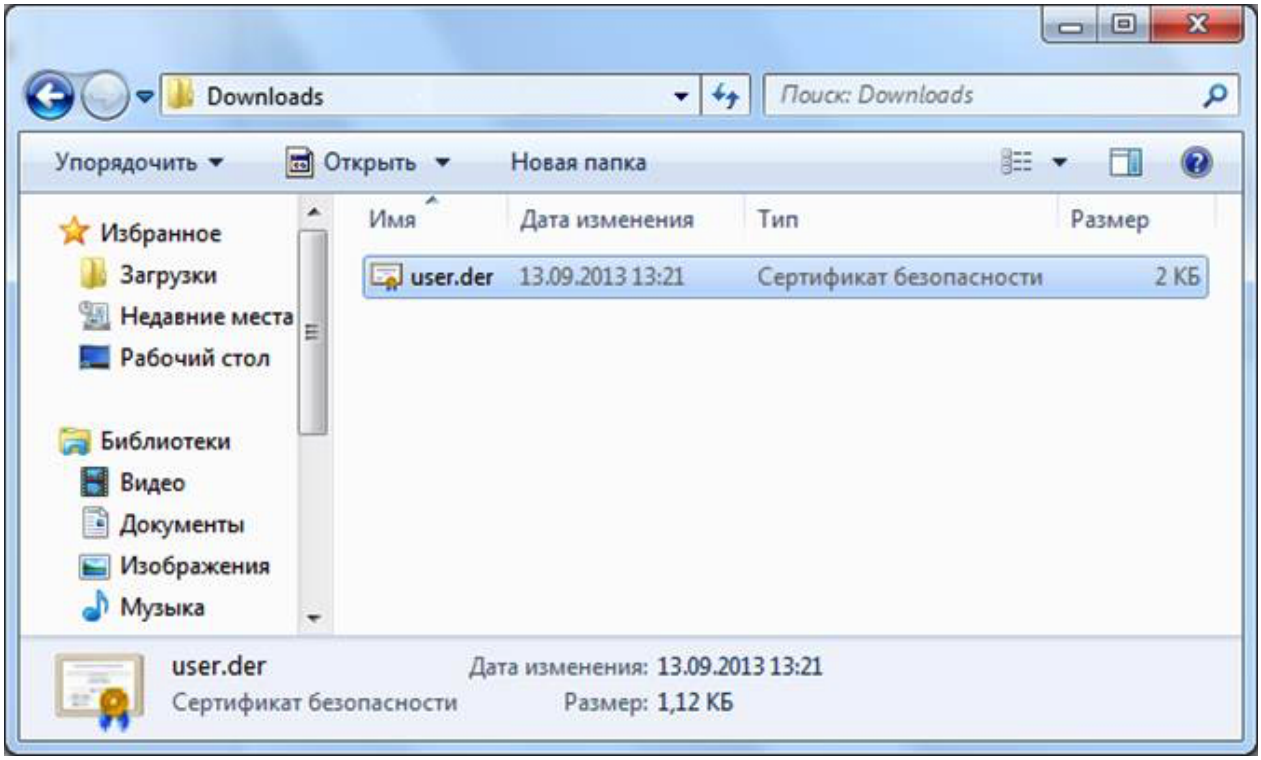


Рисунок 5 Выбор файла сертификата

Откроется информация о сертификате. Нажмите на кнопку **Установить сертификат**:

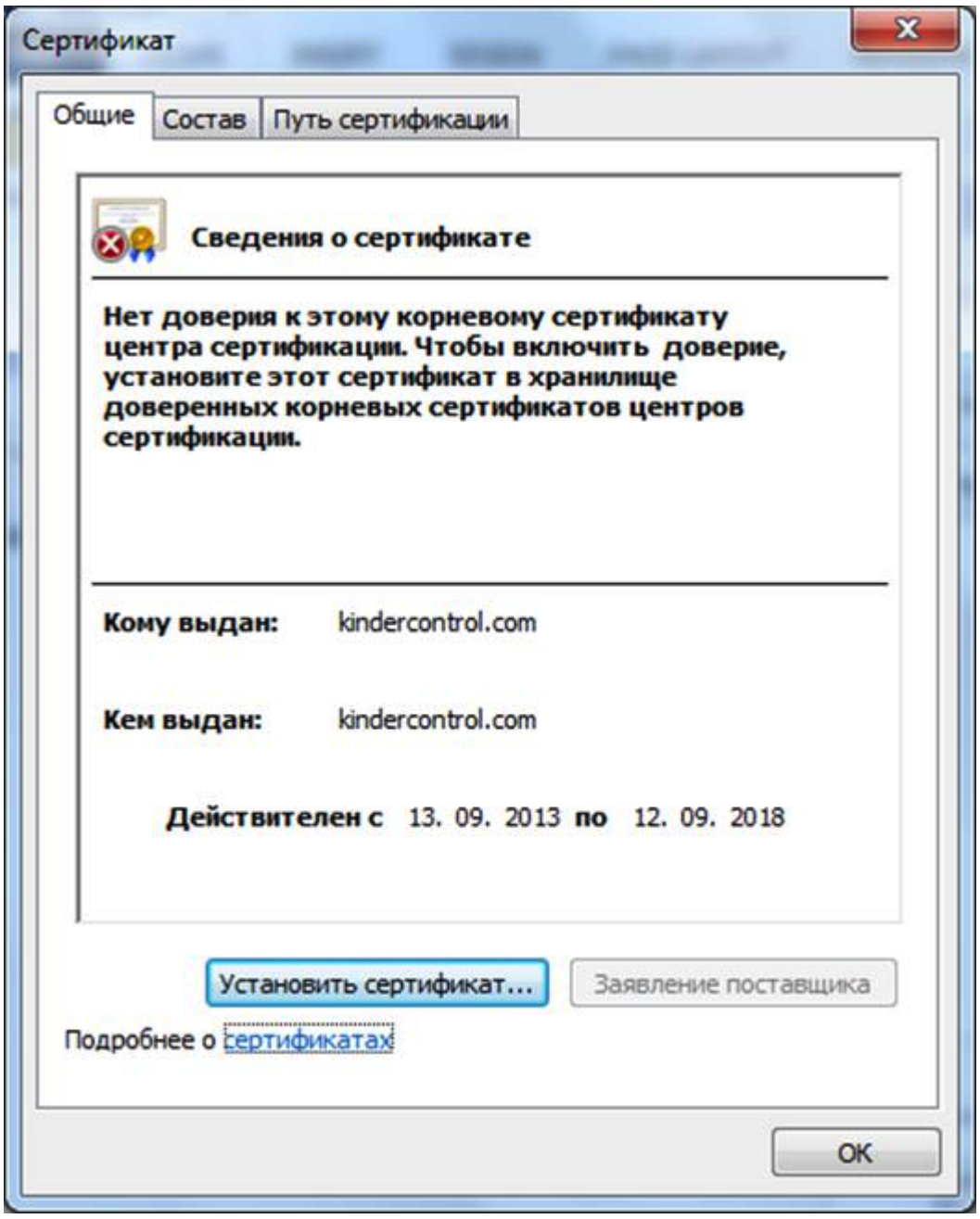


Рисунок 6 Установка сертификата

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

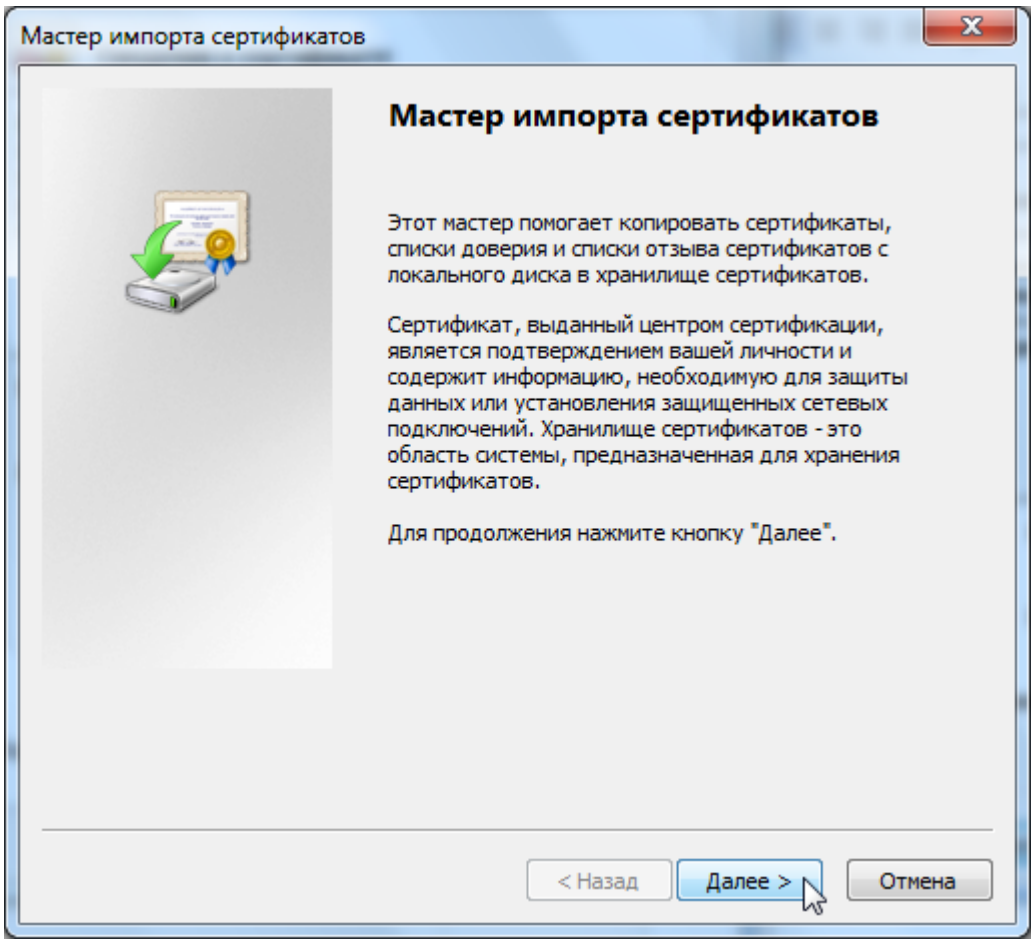


Рисунок 7 Мастер импорта сертификатов

Выберите хранилище сертификата и нажмите кнопку **Обзор**:

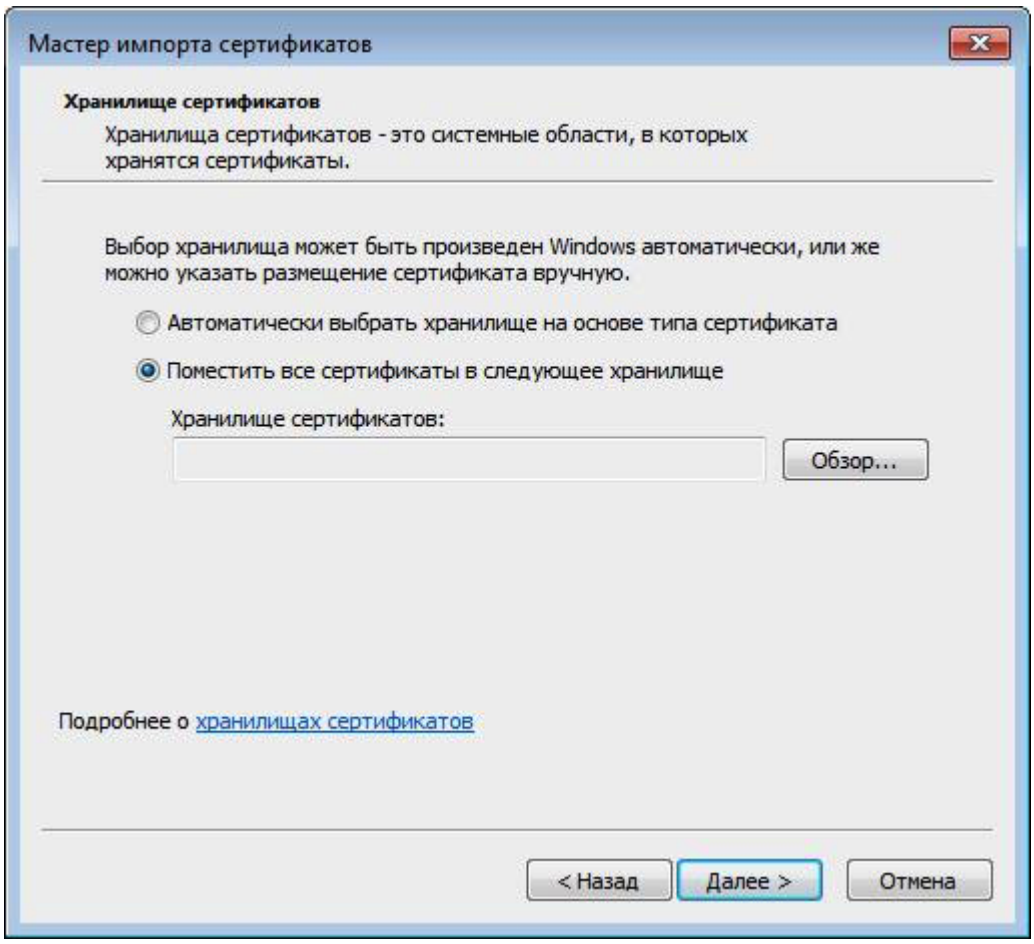


Рисунок 8 Выбор хранилища

Выберите **Доверенные корневые центры сертификации** и нажмите кнопку **ОК**:

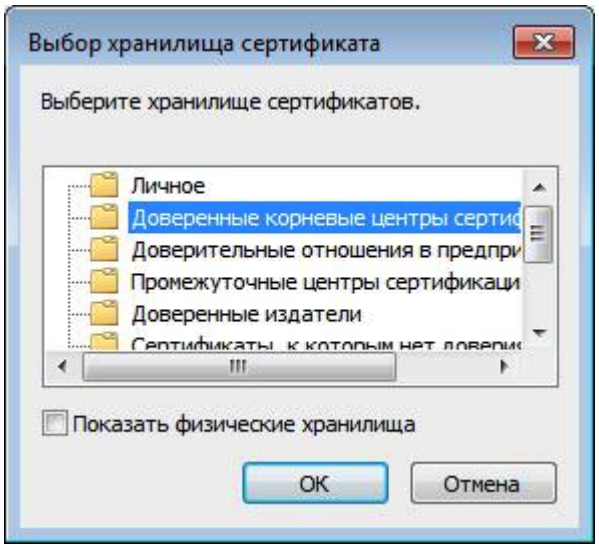


Рисунок 9 Выбор хранилища (продолжение)

Нажмите кнопку «Готово»:

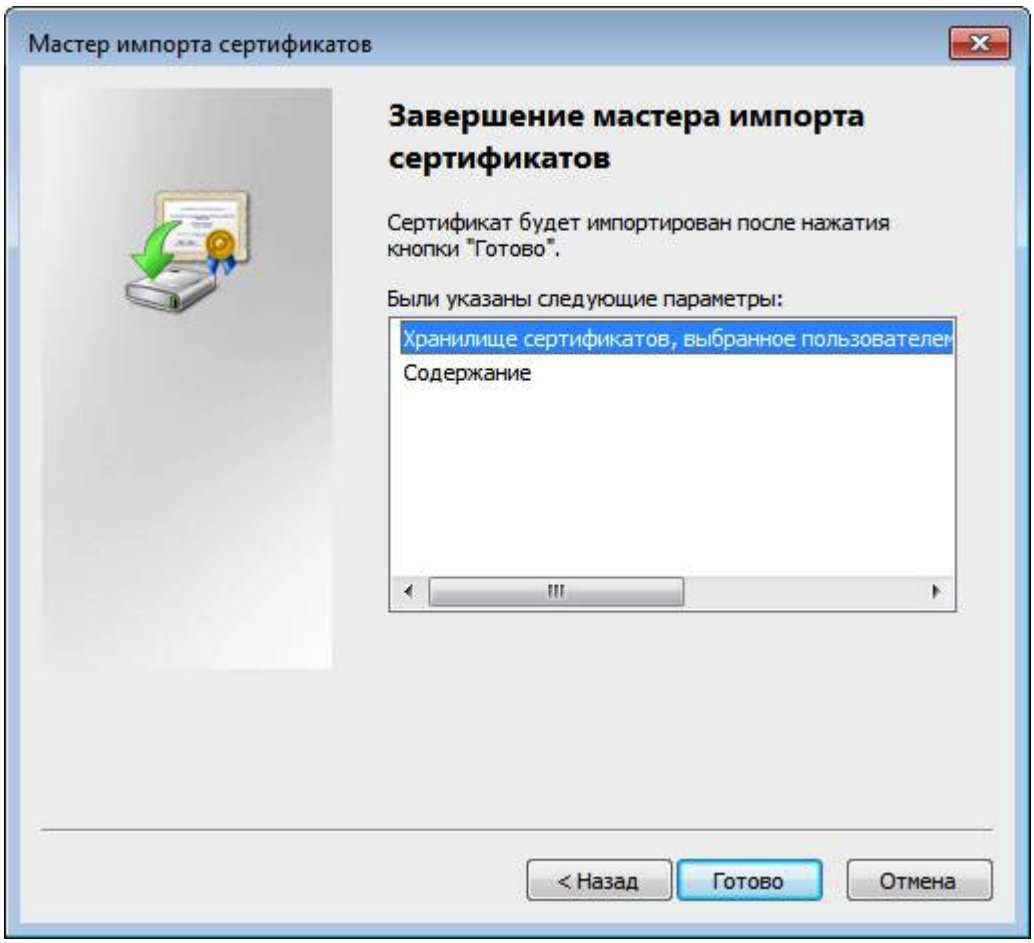


Рисунок 10 Завершение импорта

Когда появится предупреждение системы безопасности, нажмите кнопку **Да**:

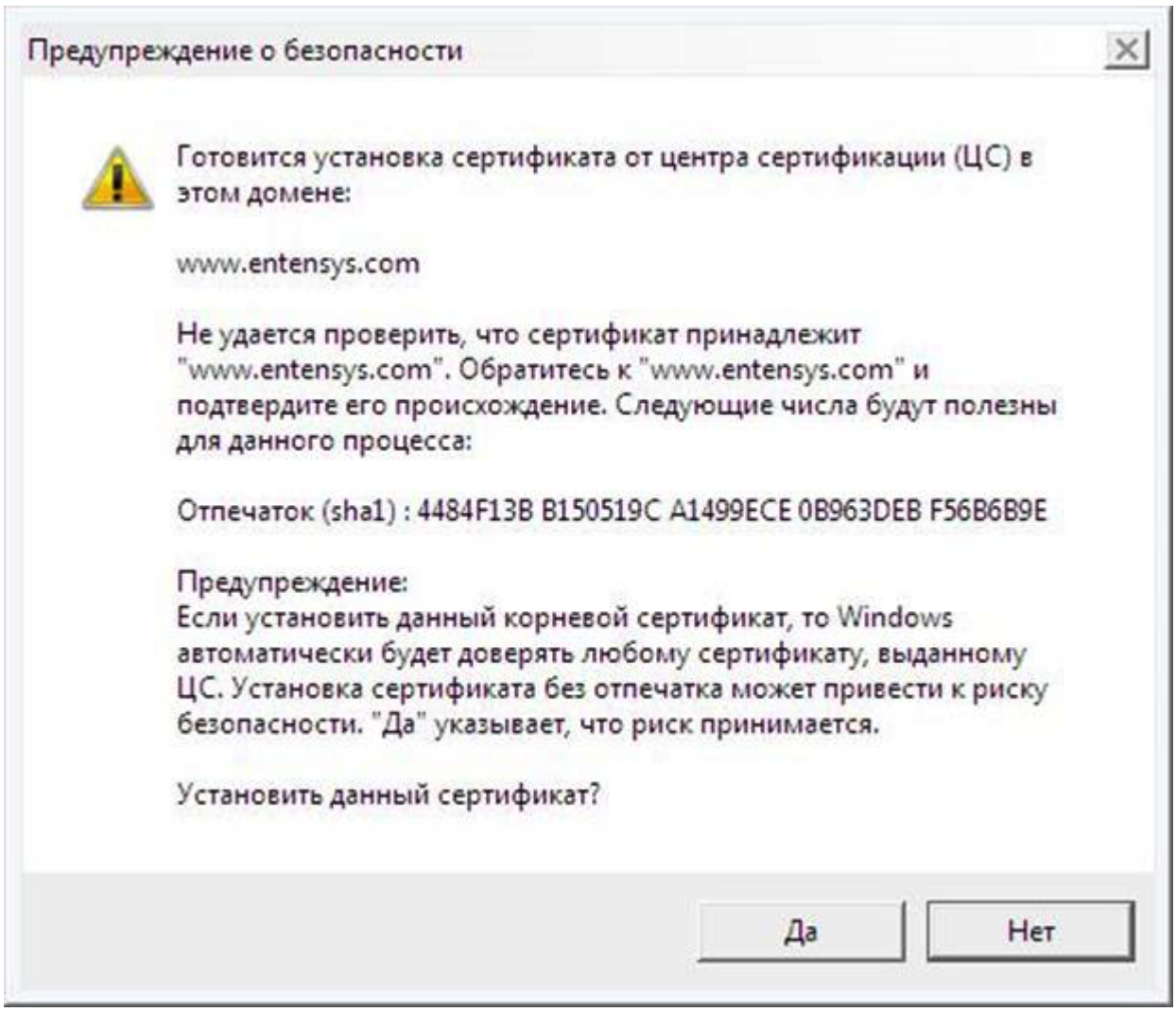


Рисунок 11 Согласие на установку сертификата

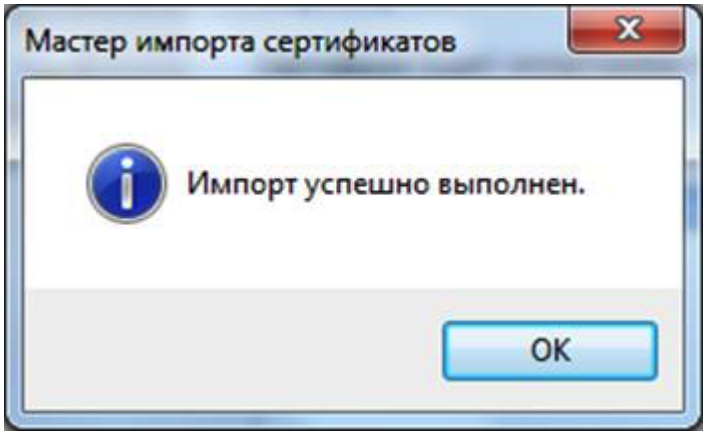


Рисунок 12 Установка завершена

Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в ОС MacOSX

Перейдите в папку, куда вы скачали pem-сертификат и дважды нажмите на него:

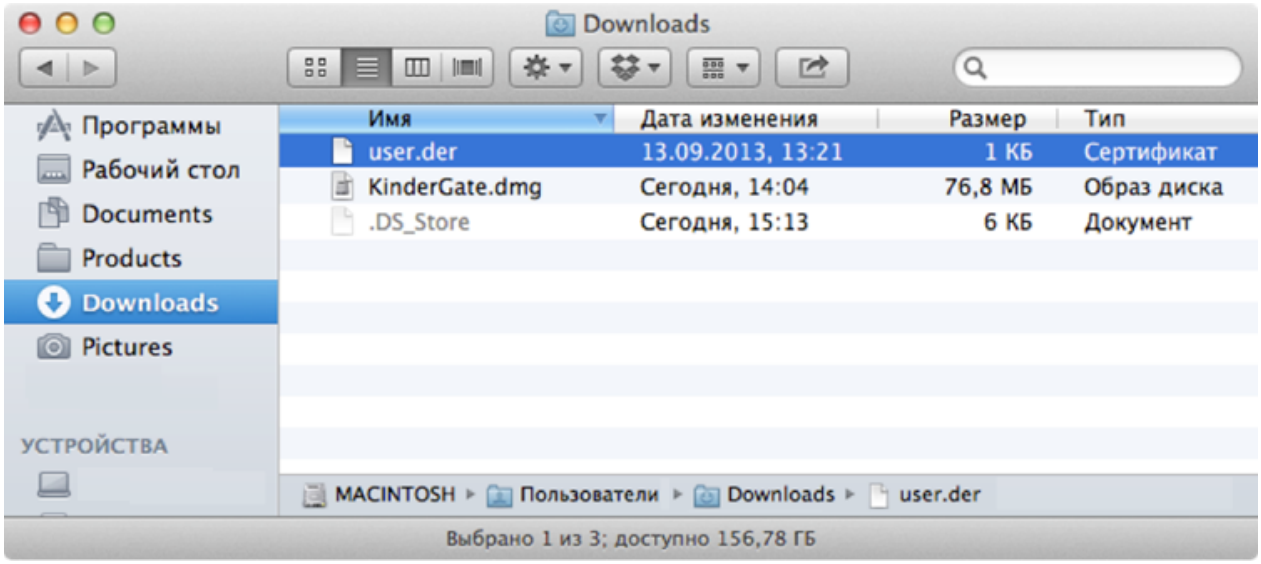


Рисунок 13 Выбор файла сертификата

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

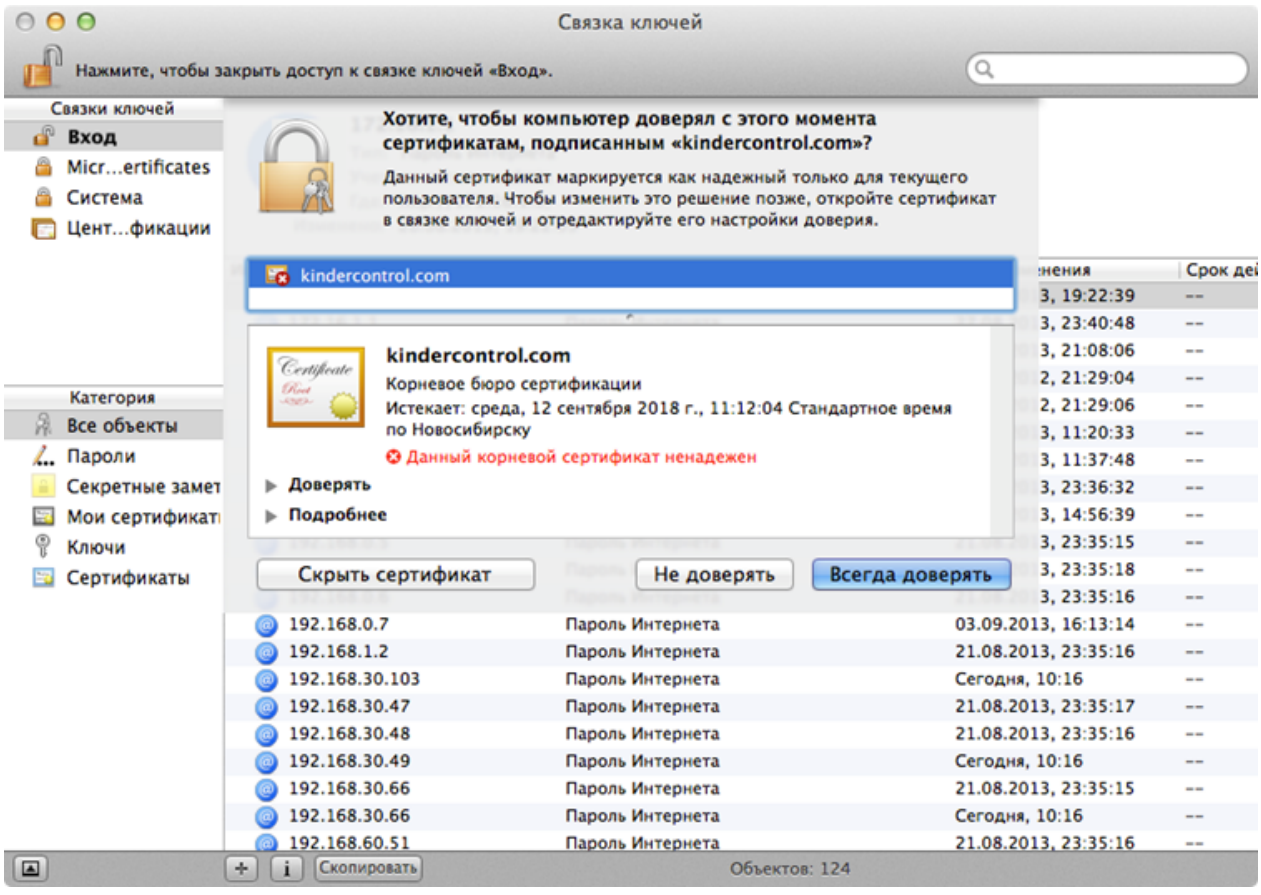


Рисунок 14 Доверие сертификату

Введите свой пароль для подтверждения данной операции:

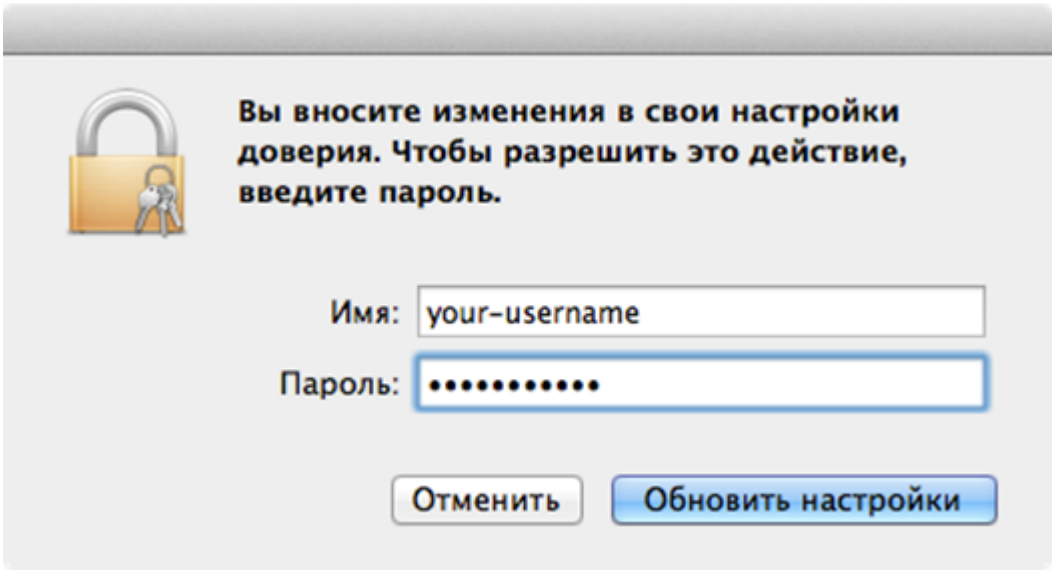


Рисунок 15 Ввод пароля

Сертификат установлен.

Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется аналогично для всех операционных систем. Рассмотрим установку на примере ОС Windows.

Откройте настройки браузера Firefox (**Инструменты → Настройки**):

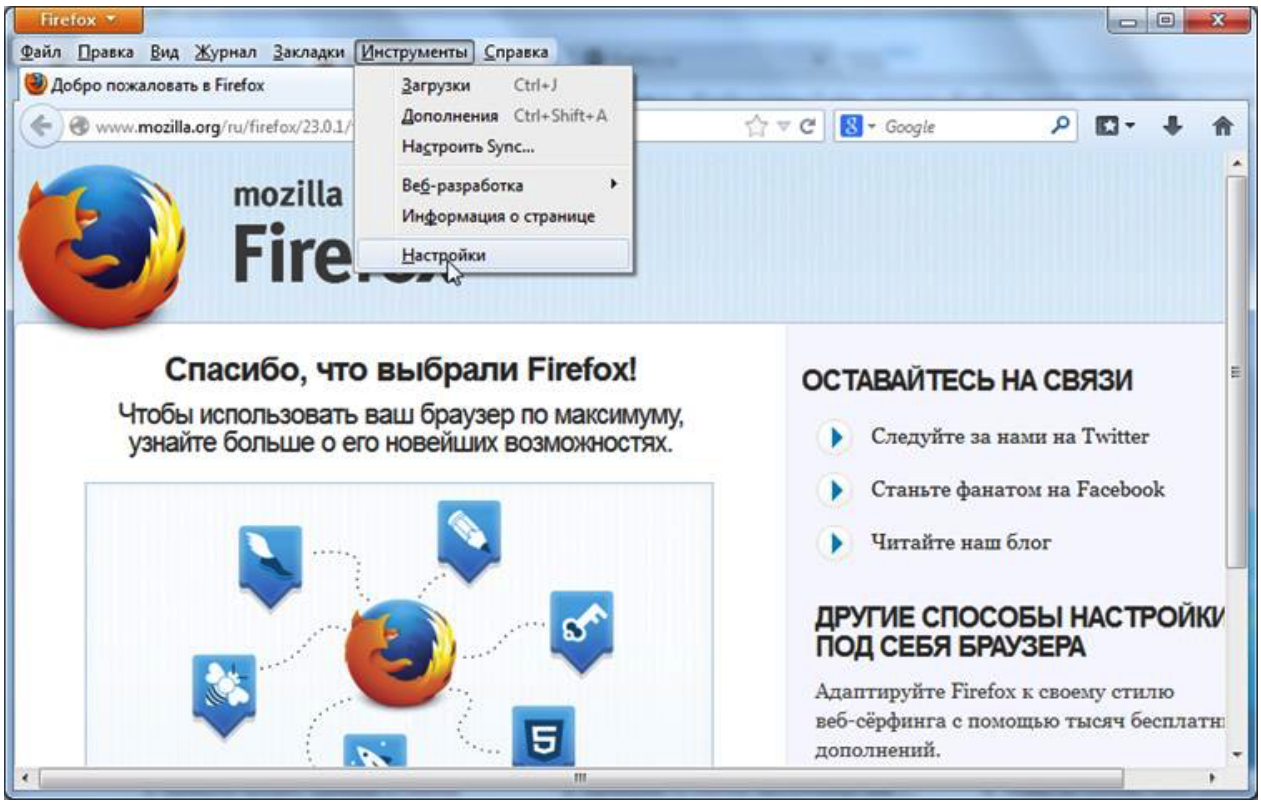


Рисунок 16 Вход в режим Настройки

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите на кнопку **Просмотр сертификатов**:

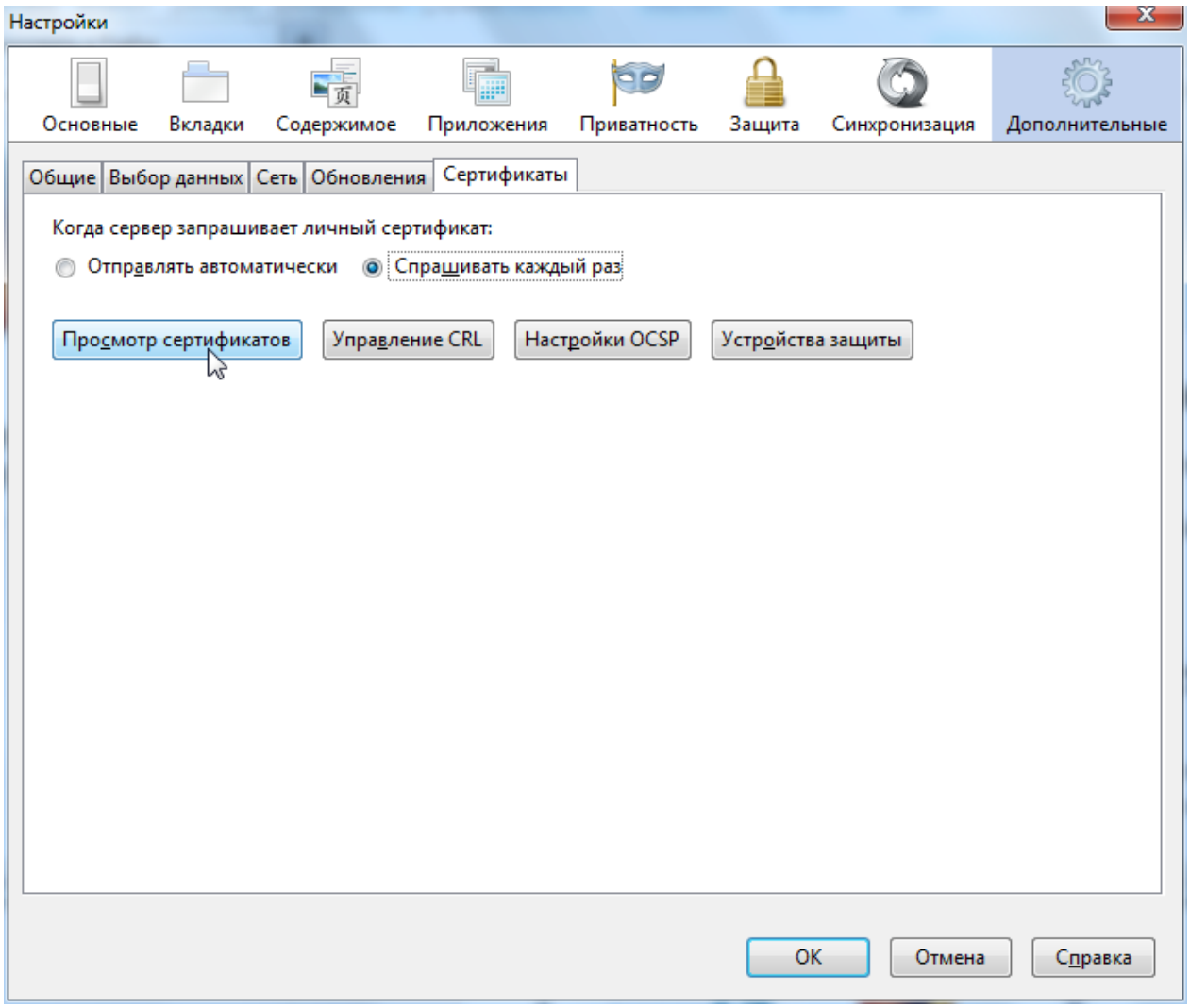


Рисунок 17 Раздел Сертификаты

Нажмите кнопку **Импортировать** и укажите путь к скачанному pem-сертификату:

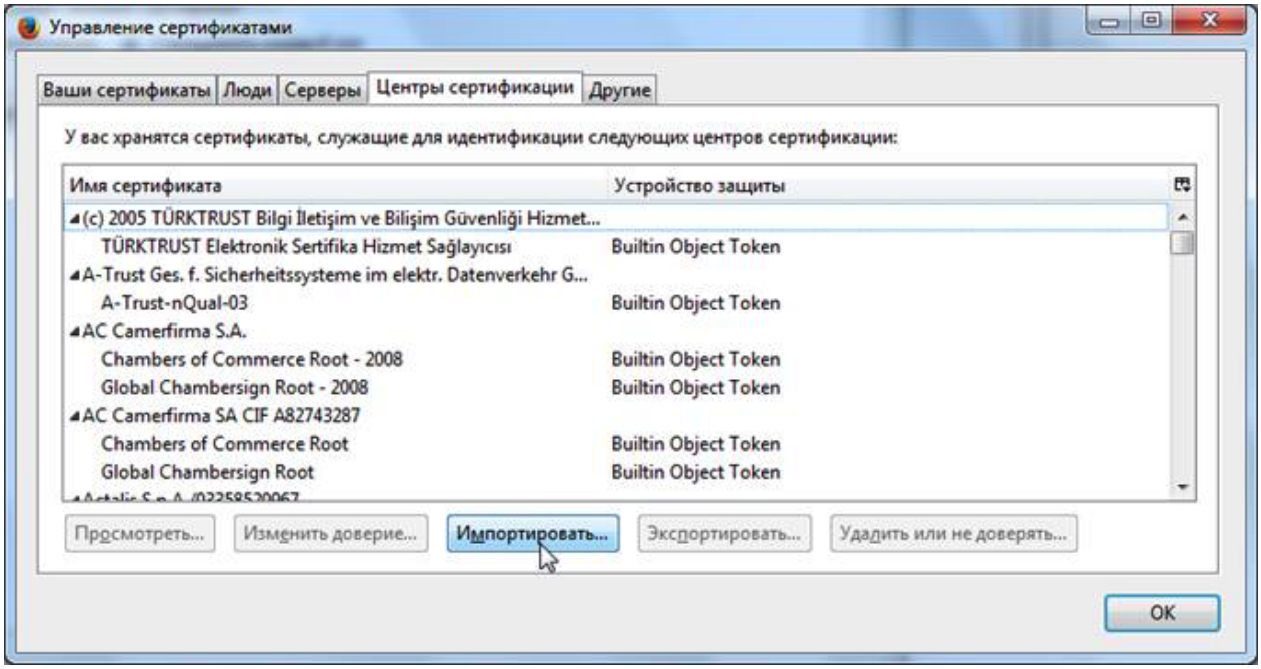


Рисунок 18 Список установленных сертификатов

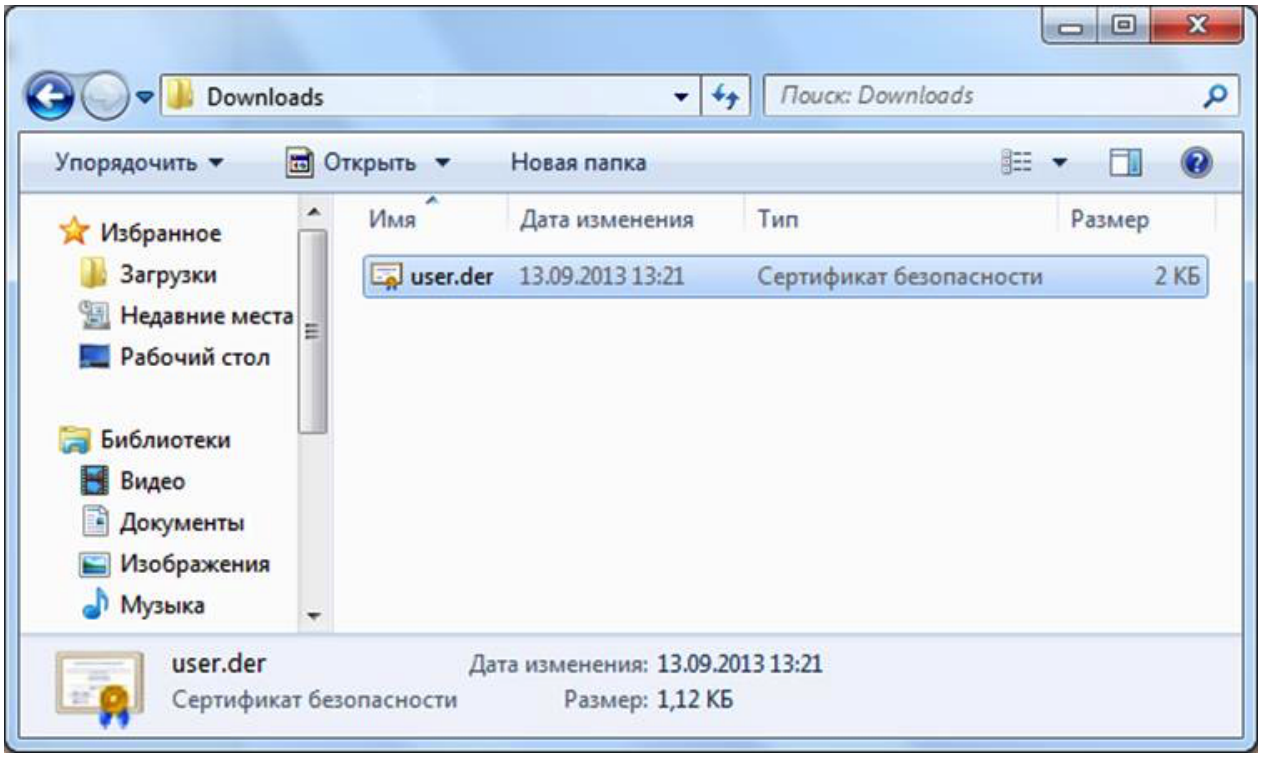


Рисунок 19 Выбор файла сертификата

Установите галочку **Доверять при идентификации веб-сайтов** и нажмите **OK**:

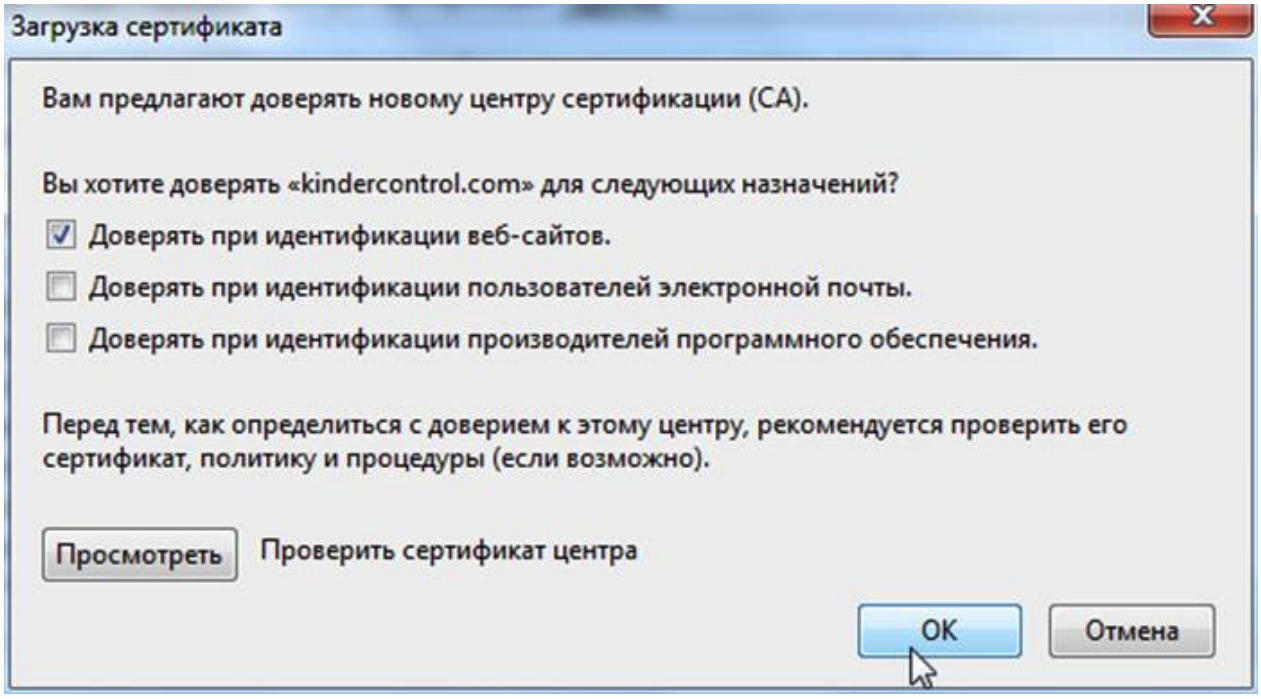


Рисунок 20 Выбор типа доверия

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
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения
	Мода и красота

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
	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-104№ 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 их прекурсоров, пропаганда каких-либо	Ненависть и нетерпимость

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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 негосударственных учреждений	Некоммерческие и неправительственные организации

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
продукции и табачных изделий	
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 подрывающих его репутацию)	Преступная деятельность

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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, пропагандирующие потребление табака;	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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

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

Тип поля	Название поля	Описание	Пример значения
	Severity	Важность события.	Может принимать значения: • 1 — информационные. • 4 — предупреждения. • 7 — ошибки. • 10 — критичные.
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@erstheta tica
	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

Тип поля	Название поля	Описание	Пример значения
	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
	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@erstheta tica
	act	Действие, принятое	captive

Тип поля	Название поля	Описание	Пример значения
		устройством в соответствии с настроенными политиками.	
	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)
	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	http://www.secure.com

Тип поля	Название поля	Описание	Пример значения
		содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	
	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
	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	Source Zone

Тип поля	Название поля	Описание	Пример значения
		индикации зоны источника.	
	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)
	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

Тип поля	Название поля	Описание	Пример значения
	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 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
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302

Формат журнала веб-доступа **CEF Compact**:

> **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.
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@ntoorereaeda

Тип поля	Название поля	Описание	Пример значения
	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)
	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

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. 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
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted

Тип поля	Название поля	Описание	Пример значения
	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.	{"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"}]}
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала DNS **CEF Compact**:

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
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept

Тип поля	Название поля	Описание	Пример значения
	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
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении	40

Тип поля	Название поля	Описание	Пример значения
		назначение — источник.	
	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	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	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)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3

Тип поля	Название поля	Описание	Пример значения
	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**:

Формат журнала СОВ

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.	idps
	Signature	Название сработавшей сигнатуры СОВ.	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@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	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.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40

Тип поля	Название поля	Описание	Пример значения
	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
	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

Тип поля	Название поля	Описание	Пример значения
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Формат журнала СОВ **CEF Compact**:

Формат журнала АСУ ТП

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.	scada
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
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@erstheta tica
	act	Действие, принятое устройством в соответствии с	accept

Тип поля	Название поля	Описание	Пример значения
		настроенными политиками.	
	app	Протокол прикладного уровня.	Modbus
	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.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	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.	

Тип поля	Название поля	Описание	Пример значения
			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 указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==","mb_message":"response","mb_addr":0}

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

Тип поля	Название поля	Описание	Пример значения
	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@erstheta tica
	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

Тип поля	Название поля	Описание	Пример значения
	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 указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone

Тип поля	Название поля	Описание	Пример значения
	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**:

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@einerson stal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark
	app		SMTP

Тип поля	Название поля	Описание	Пример значения
		Протокол прикладного уровня.	
	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
	cs1	Название правила защиты почтового трафика.	Mail security rule

Тип поля	Название поля	Описание	Пример значения
	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
	cs6	Email получателя.	receiver@example.com
	flexString1Label	Поле используется для указания	From

Тип поля	Название поля	Описание	Пример значения
		почтового адреса отправителя.	
	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**:

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
	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@ntoorereaeda
	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:

Тип поля	Название поля	Описание	Пример значения
			S-1-5-21-3795870133-5220325-2125745684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: % {S-1-5-21-3795870133-5220325-2125745684-513} % {S-1-1-0} % {S-1-5-32-544} % {S-1-5-32-555} % {S-1-5-32-545} % {S-1-5-32-554} % {S-1-5-2} % {S-1-5-11} % {S-1-5-15} % {S-1-5-21-3795870133-5220325-2125745684-512} % {S-1-5-21-3795870133-5220325-2125745684-572} % {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

Тип поля	Название поля	Описание	Пример значения
			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 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

Тип поля	Название поля	Описание	Пример значения
	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
	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

Тип поля	Название поля	Описание	Пример значения
	cs4	Категория события.	Group Membership
	cs5Label	Поле используется для указания файла журнала Windows.	logFile
	cs5	Файл журнала Windows	Security
	cs6Label	Поле используется для указания источника из журнала AD.	sourceName
	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.	['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}\

Тип поля	Название поля	Описание	Пример значения
			\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}']

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;

Тип поля	Название поля	Описание	Пример значения
			• 5 — notifications; • 6 — informational; • 7 — debugging.
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@ntoorereaeda
	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		Hostname

Тип поля	Название поля	Описание	Пример значения
		Поле используется для указания имени устройства, на котором произошло событие.	
	cs1	Имя компьютера, на котором произошло событие.	node1
	cs2Label	Поле используется для указания приложения, вызвавшего событие.	Tag
	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 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@ntoorereaeda
	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: yyyy-mm-ddThh: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.	{"rule":{"logrotate": 12,"attributes": {"timezone":"Asia/ Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
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.	{"guid":"37333739-3733-3734-3635-366400000000","name":"System","groups":[]}}

Описание журнала веб-доступа

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh: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.	"url_cats":[{"id": 39,"name":"Social Networking","threat_level":3}]

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: yyyy-mm-ddThh: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.	{"url_cats":[{"id": 37,"name":"Search Engines & Portals","threat_level":1}]}
proto		Используемый протокол 4-го уровня.	UDP
host		Имя хоста.	google.com
data		Поле используется для указания передаваемых данных.	{"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"}]}
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: yyyy-mm-ddThh: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 СОВ

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh: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
packets_sent		1

Название поля			Описание	Пример значения
			Количество пакетов, переданных в направлении источник — назначение.	
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.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name			Allow trusted to untrusted

Название поля			Описание	Пример значения
			Название правила, срабатывание которого вызвало событие.	
	type		Тип сработавшего правила	idps
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	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.	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)

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 АСУ ТП

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Критичность АСУ ТП.	1
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	**pdu_varname**	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998

Название поля	Описание	Пример значения
mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
mb_unit_id	Адрес устройства.	186
mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122
mb_quantity	Количество значений для чтения.	875
mb_payload	Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdc24f9883
mb_or_mask	Значение маски OR команды Mask Write Register.	1024
mb_message	Сообщение Modbus.	exception
mb_exception_code	Код ошибки. Актуален для типа сообщения error_response.	255
mb_and_mask	Значение маски AND команды Mask Write Register.	121
mb_addr	Адрес регистра.	3154
iec104_msgtype	Тип запроса.	request, response, error_response
iec104_ioa	Адрес объекта информации, который позволяет однозначно идентифицировать	23

Название поля			Описание	Пример значения
			приёмной стороной тип события.	
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol			Протокол прикладного уровня.	Modbus
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
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.
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)

Название поля		Описание	Пример значения
	ip	IPv4-адрес назначения трафика.	104.19.197.151
	port	Порт назначения	Может принимать значения от 0 до 65535.
rule	**guid**	Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name	Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

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

Название поля			Описание	Пример значения
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.	FA:16:3E:65:1C:B4
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.
	mac		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.	SSH Rule Example
	type		Тип сработавшего правила.	ssh
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 защиты почтового трафика

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
action	Действие, принятое устройством в соответствии с настроенными политиками.	mark
bytes_sent	Количество байтов, переданных в направлении источник — назначение.	0
bytes_recv	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		true, false

Название поля			Описание	Пример значения
			Поле указывает было ли содержимое расшифровано.	
from			Почтовый адрес отправителя.	sender@example.com
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)

Название поля			Описание	Пример значения
	ip		IPv4-адрес назначения трафика.	10.10.10.10
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	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: yyyy-mm-ddThh: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

Название поля	Описание	Пример значения
endpoint_name	Имя конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	dep.local
user_name	Поле «Пользователь» из журнала AD.	user1.dep.local
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: \t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID: \t\t0x0\r\n\r\nLogon Type: \t\t\t3\r\n\r\nNew Logon: \r\n\tSecurity ID: \t\tS-1-5-21-3795870133-5220325-2125745684-1103\r\n\tAccount Name: \t\tuser1\r\n\tAccount Domain:\t\tDEP\r\n\tLogon ID: \t\t0x7A25A21\r\n\r\nEvent in sequence:\t\t1 of 1\r\n\r\nGroup Membership: \t\t\t\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-1-5-21-3795870133-522032

Название поля	Описание	Пример значения
		5-2125745684-512}\r\n\t\t% {S-1-5-21-3795870133-522032 5-2125745684-572}\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 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.	['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325 -2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\ \n\\t\\t% {S-1-5-21-3795870133-522032 5-2125745684-513}\\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}

Название поля	Описание	Пример значения
		\\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}']
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: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
syslog_facility		1

Название поля		Описание	Пример значения
		Тип источника события syslog. Например, user-level messages. Подробнее о значениях syslog facility смотрите в RFC 5424.	
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 UserID

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z

Название поля			Описание	Пример значения
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons			Причина, по которой было создано событие.	{\"user_groups_sids\": [\"S-1-5-21-3795870133-522032 5-2125745684-513\", \"S-1-5-21-3795870133-522032 5-2125745684-512\", \"S-1-5-21-3795870133-522032 5-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-522032 5-2125745684-1103\",\"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-4e92-8331-23 9406ec34da
	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: 00000000-0000-0000-000 0-000000000000.	745591c3-9d21-092d-8db4-5 b9b0000044f
	name		Имя пользователя.	user1
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	aa218609-8716-9252- df20-88c43a0d0bf6

Название поля			Описание	Пример значения
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local

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.
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API.
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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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 UserGate, если он выступает в качестве DNS-сервера)	Сервис получения информации (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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Связь с UserGate Management Center	TCP	9712	Исходящий (от UG NGFW до UGMC)	Первоначальная 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)	Первоначальная установка связи и обмен ключами шифрования с сервером

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				UserGate Log Analyzer.
		2023	Входящий (от LogAn к UG NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	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).

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Captive-портал и страница блокировки	TCP	80, 443, 8002	Входящий (от браузера клиента на UG NGFW)	Отображение страницы авторизации Captive-портала и страницы блокировки.
		8043		При активации опции "HTTPS для страницы аутентификации".
Kerberos	TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей 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, необходимы

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				й 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.
Прокси-агент	UDP	8090	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый 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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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.
BGP	TCP	179	Исходящий (передача информации соседним BGP-маршрутизаторам)/ Входящий (получение информации от соседних BGP-маршрутизаторов)	Сервис динамической маршрутизации BGP.
OSPF	89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам / Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
RIP	UDP	520	Исходящий (распространение соседним маршрутизаторам RIP-маршрутов)/ Входящий (получение от соседних маршрутизаторов RIP-маршрутов)	Сервис динамической маршрутизации RIP.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
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).

Наименование	Описание
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.
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.

Наименование	Описание
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.
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.

Наименование	Описание
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.
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=Russia/L=Novosibirsk/O=UserGate/OU=QA/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 extentions 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 (sever-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                 = u1          #             Обязательный
                                 # Идентификатор пользователя, которому
выдан сертификат
```

```
                                    # Может быть учетной записью, под
которой будет выполняться подключение к vpn-серверу

[ v3_req ]
keyUsage           = critical, digitalSignature
extendedKeyUsage   = clientAuth
subjectAltName     = otherName:msUPN;UTF8:u1@ep.local # Пользователь,
под учетной записью которого будет выполняться подключение к VPN-
серверу.
```

Поле subjectAltName используется, если в Профиле пользовательских сертификатов 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 #
генерация пароля
$ openssl rsa -passin pass:1234 -in client.pass.key -out client-key.pem
# генерация ключа
```

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 репозиторий Локальный компьютер, хранилище — Автоматически выбрать хранилище, по умолчанию направится в 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 смотрите в разделе Настройка VPN). 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 должны совпадать с атрибутами сертификата **CN и\или SAN:principal name**.

Действия на стороне VPN-сервера

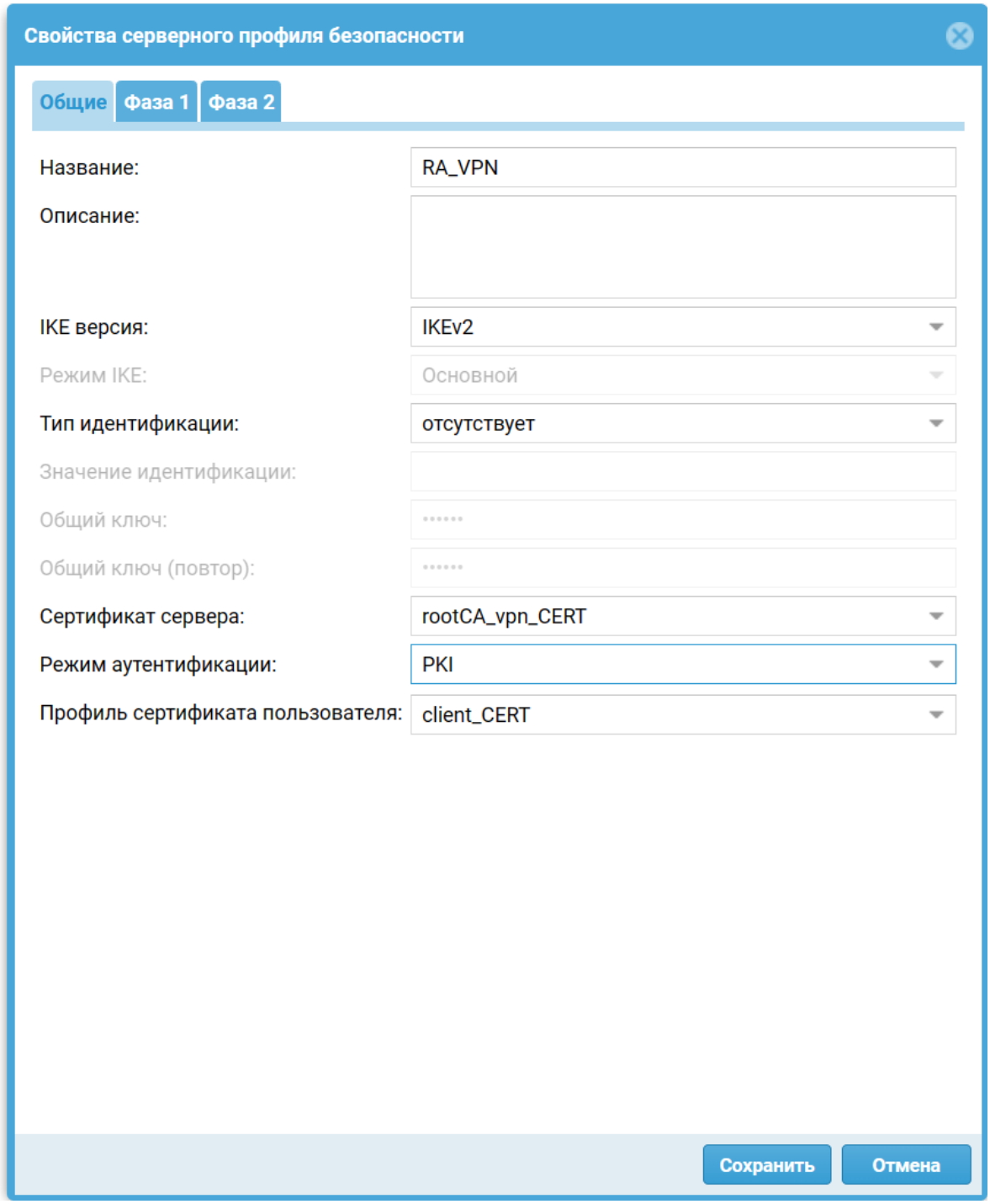
1. Импортировать корневой сертификат (rootCA) в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Сертификаты** и нажать кнопку **Импортировать.**

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 пользовательских сертификатов в консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого перейти в раздел **UserGate → Профили пользовательских 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.

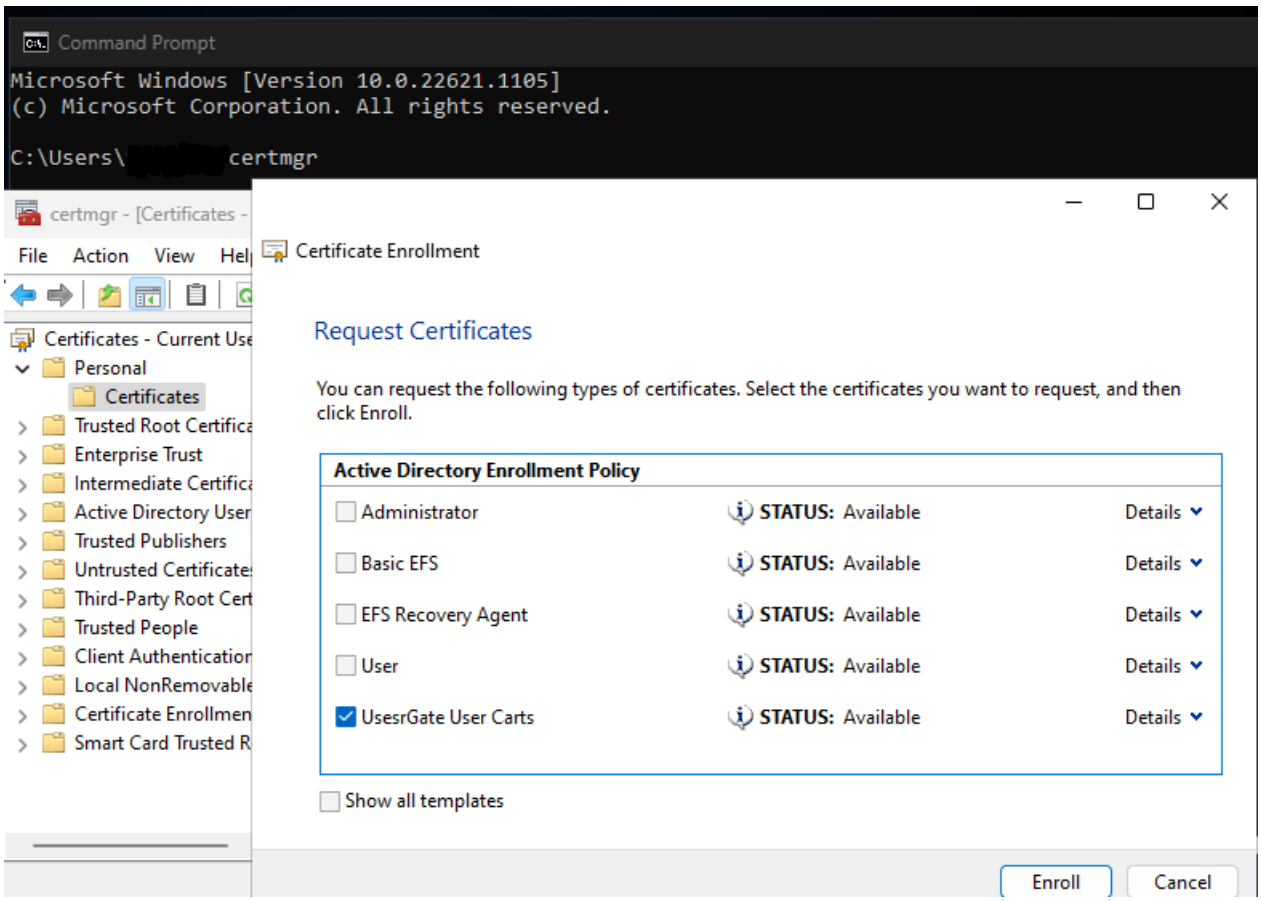
4. В разделе **VPN → Серверные профили безопасности** добавить в **Remote access VPN profile**:

- Сертификат в поле **Сертификат сервера.**
- Выбрать созданный **Профиль пользовательского сертификата.**
- Выбрать **Режим аутентификации** — посредством сертификатов **PKI.**



Действия на стороне VPN-клиента

1. Запросить сертификат на клиентской машине согласно созданному раннее шаблону пользовательского сертификата.



2. Полученный сертификат расположить в репозиторий Локальный компьютер, хранилище — Личное.