UserGate

UserGate SWG 7.5.x
Руководство администратора

Оглавление

- О UserGate SWG
  - Общие сведения
- Лицензирование
  - Лицензирование UserGate SWG
- Интерфейс
  - Интерфейс UserGate SWG
- Первоначальная настройка
  - Общие сведения
  - Развертывание виртуального образа
  - Автоматизация развертывания UserGate SWG с помощью Cloud-init
  - Требования к сетевому окружению
  - Подключение к UserGate SWG
- Настройка устройства
  - Общие параметры
  - Управление устройством
  - Управление доступом к интерфейсам администрирования
  - Управление сертификатами
  - Профили клиентских сертификатов
  - Системные утилиты
  - Расширение системного раздела
  - Работа с вышестоящими прокси-серверами
  - Кластеризация и отказоустойчивость
- Настройка сети
  - Настройка зон
  - Настройка интерфейсов
  - Настройка шлюзов
  - Настройка DHCP
  - Настройка DNS
  - WCCP
  - Виртуальные маршрутизаторы
- Пользователи и устройства
  - Пользователи и группы
  - Серверы аутентификации
  - Профили аутентификации
  - Настройка Captive-портала
  - Пользователи терминальных серверов
  - Профили MFA
  - UserID
  - Radius accounting
  - UserID-агент для серверов AD, WEC

    - Работа с доверенными браузерами
- Политики сети
    - Общие сведения
    - Межсетевой экран
    - NAT и маршрутизация
    - Балансировка нагрузки
    - Пропускная способность
- Политики безопасности
    - Общие сведения
    - Фильтрация контента
    - Веб-безопасность
    - Инспектирование SSL
    - Работа с внешними ICAP-серверами
- Глобальный портал
    - Общие сведения
    - Веб-портал (SSL VPN)
    - Публикация ресурсов с помощью reverse-прокси
- Библиотеки элементов
    - Общие сведения
    - Морфология
    - IP-адреса
    - User agent браузеров
    - Типы контента
    - Списки URL
    - Календари
    - Полосы пропускания
    - Шаблоны страниц
    - Категории URL
    - Измененные категории URL
    - Почтовые адреса
    - Номера телефонов
    - Профили оповещений
    - Профили LLDP
    - Профили SSL
    - Профили пересылки SSL
    - Профили BFD
    - Syslog-фильтры UserID агента
    - Сценарии
    - Теги
- Диагностика и мониторинг
    - Мониторинг трафика
    - Маршруты
    - OSPF
    - Веб-портал
    - Захват пакетов

    - Запросы в белый список
    - Трассировка правил
    - Ping
    - Traceroute
    - Запрос DNS
    - LLDP-соседи
    - Статистика LLDP
    - Оповещения
        - Правила оповещений
        - SNMP
        - Параметры SNMP
        - Профили безопасности SNMP
- Журналы и отчеты
    - Журналы
        - Описание
        - Журнал событий
        - Журнал веб-доступа
        - Журнал DNS
        - Журнал трафика
        - История поиска
        - UserID-агент
        - Поиск и фильтрация данных
        - Экспорт журналов
    - Отчеты
        - Описание
        - Шаблоны отчетов
        - Правила отчетов
        - Созданные отчеты
- Интерфейс командной строки
    - Общие положения
        - Общие положения
    - Команды, доступные до первоначальной инициализации узла
        - Команды, доступные до первичной инициализации узла
    - Первоначальная инициализация
        - Первоначальная инициализация UserGate SWG
    - Команды диагностики и мониторинга
        - Команды диагностики и мониторинга
    - Режим конфигурации
        - Режим конфигурации (описание)
    - Настройка устройства в CLI
        - Настройка общих параметров устройства
        - Настройка кластеров
        - Настройка управления доступом к консоли UserGate SWG
        - Настройка сертификатов
        - Настройка прокси-сервера

    - Настройка работы с вышестоящими прокси-серверами
    - Настройка параметров мониторинга устройства
    - Настройка профилей клиентских сертификатов
    - Настройка параметров управления телеметрией
  - Настройка сетевых параметров
    - Зоны
    - Интерфейсы
    - Шлюзы
    - DHCP
    - DNS-настройки
    - Настройка виртуальных маршрутизаторов
    - Настройка WCCP
  - Настройка раздела Пользователи и устройства
    - Настройка групп пользователей
    - Настройки пользователей
    - Настройка серверов аутентификации
    - Настройка профилей аутентификации
    - Настройка Captive-профилей
    - Captive-портал
    - Настройка терминальных серверов
    - Настройка профилей MFA (многофакторной аутентификации)
    - Просмотр информации об авторизованных пользователях
    - Настройка применения политик к пользователям
    - Настройка подключения к серверу регистрации доверенных браузеров
  - Настройка раздела Политики сети
    - Настройка правил межсетевого экрана
    - Настройка правил NAT и маршрутизации
    - Настройка балансировки нагрузки
    - Настройка правил управления пропускной способностью
  - Настройка раздела Политики безопасности
    - Настройка правил фильтрации контента
    - Настройка правил веб-безопасности
    - Настройка правил инспектирования SSL
    - Настройка правил ICAP
    - Настройка ICAP-серверов
  - Настройка глобального портала
    - Настройка веб-портала
    - Настройка правил reverse-прокси
    - Настройка серверов reverse-прокси
  - Настройка библиотек
    - Настройка библиотек (Описание)
  - Настройка раздела журналы и отчеты
    - Настройка экспорта журналов
    - Настройка отчетов

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

О USERGATE SWG

Общие сведения

UserGate Secure Web Gateway (SWG) — это компонент системы информационной безопасности, предназначенный для контроля, фильтрации и защиты веб-трафика пользователей при доступе к интернет-ресурсам. UserGate SWG действует как специализированный сетевой шлюз между пользовательскими устройствами, внутренними информационными системами и внешними веб-ресурсами, анализируя и применяя политики безопасности к HTTP/HTTPS-трафику.

В рамках архитектуры информационной безопасности организации UserGate SWG выполняет следующие задачи:

1. Контроль доступа к интернет-ресурсам.

Система обеспечивает централизованное управление доступом пользователей к веб-ресурсам на основе категорий сайтов, списков веб-ресурсов, политик организации и пользовательских групп. Это позволяет ограничивать доступ к нежелательному или потенциально опасному контенту.

2. Фильтрация и инспекция веб-трафика.

Система выполняет глубокий анализ веб-трафика, включая проверку содержимого HTTP/HTTPS-запросов и ответов. Используется механизм TLS/SSL-инспекции для анализа зашифрованного трафика и выявления скрытых угроз.

3. Контроль загрузки и передачи файлов.

Система осуществляет проверку файлов, передаваемых через веб-каналы, включая загрузки из интернета и отправку данных на внешние ресурсы. Проверка может включать антивирусный анализ и использование изолированных сред для выявления неизвестных угроз.

4. Предотвращение утечки данных.

Система может контролировать передачу конфиденциальной информации через веб-каналы и предотвращать несанкционированную отправку

данных за пределы организации. Трафик и файлы могут передаваться на внешние DLP-системы для анализа и блокировки каналов утечки чувствительных данных.

5. Идентификация и учет действий пользователей.

Система поддерживает интеграцию с корпоративными системами управления аутентификацией и доступом (например, каталогами пользователей), что позволяет применять политики безопасности на уровне конкретных пользователей или групп, а также обеспечивать журналирование активности.

6. Снижение нагрузки на межсетевые экраны и каналы связи.

Ресурсоемкие операции SSL-инспектирования и веб-фильтрации выполняются на специализированном шлюзе — SWG, благодаря чему ограничивается нецелевой трафик и снижается нагрузка на межсетевые экраны периметра сети.

7. Централизованное журналирование и мониторинг.

Система ведет регистрацию событий безопасности, связанных с веб-активностью пользователей, включая попытки доступа к запрещенным ресурсам, загрузку файлов и обнаруженные угрозы. Полученные данные могут передаваться в системы централизованного мониторинга и корреляции событий безопасности.

UserGate SWG может интегрироваться с другими средствами защиты информации, включая межсетевые экраны, системы анализа событий безопасности и платформы управления доступом. Такое взаимодействие обеспечивает комплексную защиту веб-каналов и повышает уровень контроля над использованием интернет-ресурсов в организации.

UserGate SWG поставляется в виде программно-аппаратного комплекса (ПАК), либо в виде образа виртуальной машины, предназначенного для развертывания в виртуальной среде.

ЛИЦЕНЗИРОВАНИЕ

Лицензирование UserGate SWG

Для использования UserGate SWG необходима базовая лицензия, в рамках которой предоставляется бессрочный доступ к основным функциям устройства. Чтобы получать обновления UserGate SWG и использовать его расширенные функции, вам необходимо приобрести дополнительные лицензии.

В веб-интерфейсе UserGate SWG вы можете активировать и обновить лицензию, а также проверить срок ее действия в онлайн-режиме. Если доступ к серверу лицензирования отсутствует, вы можете активировать лицензию офлайн.

Базовая лицензия

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

- **Тип аппаратной платформы**, если UserGate SWG поставляется в виде программно-аппаратного комплекса (ПАК). Тип аппаратной платформы должен совпадать с тем, который указан в лицензии.
- **Количество ядер виртуальной машины**, если UserGate SWG поставляется в виде образа виртуальной машины. Количество поддерживаемых ядер процессора должно совпадать с количеством ядер, разрешенных лицензией.

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

Дополнительные лицензии

Дополнительно лицензируются следующие модули UserGate SWG.

Модуль	Предоставляемые функции	По истечении лицензии
Security Updates (SU)	Годовая подписка на обновление ПО UserGate	Прекращается обновление ПО. Продолжает действовать последняя установленная версия
	Годовая подписка на потоковый антивирус UserGate	Отключается антивирус

Модуль	Предоставляемые функции	По истечении лицензии
Потоковый антивирус UserGate		
Cluster	Поддержка кластеризации. Срок действия лицензии на модуль не ограничен	—

Процедуры активации лицензий

Онлайн-активация

При онлайн-активации устройство UserGate обращается к серверу лицензирования `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 список модулей, разрешенных данной лицензией.

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

В дальнейшем при работе устройства UserGate проверка лицензии происходит один раз в сутки. Если проверка прошла успешно, в журнале событий фиксируется запись об этом событии. Устройство продолжает работать в штатном режиме.

При недоступности сервера лицензирования система выполняет 14 попыток соединения с интервалом 120 секунд. Если ни одна из попыток не увенчалась успехом, дальнейшие запросы приостанавливаются на 24 часа. По истечении этого периода цикл из 14 попыток возобновляется. В случае, если на протяжении срока действия лицензии связь с сервером так и не была установлена, по окончании лицензионного периода доступ к соответствующим модулям блокируется. Каждый сбой подключения к серверу активации фиксируется в журнале событий с указанием ошибки.

Порядок действий при онлайн-активации

Для регистрации устройства:

1. В веб-консоли администратора устройства перейдите в раздел **Дашборды**,

2. В виджете **Лицензия** нажмите **Нет лицензии**, введите ПИН-код и зарегистрируйте устройство.

Если узел находится в закрытом контуре без прямого доступа в интернет активировать или обновить лицензию можно через прокси-сервер. Для этого выберите режим **Использовать прокси-сервер для активации и апдейтов**. Далее укажите IP-адрес и порт вышестоящего прокси-сервера. При необходимости укажите логин и пароль для аутентификации на прокси-сервере.

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

Офлайн-активация

Офлайн-активация лицензий необходима для устройств UserGate, находящихся в изолированной сети без доступа к интернету и без возможности активации через прокси-сервер.

Процесс офлайн-лицензирования включает следующие этапы:

1. Генерация запроса — создание на лицензируемом устройстве файла запроса для офлайн-активации.

2. Активация запроса — обработка сгенерированного файла запроса с помощью сервиса офлайн-активации ПИН-кодов.

3. Применение лицензии — загрузка активированного файла обратно на лицензируемое устройство.

Генерация запроса

Чтобы сгенерировать файл запроса для офлайн-активации лицензии:

1. Зайдите с помощью веб-браузера на лицензируемое устройство по следующему адресу: https://<IP-address>:8001?features=offline-reg .

IP-address — это IP-адрес лицензируемого устройства.

2. В веб-консоли устройства перейдите в раздел **Дашборды**.

3. В виджете **Лицензия** нажмите **Нет лицензии**.

4. В окне активации устройства нажмите **Начать активацию в автономном режиме**.

5. Введите ПИН-код устройства и скачайте сгенерированный файл запроса для офлайн-активации.

Активация запроса

С компьютера, имеющего доступ в интернет, обратитесь в сервис офлайн-активации (для входа в сервис потребуется авторизация в Едином центре авторизации) и активируйте сгенерированный файл запроса.

Применение лицензии

Загрузите активированный файл на лицензируемое устройство. Для этого:

1. В разделе **Дашборды** лицензируемого устройства в виджете **Лицензия** откройте окно офлайн-активации.

2. Выберите **Завершить активацию в автономном режиме**.

3. Укажите активированный файл, полученный в сервисе офлайн-активации.

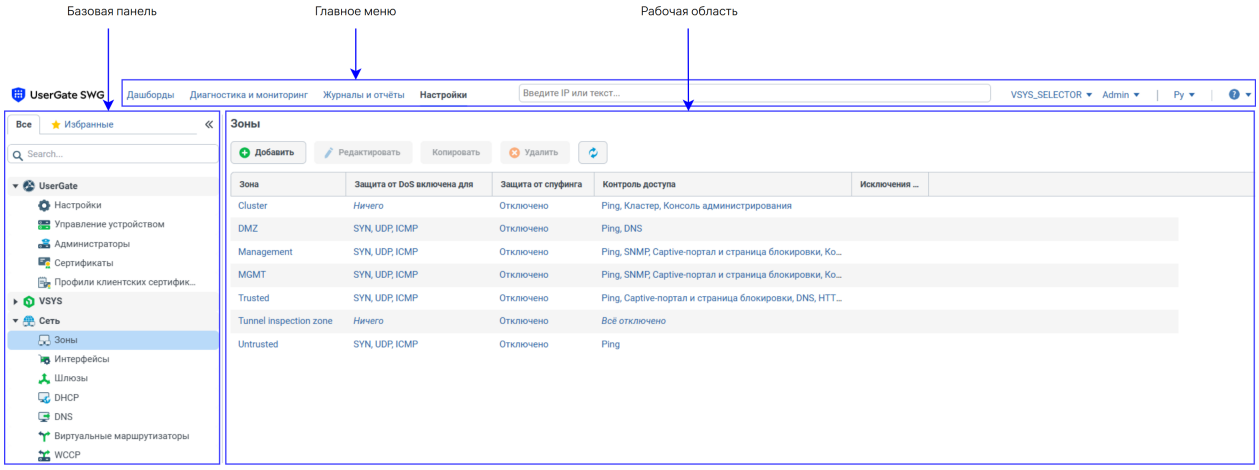
Процесс лицензирования завершен.

Подробнее о процедуре офлайн-активации лицензии — в разделе «Офлайн-активация лицензий».

ИНТЕРФЕЙС

Интерфейс UserGate SWG

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



Главное меню

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

- **Дашборды** — страница со статистическими данными о состоянии устройства и результатах его работы, представленными в виде таблиц, списков и графиков. При входе в UserGate SWG эта страница открывается по умолчанию. Подробнее о дашбордах — в разделе «Работа с дашбордами и виджетами».

- **Диагностика и мониторинг** — страница для отслеживания сетевого трафика, просмотра сетевой конфигурации, выполнения захвата пакетов, запуска базовых сетевых утилит, а также для управления оповещениями.

- **Журналы и отчеты** — страница для просмотра журналов и настройки генерации отчетов.

- **Настройки** — страница для настройки устройства и политик безопасности.

Также в главном меню находятся следующие элементы управления:

- Поле поиска — поиск по выполняется в разделах **Фильтрация контента** и **Межсетевой экран**. Вы можете искать правила межсетевого экрана по их названию, описанию, сценарию, а также по зоне, имени, адресу источника или назначения. При поиске по адресу источника или назначения также доступен поиск по IP-адресу в подсетях. Например, если в правиле в качестве адреса назначения указана подсеть 192.168.1.0/24, правило будет найдено по IP-адресу 192.168.1.5.

  Результаты поиска отображаются под полем в раскрывающемся окне.

В окне найденных элементов вы можете:

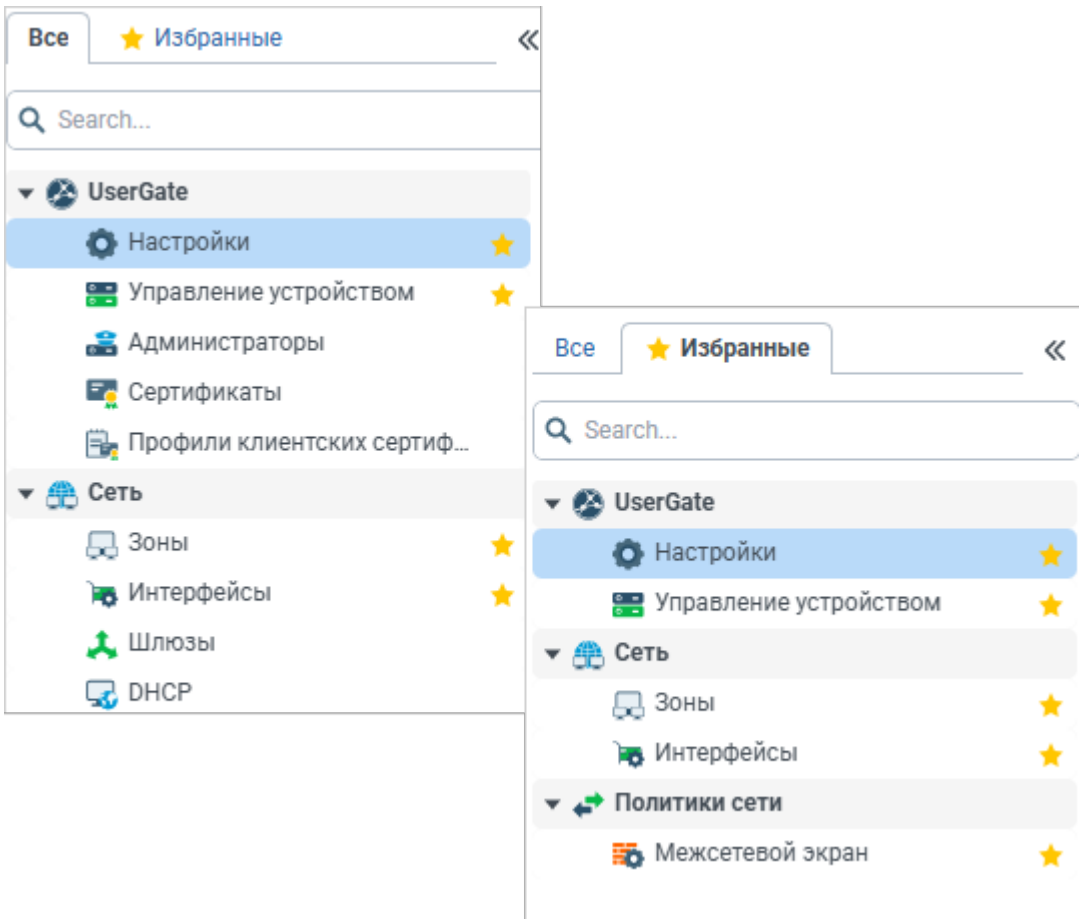
- Фильтровать результаты, выбирая нужные разделы на панели **Фильтр**. При изменении фильтра нужно обновить результаты поиска, нажав на соответствующую кнопку.
- Просматривать подробную информацию по найденному элементу, наведя на него курсор.
- Перейти на страницу раздела с найденным элементом, нажав **Показать** в строке выбранного элемента.
- Изменить параметры найденного элемента. Если изменение параметров доступно, по нажатию на название элемента откроется окно с его параметрами.

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

Страницы интерфейса

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

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



ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Общие сведения

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

Развертывание виртуального образа

UserGate SWG Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают системы

виртуализации VMware, Oracle VirtualBox, и в формате Qcow2 для систем виртуализации QEMU-KVM. Для Microsoft Hyper-V поставляется образ диска виртуальной машины.

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

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

Работа с виртуальным образом

Для начала работы с виртуальным образом выполните следующие шаги:

1. Скачайте последнюю версию виртуального образа с официального сайта UserGate.

2. Импортируйте образ в свою систему виртуализации. Инструкцию по импорту образа вы можете найти на сайтах систем виртуализации, например VirtualBox или VMware. Для Microsoft Hyper-V необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.

3. До включения виртуальной машины настройте её параметры в своей системе виртуализации:

   - Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8 ГБ и добавьте по 1 ГБ на каждые 100 пользователей.

   - Добавьте дополнительный диск нужного размера. Размер диска по умолчанию составляет 100 ГБ, чего обычно недостаточно для хранения всех журналов и параметров. Используя свойства

виртуальной машины, установите размер диска не меньше 200 ГБ. Рекомендованный размер — 300 ГБ или больше.

4. Для систем виртуализации QEMU-KVM размер системной области по умолчанию составляет 8 ГБ. При первом запуске система сама определит наличие дополнительного диска и расширит свои системные разделы. Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:

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

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

UserGate SWG поставляется с четырьмя интерфейсами, назначенными в зоны:

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

Порядок нумерации интерфейсов в виртуальной среде

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

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

После сброса до первоначального состояния (factory reset) при изменении количества сетевых адаптеров в системе (при добавлении или удалении

адаптеров средствами гипервизора) происходит сортировка интерфейсов и их маппинг.

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

При сортировке интерфейсов по параметру H/W path:

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

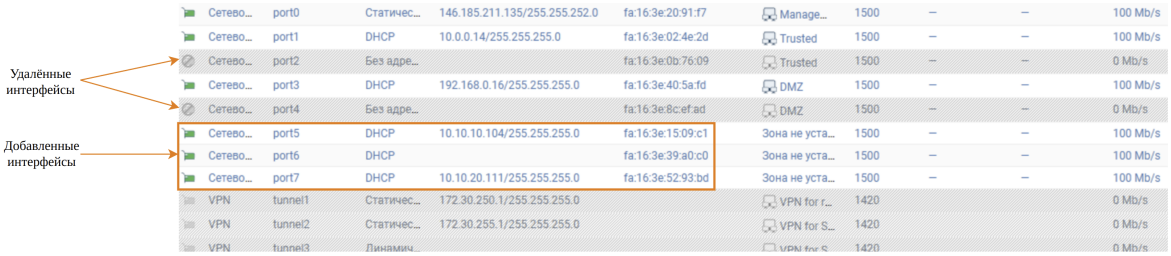
```
Admin@canntoralcti> show network interface-mapping

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

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

При сортировке интерфейсов по MAC-адресам:

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




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

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

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

Важно!

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

Примечание

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

Оптимизация производительности сетевых интерфейсов на основе virtio

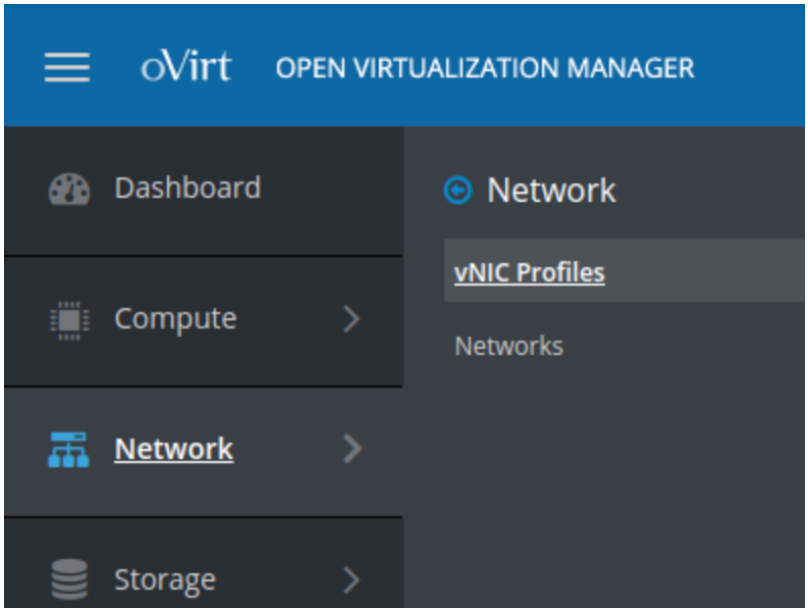
Для оптимизации производительности сетевых интерфейсов на основе virtio в средах виртуализации KVM, oVirt, zVirt рекомендуется включить на гипервизоре режим Multi Queues и устанавливать 8 очередей на сетевой интерфейс. Например, в случае платформы OVirt (см. документацию oVirt), для того чтобы выставить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

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

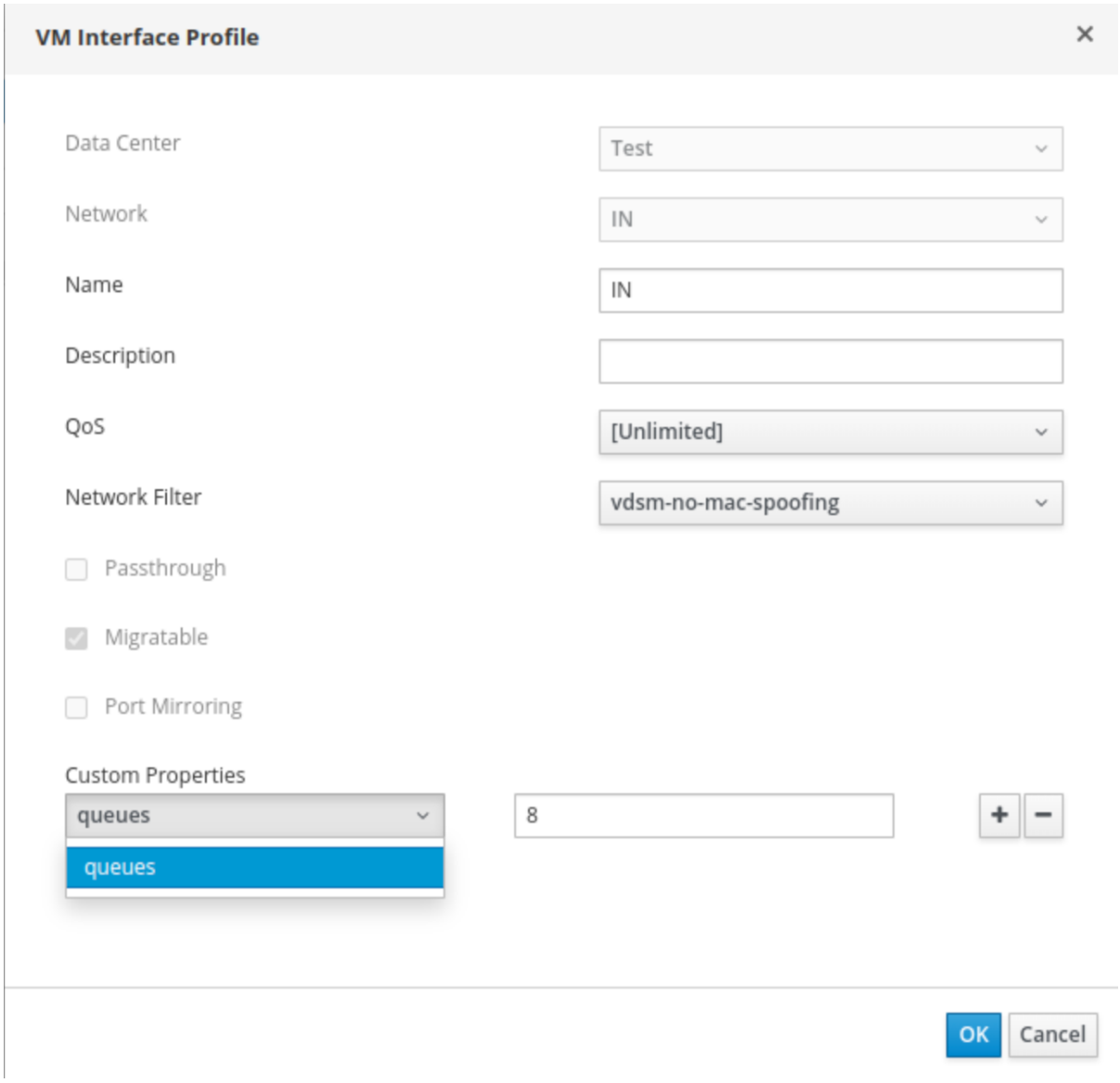
Вместо параметра `other-nic-properties` нужно вставить список существующих кастомизированных правил (если такие правила есть). Посмотреть, существуют ли кастомизированные правила, можно с помощью команды:

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

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



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



Автоматизация развертывания UserGate SWG с помощью Cloud-init

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

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

Другие модули Cloud-init не поддерживаются.

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

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

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

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

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

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

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

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

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

Настройки могут быть переданы в SWG:

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

- Через подключаемый ISO-диск. На диске должны быть файлы `meta-data`, `user-data`, `vendor-data` со следующим содержимым:
  - meta-data: `instance-id: vm1`
  - user-data — с CLI-командами настройки инстанса:

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

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

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

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

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

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

Требования к сетевому окружению

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

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

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

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

Подробнее о требованиях сетевой доступности — в приложении «Требования к сетевому окружению».

Подключение к UserGate SWG

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

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

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

Остальные интерфейсы отключены и требуют последующей настройки.

Для первоначальной настройки выполните следующие шаги:

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

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

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

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

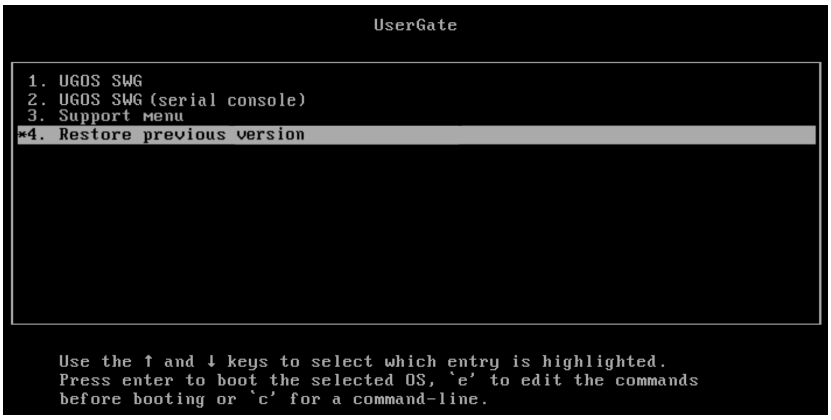
Шаг	Описание
Настроить авторизацию пользователей	В разделе **Настройки → Пользователи и устройства** создайте необходимые методы авторизации пользователей. Самый простой вариант — создать локальных пользователей SWG в разделе **Настройки → Пользователи и устройства → Пользователи** с заданными IP-адресами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

НАСТРОЙКА УСТРОЙСТВА

Общие параметры

В разделе **Настройки → UserGate → Настройки** устанавливаются базовые параметры UserGate SWG.

Параметр	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	Возможны следующие способы аутентификации пользователя (администратора) при входе в веб-консоль управления: • **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 браузере. При включении этого режима аутентификация по имени и паролю отключается. Вернуть режим аутентификации по имени и паролю можно с помощью команд CLI. • **Профиль клиентского сертификата.** Аутентификация 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	Профиль SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Профили SSL»
Профиль SSL для страниц блокировки/авторизации	Профиль SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации captive-портала. Подробнее о профилях SSL — в разделе «Профили SSL»
Таймер автоматического закрытия сессии (мин.)	Таймер автоматического закрытия сессии в случае отсутствия активности администратора в веб-консоли
Автоматическое закрытие сессии по таймеру	Включение или отключение автоматического закрытия сессии по таймеру
Настройка времени сервера	Настройка параметров установки точного времени. • **Использовать NTP** — использовать серверы NTP из указанного списка для синхронизации времени.

Параметр	Описание
	• **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
Учет изменений	При включенном учете изменений и создании **Типов изменений** любое изменение в конфигурации, вносимое администратором через веб-консоль, будет требовать указания типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • распоряжение; • приказ; • регламентные работы. Количество типов изменений не ограничено
Центр обновлений	Параметры для управления скачиванием обновлений программного обеспечения UserGate (UGOS) и системных библиотек, предоставляемых по подписке (база категорий URL-фильтрации, СОВ, списки IP-адресов, URL, типов контента и другие). **Обновления ПО** — настройка канала обновлений (стабильные, бета), проверки наличия новых обновлений UGOS и скачивание офлайн-обновлений. При установке обновления можно задать точку восстановления устройства. Если точка восстановления была создана, после успешного завершения обновления в стартовом меню устройства появится опция восстановления предыдущей версии ПО. 

Параметр	Описание
	Обновления библиотек — проверка наличия обновлений библиотек, скачивание обновлений и настройка расписания автоматической проверки и скачивания библиотек. Проверить наличие обновлений библиотек и скачать последние обновления можно по ссылке **Проверить обновления**. Настроить автоматическое обновление библиотек можно по ссылке **Настроить**. Для каждой библиотеки можно настроить расписание автоматической проверки и скачивания обновлений. Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями. При установке флажка **Единое расписание для всех обновлений** расписание текущей библиотеки будет применено ко всем библиотекам. **Примечание** В целях уменьшения нагрузки на систему рекомендуется устанавливать автоматическое обновление только для используемых библиотек
Модули	Вы можете настроить следующие модули UserGate SWG: • **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.

Параметр	Описание
	Невозможно использовать следующие порты, поскольку они используются внутренними сервисами UserGate SWG: 2200, 8001, 4369, 9000-9100. • **Домен Auth captive-портала** — служебный домен, который используется SWG при авторизации пользователей через captive-портал. Необходимо, чтобы пользователи могли преобразовывать указанный здесь домен в IP-адрес интерфейса SWG, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес SWG, то преобразование 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 SWG для окончания сессии (logout). Необходимо, чтобы пользователи могли преобразовывать указанный здесь домен в IP-адрес интерфейса SWG, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес SWG, то преобразование настроено автоматически. По умолчанию используется имя logout.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Домен Cert captive-портала** — служебный домен, который используется SWG при авторизации пользователей через captive-портал с помощью сертификатов. Необходимо, чтобы пользователи могли преобразовывать указанный здесь домен в IP-адрес интерфейса SWG, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес SWG, то преобразование адресов настроено автоматически. По умолчанию используется имя cert.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 преобразовывать указанный здесь домен в IP-адрес интерфейса SWG, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес SWG, то преобразование настроено автоматически. По умолчанию используется имя block.captive, которое может быть изменено на другое доменное имя, принятое в организации.

Параметр	Описание

	• **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 преобразовывать указанный здесь домен в IP-адрес интерфейса SWG, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то преобразование настроено автоматически. По умолчанию используется имя `ftpclient.captive`, которое может быть изменено на другое доменное имя, принятое в организации.
	• **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, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения:
	  ◦ **Transmit delay** — задержка передачи. Указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например изменение имени узла или адреса управления. Может принимать значения от 1 до 3600, задается 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

Состояние базы данных журналов	В этом блоке указана информация о сервере базы данных журналов. • **Сервер**. Внешний сервер базы данных журналов — LogAn или локальный сервер.

Параметр	Описание
	• **Версия сервера** — версия ПО сервера базы данных журналов. • **Версия устройства** — версия ПО самого устройства. • **Код устройства** — уникальный код устройства для интеграции с внешним сервером Log Analyzer. **Примечание** При интеграции с внешним сервером UserGate Log Analyzer обработка и экспорт журналов, создание отчетов и обработка других статистических данных производятся сервером Log Analyzer
Веб-портал	Параметры для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (SSL VPN). Подробное описание этих параметров — в разделе «Веб-портал»
Настройка кэширования HTTP	Вы можете настроить следующие параметры кэша прокси-сервера: • **Включен/Выключен** — включение или отключение кэширования. • **Исключения кэширования** — список URL, которые не будут кэшироваться. • **Максимальный размер объекта (МБ)** — объекты с размером, превышающим указанный в этом параметре, не будут кэшироваться. Рекомендуется оставить значение по умолчанию — 1 МБ. • **Размер RAM-кэша (МБ)** — размер оперативной памяти, отведенный под кэширование. Не рекомендуется использовать значение, превышающее 20% от объема оперативной памяти системы

Управление устройством

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

- кластеры отказоустойчивости;

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

Информация о настройке кластеров приведена в разделе «Кластеризация и отказоустойчивость».

Диагностика

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

Параметры диагностики

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

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

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

Управление журналами

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

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

Удаленный помощник

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

Процесс подключения к устройству происходит следующим образом:

1. Администратор устройства UserGate активирует функцию удаленного помощника.

2. Устройство устанавливает защищенное соединение с сервером удаленного помощника UserGate по протоколу SSH. При успешном подключении в интерфейсе устройства UserGate отобразятся параметры сеансового доступа: идентификатор и токен.

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

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

Операции с сервером

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

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

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

Управление резервным копированием

В этом блоке вы можете:

- создавать резервные копии;
- восстанавливать устройство из резервной копии;
- настраивать расписание экспорта резервных копий на удаленный сервер;
- настраивать SSH-ключи.

Чтобы создать резервную копию устройства:

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

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

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

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

Запись о создании резервной копии отобразится в журнале событий устройства.

Чтобы восстановить устройство из резервной копии:

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

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

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

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

Чтобы создать правило экспорта резервной копии устройства:

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

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

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

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

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

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

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

При ручном вводе также можно использовать следующие символы:

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

5. Нажмите **Сохранить**.

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

Чтобы настроить SSH-ключи:

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

2. Нажмите **Сгенерировать новый ключ**.

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

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

3. Добавьте открытый SSH-ключ на удаленный сервер.

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

Экспорт и импорт настроек

В этом блоке вы можете экспортировать текущие параметры UserGate SWG в виде файлов экспорта в формате BIN. Впоследствии такие файлы могут понадобиться для восстановления параметров устройства, а также для импорта в другие SWG.

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

Чтобы экспортировать все параметры устройства:

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

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

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

Чтобы экспортировать только сетевые параметры устройства:

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

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

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

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

Чтобы создать правило экспорта параметров устройства:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Добавить**.

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

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

   - тип — FTP или SSH;

- адрес;
- порт для подключения;
- учетные данные для авторизации;
- путь к существующей папке для сохранения файлов экспорта.

> **Примечание**
> **Для авторизации на удаленном SSH-сервере вы можете использовать SSH-ключи. Для этого их нужно предварительно настроить.**

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

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

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

При ручном вводе также можно использовать следующие символы:

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

5. Нажмите **Сохранить**.

Вы можете восстанавливать параметры устройства из файлов экспорта. Эти файлы не содержат данные о кластерах и лицензии, поэтому после

восстановления параметров вам потребуется повторно активировать лицензию и настроить кластеры. Кроме того, если для входа в UserGate SWG вы используете многофакторную аутентификацию через TOTP, после восстановления необходимо повторно добавить ключи инициализации.

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

> **Внимание!**
> **При восстановлении параметров UserGate SWG из файла экспорта, созданного в более поздней версии устройства, работоспособность сервера UserGate SWG не гарантируется.**

Чтобы восстановить параметры устройства из файла экспорта:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Импорт**.

2. Выберите файл экспорта.

3. В окне **Импортировать настройки** выберите тип импорта (все параметры или только сетевые).

4. Нажмите **Старт**.

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

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

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

Управление доступом к интерфейсам администрирования

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

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

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

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

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

разделе **Настройки → Пользователи и устройства → Профили аутентификации**.

Инструкции по настройке серверов аутентификации приведены в разделе «Серверы аутентификации», по настройке профилей аутентификации — в разделе «Профили аутентификации».

Вы можете удалять созданные учетные записи и изменять их параметры, а также управлять состоянием учетных записей (включать и отключать их). Кроме того, вы можете разблокировать локальную учетную запись, которая была заблокирована (например в случае, если было превышено количество неудачных попыток аутентификации).

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

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

Создание профиля доступа

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

Чтобы создать профиль доступа:

1. В разделе **Настройки → UserGate → Администраторы → Профили администраторов** нажмите **Добавить**.

2. На вкладке **Общие** укажите название профиля.

3. На вкладке **Разрешение доступа** выберите действия, которые может выполнять администратор в веб-интерфейсе.

4. На вкладке **Разрешение для API** выберите действия, которые может выполнять администратор при подключении через REST API.

5. На вкладке **Разрешение для CLI** разрешите или запретите администратору доступ к интерфейсу командной строки.

6. Нажмите **Сохранить**.

Теперь вы можете перейти к созданию учетной записи администратора.

Создание учетной записи администратора

Чтобы создать учетную запись администратора:

1. В разделе **Настройки → UserGate → Администраторы** в блоке в блоке **Администраторы** нажмите **Добавить** и выберите тип учетной записи.

2. Выберите профиль доступа и укажите параметры, необходимые для выбранного типа учетной записи.

3. Нажмите **Сохранить**.

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

Настройка парольной политики

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

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

Чтобы настроить парольную политику:

1. В разделе **Настройки → UserGate → Администраторы** в блоке в блоке **Администраторы** нажмите **Еще → Настроить**.

2. Укажите параметры, которым должен соответствовать пароль локальной учетной записи администратора.

3. Нажмите **Сохранить**.

Настройка цифровых сертификатов

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

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

Чтобы настроить цифровые сертификаты:

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

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

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

Будут созданы файл закрытого ключа `ca-key.pem` и файл открытого ключа и файл открытого ключа `ca.pem`. Импортируйте открытый ключ на сервер UserGate SWG.

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

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

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

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

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

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

Управление сертификатами

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

Для выполнения этих функций SWG использует различные типы сертификатов.

Сертификат	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли SWG
SSL captive-портала	Используется для создания безопасного HTTPS-подключения пользователей к странице авторизации captive-портала, отображения страницы блокировки и страницы Logout captive-портала, для работы прокси-сервера FTP. Этот сертификат должен быть выпущен со следующими параметрами: • `Subject name` — значение, установленное для домена **Домен Auth captive-портала** в разделе **Настройки → UserGate → Настройки → Модули**. • `Subject Alternative names` — необходимо указать все домены, для которых используется данный сертификат и которые заданы на странице **Настройки → UserGate → Настройки**: ◦ **Домен Auth captive-портала**; ◦ **Домен Logout captive-портала**; ◦ **Домен страницы блокировки**; ◦ **FTP поверх HTTP**; ◦ **Адрес веб-портала**.

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

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

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

Создание сертификата

Чтобы создать новый сертификат:

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

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

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

Экспорт и импорт сертификатов

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

Чтобы экспортировать сертификат:

1. В разделе **Настройки → UserGate → Сертификаты** выделите нужный сертификат в списке и нажмите **Экспорт**.

2. Выберите тип сертификата для экспорта:

   - **Экспорт сертификата** — экспортируются данные сертификата в DER-формате без экспортирования закрытого ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для SSL-инспектирования, для его установки в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом — в приложении «Установка сертификата локального удостоверяющего центра».

   - **Экспорт CSR** — экспортируется CSR сертификата, например для его подписи удостоверяющим центром.

Примечание

Рекомендуется сохранять сертификат, чтобы впоследствии иметь возможность его восстановить.

Примечание

В целях безопасности UserGate не разрешает экспорт закрытых ключей сертификатов.

Примечание

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

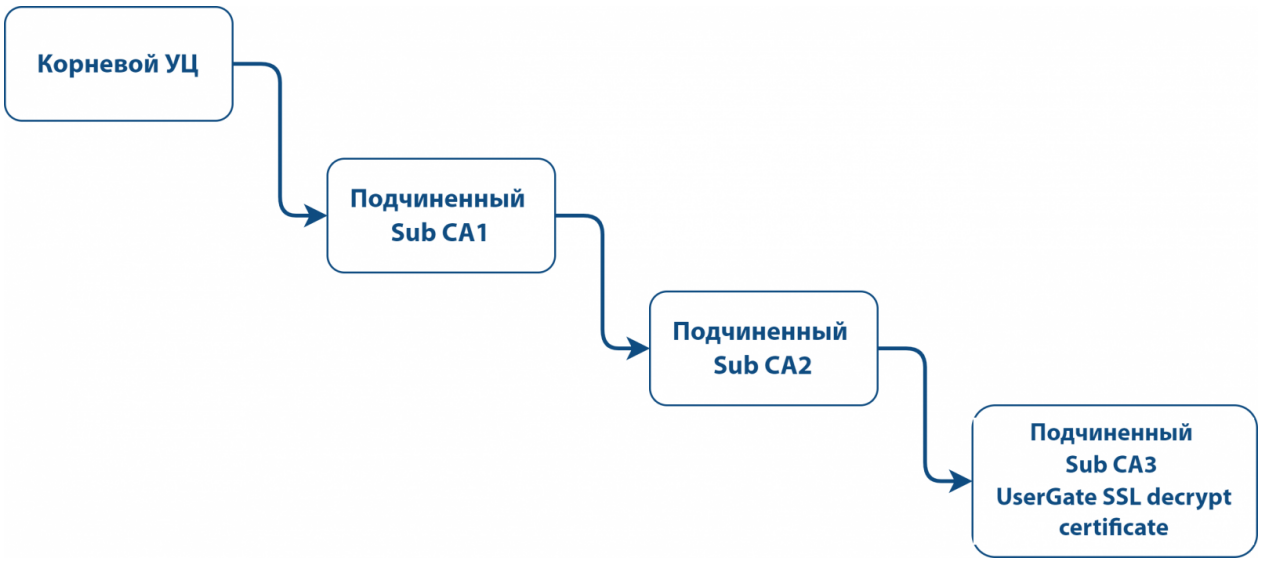
Чтобы импортировать сертификат:

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

Использование корпоративного УЦ для создания сертификата SSL-инспектирования

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

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



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

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

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

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

Для выполнения этой задачи:

1. В разделе **Настройки → UserGate → Сертификаты** нажмите **Новый CSR**, заполните необходимые поля и создайте CSR.
   Будут созданы закрытый ключ и файл запроса.

2. В списке сертификатов выделите CSR и с помощью кнопки **Экспорт** скачайте файл запроса.

3. В Microsoft CA создайте сертификат на основе полученного CSR-файла с помощью утилиты certreq (`certreq.exe -submit -attrib "CertificateTemplate:SubCA" HTTPS_csr.pem`) или с помощью веб-консоли Microsoft CA, указав в качестве шаблона «Подчиненный центр сертификации». Вы получите сертификат (открытый ключ), подписанный УЦ Sub CA2.

4. Скачайте созданный сертификат из веб-консоли Microsoft CA.

5. В UserGate SWG на вкладе **Сертификаты** выберите созданный ранее CSR-файл и нажмите **Редактировать**. Загрузите файл сертификата и нажмите **Сохранить**.

6. На вкладе **Сертификаты** повторно выберите созданный ранее CSR-файл и нажмите **Редактировать**. В поле **Используется** укажите **SSL-инспектирование** и нажмите **Сохранить**.

7. В веб-консоли Microsoft CA выберите и скачайте сертификаты для УЦ Sub CA1 и Sub CA2.

8. На вкладе **Сертификаты** с помощью кнопки Импорт загрузите скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2.

9. На вкладе **Сертификаты** для каждого из этих сертификатов нажмите **Редактировать**, в поле **Используется** укажите **SSL-инспектирование (промежуточный)** и нажмите **Сохранить**.

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

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

Профили клиентских сертификатов

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

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

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

Чтобы создать профиль клиентского сертификата:

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

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

Наименование	Описание
	Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, используется первое значение, указанное в сертификате
Сертификаты УЦ	Сертификаты корневых и промежуточных удостоверяющих центров, которые участвовали в выдаче сертификатов клиентов. Используются для проверки иерархии доверия к сертификату клиента. Сертификат клиента проверяется на подлинность для каждого сертификата УЦ из списка. Перебор списка идет сверху вниз
Проверка отозванных сертификатов	В списках отозванных сертификатов (CRL) содержатся сертификаты, которые были скомпрометированы либо срок действия которых истек. Такие сертификаты больше не могут использоваться для аутентификации. Возможно установить следующие значения параметра: • **Не проверять** — доступ будет предоставляться вне зависимости от того, является ли сертификат отозванным. • **Вся цепочка** — проверять все сертификаты в иерархии и требовать, чтобы они все были действительными. В профиль в разделе **Сертификаты УЦ** должны быть добавлены сертификаты корневого и всех промежуточных удостоверяющих центров, которые участвовали в выдаче сертификатов клиентов. • **Сертификат пользователя** — проверять только сертификат клиента. В профиль в разделе **Сертификаты УЦ** должен быть добавлен сертификат удостоверяющего центра, которым подписан сертификат клиента. • **Считать валидным, если статус неизвестен** — проверять сертификат и, если его статус не удалось определить по каким-то причинам (например, UG SWG не смог получить CRL), считать сертификат действительным. При этом сертификат в результате проверки может получить статус invalid, если он найден в списке отозванных
Тайм-аут проверки	Дополнительный связанный параметр определяет интервал времени, по истечении которого UserGate SWG перестает ожидать ответа о статусе сертификата от службы списков отозванных сертификатов. В этом случае

Наименование	Описание
	сертификат считается подлинным, и при соблюдении прочих условий аутентификация по нему может быть выполнена

Системные утилиты

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

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

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

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

Действие	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление
Expand data partition	Увеличение раздела для хранения данных. Эта операция обычно используется после увеличения дискового

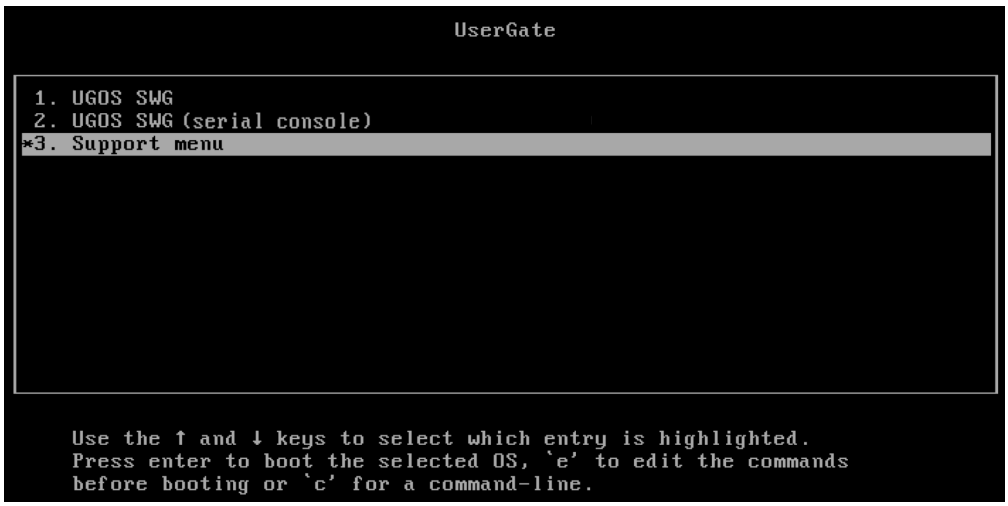
Действие	Описание
	пространства, выделенного гипервизором для виртуальной машины UserGate SWG. **Важно!** **Для расширения системного раздела с сохранением данных и параметров UserGate SWG необходимо с помощью средств гипервизора добавить новый диск и затем выполнить операцию Expand data partition, как указано в разделе «Расширение системного раздела»**
Create backup	Создание полной копии диска UserGate SWG на внешнем USB-носителе. **Важно!** **Перед созданием резервной копии USB-носитель будет отформатирован**
Restore from backup	Восстановление UserGate SWG с внешнего USB-носителя
Factory reset	Сброс состояния UserGate SWG. Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
Exit	Выход и перезагрузка устройства

Расширение системного раздела

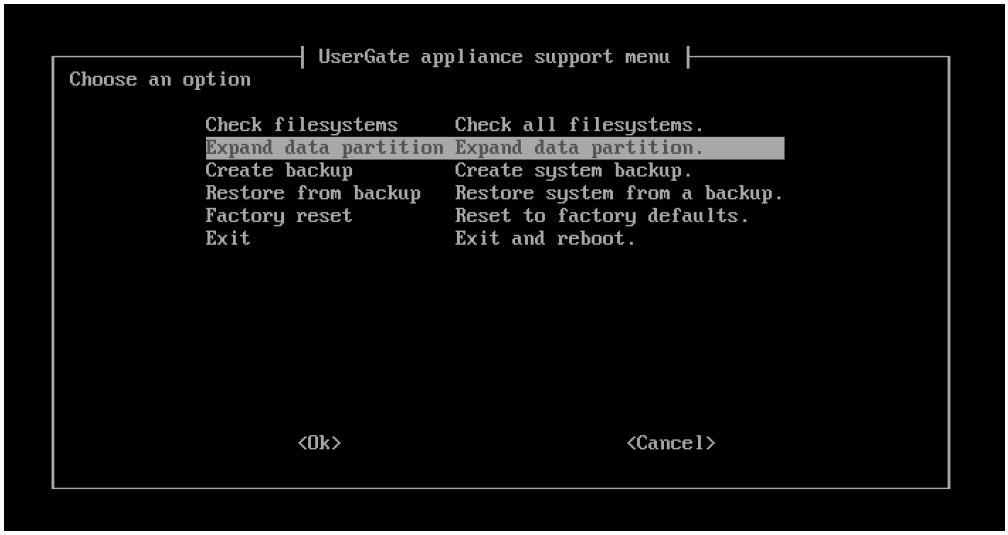
Для расширения системного раздела с сохранением конфигурации и данных узла UserGate:

1. С помощью гипервизора добавьте новый диск необходимого размера в свойствах виртуальной машины UserGate.

2. В меню загрузки узла UserGate войдите в раздел **Support menu**.



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



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

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

Работа с вышестоящими прокси-серверами

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

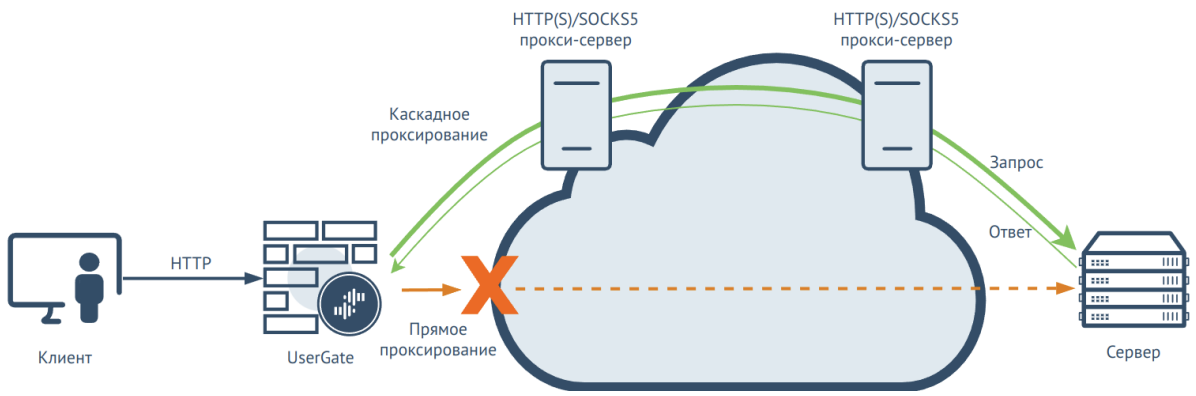
С помощью каскадной иерархии вы можете управлять доступом пользователей к веб-ресурсам. Например, используя вышестоящий прокси-сервер, можно обойти региональные ограничения или получить доступ к веб-ресурсам, обращение к которым возможно только через определенные сети.

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

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

Использование вышестоящего прокси-сервера

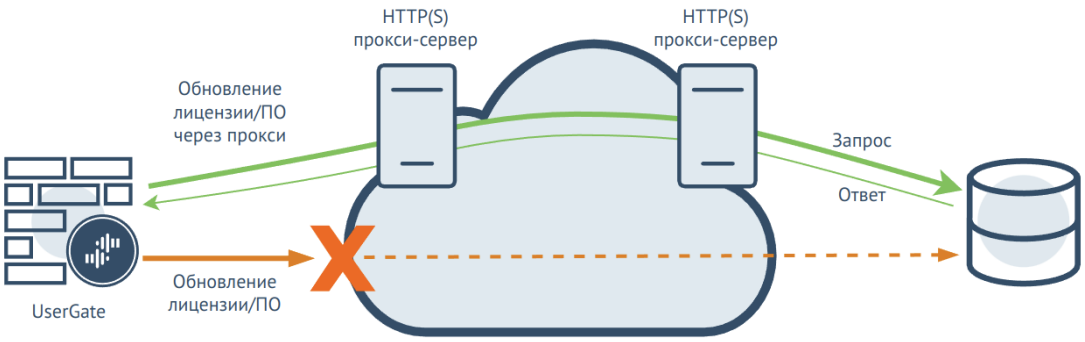
Для перенаправления трафика. Входящий веб-трафик, отфильтрованный правилами UserGate SWG, перенаправляется на вышестоящий прокси-сервер. В этом случае вышестоящим может быть прокси-сервер HTTP, HTTPS или SOCKS5. Процесс перенаправления трафика представлен на рисунке ниже.



При запросе клиентом внешнего ресурса устанавливаются две TCP-сессии: первая — между клиентом и UserGate SWG, вторая — между UserGate SWG и вышестоящим прокси-сервером. Адрес назначения трафика — это IP-адрес вышестоящего прокси-сервера, для межсетевого экрана трафик является

транзитным. Если ранее на UserGate SWG было настроено запрещающее правило по IP-адресам назначения, то оно не будет срабатывать.

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



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

Настройка прокси-сервера для перенаправления трафика

> **Примечание**
>
> **Вы можете настраивать вышестоящий прокси-сервер для перенаправления трафика как в веб-интерфейсе, так и в интерфейсе командной строки UserGate SWG. Ниже приведены инструкции для веб-интерфейса устройства.**

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

- Подключить прокси-сервер к UserGate SWG.
- Создать профиль вышестоящего прокси-сервера. С помощью профилей вы можете выбирать прокси-серверы, которые будут использоваться в качестве вышестоящего прокси-сервера, а также изменять параметры проверки их состояния. Это обеспечивает отказоустойчивое подключение вышестоящего прокси-сервера к UserGate SWG.

- Создать правило вышестоящего прокси-сервера. С помощью правил вы можете управлять доступом к выбранным веб-ресурсам. В качестве условий срабатывания правила можно выбрать зоны и адреса источника, пользователей и их группы, URL-категории и URL-списки.

Чтобы подключить прокси-сервер к UserGate SWG:

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

2. Укажите параметры подключения прокси-сервера.

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

3. Нажмите **Сохранить**.

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

Чтобы создать профиль вышестоящего прокси-сервера:

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

2. На вкладке **Общие** укажите название и описание профиля.

3. На вкладке **Серверы вышестоящего прокси** выберите прокси-серверы.

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

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

   - адрес веб-ресурса, к которому будет подключаться вышестоящий прокси-сервер;

- метод HTTP-запроса, посредством которого выполняется подключение к веб-ресурсу;
- интервал проверки;
- время ожидания ответа.

5. Нажмите **Сохранить**.

Созданный профиль отобразится в списке профилей раздела.

Чтобы создать правило вышестоящего прокси-сервера:

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

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

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

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

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

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

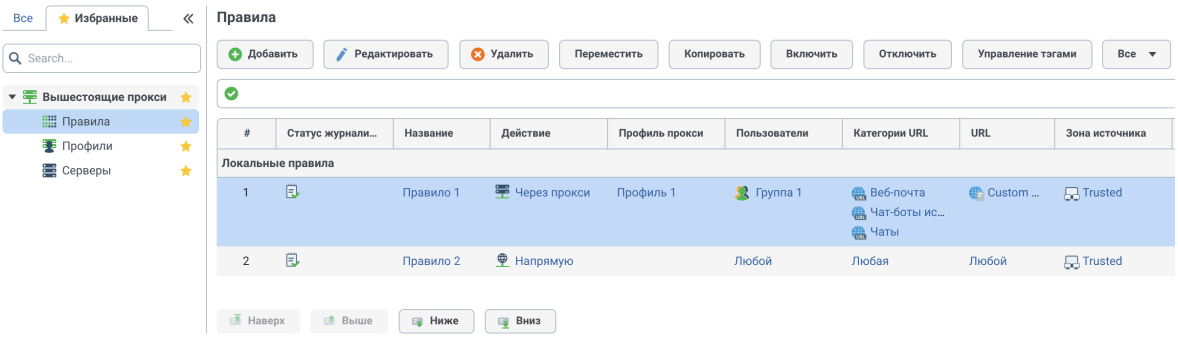
Вы можете выбирать объекты из списков или создавать новые по кнопке **Создать и добавить новый объект**. При установке флажка **Инвертировать** (соответствует логическому отрицанию) указанные объекты будут исключены из условий срабатывания правила.

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

Вы можете выбирать календари из списка или создавать новые по кнопке из списка или создавать новые по кнопке **Создать и добавить новый объект**.

5. Нажмите **Сохранить**.

Созданное правило отобразится в списке правил раздела. Правила применяются поочередно в том порядке, в котором они указаны в списке. Срабатывает первое правило среди тех, в которых совпали все указанные условия. Для изменения порядка применения правил используйте кнопки **Выше**, **Ниже**, **Наверх**, **Вниз** или перетащите правила курсором.



Настройка прокси-сервера для получения лицензий и обновлений

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

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии** (при активации лицензии) или **Зарегистрированная версия** (при обновлении лицензии).

2. В окне активации устройства установите флажок **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.

3. Выполните активацию или обновление лицензии.

Кластеризация и отказоустойчивость

Вы можете объединить несколько узлов в кластер и управлять им как единым логическим устройством.

UserGate SWG поддерживает два типа кластеров:

- **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые параметры фильтрации и обработки трафика в рамках кластера. Такая синхронизация гарантирует, что набор политик будет одинаковым на всех узлах кластера и все изменения конфигурации будут выполняться с минимальными задержками.

- **Кластер отказоустойчивости.** Если в сети настроен кластер конфигурации, то до четырех узлов, входящих в него, можно объединить в кластер отказоустойчивости, который обеспечит непрерывную фильтрацию и обработку трафика. В дополнение к возможностям кластера конфигурации кластер отказоустойчивости поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла кластера на другой, — за исключением сессий, использующих прокси-сервер, например трафик HTTP(S). Поддерживаются два режима работы кластера отказоустойчивости: «активный — активный» и «активный — пассивный». Вы можете собрать несколько кластеров отказоустойчивости. Например, если в кластер конфигурации добавлены узлы A, B, C и D, на их основе можно создать два кластера отказоустойчивости — A-B и C-D.

Важно!

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

Настройка кластера конфигурации

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

Чтобы настроить кластер конфигурации:

1. Выполните первоначальную настройку первого узла кластера. Убедитесь, что активированная лицензия на первом узле (раздел **Дашборды → Лицензия**) включает в себя модуль Cluster.

2. В веб-консоли первого узла в разделе **Настройки → Сеть → Зоны** добавьте зону, в которой будет выполняться репликация кластера, или выберите существующую зону **Cluster**. Убедитесь, что для выбранной зоны в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешены сервисы **Консоль администрирования** и **Кластер**.

> **Важно!**
> **Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например к интернету.**

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

4. В окне **Свойства интерфейса**:

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

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

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

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

8. В блоке **Шаг 1** укажите параметры дополнительного узла: кластерный интерфейс, его IP-адрес, маску подсети и IP-адрес шлюза (в случае, если первый и дополнительный узлы кластера находятся в разных подсетях). Например, если оба узла находятся в одной подсети, кластерному

интерфейсу `eth2` первого узла может быть назначен IP-адрес `192.168.100.5/24`, а интерфейсу `eth2` дополнительного узла в этом случае можно назначить IP-адрес `192.168.100.6/24`.

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

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

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

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

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

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

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

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

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

- Зеленый: узел доступен.
- Оранжевый: узел недоступен, идет перезагрузка узла.
- Красный: узел недоступен, связь с узлом потеряна.
- Черный: идет запуск узла.

Кластер отказоустойчивости «активный — пассивный»

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

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

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

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

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

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

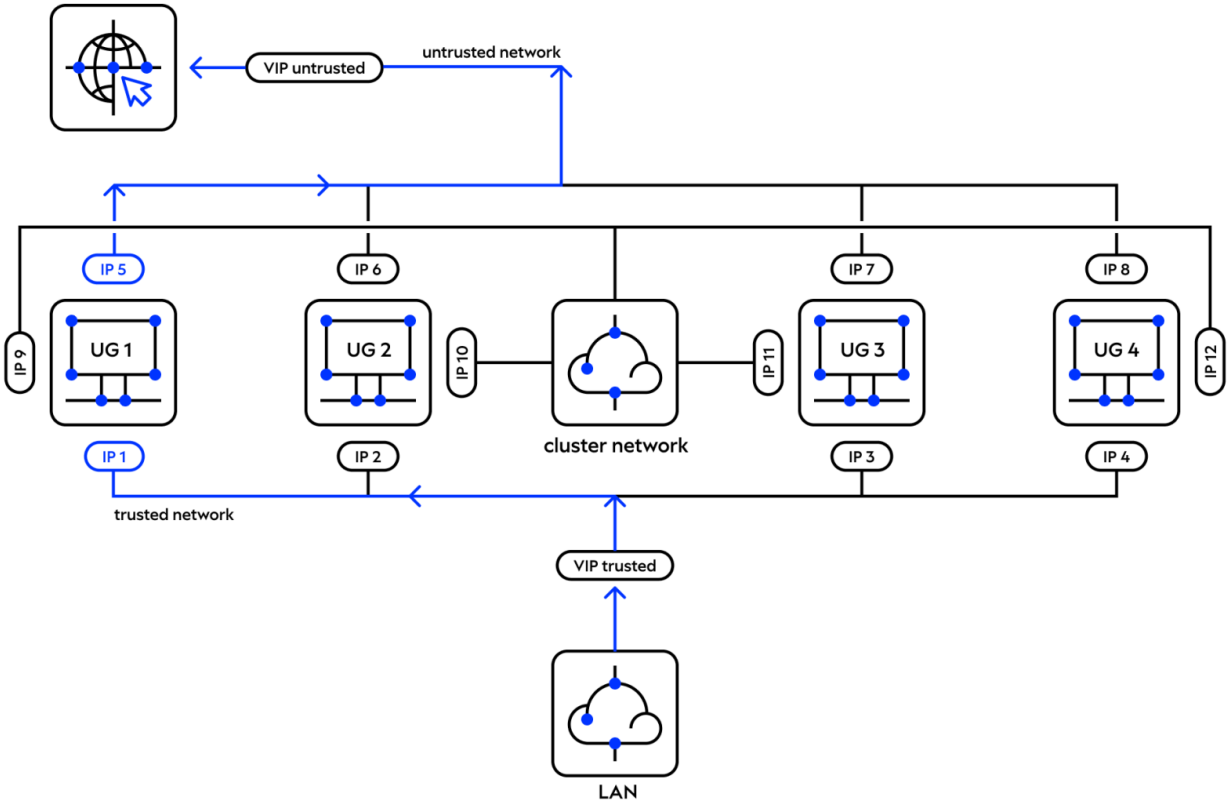
- Сбой в работе ПО UserGate SWG.

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

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

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

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



Кластер отказоустойчивости «активный — активный»

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

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

Примечание

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

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

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

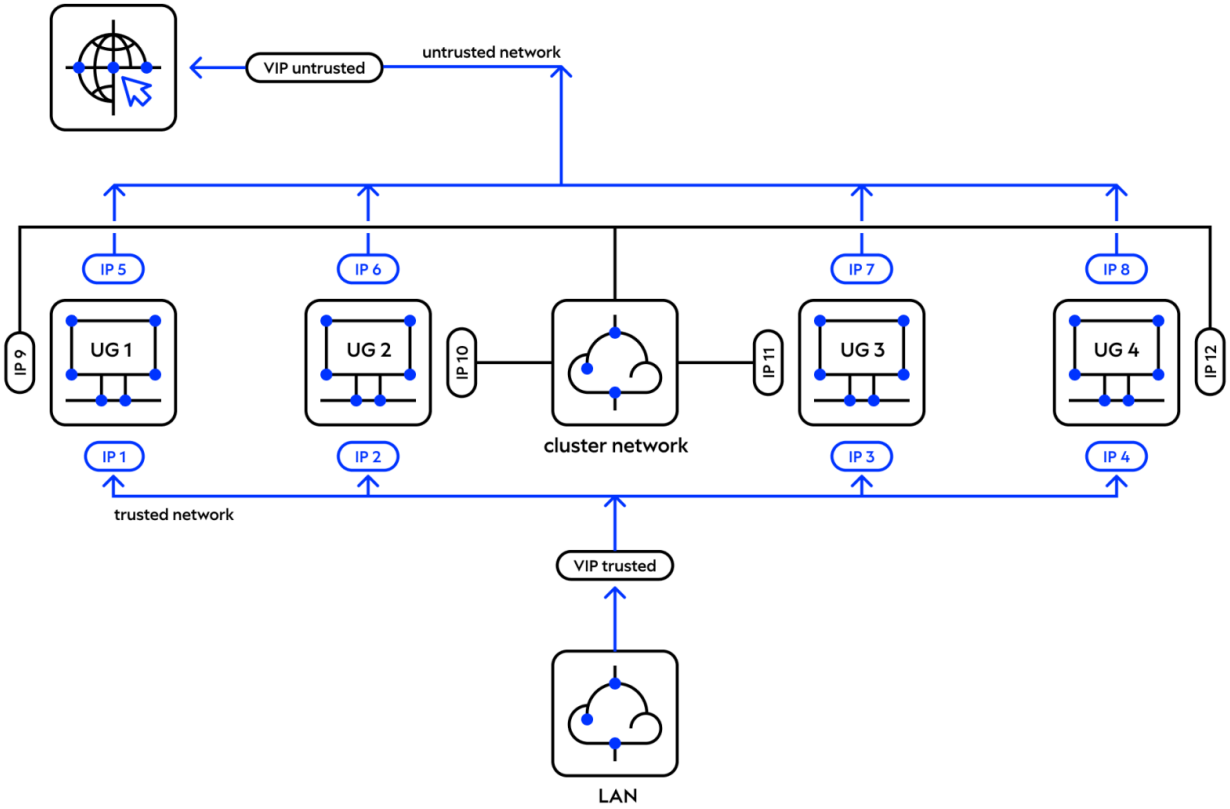
Примечание

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

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

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

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



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

Настройка кластера отказоустойчивости

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

Чтобы настроить кластер отказоустойчивости:

1. В разделе **Настройки → Сеть → Зоны** выберите зону, в которой планируется добавлять кластерные интерфейсы (зона `Cluster` на рисунках выше), и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешите сервис **VRRP**.

2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между узлами кластера:

- Выберите сетевой интерфейс, который будет участвовать в организации кластера.
- В окне **Свойства интерфейса** на вкладке **Общие** установите флажок **Включено** и назначьте интерфейсу кластерную зону.
- На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.

3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.

4. В окне **Свойства кластера отказоустойчивости** на вкладке **Общие** установите флажок **Включено**, введите название кластера и выберите режим кластера:

- **Активный — Пассивный** (значение по умолчанию) — трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен.
- **Активный — Активный** — нагрузка распределяется мастер-узлом на остальные узлы кластера.

5. На вкладке **Узлы** в блоке **Доступные узлы** выберите от двух до четырех узлов, затем в блоке **Настройка кластера** назначьте одному из узлов роль мастер-узла.

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

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

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

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

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

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

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

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

В таблице описаны дополнительные параметры кластера отказоустойчивости.

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

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

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

Диагностика узлов кластера отказоустойчивости

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

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

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

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

Чтобы настроить диагностику узлов кластера:

1. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** выберите кластер и нажмите **Редактировать**.

2. В окне **Свойства кластера отказоустойчивости** выберите вкладку **Диагностика**.

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

> **Примечание**
> **Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. Подробнее об этом — в разделе «Настройка шлюзов».**

4. Настройте параметры проверки доступности шлюзов:

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

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

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

7. Настройте параметры проверки доступности ресурсов:

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

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

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

9. Сохраните изменения.

Настройка кластера отказоустойчивости в облачной среде Yandex Cloud

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

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

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

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

1. Создайте в Yandex Cloud сервисный аккаунт с ролью `vpc.privateAdmin`.

2. Разверните в Yandex Cloud две виртуальные машины UserGate SWG и объедините их в кластер конфигурации.

> **Примечание**
> **Сервис Yandex Cloud поддерживает развертывание виртуальных машин как в одной сетевой зоне, так и в разных. Подробнее об этом — в справке сервиса.**

3. В веб-интерфейсе сервиса Yandex Cloud в параметрах каждой виртуальной машины добавьте созданный сервисный аккаунт.

4. Создайте таблицу маршрутизации Yandex Cloud. Когда кластер отказоустойчивости будет настроен, UserGate SWG передаст в эту таблицу IP-адрес сетевого интерфейса мастер-узла, через который будет направляться трафик. В случае если мастер-узел выйдет из строя, в таблицу статической маршрутизации Yandex Cloud будет передан IP-адрес резервного узла, и трафик перенаправится на этот IP-адрес.

Чтобы настроить кластер отказоустойчивости в облачной среде:

1. В разделе **Настройки → Сеть → Зоны** выберите или создайте зону для кластера и в окне **Свойства сетевой зоны** на вкладке **Контроль доступа** разрешите сервис **VRRP**.

2. В разделе **Настройки → Сеть → Интерфейсы** для каждого узла настройте интерфейсы для обмена VRRP-объявлениями между узлами кластера:

- Выберите сетевой интерфейс, который будет участвовать в организации кластера.
- В окне **Свойства интерфейса** на вкладке **Общие** назначьте интерфейсу кластерную зону.
- На вкладке **Сеть** добавьте IP-адрес, если он еще не был добавлен.
- Убедитесь, что на вкладке **Общие** установлен флажок **Включено**.

3. В разделе **Настройки → Консоль администратора → Кластеры отказоустойчивости** нажмите **Добавить**.

4. В окне **Свойства кластера отказоустойчивости** на вкладке **Узлы** в блоке **Доступные узлы** выберите виртуальные машины, развернутые в Yandex

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

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

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

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

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

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

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

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

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

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

13. Сохраните изменения.

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

Особенности настройки кластера отказоустойчивости с узлами в разных зонах Yandex Cloud

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

Для каждого узла кластера выполните следующие действия:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** нажмите **Добавить**.

2. В раскрывающемся списке выберите **Статические маршруты** и нажмите **Добавить**.

3. В окне **Свойства маршрута** укажите его название, установите флажок **Включено**.

4. Убедитесь, что установлен тип маршрута **Unicast**.

5. В поле **Адрес назначения** укажите подсеть за другим узлом кластера, на которую будет указывать маршрут.

6. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с узла, для которого настраивается маршрут.

7. Выберите сетевой интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate SWG сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.

8. Сохраните изменения.

Просмотр информации о кластере отказоустойчивости

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

Статусы кластера отказоустойчивости:

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

Статусы узлов в кластере отказоустойчивости:

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

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

НАСТРОЙКА СЕТИ

Настройка зон

Зона в UserGate SWG — это логическое объединение сетевых интерфейсов. Политики безопасности UserGate SWG 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 SWG поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление SWG
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

Администраторы UserGate SWG 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:

Шаг	Описание
1. Создайте зону.	В разделе **Настройки → Сеть → Зоны** нажмите **Добавить** и укажите название зоны
2. Настройте параметры защиты зоны от DoS (опционально).	Укажите параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Агрегировать** — если установлено, то считаются все пакеты, входящие в интерфейсы данной зоны. Если не установлено, то считаются пакеты отдельно для каждого IP-адреса. • **Порог уведомления** — при превышении количества запросов над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** — при превышении количества запросов над указанным значением SWG

Шаг	Описание
	начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 3000 запросов в секунду, для порога отбрасывания пакетов — 6000 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах, за исключением интерфейсов зоны **Cluster**. Необходимо увеличить пороговое значение отбрасывания пакетов для протокола UDP, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN. **Исключения защиты от DoS** — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для сервиса IP-телефонии, так как он шлет большое количество UDP-пакетов.
3. Настройте параметры контроля доступа зоны (опционально).	Укажите предоставляемые UserGate SWG 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 SWG. • **SNMP** — доступ к SWG по протоколу SNMP (UDP 161). • **Captive-портал** и **страница блокировки** — необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • **Кластер** — сервис, необходимый для объединения нескольких узлов SWG в кластер (TCP 4369, TCP 9000-9100). • **VRRP** — сервис, необходимый для объединения нескольких узлов SWG в отказоустойчивый кластер (IP протокол 112). • **Консоль администрирования** — доступ к веб-консоли управления (TCP 8001). • **DNS** — доступ к сервису DNS-прокси (TCP 53, UDP 53). • **HTTP(S)-прокси** — доступ к сервису HTTP(S)-прокси (TCP 8090). • **Агент авторизации** — доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.

Шаг	Описание
	• **Reverse-прокси** — сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Подробнее — в разделе «Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси». • **Web-портал** — сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Подробнее — в разделе «Веб-портал». • **Log Analyzer/SIEM** — сервис для подключения к анализатору журналов Log Analyzer (TCP 2023 и 9713). • **OSPF** — сервис динамической маршрутизации OSPF. Подробнее — в разделе «OSPF». • **BGP** — сервис динамической маршрутизации BGP. Подробнее — в разделе «BGP». • **RIP** — сервис динамической маршрутизации «RIP». • **BFD** — сервис быстрого обнаружения сбоев в сетевом соединении. • **Multicast** — сервис мультикаста. • **NTP сервис** — разрешает доступ к сервису точного времени, запущенному на сервере SWG. • **UserID syslog коллектор** — сервис для разрешения получения информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт TCP 514). • **API XML RPC поверх HTTPS** — разрешает доступ к API поверх HTTPS (TCP 4443). Подробнее о требованиях сетевой доступности — в приложении «Требования к сетевому окружению»
4. Настройте 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	Описание
5. Настройте 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 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 — в разделе «IP-адреса»

Настройка интерфейсов

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

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

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

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

- Состояние интерфейса — включен или отключен.
- Тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
- Зона, к которой относится интерфейс.
- Профиль NetFlow для отправки статистических данных на NetFlow-коллектор.
- Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol. Доступен только для физических сетевых интерфейсов.
- Алиас (псевдоним) — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.

- Физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, получаемый по DHCP.
- Параметры работы DHCP-ретранслятора. Для работы DHCP-ретранслятора его необходимо включить на вкладке **DHCP-релей**, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

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

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

Создание VLAN-интерфейса

Для создания VLAN-интерфейса:

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

Параметр	Описание
Включено	Включение VLAN-интерфейса
Название	Название VLAN-интерфейса. Название присваивается автоматически на основе имени физического порта и тега VLAN
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе «Теги»
Описание	Опциональное описание интерфейса
Тип интерфейса	Выбор типа интерфейса — **Layer 3** или **Mirror**. Интерфейсу, работающему в режиме **Layer 3**, можно назначить IP-адрес и использовать его в правилах межсетевого экрана,

Параметр	Описание
	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
Интерфейс	Физический интерфейс, на котором создается VLAN-интерфейс
Зона	Зона, которой принадлежит VLAN-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.**
Сеть	Способ присвоения IP-адреса (**Режим**) — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS
DHCP-релей	Настройка работы DHCP-ретранслятора на VLAN-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько серверов DHCP, на которые необходимо пересылать DHCP-запросы клиентов

Создание бонд-интерфейса

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

Для создания бонд-интерфейса:

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

Параметр	Описание
Включено	Включение бонд-интерфейса
Название	Название бонд-интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе «Теги»
Имя узла	Имя узла в кластере, на котором создается данный бонд-интерфейс
Зона	Зона, которой принадлежит бонд-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.**
Интерфейсы	Интерфейс или интерфейсы, которые будут использованы для построения бонд-интерфейса
Режим	Режим работы бонд-интерфейса должен совпадать с режимом работы интерфейса на соседнем устройстве, к которому он подключается. Доступные режимы работы: • **Round robin.** Режим применяется с целью балансировки нагрузки и обеспечения отказоустойчивости. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. • **Active backup**. Режим применяется с целью обеспечения отказоустойчивости. Активен только один сетевой интерфейс из всех объединенных интерфейсов. Переключение на резервный интерфейс происходит исключительно при отказе активного. В целях корректной работы с сетевым оборудованием MAC-адрес бонд-интерфейса анонсируется через один физический порт.

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

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

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

Создание моста (bridge-интерфейс)

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

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

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

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

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

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

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

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

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

Подробнее о сетевых интерфейсах, поддерживающих режим байпас, смотрите в руководствах по эксплуатации на модели ПАК UserGate.

Для создания моста:

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

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе «Теги»
Имя узла	Имя узла в кластере, на котором создается bridge-интерфейс
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, к которой принадлежит интерфейс
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов **Важно!** **Значение параметра не может содержать символы кириллицы.**
Интерфейсы моста	Два интерфейса, которые будут использованы для построения моста
Интерфейсы байпас-моста	Пара интерфейсов, которые можно использовать для построения байпас-моста. Требуется поддержка оборудования ПАК UserGate SWG
STP (Spanning Tree Protocol)	Использование алгоритма 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. Возможность изменить размер MTU, размер MSS
DHCP-релей	

Параметр	Описание
	Настройка работы DHCP-ретранслятора на bridge-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Создание PPPoE-интерфейса

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

Для создания PPPoE-интерфейса:

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

Параметры	Описание
Включено	Включение PPPoE-интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе «Теги»
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается PPPoE-интерфейс
Интерфейс	Интерфейс, на котором будет создаваться PPPoE-интерфейс
Зона	Зона, к которой принадлежит PPPoE-интерфейс

Параметры	Описание
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов **Важно!** **Значение параметра не может содержать символы кириллицы.**
MTU	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet
MSS	Размер MSS. Корректные значения: 0 или число в диапазоне от 4 до значения, полученного по формуле (MTU - 40)
Логин	Имя пользователя для соединения PPPoE
Пароль	Пароль пользователя для соединения PPPoE
Переподключаться автоматически	Повторное автоматическое установление соединения при обрыве связи
Тип аутентификации	Протоколы аутентификации, использующиеся в протоколе PPP: • **CHAP** (Challenge Handshake Authentication Protocol) — протокол аутентификации с косвенным согласованием. Алгоритм проверки подлинности, предусматривающий передачу не самого пароля пользователя, а косвенных сведений о нем. • **PAP** (Password Authentication Protocol) — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удаленного доступа открытым текстом (без шифрования)
Интервал между попытками подключения (сек.)	Интервал времени в секундах между разрывом и повторной попыткой установления соединения
Маршрут по умолчанию	Устанавливает PPPoE-интерфейс в качестве маршрута по умолчанию
	Интервал проверки соединения

Параметры	Описание
Интервал проверки соединения (сек.)	
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которых UserGate SWG считает, что соединение отсутствует, и разрывает его
Использовать DNS-сервер провайдера	Если опция включена, то UserGate SWG использует DNS-серверы, выданные провайдером
Количество попыток подключения	Количество последовательных неудачных попыток подключения, по достижении которого автоматическое восстановление соединения прекращается
PPPoE-сервис	Имя сервиса указывается, если его предоставил провайдер. Если имя сервиса не используется, поле необходимо оставить пустым

Создание loopback-интерфейса

Для создания loopback-интерфейса:

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

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса в виде `loopbackN`, где `N` — целое число
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе «Теги»
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается интерфейс
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, которой принадлежит интерфейс.
Профиль LLDP	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе «Профили LLDP»

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

Настройка шлюзов

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

Пример настройки сети с двумя провайдерами:

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

Добавление шлюза

Чтобы добавить шлюз:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Добавить**.

2. В окне **Свойства шлюза** укажите его параметры: название, имя узла UserGate SWG, сетевой интерфейс (по умолчанию назначается автоматически), виртуальный маршрутизатор и IP-адрес шлюза.

> **Примечание**
> **Подробнее о виртуальных маршрутизаторах — в разделе «Виртуальные маршрутизаторы».**

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

Настройка балансировки

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

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

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

Чтобы настроить балансировку трафика между шлюзами:

1. В разделе **Настройки → Сеть → Шлюзы** выберите шлюз, который будут участвовать в балансировке, и нажмите **Редактировать**.

2. В окне **Свойства шлюза** укажите вес шлюза, установите флажок **Балансировка** и сохраните изменения.

3. Выполните настройку других шлюзов, участвующих в балансировке.

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

Настройка проверки сети

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

Проверка сети может быть полезна в следующих случаях:

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

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

Чем ниже порог, тем строже критерий доступности. Например:

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

Чтобы настроить проверку сети:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Проверка сети**.
2. В окне **Свойства проверки сети** установите флажок **Включено**.

3. Нажмите кнопку **Добавить** и укажите IP-адреса для проверки доступа в интернет.

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

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

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

Индикаторы доступности шлюзов теперь будут отражать результаты проверки сети.

Настройка DHCP

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

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

В UserGate SWG 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.

Наименование	Описание
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

Для корректной работы устройства необходимо, чтобы UserGate SWG 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 настроить следующие параметры в разделе DNS-прокси.

Параметр	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 SWG 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 **Важно!** **Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.** **Важно!** **Правила контентной фильтрации, использующие список IP-адресов во вкладке Назначение → Адрес доставки, не обрабатываются модулем DNS-фильтрации. Обработка таких правил выполняется средствами модуля контентной фильтрации.**

Параметр	Описание
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 SWG 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:

1. В блоке **DNS-прокси** нажмите **Добавить**, задайте **Название** и **Описание** (опционально).

2. Укажите список доменов, которые необходимо перенаправлять. Например, `localdomain.local`. Допускается использование символа '*' для указания шаблона доменов.

3. Укажите список IP-адресов DNS-серверов, на которые необходимо пересылать запросы на указанные домены.

С помощью DNS-прокси можно задавать статические записи типа host (A-запись). Чтобы создать статическую запись:

1. В блоке **Статические записи** нажмите **Добавить**, задайте **Название** и **Описание** (опционально).

2. Укажите FQDN статической записи. Например, www.example.com.

3. Укажите список IP-адресов, которые UserGate SWG будет возвращать при запросе этого FQDN.

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.

SWG 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 (SWG) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в SWG:

1. Настройте сервер WCCP в соответствии с его инструкцией.

2. Настройте сервисные группы WCCP. В веб-консоли UserGate SWG в разделе **Настройки → Сеть → WCCP** нажмите **Добавить** и создайте одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры.

Параметр	Описание
Включено	Включение или отключение сервисной группы
Название	Название сервисной группы
Описание	Описание сервисной группы
Сервисная группа	

Параметр	Описание
	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 SWG в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP
Способ перенаправления трафика	Определение способа перенаправления трафика с серверов WCCP на UserGate SWG. Возможны значения: • **gre** — использовать туннель Generic Routing Encapsulation (GRE). • **L2** — использовать перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес SWG. Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и SWG 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-адреса источника UserGate SWG будет использовать IP-адрес компьютера клиента, а зона источника не будет определена. В связи с этим, в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).**
Способ возврата трафика	Определение способа перенаправления трафика с UserGate SWG на серверы WCCP. Возможны значения: • **gre** — использовать туннель Generic Routing Encapsulation (GRE). • **L2** — использовать перенаправление L2. В этом случае UserGate SWG (WCCP-лиент) изменит MAC-адрес назначения в пакете на адрес маршрутизатора (WCCP-сервер).

Параметр	Описание
	Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate SWG 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. Несколько портов указываются через запятую: • `80, 442, 8080` Для перенаправления трафика на основании значений портов источника поставьте флажок **Порт источника** **Важно!** **UserGate SWG может применять фильтрацию только для перенаправленного TCP-трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate SWG с другими портами, будет отправляться в интернет без фильтрации.**
Протокол	Укажите протокол — TCP или UDP
Роутеры WCCP	Укажите IP-адреса серверов WCCP
Способ назначения	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможные варианты: • Хэш — распределение трафика на основе хэш-суммы, вычисленной по указанным полям IP-пакета. ◦ Альтернативный хэш — если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиент 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

Параметр	Описание
	проконсультируйтесь с документацией производителя сервера WCCP

Виртуальные маршрутизаторы

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

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

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

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

Виртуальные маршрутизаторы имеют следующие ограничения:

- Ряд сервисов может быть использован только в виртуальном маршрутизаторе, созданном по умолчанию:
  - WCCP;
  - ICAP;
  - DNS;
  - авторизация;
  - любой сетевой трафик, генерируемый самим устройством: проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS-сообщений, SNMP-трапов и т. п.;

  - подключение UserGate MC к UserGate SWG возможно только в случае, если порт UserGate SWG находится в виртуальном маршрутизаторе, созданном по умолчанию.

- Действие правил NAT, DNAT, Port forwarding распространяется на все виртуальные маршрутизаторы.
- Зоны являются глобальными — параметры зоны и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

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

Создание виртуального маршрутизатора

Чтобы создать новый виртуальный маршрутизатор:

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

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

2. На вкладке **Интерфейсы** укажите интерфейсы, которые должны принадлежать новому виртуальному маршрутизатору. Интерфейсы, относящиеся к другим виртуальным маршрутизаторам, не могут быть добавлены. Любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. Допускается использовать интерфейсы

всех типов — физические, виртуальные (VLAN), bond-интерфейсы, VPN-интерфейсы и другие.

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

1. Статические маршруты (кроме маршрута по умолчанию). Подробнее о статических маршрутах — в разделе «Статические маршруты». Маршрут по умолчанию добавляется в разделе **Настройки → Сеть → Шлюзы**. Подробнее о настройке шлюзов — в разделе «Настройка шлюзов».

2. Динамические маршруты, получаемые с помощью протокола маршрутизации OSPF. Подробнее — в разделе «OSPF».

3. Динамические маршруты, получаемые с помощью протокола маршрутизации BGP. Подробнее — в разделе «BGP».

4. Динамические маршруты, получаемые с помощью протокола маршрутизации RIP. Подробнее — в разделе «RIP».

5. Мультикастинг. Подробнее — в разделе «Мультикастинг».

Статические маршруты

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

Для добавления статического маршрута:

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

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

3. Выберите тип маршрута:

   - **Unicast** — стандартный тип маршрута. Отправляет трафик на адреса назначения через заданный шлюз.

   - **Blackhole** — трафик отбрасывается без информирования источника о том, что данные не достигли адресата.

- **Unreachable** — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (тип 3, код 1).
- **Prohibit** — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (тип 3, код 13).

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

5. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с устройства.

6. Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate SWG сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.

7. Задайте метрику маршрута. Если маршрутов в сеть несколько, то чем меньше значение метрики, тем выше приоритет маршрута.

Протоколы динамической маршрутизации

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

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

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

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

OSPF

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

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

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

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

Для настройки параметров OSPF в UserGate SWG:

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

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

3. Для начала настройки параметров OSPF установите флажок **Включено** и укажите идентификатор маршрутизатора. Идентификатор должен быть уникальным и задан в формате IPv4. Для удобства он может совпадать с одним из IP-адресов интерфейсов UserGate SWG, относящихся к выбранному виртуальному маршрутизатору.

4. Настройте параметры интерфейсов, на которых будет работать OSPF.

Параметр	Описание
Включено	Включение или отключение использования интерфейса
Интерфейс	

Параметр	Описание
	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в выбранный виртуальный маршрутизатор
Тип сети	Тип сети для оптимизации процесса установления соседства. Доступны следующие параметры: • **Не установлен**; • **Broadcast**; • **Point-to-point**; • **Point-to-multipoint**
Пассивный режим	Включение или отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается пересылать пакеты обновления протокола маршрутизации
Стоимость	Стоимость (cost) канала интерфейса. Значение передается в объявлениях о состоянии (Link-State Advertisement, LSA) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию — 1
Приоритет	Целое число от 0 до 255. Чем выше значение, тем больше вероятность того, что маршрутизатор станет назначенным (Designated Router, DR) в сети и будет рассылать LSA. Значение 0 исключает маршрутизатор из процедуры выбора DR. Значение по умолчанию — 1
Интервал hello	Интервал в секундах, через который маршрутизатор посылает hello-пакеты. Этот интервал должен быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию — 10 секунд
Интервал dead	Время в секундах, по истечении которого соседний маршрутизатор считается неактивным. Время исчисляется с момента приема последнего hello-пакета от соседнего маршрутизатора. Значение по умолчанию — 40 секунд
Интервал повторения	Устанавливает интервал повторной отправки пакета LSA. Значение по умолчанию — 5 секунд
Задержка передачи	Устанавливает время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию — 1 секунда
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга OSPF. Это позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF.

Параметр	Описание
	Подробнее — в разделе «Профили BFD»
Аутентификация	Включает требование аутентификации каждого принимаемого маршрутизатором OSPF-сообщения. Аутентификация обычно используется для предотвращения внедрения ложного маршрута от нелегитимных маршрутизаторов
Тип аутентификации	Возможные значения: • **Plain** — передача ключа в открытом виде для аутентификации маршрутизаторов. Необходимо указать значение поля **Ключ**. • **Digest** — использование хеш-суммы MD5 для ключа аутентификации OSPF-пакетов. Необходимо указать **Ключ** и **MD5 key ID**. Для корректной работы эти параметры должны быть идентичными на всех маршрутизаторах. Значение параметра **Ключ** может содержать только буквы латинского алфавита, цифры и символ подчеркивания. Максимальное количество символов — 16

5. Настройте параметры областей OSPF.

Параметр	Описание
Включено	Включает или отключает использование области
Имя	Имя области
Стоимость	Стоимость (cost) маршрута по умолчанию, анонсируемая в тупиковую область (stub area). Значение по умолчанию — 1. Если тупиковая область подключена к нескольким пограничным маршрутизаторам области (Area Border Router, ABR), администратор может назначать разные стоимости маршрута по умолчанию для каждого ABR. Это позволяет управлять исходящим из области трафиком, направляя его через предпочтительный шлюз
Идентификатор области	Идентификатор области (area ID) может быть указан в десятичном формате или в формате записи IP-адреса. Для установления соседства OSPF идентификатор области должен совпадать на соседних маршрутизаторах
Тип аутентификации	Возможные значения: • **Нет** — не требовать аутентификацию OSPF-пакетов.

Параметр	Описание
	• **Plain** — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. • **Digest** — использование MD5 хеш-суммы для ключа аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне области
Тип области	Доступные типы областей: • **Нормальная** — обычная область, которая создается по умолчанию. Эта область принимает обновления каналов, суммарные маршруты и внешние маршруты. • **Тупиковая** (stub) — тупиковая область не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других областей. Если маршрутизаторам из тупиковой области необходимо передавать информацию за границу автономной системы, они используют маршрут по умолчанию. В тупиковой области не может находиться пограничный маршрутизатор автономной системы (Autonomous System Boundary Router, ASBR). • **NSSA** — Not-so-stubby area. NSSA-область определяет дополнительный тип LSA — LSA type 7. В NSSA-области может находиться ASBR
Не суммировать	Запрещает добавление суммированных маршрутов в тупиковые типы областей
Интерфейсы	Интерфейсы OSPF, на которых будет доступна эта область
Виртуальные линки	Специальное соединение, которое позволяет соединять части областей или присоединить область через другую магистральную область. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение в случае выхода из строя основных соединений. Укажите идентификаторы маршрутизаторов, которые доступны через такую область

6. Карты маршрутов (route map) позволяют фильтровать маршруты при перераспределении и изменять различные атрибуты выбранных

маршрутов. На вкладке **Routemaps** указаны глобальные параметры для создания карты маршрутов.

Параметр	Описание
Название	Название карты маршрутов. Не может содержать символы кириллицы
Действие	Устанавливает действие для этой карты маршрутов. Возможные значения: • **Разрешить** — разрешает прохождение данных, отвечающих условиям карты маршрутов. • **Запретить** — запрещает прохождение данных, не отвечающих условиям карты маршрутов
Сравнивать по	Условия применения карты маршрутов. Возможные значения: • **IP**. Если выбрано это условие, на вкладке **IP-адреса** надо добавьте все необходимые IP-адреса для этого условия с возможностью указать **le** (less or equal) и **ge** (greater or equal). Например: ◦ `10.0.0.0/8` — только сеть 10.0.0.0/8. ◦ `10.0.0.0/8::11` — маршруты с первым октетом, равным 10, и префиксом от 8 до 11. ◦ `10.0.0.0/8:11:13` — маршруты с первым октетом, равным 10, и префиксом от 11 до 13. • **AS-путь**. Если выбрано это условие, то в закладке **AS-путь** добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как: ◦ пробел; ◦ запятая; ◦ начало строки; ◦ конец строки; ◦ AS set delimiter { and }; ◦ AS confederation delimiter (and). • **Community**. Если выбрано это условие, на вкладке **Communit y** добавьте все необходимых для него BGP-community
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов

Параметр	Описание
Установить метрику	**Установить метрику для отфильтрованных маршрутов**
Установить предпочтение	**Установить предпочтение для отфильтрованных маршрутов**
Установить AS-prepend	**Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута**
Установить community	Установить (заменить) значение BGP-community для отфильтрованных маршрутов на указанное
Добавлять community	**Установить значение BGP-community для отфильтрованных маршрутов**

7. Если необходимо, на вкладке **Route redistribution** настройте перераспределения анонсируемых маршрутов из других протоколов в OSPF. Укажите следующие параметры:

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

BGP

BGP (Border Gateway Protocol) — динамический протокол маршрутизации, относящийся к классу протоколов маршрутизации внешнего шлюза (Exterior

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

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

Для настройки BGP в UserGate SWG:

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

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

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

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

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

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

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

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

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

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

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

Сравнивать по	Условия применения route map:
	• **IP**. Если выбрано это условие, на вкладке **IP-адреса** добавьте все необходимые для него IP-адреса.
	• **AS-путь**. Если выбрано это условие, на вкладке **AS-путь** добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как:
	  ◦ пробел;
	  ◦ запятая;
	  ◦ начало строки;
	  ◦ конец строки;
	  ◦ AS set delimiter { and };
	  ◦ AS confederation delimiter (and).
	• **Community**. Если выбрано это условие, на вкладке **Communit y** добавьте строки всех необходимых для него BGP-community

Параметр	Описание
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов
Установить метрику	Установить метрику для отфильтрованных маршрутов
Установить предпочтение	Установить предпочтение для отфильтрованных маршрутов
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута
Community	Установить значение BGP-community для отфильтрованных маршрутов

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

Параметр	Описание
Название	Название фильтра
Действие	Устанавливает действие для фильтра: • **Разрешить** — разрешает прохождение данных, отвечающих условиям фильтра. • **Запретить** — запрещает прохождение данных, не отвечающих условиям фильтра

Фильтровать по	Условия применения фильтра:
	• **IP**. Если выбрано это условие, на вкладке **IP-адреса** добавьте IP-адреса для этого условия. Адреса могут быть указаны в следующих форматах:
	  ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8.
	  ◦ 10.0.0.0/8::11 — маршруты, у которых первый октет 10 и префикс от 8 до 11.
	  ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13.
	• **AS-путь**. Если выбрано это условие, на вкладке **AS-путь** добавьте номера автономных систем для этого условия

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

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

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

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

Пример настройки BGP для кластера UserGate SWG — в статье «Варианты настройки BGP для кластера Актив-Пассив».

RIP

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

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

Для настройки RIP в UserGate SWG:

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

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **RIP** и установите флажок **Включено**.

3. Настройте параметры протокола RIP:

   - **Версия RIP** — определяет версию протокола RIP. Как правило используется версия 2.

   - **Метрика по умолчанию** — целочисленное значение в интервале от 1 до 15. Обычно значение метрики по умолчанию равно 1.

   - **Административное расстояние** — стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP

— 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).

- **Отправлять себя в качестве маршрута по умолчанию** — оповещать другие маршрутизаторы о том, что этот маршрутизатор имеет маршрут по умолчанию.

4. Маршрутизатор RIP будет отправлять обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. На вкладке **Сети RIP** укажите как минимум одну сеть для корректной работы протокола. При настройке сетей RIP администратор может указать сеть в виде CIDR, например 192.168.1.0/24, либо указать сетевой интерфейс, с которого будут отправляться обновления.

5. На вкладке **Интерфейсы** добавьте интерфейсы, на которых будет работать RIP.

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

6. Параметры редистрибуции маршрутов позволяют указать, какие из маршрутов необходимо отправлять соседям. Вы можете задать для

редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGP, а также статические маршруты в непосредственно подключенные к UserGate SWG сети (connected) или маршруты, добавленные администратором в разделе **Маршруты** (kernel).

Мультикастинг

Технология IP-мультикастинга позволяет существенно сократить передаваемый объем трафика, доставляя единый поток информации одновременно множеству потребителей. Применение этой технологии особенно эффективно для доставки голосового и видеотрафика. Традиционные методы доставки трафика — это юникаст (доставка от точки к точке) и бродкаст (широковещательная посылка трафика). Мультикаст-метод позволяет доставить трафик группе узлов (мультикаст-группа). Узлы (получатели), которые хотят получать этот трафик, должны присоединиться к соответствующей мультикаст-группе. Для присоединения узлов к мультикаст-группе используется протокол Internet Group Management Protocol (IGMP). Мультикаст-группа идентифицируется с помощью группового адреса. Для мультикастовых адресов выделена подсеть класса D со следующим диапазоном адресов для трансляций: 224.0.0.0 — 239.255.255.255.

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

Маршрутизаторы в мультикастинговой среде могут иметь следующие роли:

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

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

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

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

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

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

В режиме работы ASM приемник трансляции указывает мультикаст-группу, от которой он будет получать трансляцию. Для работы режима необходимо наличие маршрутизатора с ролью RP. RP определяет источник трансляции для группы приемника. Далее источник и приемник выбирают лучший сетевой путь для пересылки мультикаст-трафика. В этом режиме используется следующая адресация:

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

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

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

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **Мультикаст-маршрутизатор** и установите флажок **Включено**.

3. Настройте общие параметры мультикастинга:

   - **Использовать ECMP** — распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если эта опция отключена, то весь трафик на определенный узел назначения будет пересылаться только через один из маршрутизаторов (next hop).

- **Использовать ECMP rebalance** — если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). При отключенной опции перераспределяются только те потоки, которые передавались через отключенный интерфейс.
- **JOIN/PRUNE интервал** — интервал в секундах для отправки сообщений PIM JOIN и PIM PRUNE для управления потоком мультикаст-трафика.
- **Интервал register suppress** — таймер в секундах, который временно запрещает маршрутизатору-источнику инкапсулировать мультикаст-трафик в пакеты PIM Register.
- **Keep-alive-таймер** — интервал в секундах (31–60 000), через который маршрутизатор будет посылать сообщения keepalive соседям. Это же значение интервала используется маршрутизатором для принятия решения о недоступности соседа.

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

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

Параметр	Описание
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга. Позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса. Подробнее — в разделе «Профили BFD»

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

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

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

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

ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Пользователи и группы

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности UserGate SWG 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 UserGate SWG. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. UserGate SWG 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.

UserGate SWG определяет следующие типы пользователей:

Тип	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 UserGate SWG — 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 UserGate SWG, например RADIUS, TACACS+, Kerberos, SAML.

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

LDAP-коннектор

LDAP-коннектор позволяет:

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

Для создания LDAP-коннектора в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить LDAP-коннектор** и укажите параметры коннектора.

Параметр	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 UserGate SWG получит адрес контроллера домена с помощью DNS-запроса. Если указан

Параметр	Описание
	FQDN домена, то при отключении основного контроллера домена, UserGate SWG будет использовать резервный. В случае недоступности части контроллеров домена с площадки, где работает UserGate SWG, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену
Срок жизни LDAP-кэша	Срок жизни LDAP-кэша (от 1 до 48 часов). Новый срок жизни применяется к новым записям, добавляемым в LDAP-кэш после того, как администратор его установит
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. При наличии поддоменов, в которых может происходить авторизация пользователей, на вкладке **Домены LDAP** необходимо указывать все варианты таких поддоменов. Здесь же можно указать короткое netbios имя домена. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Подробнее о настройке Captive-портала — в разделе «Настройка Captive-портала»
Пути поиска	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`
Kerberos keytab	Здесь можно загрузить keytab-файл для аутентификации Kerberos. Подробнее об аутентификации Kerberos и создании keytab-файла — в разделе «Метод аутентификации Kerberos»

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

> **Примечание**
> **Для аутентификации 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. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

Для добавления пользователя или группы пользователей LDAP в правила фильтрации нажмите **Добавить пользователя LDAP/Добавить группу LDAP**, в поле поиска укажите как минимум один символ, входящий в имена искомых объектов, после чего нажмите **Поиск** и выберите желаемые группы или пользователей.

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть UserGate SWG выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate SWG 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 UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 аутентификацию).

Для создания сервера аутентификации RADIUS в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберитеь **Добавить RADIUS-сервер** и укажите параметры сервера.

Параметр	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

Параметр	Описание
Порт	UDP-порт, на котором сервер RADIUS слушает запросы на аутентификацию. По умолчанию это порт UDP 1812

После создания сервера аутентификации настройте Captive-портал для использования метода RADIUS. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При аутентификации через TACACS+ UserGate SWG 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 UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 аутентификацию).

Для создания сервера аутентификации TACACS+ в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить TACACS+-сервер** и укажите параметры сервера.

Параметр	Описание
Включен	Включает или отключает использование данного сервера аутентификации
Название сервера	Название сервера аутентификации
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации
Адрес	IP-адрес сервера TACACS+
Порт	Порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт TCP 49
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+

Параметр	Описание
	Важно! **Чтобы эта опция работала, необходимо настроить ее также на стороне сервера TACACS+.**
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет аутентифицировать 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 аутентификацию на всех ресурсах, поддерживающих аутентификацию SAML. UserGate SWG может быть настроен в качестве сервис-провайдера SAML, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в UserGate SWG 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 аутентификации с помощью сервера SAML IDP:

1. На контроллере домена создайте DNS-запись, соответствующую UserGate SWG, для использования в качестве домена для `auth.captive`. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

2. Настройте DNS-серверы на UserGate SWG. В параметрах UserGate SWG в качестве системных DNS-серверов укажите IP-адреса контроллеров домена.

3. Измените адрес домена auth captive-портала в разделе **Настройки → UserGate → Настройки** на созданную на предыдущем шаге запись DNS. Подробнее об изменении адреса домена auth Captive-портала — в разделе «Общие настройки».

4. Настройте сервер SAML IDP. Добавьте на сервере SAML IDP запись о сервис-провайдере UserGate SWG, указывая созданное на шаге 1 FQDN-имя.

5. В разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить SAML IDP-сервер** и укажите параметры сервера.

Параметр	Описание
Включен	Включение или отключение использования данного сервера аутентификации
Название сервера	Название сервера аутентификации
Описание	Описание сервера аутентификации
SAML metadata URL	URL на сервере SAML IDP, откуда можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии **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. Возможные 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 (подробнее — в разделе «Управление сертификатами»). • Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе **Настройки → UserGate → Сертификаты**, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP. • Не использовать сертификат
Single sign-on URL	URL, используемый 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. Возможные варианты — POST и Redirect. Смотрите

Параметр	Описание
	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. Возможные 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 аутентификации с помощью NTLM UserGate SWG работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в интернет.

Сервер NTLM не может предоставить список пользователей в UserGate SWG, поэтому, если пользователи не были заведены в UserGate SWG 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 UserGate SWG не отличается от режима работы утентификации.

Для настройки аутентификации с помощью NTLM:

1. Настройте синхронизацию времени с контроллером домена. В настройках UserGate SWG в разделе **Настройки → UserGate → Настройки** включите синхронизацию времени с серверами NTP, в качестве основного и (опционально) запасного NTP-сервера укажите IP-адреса контроллеров домена.

2. На контроллере домена создайте DNS-записи, соответствующие UserGate SWG для использования в качестве домена для `auth.captive` и logout.captive..В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

3. Для домена auth Captive-портала укажите созданную на предыдущем шаге запись DNS. Для домена logout Captive-портала укажите созданную на предыдущем шаге запись DNS. Подробнее об изменении адресов доменов auth Captive-портала и logout Captive-портала — в разделе «Настройка Captive-портала».

4. Добавьте NTLM-сервер. В разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить**, выберите **Добавить NTLM-сервер** и укажите название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена определялось в IP-адреса контроллеров домена.

5. Создайте правило Captive-портала с аутентификацией NTLM. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

6. Разрешите доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM.

7. Для аутентификации в стандартном режиме настройте обязательное использование прокси-сервера на компьютерах пользователей. Укажите IP-адрес интерфейса UserGate SWG 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 UserGate SWG имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.**

8. Для аутентификации в прозрачном режиме настройте 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 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) аутентифицировать пользователей домена Active Directory. При аутентификации через Kerberos UserGate SWG 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 аутентификации с помощью Kerberos:

1. На контроллере домена создайте DNS-записи UserGate SWG для использования в качестве доменов для auth.captive и logout.captive. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

> **Важно!**
> **Для корректной работы создайте записи типа A, не используйте CNAME-записи.**

2. Создайте учетную запись в домене AD и отключите для нее требование смены пароля.

> **Важно!**
> **Не используйте символы национальных алфавитов, например кириллицу, в имени учетной записи или в организационных единицах Active Directory, где вы планируете создать учетную запись.**

Важно!

Не используйте в качестве учетной записи для Kerberos запись, созданную для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.

3. На контроллере домена создайте keytab-файл, выполнив команду вида:

```
ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DO
MAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:
\utm.keytab
```

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 учетной записи в домене, созданное на шаге 2 (имя realm-домена обязательно большими буквами).

4. Настройте DNS-серверы на UserGate SWG. В качестве системных DNS-серверов укажите IP-адреса контроллеров домена.

5. Включите на UserGate SWG в разделе **Настройки → UserGate → Настройки** синхронизацию времени с серверами NTP, в качестве основного и (опционально) запасного NTP-сервера укажите IP-адреса контроллеров домена.

6. Измените адрес домена auth captive-портала и опционально адрес домена logout captive-портала в разделе **Настройки → UserGate → Настройки** на созданные ранее записи DNS. Подробнее об изменении адресов доменов — в разделе «Общие настройки».

7. Создайте сервер аутентификации LDAP и загрузите полученный на предыдущем шаге keytab-файл. Подробнее о настройке LDAP-коннектора — разделе «LDAP-коннектор».

> **Важно!**
> **Не используйте в качестве учетной записи для LDAP-коннектора запись, созданную ранее для работы Kerberos. Необходимо использовать отдельную учетную запись.**

8. Создайте правило Captive-портала для использования метода аутентификации Kerberos. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

9. Откройте доступ к сервису HTTP(S)-прокси в свойствах контроля доступа зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.

10. Для аутентификации в стандартном режиме настройте обязательное использование прокси-сервера на компьютерах пользователей. Укажите FQDN UserGate SWG в качестве адреса прокси-сервера.

11. Для аутентификации в прозрачном режиме настройте 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 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 этот тип аутентификации для пользователей, поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификацию 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 аутентификации с помощью HTTP Basic:

1. На контроллере домена создайте DNS-записи, соответствующие UserGate SWG, для использования в качестве домена для auth.captive и logout.captive. В качестве IP-адреса укажите адрес интерфейса UserGate SWG, принадлежащего зоне Trusted.

2. Измените адрес домена auth Captive-портала и (опционально) адрес домена logout Captive-портала в разделе **Настройки → UserGate → Настройки** на созданные на предыдущем шаге записи DNS. Подробнее об изменении адресов доменов — в разделе «Общие настройки».

3. Создайте правило Captive-портала для использования метода аутентификации HTTP Basic. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

4. Откройте доступ к сервису HTTP(S)-прокси в свойствах контроля доступа зоны, из которой происходит авторизация с помощью HTTP Basic.

5. На устройствах, с которых выполняется авторизация, укажите обязательное использование прокси-сервера. Укажите IP-адрес зоны Trusted интерфейса UserGate SWG в качестве адреса прокси-сервера.

Профили аутентификации

Профиль аутентификации позволяет указать набор способов и параметров аутентификации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах UserGate SWG, например Captive-портал, веб-портал и т. д. Чтобы создать профиль аутентификации, в разделе **Настройки → Пользователи и устройства → Профили аутентификации** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Название	Название профиля
Описание	Описание профиля
Профиль MFA	Профиль многофакторной аутентификации. Должен быть предварительно создан в разделе **Профили MFA**, если планируется использовать многофакторную

Параметр	Описание
	аутентификацию. Профиль определяет способ доставки одноразового пароля для дополнительного метода аутентификации. Подробнее о настройке профилей MFA — в разделе «Профили MFA» **Важно!** **Многофакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только с теми, где пользователь явно вводит свои учетные данные в веб-форму страницы аутентификации. В связи с этим, многофакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.**
Время бездействия до отключения	Этот параметр определяет, через сколько секунд UserGate SWG переведет пользователя из состояния Known users в состояние Unknown users при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя)
Время жизни авторизованного пользователя	Этот параметр определяет, через сколько секунд UserGate SWG переведет пользователя из состояния Known users в состояние Unknown users. По прошествии указанного времени пользователю потребуется повторно аутентифицироваться на Captive-портале
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток аутентификации через Captive-портал до блокировки учетной записи пользователя
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов аутентификации, таких как: • **Локальный пользователь** — аутентификация по базе данных локально заведенных пользователей.

Параметр	Описание
	• **Принять политику** — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Этот тип аутентификации необходимо применять совместно с профилем Captive-портала, в котором используется страница аутентификации Captive portal policy. • **HTTP Basic** — аутентификация с помощью устаревшего метода HTTP Basic. • **Аутентификация Kerberos** — аутентификация по протоколу Kerberos

Настройка Captive-портала

Captive-портал позволяет аутентифицировать неизвестных пользователей с помощью методов аутентификации 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 пользователи, у которых в свойствах явно указан IP-адрес, или пользователи, идентифицированные с помощью агентов авторизации терминальных серверов, не аутентифицируются на Captive-портале. Такие пользователи уже относятся к типу Known users и не требуют дополнительной идентификации.

- Аутентификация с помощью Captive-портала возможна только для протокола HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователей 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 аутентификацию на Captive-портале.

- Необходимо настроить инспектирование SSL, иначе аутентификация по протоколу HTTPS работать не будет.

- Если Captive-портал использует метод аутентификации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Для настройки Captive-портала:

1. Создайте метод аутентификации, например аутентификацию с помощью домена Active Directory. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** нажмите **Добавить** и создайте сервер аутентификации.

2. Создайте профиль аутентификации, в котором укажите необходимые методы аутентификации. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Профили аутентификации** нажмите **Добавить** и создайте профиль аутентификации, используя созданный ранее метод аутентификации.

3. Создайте Captive-профиль, в котором укажите необходимые профили аутентификации. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Captive-профили** нажмите нажмите **Добавить** и создайте Captive-профиль, используя созданный ранее профиль аутентификации.

4. Создайте правило Captive-портала. Правило Captive-портала определяет трафик, к которому должны быть применены методы аутентификации пользователей, указанные в Captive-профиле. В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Captive-портал** нажмите **Добавить** и создайте правило Captive-портала.

5. Настройте DNS для доменов auth.captive и logout.captive. Служебные доменные имена auth.captive и logout.captive используются в UserGate SWG для аутентификации пользователей. Если клиенты не используют UserGate SWG в качестве DNS-сервера необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса UserGate SWG, который подключен в клиентскую сеть. Альтернативное решение — настроить параметры «Домен auth captive-портала» и «Домен logout captive-портала». Подробнее об этих параметрах — в разделе «Общие настройки».

При создании Captive-профиля укажите следующие параметры.

Параметр	Описание
Название	Название Captive-профиля
Описание	Описание Captive-профиля

Параметр	Описание
Шаблон страницы авторизации	Выбор шаблона страницы аутентификации. Создавать страницы аутентификации можно в разделе **Настройки → Библиотеки → Шаблоны страниц**. Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth)
Метод идентификации	Метод, с помощью которого UserGate SWG сохраняет данные о пользователе. Возможные варианты: • **Запоминать IP-адрес**. После успешной аутентификации пользователя через Captive-портал UserGate SWG запоминает IP-адрес пользователя. Все последующие соединения с этого IP-адреса будут относятся к данному пользователю. Такой метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и UserGate SWG. Это рекомендуемое значение параметра, устанавливаемое по умолчанию. • **Запоминать cookie**. После успешной аутентификации пользователя через Captive-портал UserGate SWG добавляет в браузер пользователя cookie, с помощью которых идентифицирует последующие соединения данного пользователя. Такой метод позволяет аутентифицировать пользователей, находящихся за NAT-устройством, но аутентифицируется только протокол HTTP(S) и только в том браузере, в котором происходила аутентификация через Captive-портал. Кроме этого, для аутентификации HTTPS-сессий пользователя UserGate SWG 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 аутентификации, определяющий методы аутентификации
Режим аутентификации	Аутентификация с помощью логина и пароля через RADIUS сервер (AAA) или посредством сертификатов (PKI)
Профиль сертификата пользователя	При выборе режима аутентификации посредством сертификатов необходимо указать сконфигурированный ранее профиль пользовательских сертификатов

Параметр	Описание
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной аутентификации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL
Разрешить браузерам запомнить авторизацию	Разрешение сохранять аутентификацию в браузере на указанное время в часах. Для сохранения аутентификационной информации используются cookie
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется аутентификация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице аутентификации. Если этот параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain
Показывать CAPTCHA	При включении этой опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке **Регистрация гостевых пользователей**. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Параметр	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться два типа профилей — SMS и email. Подробнее о создания профилей оповещения — в разделе «Профили оповещений»
От	Указать, от имени кого будут отправляться оповещения
Тема оповещения	Тема оповещения (только для email-оповещений)
Письмо оповещения	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль
Дата и время окончания	Время, когда учетная запись временного пользователя будет отключена

Параметр	Описание
Время жизни	Продолжительность времени с момента первой аутентификации временного пользователя, по истечении которого его учетная запись будет отключена
Длина пароля	Длина пароля для создаваемого пользователя
Сложность пароля	Сложность пароля для создаваемого пользователя. Возможные варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи

При создании правила Captive-портала укажите следующие параметры.

Параметр	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 этой опции информация о срабатывании правила будет регистрироваться в соответствующем журнале статистики
Источник	Адреса источника. В качестве источника можно указать определенную зону, например зону LAN и диапазон адресов IP. Могут быть использованы GeoIP **Важно!** **Существует ограничение на количество GeoIP, которое может быть указано: не более 15.**

Параметр	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	Адреса назначения. В качестве адресов можно указать определенную зону, например зону WAN и диапазон адресов IP. Могут быть использованы 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 правило будет активно

Параметр	Описание
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, отметьте правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

> **Примечание**
> **Условия, указанные на вкладках правила, применяются согласно логике “И”, то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику “ИЛИ”, необходимо создать несколько правил.**

> **Примечание**
> **Правила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил, нажав соответствующие значки в консоли.**

> **Примечание**
> **При обработке правил применяется только первое сработавшее правило.**

В случае, если необходимо сменить пользователя после его аутентификации в системе или выйти из системы, необходимо перейти на URL http://logout.captive и нажать **Выйти**.

Пользователи терминальных серверов

Терминальный сервер служит для удаленного обслуживания пользователей 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

аутентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и UserGate SWG не может корректно идентифицировать сетевые подключения пользователей. Для решения этой 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 SWG 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 протоколов TCP и UDP. Протоколы, отличные от TCP и UDP, например ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей, в случае использования на терминальных серверах аутентификации Active Directory, требуется настроенный сервер аутентификации LDAP-коннектор.

Чтобы начать работу с аутентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

1. Разрешите сервис **Агент аутентификации** в свойствах контроля доступа зоны, со стороны которой расположены серверы терминального доступа.

2. Установите пароль агентов терминального сервера. В веб-консоли UserGate SWG в разделе **Настройки → UserGate → Настройки → Модули** нажмите **Настроить** напротив строки **Пароль агентов терминального сервиса** и установите пароль агентов терминального сервера.

3. Установите агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке укажите адрес UserGate SWG и установленный на предыдущем шаге пароль.

4. В веб-консоли UserGate SWG. в разделе **Настройки → Пользователи и устройства → Терминальные серверы** добавьтеь агентов терминального сервера, указав имя и адрес узла. После получения данных с указанного в настройках узла и совпадении пароля, указанного на шаге 2, аутентификация пользователей будет включена автоматически. При обновлении версии ПО UserGate SWG агенты терминальных серверов, которые ранее отображались в веб-консоли, будут продолжать работать.

UserGate теперь будет получать информацию о пользователях.

Агент терминального сервера позволяет аутентифицировать не только доменных, но и локальных пользователей терминального сервера. Для этого необходимо добавить в файл конфигурации (`%ALLUSERSPROFILE%\Entensys\Terminal Server Agent\tsagent.cfg`) следующий параметр:

```
LocalDomain = 1
```

При включении этого параметра информация о пользователях будет передаваться на UserGate SWG в формате «`имя сервера_имя пользователя`» для локальных пользователей или «`имя домена_имя пользователя`» для доменных.

Таких пользователей также необходимо добавить в UserGate SWG как локальных. О добавлении пользователей — в разделе «Пользователи». При добавлении необходимо указать логин в приведенном выше формате; пароль указывать не нужно.

Эта опция предназначена, в основном, для терминальных серверов, не включенных в домен, вход на который осуществляется с локальными учетными данными.

После изменения файла конфигурации сервис терминального агента нужно перезапустить.

> **Примечание**
> **Имя компьютера должно состоять из букв, цифр и знака подчеркивания. Использование тире в имени компьютера возможно только в том случае, если используются только доменные пользователи.**

Параметры терминального сервера могут быть изменены путем внесения изменений в файл конфигурации агента аутентификации для терминальных серверов. После внесения изменений агент аутентификации необходимо перезапустить.

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 учетных записей (system, local service, network service) и портах, используемых для соединения, на UserGate SWG.
- `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 UserGate SWG, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- `ServerAddress`: адрес устройства UserGate, принимающего соединение от агента аутентификации. Начиная с версии агента 6.2.0.49 поддерживается возможность работы с несколькими UserGate SWG одновременно. Строка `ServerAddress` может содержать несколько элементов, разделенных символом "`;`". Это могут быть как IP-адреса, так и FQDN (например, `ServerAddress=testtermserver.net; 15.0.0.203`).Все адреса определяются в момент старта и в момент изменений в настройках сетевых адаптеров. Рассылки о пользователях дублируются на все адреса.
- `UserCount`: максимальное количество пользователей.
- `BlockDNS`: может принимать значения `0` или `1`. При `BlockDNS=1` происходит замена порта источника на свободный порт из выделенного для пользователя диапазона при DNS запросе (UDP:53); при `BlockDNS=0` — отправка трафика происходит без замены порта.
- `BlockUDP`: может принимать значения `0` или `1`. Значение параметра `BlockUDP=1` соответствует замене порта источника на свободный порт из выделенного для пользователя диапазона при отправке трафика UDP; при `BlockUDP=0` — отправка трафика происходит без замены порта.
- `ExcludeIP`: в случае, если на терминальном сервере настроены несколько IP-адресов, то все они будут использованы для аутентификации пользователей. Параметр `ExcludeIP` позволяет ограничить аутентификацию пользователей с определенных 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

Многофакторная аутентификация (MFA) — это метод идентификации и аутентификации пользователя, где используются два или более различных типа идентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

UserGate SWG поддерживает многофакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации, одноразового токена или пароля — в качестве второго. Доступны следующие методы получение одноразовых токенов или паролей:

- **TOTP** (Time-based One Time Password) — получение одноразового токена. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром. В качестве TOTP-токена могут выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например Google Authenticator.
- **SMS** — получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в UserGate SWG 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 SWG или в доменной учетной записи в Active Directory.

Чтобы настроить многофакторную аутентификацию:

1. Настройте аутентификацию с помощью Captive-портала. Многофакторная аутентификация работает только при аутентификации пользователей с помощью Captive-портала. Подробнее о Captive-портале — в разделе «Настройка Captive-портала».

2. Создайте профиль многофакторной аутентификации. В веб-консоли UserGate SWG перейдите в раздел **Настройки → Пользователи и устройства → Профили MFA** создайте профиль многофакторной аутентификации. При создании

профиля укажите метод доставки второго фактора аутентификации. Доступны три метода доставки:

- **MFA через TOTP** — доставка второго фактора аутентификации с помощью токенов TOTP.
- **MFA через SMS** — доставка второго фактора аутентификации с помощью SMS.
- **MFA через email** — доставка второго фактора аутентификации с помощью email.

Параметры для настройки метода **MFA через TOTP**.

Параметр	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 аутентификации. Для этого варианта выберите **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 UserGate SWG или в доменной учетной записи в Active Directory. Для этого варианта выберите 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 UserGate SWG или в доменной учетной записи в Active Directory. Для этого варианта выберите 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 пользователя в списке (**Настройка → Пользователи и устройства → Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей аутентификации пользователю будет предложено заново инициализировать свой токен.

Параметры для настройки метода **MFA через SMS**.

Параметр	Описание
Название	Название профиля MFA
Описание	Описание профиля MFA
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробнее о настройке профилей отсылки сообщений через SMS — в разделе «Профили оповещений»
От	Указать автора отправки сообщения
Содержимое	Тело сообщения. В сообщении можно использовать специальную переменную `{2fa_auth_code}`, которая будут заменена на одноразовый пароль
Время жизни MFA кода	Срок действия одноразового пароля

Параметры для настройки метода **MFA через email**.

Параметр	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. Подробнее о настройке профилей отсылки сообщений по электронной почте — в разделе «Профили оповещений»
От	Указать автора сообщения
Тема	Тема сообщения
Содержимое	Тело сообщения. В сообщении можно использовать специальную переменную `{2fa_auth_code}`, которая будут заменена на одноразовый пароль

Параметр	Описание
Время жизни MFA кода	Срок действия одноразового пароля

UserID

UserID — технология прозрачной аутентификации пользователей. Источниками данных для однозначной идентификации пользователей являются журналы безопасности операционных систем доменных контроллеров, данные журналов серверов приложений и доступа, в которых пользователи уже аутентифицированы.

Чтобы создавать политики, включающие пользователей и группы, межсетевому экрану необходимо сопоставить IP-адреса с пользователями, получившими эти адреса и извлечь информацию о группах, в которые они входят. UserID предоставляет несколько методов, позволяющих выполнить такое сопоставление. Например, для получения информации о пользователях UserID может просматривать журналы на серверах в поисках сообщений от служб аутентификации. Те пользователи, чьи имена не удалось сопоставить с IP-адресами, могут быть перенаправлены на специальный портал (Captive Portal) для прохождения аутентификации. Для получения информации о группах межсетевой экран подключается напрямую к серверам LDAP.

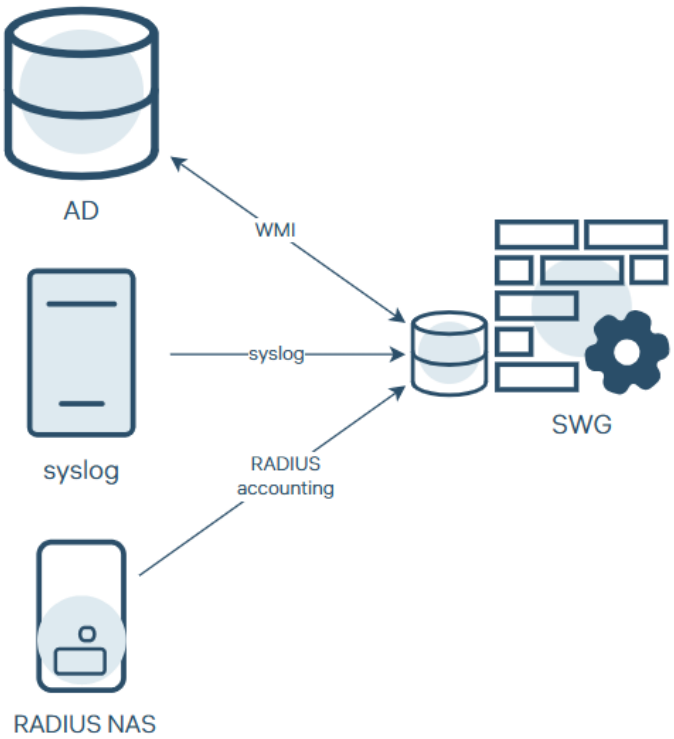
В качестве источников данных для аутентификации в UserID используются журналы Microsoft Active Directory, данные, полученные по syslog или сообщения RADIUS accounting.

Для конечных пользователей работа UserID полностью прозрачна, то есть пользователям нет необходимости в явном виде проходить аутентификацию на UserGate SWG.

Принцип работы UserID

В зависимости от сценария использования и настройки UserID-агент получает данные о событиях, связанных с аутентификацией пользователей, одним из следующих способов:

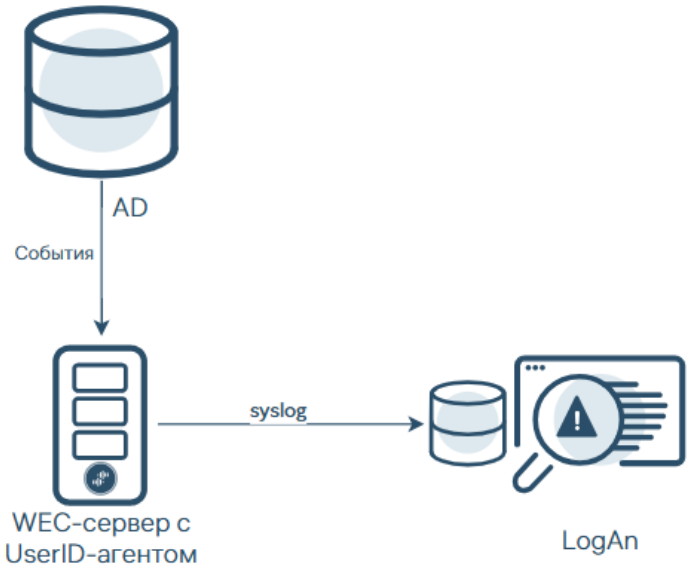
- Непосредственное получение данных узлом с UserID-агентом от источников данных аутентификации с помощью настроенных коннекторов:
  - UserID-агент может подключаться к контроллеру домена AD с помощью технологии WMI и считывать журналы событий безопасности;
  - UserID-агент может принимать со сторонних серверов сообщения по протоколу syslog;
  - UserID-агент может принимать со сторонних RADIUS NAS-серверов сообщения RADIUS accounting.



- Получение данных через посредника — специального программного агента, который устанавливается на контроллер домена или сервер-сборщик событий (WEC).

  Программный агент UserID для AD- и WEC-серверов устанавливается на контроллер домена (AD) или сервер-сборщик событий домена (WEC), считывает необходимую для идентификации пользователя информацию из

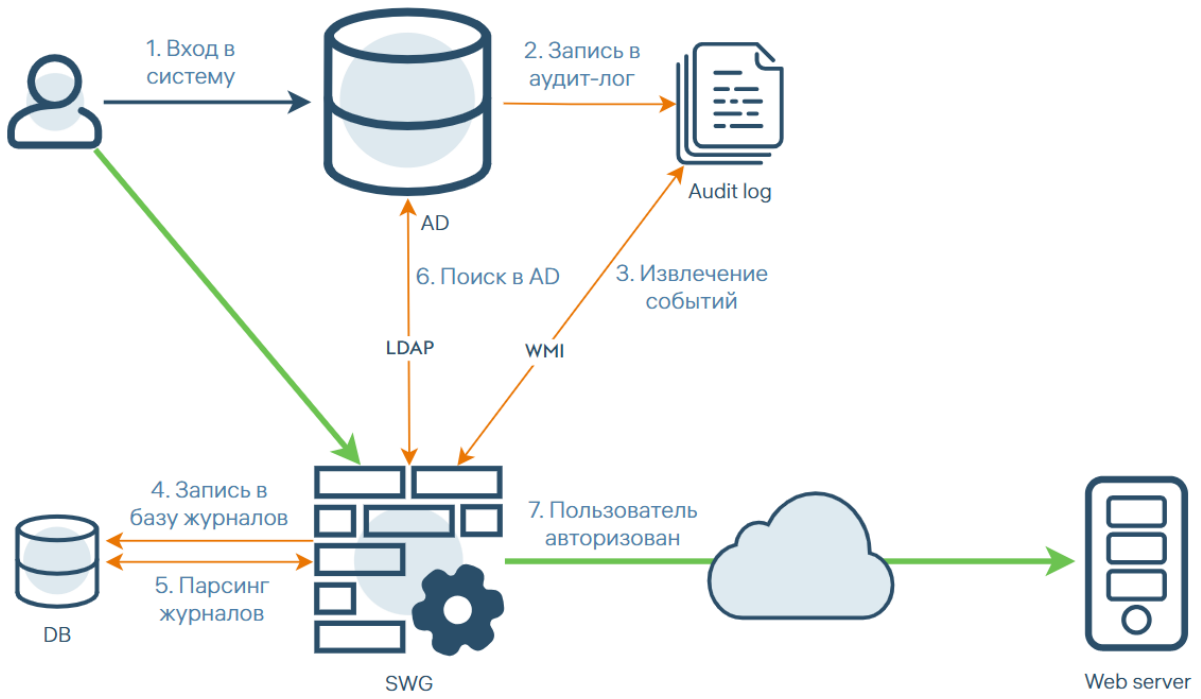
журналов безопасности Windows и пересылает ее в формате syslog на коллектор UserID на UserGate Log Analyzer или UserGate SWG (подробнее об агенте — в разделе «UserID-агент для AD/WEC»).



Главные достоинства такого способа получения данных из домена AD:

- Не требуется предоставлять доступ извне в контроллер домена для сбора данных об аутентификации пользователей, как это требуется при доступе по технологии WMI.
- Не требуется создавать в домене специальную учетную запись с особыми привилегиями для узлов, на которых работает UserID-агент.

Рассмотрим принцип работы технологии UserID на примере сценария взаимодействия с Active Directory в качестве источника данных для аутентификации пользователей через технологию WMI.



На контроллере домена AD работает аудит событий безопасности, который записывает события по настроенным категориям в специальный журнал аудита.

После создания и настройки UserID-агента и коннектора Microsoft Active Directory на UserGate SWG, UserID-агент начинает периодически отправлять на контроллер AD WMI-запросы для извлечения следующих событий по Event ID из журнала аудита:

- 4624 — успешный вход в систему;
- 4768 — запрос билета аутентификации Kerberos TGT;
- 4769 — запрос билета аутентификации Kerberos TGS;
- 4770 — обновление билета аутентификации Kerberos TGS;
- 4627 — сведения о членстве в группах.

Данные события позволяют UserID-агенту получать информацию о регистрации пользователей и членстве в группах. Полученная информация записывается в специальную системную базу данных на UserGate SWG.

Информация из Microsoft AD о выходе пользователя из системы в настоящий момент не обрабатывается.

UserID-агент периодически обращается к этой базе данных, извлекает из записей имя пользователя, домен, SID, IP-адрес, список групп пользователя. Эти данные кешируются. Интервал поиска записей в базе данных можно задать в

настройках UserID-агента. Время жизни данных о пользователе в кеш-памяти устанавливается в настройках коннектора UserID-агента на UserGate SWG.

В случае, если список групп, в которые входит пользователь, не был получен, UserID-агент обращается к контроллеру домена по протоколу LDAP в соответствии с настроенным профилем аутентификации для получения информации о группах.

При обработке сетевого трафика, в том случае, если в правилах настроены условия для определенных пользователей и групп, UserGate SWG обращается к кеш-памяти для поиска информации о том, какие пользователи зарегистрированы с какими IP-адресами. Эта информация используется для принятия решения о том, как будут обрабатываться пакеты.

Завершение сессий пользователей может принудительно инициироваться администратором UserGate SWG. Для этого администратор может выполнить сброс всех пользователей или сброс отдельного пользователя:

- В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → Серверы аутентификации** на панели инструментов нажмите на панели инструментов нажмите **Сбросить аутентификацию всех пользователей**.
- В консоли CLI — выполните команду:

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

В сценарии с использованием серверов-источников данных syslog в качестве источника данных аутентификации пользователей принцип работы аналогичен, только UserGate SWG в этом случае выступает в роли syslog listener — принимает сообщения от отправителя syslog. Номер порта и протокол устанавливаются в настройках UserID-агента, по умолчанию — порт TCP 514. Нужные события фильтруются в потоке принятых данных с помощью настроенных фильтров из библиотеки Syslog фильтры UserID-агента. В этом случае в базу данных сохраняются: имя пользователя, IP-адрес, SID (опционально). Для получения информации о группах, в которых зарегистрирован пользователь, UserID-агент обращается к контроллеру домена по LDAP-протоколу в соответствии с настроенным профилем аутентификации UserID-агента.

В сценарии с использованием сообщений RADIUS accounting в качестве источника данных аутентификации пользователей принцип работы в целом схож. UserGate SWG выступает в роли пропускного RADIUS-сервера

— принимает сообщения RADIUS accounting от серверов NAS (по порту UDP 1813) и проверяет пользователя на контроллере домена AD по LDAP в соответствии с настроенным профилем аутентификации UserID-агента.

Настройка UserID-агента на UserGate SWG не является кластерной, а значит ее нужно производить на каждом узле отдельно. После настройки UserID-агент будет работать самостоятельно и самостоятельно получать данные о событиях логин\логаут из журналов источников.

Помимо UserGate SWG UserID может работать на устройствах UserGate Log Analyzer. Подробнее о работе UserID на Log Analyzer читайте в руководстве администратора UserGate Log Analyzer. Использование UserGate Log Analyzer позволяет масштабировать технологию UserID на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer аналогичен принципу работы на UserGate SWG. Найденные в собранных данных события отправляются на другие узлы UserGate SWG в соответствии с политикой UserID Sharing, настроенной с помощью профилей редистрибуции. При необходимости можно отправлять разные данные на разные узлы UserGate SWG. На SWG отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate SWG в сети.

Примечание

В инфраструктурах с серверами Active Directory и высоким потоком событий аутентификации (свыше 50 событий в секунду) для корректной работы функции UserID рекомендуется применять сценарий сбора событий через AD/WEC-агент вместо сценария с технологией WMI. Это связано с ограниченной производительностью технологии WMI, которая может вызывать ошибки при получении данных и приводить к некорректной работе правил фильтрации.

Алгоритм настройки UserID

Для настройки работы UserID необходимо выполнить ряд действий как на стороне источников данных аутентификации, так и на UserGate SWG.

Настройка на стороне источников данных:

- При работе с Active Directory в качестве источника данных об аутентификации пользователей включите аудит событий безопасности. Потребуются следующие категории:
  - Audit LogOn;
  - Audit LogOff;
  - Audit Kerberos Authentication Service;
  - Audit Group Membership;
  - Audit Kerberos Service Ticket Operations.
- При работе с серверами-источниками данных syslog настройте отправку журналов на адрес UserID-агента (то есть на IP-адрес UserGate SWG; номер порта и протокол устанавливаются в настройках UserID-агента, по умолчанию порт TCP 514).
- При работе с серверами RADIUS NAS настройте отправку сообщений RADIUS accounting на адрес UserID-агента (то есть на IP-адрес UserGate SWG, порт UDP 1813).

Настройка на стороне UserGate SWG:

- Создайте сервер аутентификации для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе «Серверы аутентификации».
- Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе «Профили аутентификации».
- Для сценария с серверами-источниками данных syslog активируйте сервис **UserID syslog collector** в параметрах контроля доступа зоны, где будет находиться отправитель syslog. Для сценария с RADIUS NAS-серверами активируйте сервис **Агент аутентификации** в настройках контроля доступа зон, где будет находиться серверы RADIUS NAS. Подробнее о создании и настройке зон — в разделе «Настройка зон».
- Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.
- Настройте общие параметры UserID-агента.

Создание коннектора UserID-агента

Коннектор UserID-агента в веб-консоли UserGate SWG создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмитеь **Добавить** на панели инструментов и выберите тип создаваемого коннектора:

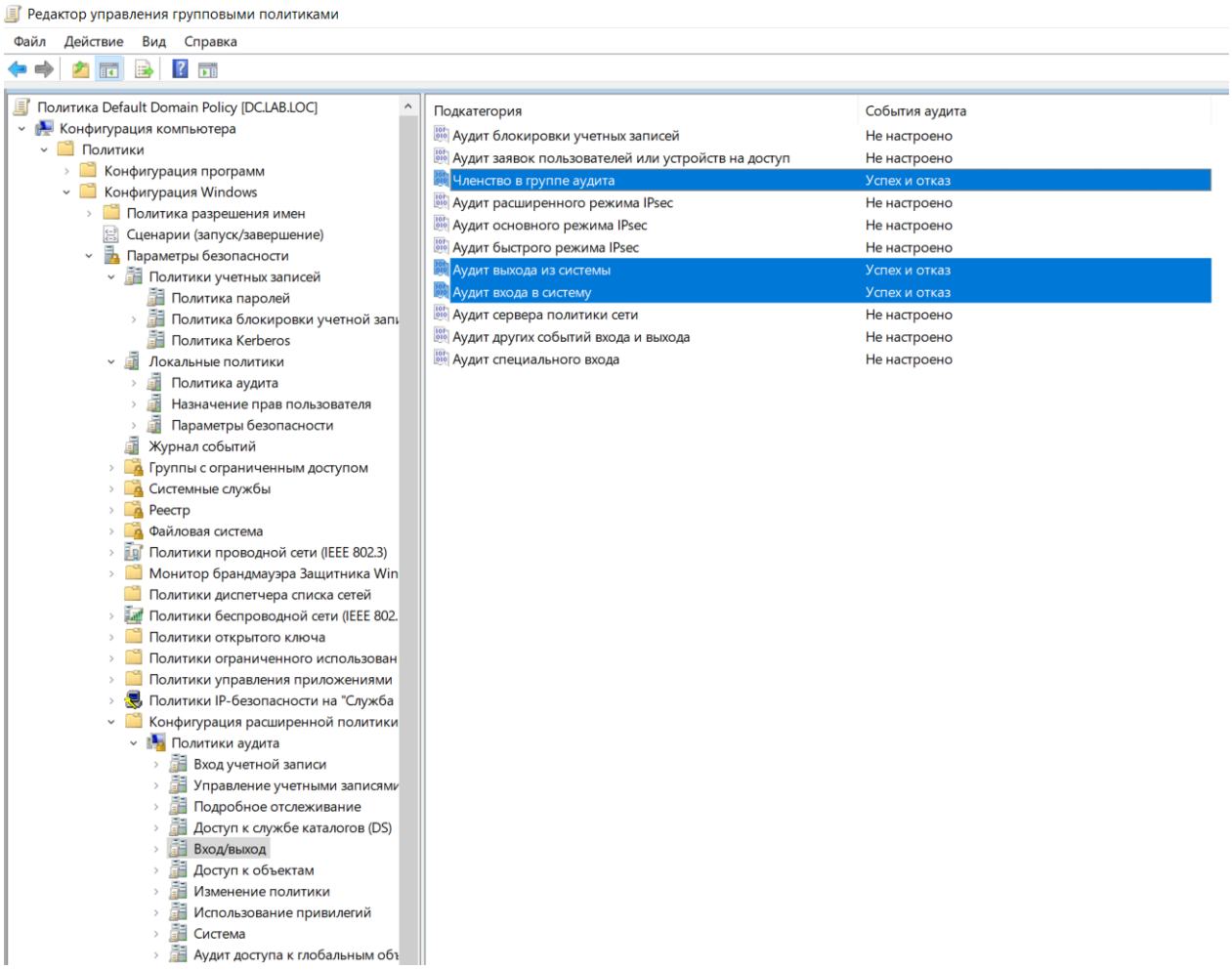
- Microsoft Active Directory;
- Отправитель syslog;
- RADIUS-сервер.

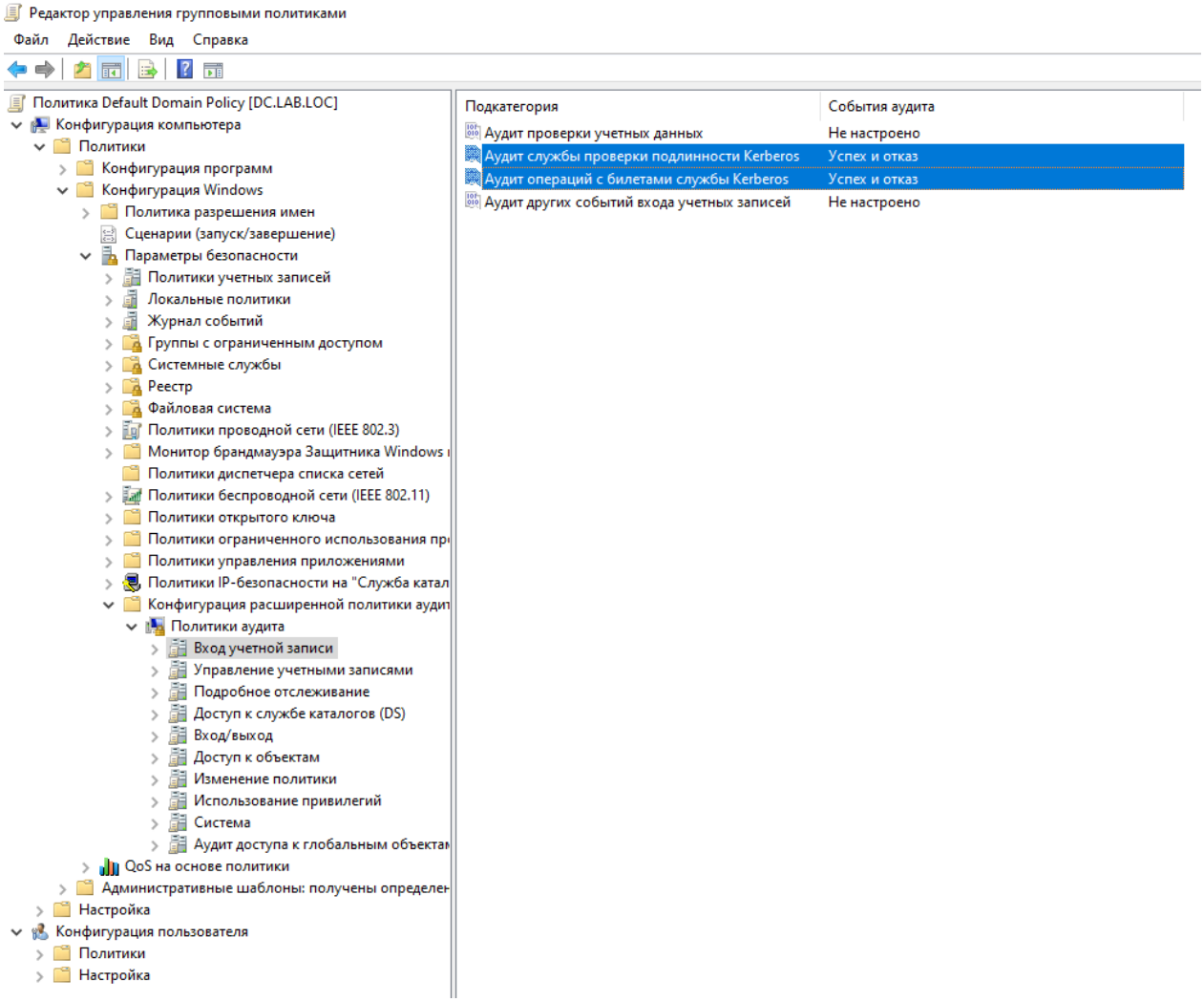
Microsoft Active Directory

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

1. Настройте источник событий.
2. Настройте параметры коннектора UserID-агента для мониторинга AD.

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


Редактор управления групповыми политиками
Файл Действие Вид Справка
Политика Default Domain Policy [DC.LAB.LOC]
Конфигурация компьютера
Политики
Конфигурация программ
Конфигурация Windows
Политика разрешения имен
Сценарии (запуск/завершение)
Параметры безопасности
Политики учетных записей
Политика паролей
Политика блокировки учетной запи
Политика Kerberos
Локальные политики
Политика аудита
Назначение прав пользователя
Параметры безопасности
Журнал событий
Группы с ограниченным доступом
Системные службы
Реестр
Файловая система
Политики проводной сети (IEEE 802.3)
Монитор брандмауэра Защитника Win
Политики диспетчера списка сетей
Политики беспроводной сети (IEEE 802.
Политики открытого ключа
Политики ограниченного использован
Политики управления приложениями
Политики IP-безопасности на "Служба
Конфигурация расширенной политики
Политики аудита
Вход учетной записи
Управление учетными записями
Подробное отслеживание
Доступ к службе каталогов (DS)
Вход/выход
Доступ к объектам
Изменение политики
Использование привилегий
Система
Аудит доступа к глобальным об
Подкатегория
События аудита
Аудит блокировки учетных записей
Не настроено
Аудит заявок пользователей или устройств на доступ
Не настроено
Членство в группе аудита
Успех и отказ
Аудит расширенного режима IPsec
Не настроено
Аудит основного режима IPsec
Не настроено
Аудит быстрого режима IPsec
Не настроено
Аудит выхода из системы
Успех и отказ
Аудит входа в систему
Успех и отказ
Аудит сервера политики сети
Не настроено
Аудит других событий входа и выхода
Не настроено
Аудит специального входа
Не настроено



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

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

1. Создайте учетную запись пользователя на контроллере домена:
   - Перейдите в меню **Пуск → Диспетчер серверов → Средства → Active Directory — пользователи и компьютеры**.
   - В соответствующем Подразделении (OU) создайте **Нового пользователя** для UserID.

2. Настройте членство в группах для новой учетной записи пользователя:
   - Нажмите правой кнопкой мыши на новой учетной записи пользователя UserID и выберите **Свойства**.
   - Перейдите на вкладку **Членство в группах**.
   - Нажмите **Добавить → Дополнительно → Поиск**.
   - Выберите следующие группы:
     - **Пользователи DCOM**;
     - **Пользователи журналов производительности**;
     - **Пользователи удаленного рабочего стола**;
     - **Читатели журнала событий**.
   - Нажмите **OK**.
3. Назначьте права Distributed Component Object Model (DCOM):
   - Перейдите в меню Windows **Пуск → Администрирование → Службы компонентов**. Откроется окно **Службы компонентов**.
   - Раскройте **Службы компонентов → Компьютеры → Мой компьютер**.
   - Нажмите правой кнопкой мыши на **Мой компьютер** и выберите **Свойства**. Откроется окно **Свойства: Мой компьютер**.
   - Перейдите на вкладку **Безопасность COM**.
   - В области **Права доступа** нажмите **Изменить ограничения.**
   - Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный доступ** и **Удаленный доступ**.
   - Нажмите **OK**, чтобы сохранить параметры.
   - В окне **Свойства: Мой компьютер** нажмите в разделе **Разрешения на запуск и активацию** на **Изменить ограничения.**
   - Убедитесь, что для **Пользователи DCOM** выбрано: **Локальный запуск**, **Удаленный запуск**, **Локальная активация** и **Удаленная активация**.

- Нажмите **OK**, чтобы сохранить настройки; еще раз нажмите **OK**, чтобы закрыть окно **Свойства: Мой компьютер**.
- Выберите **Файл → Выход**, чтобы закрыть окно **Службы компонентов**.

4. Настройте назначения защиты пространства имен WMI:

- Перейдите в меню **Пуск → Выполнить**.
- Введите `wmimgmt.msc` и нажмите **OK**.
- Нажмите правой кнопкой мыши на **Элемент управления WMI (локальный)** и выберите **Свойства**.
- Перейдите на вкладку **Безопасность**.
- Нажмите **Безопасность → Добавить → Дополнительно → Поиск**.
- Выберите новую учетную запись пользователя, нажмите **OK**, пока вы не вернетесь в окно **Безопасность** для Root.
- Нажмите **Дополнительно** и выберите добавленную учетную запись пользователя.
- Нажмите **Изменить**.
- В меню **Применяется к:** выберите **Данное пространство и подпространство имен**.
- Убедитесь, что выбрано **Выполнение методов**, **Включить учетную запись**, **Включить удаленно** и **Прочесть безопасность**.
- Нажмите **OK,** пока вы не вернетесь в окно `wmimgmt`.
- Выберите **Файл → Выход**, чтобы закрыть окно `wmimgmt`.

Внимание!

Обновление Windows KB5014692 может привести к появлению ошибок доступа к WMI типа: *NTSTATUS: NT_STATUS_ACCESS_DENIED.* В этом случае можно попробовать добавить в реестр Windows следующую информацию:

```
Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat

Value Name: "RequireIntegrityActivationAuthenticationLevel"

Type: dword

Value Data: 0x00000000
```

При использовании серверов AD в качестве источников событий UserID-агент выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627).

В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **Microsoft Active Directory**. Укажите следующие параметры:

- **Включено** — включение и отключение получения журналов с источника.
- **Название** — название источника.
- **Описание** — описание источника (опционально).
- **Адрес сервера** — адрес сервера Microsoft Active Directory.
- **Протокол** — протокол доступа к AD (WMI).
- **Пользователь** — имя пользователя для подключения к AD.
- **Пароль** — пароль пользователя для подключения к AD.
- **Профиль аутентификации** — название созданного ранее профиля аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.

- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate SWG. Значение по умолчанию – 2700 секунд (45 минут).

Syslog

В случае, если в качестве источника информации выступает отправитель syslog:

1. Настройте источник событий.

Для корректной работы коннектора UserID-агента syslog, настройте сервер-источник данных syslog для отправки журналов на адрес UserID-агента. Подробнее см. документацию на отправитель syslog.

Параметры сервера syslog на UserGate SWG можно посмотреть или изменить в общих параметрах UserID-агента.

2. Разрешите сбор информации с удаленных устройств по протоколу syslog.

В параметрах контроля доступа зоны, в которой находится отправитель syslog, разрешите сервис **UserID syslog коллектор**.

3. Настройте параметры коннектора UserID-агента для отправителя syslog.

В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора **Отправитель syslog**. Далее укажите следующие данные:

- **Включено** — включение или отключение получения журналов с источника.
- **Название** — название источника.
- **Описание** — описание источника (опционально).
- **Адрес сервера** — адрес хоста, с которого UserGate SWG будет получать события по протоколу syslog.
- **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
- **Часовой пояс** — часовой пояс, установленный на источнике. При использовании UserID-агента для AD/WEC в syslog-коннекторе всегда

должно быть время в UTC независимо от настроек времени на контроллере домена.

- **Профиль аутентификации** — профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах syslog.
- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеша на UserGate SWG. Значение по умолчанию: 2700 секунд (45 минут).

На вкладке **Фильтры** выбираются фильтры для поиска необходимых записей журнала.

Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «Syslog фильтры UserID-агента».

RADIUS accounting

В случае, если источником информации выступают сообщения RADIUS accounting:

1. Настройте источник событий.

Для корректной работы коннектора UserID-агента, настройте NAS-сервер для отправки сообщений RADIUS accounting на адрес UserID-агента (порт UDP 1813). Подробнее см. документацию на NAS-сервер.

2. Разрешите получение запросов RADIUS accounting от удаленных устройств.

В параметрах контроля доступа зон, в которых находятся NAS-серверы, разрешите сервис **Агент аутентификации**.

3. Настройте параметры коннектора UserID-агента для RADIUS-сервера.

В веб-консоли UserGate SWG в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы** нажмите **Добавить** и выберите тип создаваемого коннектора: **RADIUS-сервер**. Укажите следующие данные:

- **Включено** — включение и отключение получения журналов с источника.
- **Название** — название источника.

- **Описание** — описание источника (опционально).
- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти. Значение по умолчанию – 2700 секунд (45 минут).
- **Профиль аутентификации** — профиль аутентификации, с использованием которого происходит поиск пользователя, найденного в журналах RADIUS accounting.
- **Атрибут для имени** — номер radius attribute type, в котором находится имя пользователя. Значение по умолчанию: 1.
- **Атрибут для групп** — номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
- **Домен по умолчанию** — имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
- **Секретный код** — общий ключ, используемый протоколом RADIUS для аутентификации.

На вкладке **Адреса** указываются адреса хостов (NAS-серверов), с которых UserID-агент будет получать события RADIUS accounting:

Настройка UserID-агента

Настройка общих параметров UserID-агента производится в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**. Нажмите **Редактировать** на панели инструментов.

На вкладке **Общие** настраиваются интервалы опроса дынных:

- **Интервал опроса WMI** — период опроса серверов Active Directory. Значение по умолчанию: 120 секунд.
- **Интервал опроса syslog** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей syslog-источников. Значение по умолчанию: 60 секунд.
- **Интервал опроса RADIUS** — период опроса базы данных для поиска событий начала и завершения сеанса пользователей по RADIUS-журналу. Значение по умолчанию: 120 секунд.

На вкладке **Протоколы syslog** настраиваются параметры соединения с сервером syslog.

Для протокола TCP:

- **Включено** — включение и отключение протокола TCP для приема журналов syslog.
- **Порт** — номер порта, используемого для сбора syslog-событий. По умолчанию: порт 514.
- **Максимальное количество сессий** — максимальное количество устройств, подключенных одновременно с целью отправки сообщений.
- **Безопасное соединение** — включение и отключение шифрования потока данных.
- **Файл сертификата УЦ** — сертификат удостоверяющего центра, который используется для установления безопасного соединения.
- **Файл сертификата** — сертификат, созданный пользователем и подписанный удостоверяющим центром.

Для протокола UDP:

- **Включено** — включение и отключение протокола UDP для приема журналов syslog.
- **Порт** — номер порта, используемого для сбора syslog-событий. По умолчанию: порт 514.

На вкладке **Списки Ignore server** указываются списки IP-адресов, события от которых будут проигнорированы UserID-агентом. Запись об игнорировании источника появится в журнале UserID:

Список может быть создан в разделе **Библиотеки → IP-адреса**, или при настройке UserID-агента (нажмите **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов — в разделе «IP-адреса».

Этот параметр является глобальным и относится ко всем источникам.

На вкладке **Списки Ignore user** указываются имена пользователей, события от которых будут проигнорированы UserID-агентом. Поиск производится по Common Name (CN) пользователя AD.

Этот параметр является глобальным и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.

> **Важно!**
> **При задании имени допустимо использовать символ астериск (*) только в конце строки.**

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

Журналирование

UserID-агент периодически обращается к настроенным источникам данных. Полученные события сохраняются в служебной базе данных без каких-либо изменений. Содержимое этой базы можно посмотреть в соответствующих журналах:

- Журнал Windows AD коннектора;
- Syslog коннектор;
- RADIUS коннектор.

В веб-консоли UserGate SWG журналы доступны в разделе **Журналы и отчеты → Журналы → Агент UserID**:

UserID-агент периодически обращается к служебной базе данных и извлекает из записей событий имя пользователя, SID, домен, IP-адрес, списки групп. Результаты обработки записей событий заносятся в журнал UserID-агент события аутентификации. Посмотр журнала доступен в том же разделе: **Журналы и отчеты → Журналы → Агент UserID**.

О журналах источников данных и UserID-агента — в разделе «Агент UserID» документации.

Описание форматов экспорта журналов UserID доступно в Приложении в разделе «Описание форматов журналов».

Radius accounting

UserGate SWG может прозрачно аутентифицировать пользователей, уже прошедших аутентификацию на внешнем сервере RADIUS. UserGate SWG 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 функции выполните следующие шаги:

1. Создайте необходимых локальных пользователей в UserGate SWG. Подробнее о создании пользователей — в разделе «Пользователи».

2. В разделе **Настройки → Сеть → Зоны** выберите зону, которой принадлежит интерфейс, на которой будут приходить сообщения RADIUS accounting. В свойствах контроля доступа зоны разрешите сервис **Агент авторизации**.

3. Установите пароль агентов терминального сервиса. В разделе **Настройки → UserGate → Настройки → Модули** в строке **Пароль агентов терминального сервиса** нажмите **Настроить** и укажите пароль агента терминального сервиса. Этот пароль будет использоваться в качестве RADIUS secret при настройке сервера RADIUS.

4. Добавьте источник RADIUS accounting в веб-консоли UserGate SWG. В разделе **Настройки → Пользователи и устройства → Терминальные серверы** добавьте источник информации RADIUS accounting, указав имя и IP-адрес узла.

5. Настройте отсылку информации RADIUS accounting на узел UserGate SWG, указав в качестве IP-адреса сервера IP-адрес UserGate SWG, порт UDP 1813. Укажите RADIUS secret, совпадающий с паролем агента для терминального сервера, добавленный 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).

Подробнее 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 настройки UserGate SWG будет сопоставлять имя пользователя и присылаемый RADIUS-сервером IP-адрес пользователя. В зависимости от полученной информации UserGate SWG будет работать следующим образом:

Событие	Ответ UserGate SWG
От RADIUS-сервера получено имя пользователя, который не создан на UserGate SWG	На сообщение `Accounting request` UserGate SWG отправит сообщение `Accounting reject`. Данные о пользователях не изменятся
От RADIUS-сервера получено имя существующего пользователя и указан тип `Acct-Status-Type = Start` или `Interim-Update`	Указанному пользователю присвоится полученный IP-адрес. • Имя пользователя начнет отображаться в журналах для этого IP-адреса. Пользовательские правила начнут применяться для трафика с этого IP-адреса. • Если у пользователя уже был IP-адрес, отличный от полученного, пользователю будет присвоен дополнительный IP-адрес. • Если пользователю уже присвоен этот IP-адрес, никаких изменений не произойдет. • Если этот IP-адрес присвоен другому пользователю, он будет удален у другого пользователя и будет присвоен пользователю, указанному в запросе
От RADIUS-сервера получено имя существующего пользователя и указан тип `Acct-Status-Type = Stop`	У пользователя удалится полученный IP-адрес. Имя пользователя перестанет отображаться в журналах для этого IP адреса. Пользовательские правила перестанут применяться для трафика с этого IP-адреса.

UserID-агент для серверов AD, WEC

UserID-агент для AD- и WEC-серверов — это программный компонент, который устанавливается на сервере-контроллере домена или на сервере WEC (Windows Event Collector). Агент считывает необходимую для идентификации

пользователя информацию из журналов безопасности Windows и пересылает ее в формате `syslog` в коллектор UserID на устройствах UserGate Log Analyzer или UserGate SWG.

Основные функции UserID-агента для AD- и WEC-серверов:

- Работа в качестве сервиса.
- Настройка параметров работы через файл конфигурации.
- Чтение журналов безопасности Windows и отправка событий на UserID-коллектор через `syslog`.
- Ведение файла журнала и его ротация. Возможность включить режим отладки журналирования.

Для работы агента в качестве источника данных в сценарии аутентификации с помощью UserID необходимо:

1. Установить и настроить UserID-агент для AD- и WEC-серверов.
2. Настроить сбор информации об аутентификации пользователей на UserGate Log Analyser или на UserGate SWG в зависимости от варианта интеграции.
3. Настроить работу функции UserID на UserGate Log Analyzer или на UserGate SWG.

Установка и настройка агента

UserID-агент для AD- и WEC-серверов поставляется в формате установочного файла.

Для установки агента:

1. Скачайте последнюю версию агента с официального сайта UserGate.
2. Распакуйте архив и запустите установочный файл *.msi.
3. После завершения инсталляции перейдите в рабочую папку агента (по умолчанию: `C:\Program Files (x86)\UserGate\useridagent`) и отредактируйте файл конфигурации `useridagent.cfg`, добавив параметры вашей сети. Подробнее о параметрах и формате файла конфигурации — в разделе «Настройка».

4. Перезапустите сервис `UserIDAgent` через встроенное приложение `Services` (Службы Windows).

Удалить агент можно через панель управления:

1. Нажмите комбинацию клавиш `Win + R` и выполните команду `control`.

2. В панели управления перейдите в раздел **Программы → Программы и компоненты**.

3. Найдите в списке нужное приложение и нажмите **Удалить**.

Настройка

Чтобы настроить агент, отредактируйте его конфигурационный файл. Вы можете изменить или добавить следующие параметры:

- `EventFileNames` — имена журналов для чтения. Значение по умолчанию: `Security`.
- `MaxLogSize` — максимальный размер файла журнала в МБ. Значение по умолчанию: `10`.
- `EventIDs` — номера событий для пересылки. Например, `4624,4634` (ID событий входа в сеть и выхода из сети).
- `DebugLogs` — включение или отключение режима отладки. `0` — журналируются основные события, `1` — журналируется расширенный список событий. Значение по умолчанию: `1`.
- `UserExclude` — список пользователей, для которых события не должны собираться.
- `NetworkList` — список подсетей, в которых собираются события UserID.
- `GatewayList` — список шлюзов (узлы UserGate Log Analyzer, UserGate SWG), на которые отправляются найденные события.

Синтаксис конфигурационного файла:

- Разделителем между параметрами в списках является символ запятой, пробелы после запятой игнорируются.
- Строки, начинающиеся с символов: «`;`» и «#», являются комментариями.
- Раздел `[default]` является необязательным, однако при его использовании раздел должен сохранять указанное название. Перечень

подсетей и шлюзов следует указывать в других разделах, названия которых могут быть произвольными. Новый раздел начинается со строки, содержащей символ «`[`».

- В файле конфигурации должен быть минимум один раздел с одним маршрутом и одним шлюзом.

Пример конфигурации:

```
[default]
MaxLogSize=10
EventIDs=4634, 4624
EventFileNames=Security
DebugLogs=1
UserExclude=adm_,sys_
[net1]
NetworkList=192.168.30.0/24,172.30.250.0/24
GatewayList=192.168.45.1:514,192.168.45.2:514
[net2]
NetworkList=192.168.200.0/24,10.10.0.0/16
GatewayList=192.168.45.4:514,192.168.45.5:514
```

Пример минимальной конфигурации:

```
[net1]
NetworkList=192.168.30.0/24
GatewayList=192.168.45.1
```

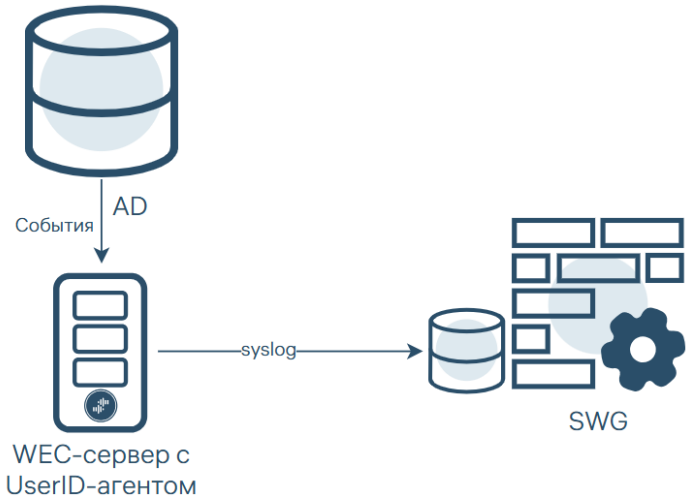
Журналирование

UserID-агент записывает информацию о событиях в файл `uidagent.log`, размер которого контролируется параметром `MaxLogSize`. При достижении лимита:

- текущий файл журнала сохраняется с расширением `*.bak`, заменяя предыдущую версию файла;
- начинается запись нового файла журнала.

Для хранения всех записей работы сервиса рекомендуется настроить внешнее копирование файлов журнала с помощью специализированных сервисов.

Интеграция с UserGate SWG



Для получения информации об аутентификации пользователей выполните настройку следующих параметров на UserGate SWG:

1. Активируйте сервис `UserID syslog collector` в параметрах контроля доступа зоны, в которой находится UserID агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе «Настройка зон».

2. Настройте параметры аутентификации для UserID-агента в домене для получения информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь:

   - Создайте сервер аутентификации на основе LDAP-коннектора для UserID-агента. Подробнее о создании и настройке серверов аутентификации — в разделе «Серверы аутентификации».

   - Создайте профиль аутентификации для UserID-агента. Подробнее о создании и настройке профилей аутентификации — в разделе «Профили аутентификации».

3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

   Коннектор UserID-агента в веб-консоли UserGate SWG создается в разделе **Настройки → Пользователи и устройства → UserID-агент коннекторы**. Нажмите **Добавить** и выберите тип создаваемого коннектора: **Отправитель syslog**. Укажите параметры коннектора:

   - На вкладке **Общие**:

     - **Включено** — включение или отключение получения журналов от источника данных.

- **Название** — название источника данных.
- **Описание** — описание источника данных.
- **Адрес сервера** — адрес узла, с которого UserGate SWG будет получать события по протоколу `syslog`.
- **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
- **Часовой пояс** — часовой пояс, установленный на источнике. При работе с AD- и WEC-серверами через UserID-агент в syslog-коннекторе всегда используется часовой пояс UTC. Этот параметр не зависит от настроек часового пояса на контроллере домена.
- **Профиль аутентификации** — профиль аутентификации, с помощью которого UserID-агент обращается к контроллеру домена по LDAP-протоколу для получения информации о группах, в которых зарегистрирован найденный в журналах syslog пользователь.
- **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate SWG. Значение по умолчанию: 2700 секунд (45 минут).

• На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «Syslog фильтры UserID-агента».

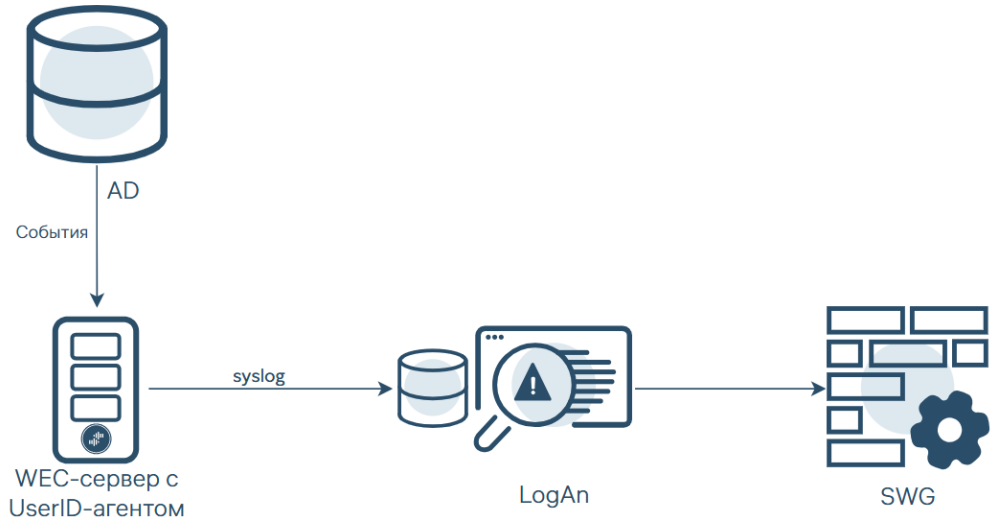
Параметры сервера syslog на UserGate SWG можно посмотреть или изменить в разделе **Настройки → Пользователи и устройства → Свойства агента UserID**.

О настройке функции UserID на UserGate SWG — в разделе «UserID».

Интеграция с UserGate Log Analyzer

Благодаря интеграции источника данных об аутентификации пользователей с UserGate Log Analyzer функцию UserID можно масштабировать на другие устройства сети. Принцип работы UserID на устройстве UserGate Log Analyzer

аналогичен принципу работы на UserGate SWG. Найденные в собранных данных события отправляются на другие UserGate SWG в соответствии с политикой UserID Sharing на основании настроенных профилей редистрибуции. На UserGate SWG отправляются только GUID пользователя, его IP-адрес и список идентификаторов групп, участником которых он является. Такая архитектура позволяет использовать один или несколько серверов UserGate Log Analyzer для централизованного сбора информации о пользователях с различных источников и далее централизованно и избирательно распространять эту информацию на узлы UserGate SWG в корпоративной сети.



Для получения информации об аутентификации пользователей выполните настройку следующих параметров на на UserGate Log Analyzer:

1. Активируйте сервис `Сборщик логов` в параметрах контроля доступа зоны, в которой находится UserID агент для AD- и WEC-серверов. Подробнее о настройке зон — в разделе «Настройка зон».

2. Создайте каталог пользователей для организации доступа UserGate LogAn к серверу AD. Доступ к AD позволяет при необходимости обновлять информацию об имени пользователя в журналах, импортированных из различных сенсоров. Подробнее о создании и настройке серверов аутентификации — в разделе «Каталоги пользователей».

3. Создайте коннектор UserID-агента в соответствии с методом получения данных аутентификации.

Коннектор UserID-агента в веб-консоли UserGate Log Analyzer создается в разделе **Настройки → Пользователи и устройства → UserID-агент**

коннекторы. Нажмите **Добавить** и выберите тип создаваемого коннектора: **Отправитель syslog**. Укажите параметры коннектора:

- На вкладке **Общие**:
    - **Включено** — включение или отключение получения журналов от источника данных.
    - **Название** — название источника данных.
    - **Описание** — описание источника данных.
    - **Адрес сервера** — адрес узла, с которого UserGate Log Analyzer будет получать события по протоколу `syslog`.
    - **Домен по умолчанию** — название домена, который используется для поиска найденных в журналах syslog пользователей.
    - **Часовой пояс** — часовой пояс, установленный на источнике. При использовании UserID-агента для AD- и WEC-серверов в syslog-коннекторе всегда должно быть время в часовом поясе UTC независимо от настроек времени на контроллере домена.
    - **Время жизни аутентифицированного пользователя (сек.)** — период времени, по истечении которого сессия пользователя будет завершена, то есть информация о нем будет удалена из кеш-памяти на UserGate SWG. Значение по умолчанию: 2700 секунд (45 минут).
    - **Профиль редистрибуции UserID** — профиль для определения круга устройств UserGate SWG, на которые отправляется информация о найденных UserID-агентом пользователях.
- На вкладке **Фильтры** выберите фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Настройки → Библиотеки → Syslog фильтры UserID-агента**. Подробнее — в разделе «Syslog фильтры UserID-агента».
- На вкладке **Каталоги пользователей** выбираются каталоги, в которых происходит поиск пользователя, найденного в логах syslog.

Общие настройки syslog-сервера на UserGate Log Analyzer можно посмотреть или изменить в разделе **Настройки → Сборщик логов → Syslog**.

О настройке функции UserID на UserGate Log Analyzer — в разделе «UserID».

Работа с доверенными браузерами

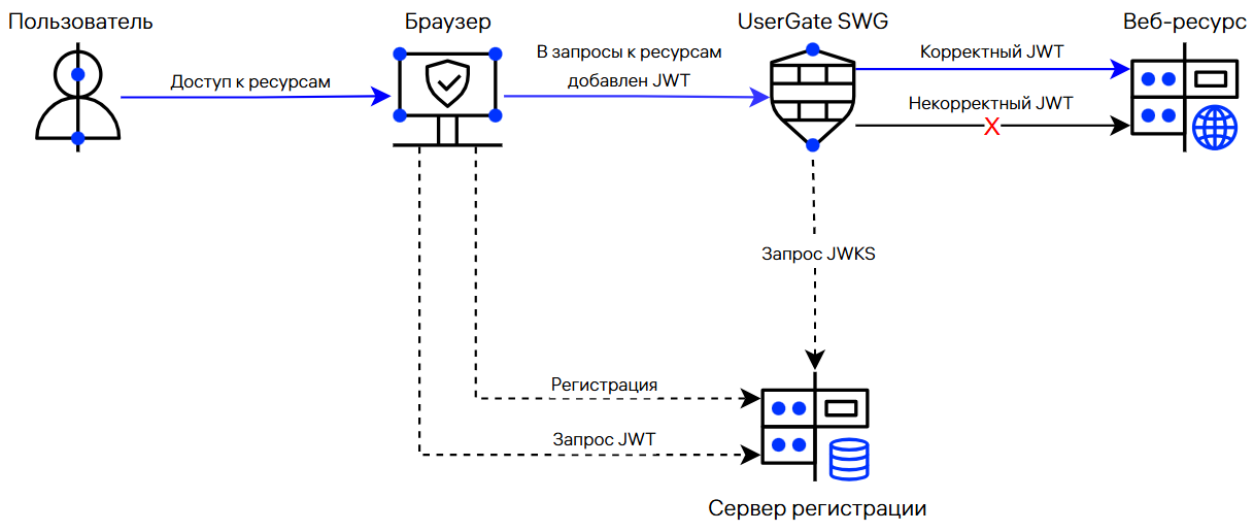
В архитектуре Zero Trust Network Access важным требованием является проверка соответствия конечных устройств установленным политикам безопасности перед предоставлением доступа к ресурсам. Поскольку основным инструментом доступа пользователей к корпоративным и интернет-ресурсам является веб-браузер, система должна обеспечивать контроль используемого браузера.

Идентификация браузера по заголовку User-Agent не обеспечивает достаточного уровня доверия, поскольку этот параметр может быть изменен. Система централизованного управления корпоративными браузерами не гарантирует, что пользователь будет работать именно через управляемый браузер. Для обеспечения безопасного доступа должны использоваться дополнительные механизмы доверенной идентификации и проверки браузера.

В UserGate SWG реализован механизм проверки подлинности браузера, который может выступать в качестве одного из условий в политиках доступа к ресурсам. В качестве доверенного браузера используется версия Яндекс Браузера для организаций.

Архитектура решения

Архитектура решения предполагает развертывание в корпоративной сети организации сервера регистрации (enrollment host), на котором будет хранится база данных зарегистрированных браузеров и выполняться генерация криптографических ключей, используемых для проверки подлинности браузеров. В качестве механизма проверки подлинности применяются методы семейства стандартов JOSE (JSON Object Signing and Encryption).



Яндекс Браузер регистрируется на сервере регистрации и регулярно запрашивает у него актуальный JWT (JSON Web Token). Этот JWT включается во все HTTPS-сообщения в специальный заголовок и служит для проверки подлинности браузера на UserGate SWG.

HTTP-заголовки, добавляемые Яндекс Браузером:

- `X-Ybe-Authorization: Bearer <JWT string>` — токен авторизации (JWT);
- `X-Ybe-DeviceId: <DeviceId>` — идентификатор устройства, по которому можно идентифицировать инсталляцию браузера в системе управления Яндекс Браузера;
- `X-Ybe-Id: <SessionId>` — идентификатор сессии.

UserGate SWG периодически обращается к серверу регистрации для получения набора открытых ключей в формате JWKS (JSON Web Key Set). При обработке сообщений, содержащих токены авторизации от доверенного браузера, и при наличии политик, включающих проверку подлинности браузера в качестве условия доступа, UserGate SWG проверяет подпись токена с помощью открытого ключа и принимает решение о предоставлении или отказе в доступе. Для предотвращения попадания токена авторизации за контур защиты UserGate SWG удаляет из сообщения служебные заголовки, добавленные Яндекс Браузером, если сработало правило, в котором есть условие проверки подлинности браузера.

Настройка работы с доверенными браузерами

Для работы с доверенными браузерами выполните следующие шаги:

1. Разверните систему управления корпоративными браузерами и настройте политику безопасности браузеров. Установите корпоративные браузеры на устройствах пользователей. Документация по настройке и развертыванию корпоративных браузеров предоставляется компанией Яндекс.

2. Разверните в корпоративной сети и настройте сервер регистрации (enrollment host). Инсталляционные файлы и документация по настройке предоставляется компанией Яндекс.

3. Настройте подключение UserGate SWG к серверу регистрации.

4. Предоставьте пользователям доступ к ресурсам через доверенный браузер на UserGate SWG с помощью правил фильтрации контента или правил reverse-прокси.

Подключение к серверу регистрации

Для подключения UserGate SWG к серверу регистрации доверенных браузеров перейдите в раздел **Настройки → Пользователи и устройства → Доверенные браузеры**, нажмите **Добавить** и укажите параметры подключения.

Параметр	Описание
Название	Название подключения
Описание	Описание подключения
URL сервиса Enrollment Host	URL сервера регистрации доверенных браузеров, развернутого в компании
Issuer в стандарте JWT	Параметр задается администратором в переменных среды сервера регистрации Яндекс Браузера (URL_IDP) и передается в составе токена JWT. Используется для идентификации сервера регистрации, выдавшего JWT, если в сети имеется нескольких таких серверов
Порт	Порт подключения к серверу регистрации доверенных браузеров. По умолчанию: 8080
Bearer-токен	Ключ доступа к серверу регистрации доверенных браузеров. Определяется администратором сервиса регистрации

Состояние подключения к серверу регистрации доверенных браузеров отображается в колонке «Статус» списка подключений веб-интерфейса.

Предоставление доступа к ресурсам через доверенный браузер

В зависимости от сценария применения UserGate SWG может использовать проверку подлинности браузера в качестве одного из условий для предоставления доступа к ресурсам в правилах фильтрации контента или в правилах reverse-прокси:

- Чтобы разрешить доступ к интернет-ресурсам только через доверенный браузер, применяйте правила фильтрации контента.
- Чтобы разрешить доступ к корпоративным ресурсам только через доверенный браузер, используйте правила реверс-прокси.

> **Примечание**
> **Убедитесь, что пользовательские устройства имеют сетевой доступ к серверу регистрации доверенных браузеров. Это необходимо для получения браузером веб-токенов (JWT).**

Настройка доступа к интернет-ресурсам через доверенный браузер

Для предоставления доступа к веб-ресурсам через доверенный браузер:

1. На UserGate SWG заранее настройте правила SSL-инспектирования и аутентификации пользователей (если пользователи или группы пользователей будут использоваться в качестве условий предоставления доступа). Подробнее о правилах инспектирования SSL — в разделе «Инспектирование SSL»; о методах аутентификации — в разделе «Пользователи и группы».

2. Создайте правило фильтрации контента, в котором проверка подлинности браузера используется в качестве дополнительного условия.

   В разделе **Настройки → Политики безопасности → Фильтрация контента**, нажмите **Добавить** и укажите обязательные параметры правила:

   - На вкладке **Общие**:
     - установите флажок включения правила;
     - укажите название правила;
     - в поле **Действие** выберите **Разрешить**.

- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров.
- Укажите дополнительные условия фильтрации трафика (например, разрешенные категории URL, списки URL, типы контента, группы пользователей и т. д.).

Подробнее о создании правил фильтрации контента — в разделе «Фильтрация контента».

3. Так как встроенное правило фильтрации контента «Default allow» разрешает любой доступ, для блокировки использования недоверенных браузеров создайте запрещающее правило с инверсным условием идентификации доверенного браузера.

Вы также можете создать дополнительное правило фильтрации контента для формирования предупреждения пользователям, использующим недоверенный браузер с указанием ссылки на ресурс для скачивания доверенного браузера на странице блокировки. Для этого:

1. В разделе **Настройки → Политики безопасности → Фильтрация контента**, нажмите **Добавить** и укажите обязательные параметры правила:

- На вкладке **Общие**:
  - установите флажок включения правила;
  - укажите название правила;
  - в поле **Действие** выберите **Запретить**;
  - выберите настроенную заранее страницу блокировки со ссылкой на скачивание доверенного Яндекс Браузера.
- На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров и включите **Инвертировать** внизу окна.

Подробнее о создании правил фильтрации контента — в разделе «Фильтрация контента»; о шаблонах страниц — в разделе «Шаблоны страниц».

2. Чтобы пользователи могли загрузить доверенный браузер, создайте разрешающее правило для доступа к указанному ресурсу и разместите его выше запрещающего правила.

Настройка доступа к корпоративным ресурсам через доверенный браузер

Для предоставления доступа к корпоративным ресурсам через доверенный браузер выполните следующие шаги:

1. Для обмена трафиком с публикуемыми ресурсами по защищенному соединению создайте на UserGate SWG профиль SSL, содержащий нужные криптографические протоколы, и импортируйте сертификат публикуемого ресурса.

   Подробнее о профилях SSL — в разделе «Профили SSL»; о сертификатах — в разделе «Управление сертификатами».

2. Создайте правило reverse-прокси, в котором проверка подлинности браузера используется в качестве дополнительного условия.

   В разделе **Настройки → Глобальный портал → Правила reverse-прокси**, нажмите **Добавить** и укажите обязательные параметры правила:

   - На вкладке **Общие**:
     - установите флажок включения правила;
     - укажите название правила;
     - выберите сервер или балансировщик reverse-прокси, которому UserGate SWG будет пересылать запросы;
     - укажите порты, на которых UserGate SWG будет слушать входящие запросы;
     - выберите заранее созданный профиль SSL и сертификат публикуемого сервера.
   - На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса, для которых будет разрешен обмен трафиком с веб-серверами.
   - На вкладке **Подмена путей** настройте переопределение путей URL
   - На вкладке **Доверенные браузеры** выберите созданное ранее подключение к серверу регистрации доверенных браузеров.

   Укажите дополнительные условия предоставления доступа (например, группы пользователей и т. д.).

Подробнее о создании правил reverse-прокси — в разделе «Публикация HTTP/HTTPS ресурсов с помощью reverse-прокси».

ПОЛИТИКИ СЕТИ

Общие сведения

Раздел «Политики сети» объединяет в себе настройки основных механизмов управления трафиком UserGate SWG.

В этом разделе администратор может:

- Управлять прохождением трафика с помощью правил межсетевого экрана. В условиях фильтрации в правилах могут быть использованы зоны и адреса источника и назначения, пользователи, группы пользователей, сервисы.
- Выполнять трансляцию IP-адресов и портов сетевых пакетов с помощью правил NAT и маршрутизации для решения задач, связанных с защитой структуры внутренней сети компании, публикацией внутренних ресурсов в интернете, объединением сетей.
- Выполнять задачи по распределению входящего трафика на публикуемых ресурсах с помощью правил балансировки нагрузки.
- Контролировать использование полосы пропускания определенными пользователями, узлами, сервисами и приложениями с помощью правил управления пропускной способностью.

События срабатывания правил регистрируются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включенной опции журналирования в свойствах правил.

Межсетевой экран

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate SWG. 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. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.**

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

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

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

Чтобы создать правило межсетевого экрана, перейдите в раздел **Настройки → Политики сети → Межсетевой экран**, нажмите **Добавить** и указать необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Действие	• **Запретить**: блокирует трафик.

Параметр	Описание
	• **Разрешить**: разрешает трафик
Отбросить и	Параметр доступен для правил, блокирующих трафик (выбрано действие **Запретить**). Параметр может принимать одно из следующих значений: • **Не выбран**. • **Посылать ICMP host unreachable** — блокировка трафика с отправкой ICMP-сообщения. • **Посылать TCP reset** — блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** **При выборе действия «Посылать TCP reset» необходимо указать сервис (вкладка «Сервис»), использующий протокол TCP.** • **Посылать TCP reset в обе стороны** — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Журналировать каждый пакет** — в журнал трафика будет записываться информация о каждом передаваемом сетевом пакете. Для этого режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • **Нет** — в этом случае информация не будет записываться
Применить правило к	Указать, к каким пакетам будет применяться правило: • Все пакеты. • Только фрагментированные пакеты. • Только нефрагментированные пакеты

Параметр	Описание
Вставить	Указать расположение правила в списке
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом * в таких списках не работают (игнорируются).** Каждые 5 минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Назначение	Зона, списки IP-адресов, списки GeoIP-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 UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По

Параметр	Описание
	истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса Обработка трафика происходит по следующей логике: • Усслования 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
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Расширенный поиск в разделе **Настройки → Политики сети → Межсетевой экран** доступен по следующим параметрам.

Параметр	Описание
`enabled`	Поиск включенных или выключенных правил. Может принимать значения: • `true` — для отображения всех включенных правил. • `false` — для отображения все выключенных правил
`pos`	Поиск по позиции правила в списке (1, 2 и т. д.)
`log`	Поиск правила по включенной или выключенной функции журналирования. Возможны следующие значения: • `true` или `enabled` — отображение правил, в которых включена функция журналирования (журналировать начало сессии или журналировать все сетевые пакеты). • `false` или `disabled` — отображение правил, в которых журналирование отключено. • `all` — отображение правил, в которых настроено журналирование всех сетевых пакетов.

Параметр	Описание
	• `start` — отображение правил, в которых настроено журналирование начала сессии
`name`	Поиск правил по названию
`action`	Поиск правил по действию, настроенному в правилах межсетевого экрана: • Разрешить (allow) — разрешает трафик. • Запретить (deny) — блокирует трафик
`zoneSource`	Поиск правил по зоне источника трафика
`ipSource`	Поиск правил по IP-адресу источника трафика. Адрес должен входить в список IP-адресов, созданный в разделе **Настройки → Библиотеки → IP-адреса** или в свойствах правила
`ipSourceName`	Поиск правил по названию IP-листа источника трафика
`countrySource`	Поиск правил по названию страны источника трафика. Страна источника может быть добавлена в свойствах правила на вкладке **Источник** (**Добавить GeoIP**)
`portSource`	Поиск правил по порту источника трафика. Порты, которые используются сервисами, можно настроить в разделе **Настройки → Библиотеки → Сервисы**
`zoneDest`	Поиск правил по зоне назначения трафика
`ipDest`	Поиск правил межсетевого экрана по IP-адресу назначения. Адрес должен входить в список IP-адресов, созданный в разделе **Настройки → Библиотеки → IP-адреса** или в свойствах правила
`ipDestName`	Поиск правил по названию IP-листа назначения трафика
`countryDest`	Поиск правил по названию страны назначения трафика. Страна назначения может быть добавлена в свойствах правила на вкладке **Назначение** (**Добавить GeoIP**)
`portDest`	Поиск правил по порту назначения трафика. Порты, которые используются сервисами, можно настроить в разделе **Настройки → Библиотеки → Сервисы**
`user`	

Параметр	Описание
	Поиск правил по пользователям, для которых они применяются. Правило может быть применено для следующих типов пользователей: • Пользователь Unknown — пользователи, не идентифицированные системой. • Пользователь Known — пользователи, идентифицированные системой с помощью серверов авторизации. • Пользователь Any — любой пользователь (Known или Unknown). • Определённый пользователь — конкретный пользователь, идентифицированный в системе. Пользователи могут быть заведены локально (локальные пользователи) или получены с внешних каталогов (например, Microsoft Active Directory). При поиске, требующем полного совпадения (операторы = или `!=`) логина пользователя, также будет производиться поиск по группам пользователей
`userId`	Поиск правил по ID пользователя; также будут отображены правила, в которых указаны группы пользователя
`group`	Поиск по группам пользователей, для которых применено правило межсетевого экрана. Группы пользователей могут быть заведены локально или получены с внешних каталогов (например, Microsoft Active Directory)
`groupId`	Поиск правила по идентификатору группы пользователей
`service`	Поиск правила по указанному типу сервиса
`active`	Поиск активных или не активных в текущий момент времени правил (во время выполнения поискового запроса): • `true` — отображение правил, для которых текущее время попадает в заданные интервалы активности. • `false` — отображение правил, для которых текущее время не попадает в заданные интервалы активности. Время работы правила может быть задано в свойствах на вкладке **Время**. Для этого используются календари, созданные в разделе **Настройки → Библиотеки → Календари** или в свойствах правила
`description`	Поиск правил по описанию правила

> **Примечание**
> **Поисковый запрос не распространятся на правило Default block. Т. е., даже если поиск правил происходит по запросу `action = allow`, правило Default block, настроенное на блокировку трафика, будет отражено в конце списка.**

NAT и маршрутизация

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, NoNAT, DNAT, NoDNAT, трансляции портов, PBR и Network mapping. UserGate SWG поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**), если в правиле включена опция журналирования.

> **Примечание**
> **GeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и трансляции портов.**

Правила NAT

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

> **Примечание**
> **Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.**

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

Чтобы создать правило NAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **NAT**
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменён адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, система будет использовать произвольный адрес из списка доступных IP-адресов, назначенных интерфейсам зоны назначения. Допускается указание диапазона IP-адресов. Например, `192.168.10.10-192.168.10.20`. В этом случае UserGate SWG будет использовать все указанные адреса для Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке

Параметр	Описание
Источник	Зона, списки IP-адресов, списки URL источника трафика, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов.** Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.

Параметр	Описание
	Важно! **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Примечание

Рекомендуется создавать общие правила NAT, например правило NAT из локальной сети (обычно зона Trusted) в интернет (обычно зона Untrusted), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

Правила NoNAT

Правила NoNAT используются, когда из работающих в системе правил NAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила.
Название	Название правила.
Теги	**Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»**
Описание	Описание правила
Тип	Тип правила. Выберите **NoNAT**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL, MAC-адреса источника трафика. Списки URL должны включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи

Параметр	Описание
	типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу.

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Подробнее о публикации ресурсов с помощью правил reverse-прокси — в разделе «Публикация 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. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.**

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

Чтобы создать правило DNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	**Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»**
Описание	Описание правила
Тип	Тип правила. Выберите **DNAT**
SNAT IP (внешний адрес)	Явное указание IP-адреса, на который будет заменён адрес источника. Если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса UserGate SWG, с которого отправлен пакет. Допускается указание диапазона IP-адресов. Например, `192.168.10.10-192.168.10.20`. **Важно!** Для замены адреса источника на указанный адрес необходимо на вкладке «DNAT» активировать Флажок «Включить SNAT»

Параметр	Описание
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP-адреса, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей.

Параметр	Описание
	Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate SWG, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов
Сервис	Тип сервиса, который необходимо опубликовать. Если не указан сервис, будут опубликованы все сервисы **Важно!** **Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100.**
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет
Включить SNAT	При включении данной опции UserGate SWG 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, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Примечание

При использовании нескольких правил DNAT с SNAT, отличающихся только условиями адреса назначения, действие SNAT будет выполняться только по первому правилу DNAT. Это обусловлено тем, что пакет, попавший под любое из этих правил, после изменения IP-адреса назначения не будет отличаться на сетевом и транспортном уровне модели OSI. При одинаковых DNAT IP необходимо в правилах DNAT иметь уникальные условия в зонах, сервисах, адресах источника.

Примечание

Трафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила NoDNAT

Правила NoDNAT используются, когда из работающих в системе правил DNAT необходимо исключить отдельные адреса узлов или подсетей без переписывания всей настроенной политики. Трафик, фильтруемый правилом NoDNAT, будет проходить через систему без трансляции адресов.

Чтобы создать правило NoDNAT, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	**Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»**
Описание	Описание правила
Тип	Тип правила. Выберите **NoDNAT**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале

Параметр	Описание
	сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Вставить	Выбор места расположения правила в общем списке
Источник	Зона, списки IP-адресов, списки URL, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей

Параметр	Описание
	в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов (внешние IP-адресов UserGate SWG, доступные из сети интернет, на которые адресован трафик внешних клиентов), списки URL назначения трафика. Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов
Сервис	Тип сервиса, который необходимо опубликовать. Если не указан сервис, будут опубликованы все сервисы **Важно!** **Следующие порты не могут быть использованы для публикации сервисов, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100.**
Использование	Статистика срабатывания о правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции портов

Правила трансляции портов (port forwarding) работают аналогично правилам DNAT, за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

Примечание

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

Чтобы создать правило трансляции портов, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **Порт-форвардинг**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов.

Параметр	Описание
	Важно! **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пят минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Использование этого параметра позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов.

Параметр	Описание
	Важно! **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Порт-форвардинг	Трансляция портов публикуемых сервисов: • **Оригинальный порт назначения** — номер TCP- или UDP-порта, на который приходят запросы; следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами UserGate SWG: 2200, 8001, 4369, 9000-9100; • **Новый порт назначения** — номер TCP- или UDP-порта, на который будут пересылаться запросы на внутренний публикуемый сервер
Адрес назначения DNAT	IP-адрес узла в локальной сети, который публикуется в интернет
Включить SNAT	При включении этой опции UserGate SWG будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Примечание

Трафик DNAT/трансляции портов не обрабатывается правилами межсетевого экрана, созданными по умолчанию (Default block).

Правила маршрутизации на основе политик

Правила маршрутизации на основе политик (policy-based routing, PBR) используются для указания определённого маршрута в интернет для выбранных узлов или сервисов. Например, в организации используются два провайдера и необходимо весь HTTP-трафик пересылать через провайдера 1, а весь остальной — через провайдера 2. Для этого необходимо указать в качестве шлюза по умолчанию интернет-шлюз провайдера 2 и настроить правило PBR для HTTPS-трафика через шлюз провайдера 1.

Примечание

Правила PBR не заменяют и не влияют на работу правил NAT. Для трансляции адресов после правила PBR необходимо поставить соответствующее правило NAT.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

Примечание

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

Чтобы создать правило PBR, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Тип	Тип правила. Выберите **Policy-based routing**
Шлюз	Выбор одного из существующих шлюзов. Шлюз может быть добавлен в разделе **Сеть → Шлюзы** **Важно!** **Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По

Параметр	Описание
	истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой

Параметр	Описание
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Правила трансляции адресов сетей

Правила трансляции адресов сетей (network mapping) позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес узла без изменений. Например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 узел 192.168.1.1 будет изменен на 192.168.2.1.

> **Примечание**
> **Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, в котором совпали все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.**

Чтобы создать правило **Network mapping**, перейдите в раздел **Настройки → Политики сети → NAT и маршрутизация,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила

Параметр	Описание
Тип	Тип правила. Выберите **Network mapping**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет** — в этом случае информация не будет записываться
Источник	Зона, списки IP-адресов, списки URL источника трафика, GeoIP, MAC-адреса источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** Флажок «Инвертировать» не влияет на работу при использовании MAC-адресов. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Список пользователей или групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства». Позволяет создавать правила NAT+SNAT для пользователей с учетом членства в группе. Например, разные группы

Параметр	Описание
	пользователей в компании или разные отделы получают доступ в интернет с разных IP-адресов для отчетности и контроля
Назначение	Списки IP-адресов, списки URL назначения трафика, GeoIP. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой

Network mapping	Указание параметров подмены сетей.
	• **Новая IP-сеть/маска** — адрес сети, на которую будет производится замена.
	• **Направление**:
	  ◦ **Входящий**, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле **Новая IP-сеть/маска**.
	  ◦ **Исходящий**, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле **Новая IP-сеть/маска**

Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний.

Параметр	Описание
	Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Балансировка нагрузки

UserGate SWG поддерживает балансировку трафика между различными сервисами. Балансировка может применяться в следующих сценариях:

- для внутренних серверов, опубликованных в интернете с использованием DNAT;
- внутренних серверов без публикации во внешней сети;
- трафика, перенаправляемого на внешние ICAP-серверы;
- трафика к серверам, публикуемым через правила reverse-proxy.

Балансировщик принимает запросы, направленные на IP-адрес виртуального сервера, и распределяет их между IP-адресами реальных серверов, применяя различные алгоритмы балансировки.

Чтобы настроить балансировку, необходимо в разделе **Настройки → Политики сети → Балансировка нагрузки** создать правила балансировки.

Балансировщик TCP/UDP

Для создания правила балансировки TCP/UDP перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки,** нажмите **Добавить**, выберите **Балансировщик TCP/UDP** и укажите необходимые параметры.

Параметр	Описание
Включен	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки

Параметр	Описание
IP-адрес виртуального сервера	Выбор адреса из списка IP-адресов, назначенных на сетевые интерфейсы узла. При необходимости вы можете добавить дополнительные IP-адреса на желаемый интерфейс
Порт	Порт, для которого необходимо производить балансировку нагрузки
Протокол	Протокол, для которого необходимо производить балансировку нагрузки (TCP или UDP)
Метод балансировки	Выбор метода распределения трафика на реальные серверы: • **Round robin** — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • **Weighted round robin** — работает аналогично методу 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 котором в данный момент установлено наименьшее число соединений. • **Weighted least connections** — работает аналогично методу least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера
Реальные серверы	Добавление пула реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать: • **IP-адрес** сервера. • **Порт** сервера — порт, на который необходимо пересылать запросы пользователей. • **Вес** — параметр для неравномерного распределения трафика на реальные серверы для режимов балансировки weighted round robin и weighted least connections. Чем больше вес, тем больше будет нагрузка на сервер. • **Режим**: ◦ **Шлюз** — для перенаправления трафика на виртуальный сервер используется маршрутизация.

Параметр	Описание
	◦ **Маскарадинг** — для перенаправления трафика на виртуальный сервер используется DNAT. ◦ **Маскарадинг с подменой IP-источника (SNAT)** — аналогично маскарадингу, но при этом UserGate SWG подменяет IP-адрес источника на свой **Важно!** **Поскольку в режиме «Шлюз» балансировщик не изменяет заголовки пакетов, обратный трафик от реального сервера должен обеспечиваться средствами маршрутизации. То есть шлюз для обратного трафика должен отличаться от адреса UserGate SWG.**
Аварийный режим	Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо его включить и указать следующие параметры: • **IP-адрес** сервера. • **Порт** сервера — порт, на который необходимо пересылать запросы пользователей. • **Режим**: ◦ **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 UserGate SWG подменяет IP-адрес источника на свой
Мониторинг	Механизм мониторинга выполняет проверку доступности реальных серверов. Недоступные серверы автоматически выводятся из пула балансировки нагрузки
Режим	Способ мониторинга реальных серверов: • **ping** — проверка доступности узла с помощью утилиты ping.

Параметр	Описание
	• **connect** — проверка работоспособности узла с помощью установления TCP-соединения на определенный порт. • **negotiate** — проверка работоспособности узла с помощью отправки определенного HTTP- или DNS-запроса и сравнения полученного ответа с ожидаемым. Для настройки этого режима выберите тип сервиса (**HTTP** или **DNS**), заполните строки **Запрос** и **Ожидаемый ответ.** Например, для HTTP-запроса: ◦ **Запрос**: `/robots.txt`; ◦ **Ожидаемый ответ**: `Disallow: /bin/`. Строка запроса в этом примере указывает 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	Время ожидания ответа на проверку
Число неудачных попыток	Количество попыток проверки реальных серверов, по достижении которого сервер будет считаться неработоспособным и будет исключен из списка балансировки

Примечание

Правила балансировки имеют более высокий приоритет и применяются до правил NAT, DNAT, Маршрутизации.

Балансировщик ICAP

Балансировщик ICAP распределяет трафик между внешними ICAP-серверами. Такое решение может применяться для антивирусного сканирования или глубокого анализа пользовательских данных с использованием DLP-систем.

Алгоритм балансировки распределяет HTTP-трафик между серверами с учетом пользовательских сессий.

Для создания балансировщика ICAP перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки**, нажмите **Добавить**, выберите **Балансировщик ICAP** и укажите необходимые параметры балансировщика.

Параметр	Описание
Включено	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки
Способ балансировки	Настройка балансировки трафика с поддержкой закрепления HTTP-запросов пользователя за определенным ICAP-сервером в рамках одной сессии. Это обеспечивает согласованную обработку пользовательского потока данных. Вы можете выбрать несколько методов привязки, они применяются последовательно, в порядке приоритета сверху вниз: • **По заголовку Cookie** — привязка выполняется на основе cookie, который генерируется самим балансировщиком. Балансировщик добавляет cookie во вложенный HTTP-ответ, закрепляя HTTP-сессию пользователя за конкретным ICAP-сервером. Все последующие HTTP-сообщения, содержащие этот cookie, направляются на тот же ICAP-сервер. • **По имени пользователя** — привязка выполняется по имени пользователя источника запроса. Механизм используется только в том случае, если система может определить имя пользователя. Если имя пользователя определить невозможно, применяется следующий доступный метод согласно приоритету. • **По IP-адресу и порту клиента** — привязка осуществляется по комбинации IP-адреса и порта источника. В этом случае все ICAP-запросы от одного и того же IP-адреса и порта направляются на один и тот же ICAP-сервер на протяжении времени действия привязки. • **По IP-адресу клиента** — привязка выполняется только по IP-адресу источника. Все ICAP-запросы от одного и того же IP-адреса направляются на один ICAP-сервер в течение времени действия привязки. Метод обеспечивает стабильную маршрутизацию HTTP-запросов пользователей с постоянным IP-адресом. • **По TCP-сессии** — привязка выполняется по TCP-соединению. В этом режиме все ICAP-запросы (REQMOD и RESPMOD), передаваемые в рамках одного TCP-соединения от ICAP-клиента, обрабатываются одним и тем же ICAP-сервером. Балансировка по TCP-сессии активна всегда, она работает, если не сработали другие выбранные методы.

Параметр	Описание
	Время закрепления — период, в течение которого сохраняется привязка запросов (от 1 до 86 400 секунд, значение по умолчанию — 3600 секунд). По истечении этого времени информация о привязке сессии удаляется, после чего распределение запросов выполняется заново. Подробнее о работе с ICAP-серверами — в разделе «Работа с внешними ICAP-серверами»
ICAP-серверы	Выбор профилей ICAP-серверов, на которые будет распределяться нагрузка. Подробнее о работе с ICAP-серверами — в разделе «Работа с внешними ICAP-серверами»

Примечание

При изменении параметров действующего правила происходит перезапуск механизма балансировки. Активные сессии с ICAP-серверами завершаются. Последующие запросы обрабатываются уже по обновленной конфигурации правила балансировки.

Балансировщик reverse-прокси

Балансировщик серверов reverse-прокси позволяет распределять трафик на внутренние серверы, публикуемые с помощью правил reverse-прокси. Этот балансировщик может быть использован в правилах reverse-прокси.

Для создания правила балансировки для серверов reverse-прокси перейдите в раздел **Настройки → Политики сети → Балансировка нагрузки,** нажмите **Добавить**, выберите **Балансировщик reverse-прокси** и укажите необходимые параметры.

Параметр	Описание
Включен	Включение или отключение правила балансировки
Название	Название правила балансировки
Описание	Описание правила балансировки
Reverse-прокси профили	Выбор профилей серверов reverse-прокси, на которые будет передаваться трафик. Подробнее о публикации ресурсов с помощью reverse-прокси — в разделе «Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси»

Пропускная способность

Правила управления пропускной способностью применяются к определенным пользователям, узлам, сервисам, приложениям.

> **Примечание**
> **Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.**

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

Чтобы создать правило управления пропускной способностью, перейдите в раздел **Настройки → Политики сети → Пропускная способность,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включает или отключает правило
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания вы можете в разделе «Полосы пропускания»
Сценарий	

Параметр	Описание
	Указывает сценарий, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии». **Важно!** **Сценарий является дополнительным условием. Если сценарий не активировался (не сработал ни один из триггеров сценария), правило не сработает**
Журналирование	Запись в журнал информации о трафике при срабатывании правила. Возможные варианты: • **Журналировать начало сессии** — в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Журналировать каждый пакет** — в журнал трафика будет записываться информация о каждом передаваемом сетевом пакете. Для этого 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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;

Параметр	Описание
	• условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Пользователи	Пользователи или группы пользователей, к которым применится правило
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Сервис	Тип сервиса. Например, HTTP, HTTPS или другой
Приложения	Список приложений, для которых необходимо ограничить полосу пропускания
Время	Время, когда правило активно

ПОЛИТИКИ БЕЗОПАСНОСТИ

Общие сведения

С помощью политик безопасности администратор может:

- Настроить фильтрацию HTTP-контента. Например, запретить некоторым пользователям доступ к определенным категориям сайтов в заданное время или настроить антивирусную проверку веб-контента.
- Настроить опции веб-безопасности. Например, включить принудительный безопасный поиск и блокировку рекламы.
- Настроить правила инспектирования SSL. Например, для всех пользователей расшифровывать HTTPS для категории «Форумы», а для определенной группы — «Социальные сети». После того, как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Настроить проверку почтовых протоколов SMTP и POP3 на наличие спама.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP.
- Настроить публикацию HTTP/HTTPS-серверов.

События срабатывания 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 защиты 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 вы можете разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS (если настроено инспектирование HTTPS). UserGate SWG может блокировать HTTPS-

трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации UserGate SWG URL filtering или по спискам URL, в которых указаны только имена узлов. В этих случаях UserGate SWG использует SNI (Server Name Indication), а при отсутствии SNI — название узла из SSL-сертификата из пользовательских запросов для определения домена.

В качестве условий правила могут быть использованы параметры:

- 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.
- User agent браузера пользователя.
- HTTP-метод.
- Результат проверки подлинности браузера. Подробнее — в разделе «Работа с доверенными браузерами».

Примечание

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

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

Примечание

Если запрещающее правило является более общим по сравнению с разрешающими правилами, то запрещающее правило отработает перед разрешающими, несмотря на порядок расположения. В итоге, запрещающее правило нужно делать более специфичным, чтобы порядок отрабатывался корректно.

Примечание

Если не создано ни одного правила, передача любого контента разрешена.

Чтобы создать правило контентной фильтрации, перейдите в раздел **Настройки → Политики безопасности → Фильтрация контента,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила
Действие	Действие правила: • **Запретить** — блокировать веб-страницу. • **Предупредить** — предупредить пользователя о том, что страница нежелательна для просмотра. Пользователь сам решает, отказаться от просмотра или нет. Запись о просмотре страницы заносится в журнал. • **Разрешить** — разрешить просмотр веб-страницы
Записывать в журнал правил	При активации этой 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.), антивирусная проверка будет выполняться только при совпадении всех условий правила

Параметр	Описание
Сценарий	Выбор сценария, который должен быть активным для срабатывания правила. Подробнее о работе сценариев — в разделе «Сценарии». **Важно!** **Сценарий является дополнительным условием. Если сценарий не активировался (не сработал ни один из триггеров сценария), правило не сработает**
Страница блокировки	Выбор страницы блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Вы можете использовать внешнюю страницу, указав **Использовать внешний URL**, либо указать страницу блокировки на UserGate SWG. В последнем случае можно выбрать желаемый шаблон страницы блокировки, который создается в разделе «Шаблоны страниц»
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Максимальное количество GeoIP, которое может быть указано: 15.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов;

Параметр	Описание
	• условия объединяются по И, если указаны GeoIP и списки IP-адресов 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 пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Максимальное количество GeoIP, которое может быть указано: 15.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов
Пользователи	Список пользователей, групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
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 работы на категории.

Параметр	Описание
	Вы можете переопределить категорию для любого сайта, на который, по вашему мнению, категория назначена не верно или не назначена совсем. Подробнее о процедуре изменения категории сайта — в разделе «Запросы в белый список» **Важно!** **Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования. Страница блокировки в таком случае показана не будет.**
URL	Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate. Вы также можете создавать собственные списки URL. Подробнее о работе со списками URL — в разделе «Списки URL» **Важно!** **Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена узлов (доменов). Страница блокировки в таком случае показана не будет.**
Типы контента	Списки типов контента. Предусмотрена возможность управления видео контентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Вы также можете создавать собственные группы типов контента. Подробнее о работе с типами контента — в разделе «Типы контента»

Параметр	Описание
Морфология	Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари, обновляемые компанией UserGate. Словари доступны на русском, английском, немецком, японском и арабском языках. Вы также можете создавать собственные словари. Подробнее о работе с морфологическими словарями — в разделе «Морфология»
Время	Период, когда правило активно. Вы можете добавить необходимые временные интервалы в разделе «Календари»
Useragent	User agent пользовательских браузеров, для которых будет применено правило. Вы можете добавить необходимые user agent в разделе «User agent браузеров»
HTTP метод	Метод, используемый в HTTP-запросах. Как правило, это POST или GET
Рефереры	Список URL, в котором указаны рефереры (адреса страниц, с которых пользователь перешел к текущему ресурсу) для текущей страницы. Правило сработает, если для этой страницы реферер совпадет со списком указанных URL. Функция часто используется, чтобы разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую
Доверенные браузеры	Проверка подлинности браузера для предоставления доступа к ресурсам. Выберите созданное ранее в разделе **Н астройки → Пользователи и устройства → Доверенные браузеры** подключение к серверу регистрации доверенных браузеров. Подробнее о создании подключения к серверу регистрации доверенных браузеров — в разделе «Работа с доверенными браузерами»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний.

Параметр	Описание
	Важно! **При настроенном инспектировании данных, передаваемых по протоколам TLS/SSL, и срабатывании правила контентной фильтрации Default allow, созданного по умолчанию, счётчик будет срабатывать только для правила инспектирования SSL.** Чтобы сбросить счётчик срабатываний, выделите правила в списке и нажмите **Сбросить счётчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Веб-безопасность

С помощью правил раздела **Веб-безопасность** вы можете включить дополнительные параметры 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 на странице. UserGate SWG решает эту проблему, блокируя рекламные баннеры.
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. 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 этого инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например при фильтрации откликов на запросы по графическому или видео контенту.
- Включение журналирования поисковых запросов пользователей.

- Блокировка приложений социальных сетей. Социальные сети играют большую роль в повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. UserGate SWG может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

- Источник трафика.
- Пользователи и группы.
- Время.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

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

> **Примечание**
> **Если не создано ни одного правила, дополнительные функции веб-безопасности не применяются.**

Чтобы создать правило веб-безопасности, перейдите в раздел **Настройки → Политики безопасности → Веб-безопасность**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»

Параметр	Описание
Описание	Описание правила
Записывать в журнал правил	При активации этой опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики
Блокировать рекламу	Блокировка рекламы. По ссылке **Исключения** вы может выбрать URL-списки сайтов, для которых блокировка рекламы не требуется
Инжектор	Встраивание произвольного кода во все веб-страницы. Для редактирования встраиваемого кода нажмите **Код инжектора**
Безопасный поиск	Принудительно включить функцию безопасного поиска
История поиска	Запись поисковых запросов пользователей в журнал
Блокировать приложения социальных сетей	Блокировка приложений в социальных сетях
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGater SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов
Пользователи	Список пользователей, групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known

Параметр	Описание
	настройте идентификацию пользователей. Подробнее об идентификации пользователей — в разделе «Пользователи и устройства»
Время	Интервал активности правила. Вы можете добавить необходимые временные интервалы в разделе «Календари»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

Инспектирование SSL

В этом разделе вы можете настроить инспекцию данных, передаваемых по протоколу TLS/SSL. UserGate SWG с функцией SSL-инспектирования выступает в роли доверенного посредника (Man-in-the-Middle, MitM).

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности.

С помощью правил раздела вы можете настроить инспектирование HTTPS только для определенных категорий, например «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и не расшифровывать другие категории, например «Финансы», «Правительство» и т. п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе — SNI (Server Name Indication). При отсутствии SNI может использоваться поле Subject Name в сертификате сервера. Содержимое поля Subject Alternative Name игнорируется.

UserGate SWG перехватывает исходящий запрос на установление SSL-соединения и производит подмену сертификата сервера на свой, выписанный внутренним корневым центром сертификации. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить корневой сертификат центра сертификации в доверенные корневые сертификаты. Подробнее — в разделе «Установка сертификата локального удостоверяющего центра».

Если корневой сертификат доверен, браузер считает полученный сертификат легитимным и устанавливает безопасное SSL-соединение между пользователем и UserGate SWG.

Далее UserGate SWG устанавливает новое, отдельное SSL-соединение с конечным сервером. В итоге UserGate SWG работает как посредник: получает данные от пользователя, проверяет их, шифрует и отправляет на внешний сервер, и наоборот.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

Примечание

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

Примечание

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

Чтобы создать правило инспектирования SSL, перейдите в раздел **Настройки → Политики безопасности → Инспектирование SSL**, нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Включено	Включение или отключение правил
Название	Название правила
Теги	Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»
Описание	Описание правила

Параметр	Описание
Записывать в журнал правил	При активации этой опции информация о срабатывание правила будет регистрироваться в «Журнале веб-доступа»
Действие	Выполняемое действие: • Расшифровать. • Не расшифровывать. • Расшифровать и переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет передана в соответствии с правилом и профилем инспектирования SSL. При выборе этого действия укажите профиль пересылки SSL. Подробнее о настройке профилей пересылки — в разделе «Профили пересылки SSL»
Профиль SSL	Выбор профиля SSL. Параметры, указанные в этом профиле, будут использованы как для установки SSL-соединения от браузера пользователя к UserGate SWG, так и при построении SSL-соединения от UserGare SWG к запрашиваемому веб-ресурсу. Подробнее о профилях SSL — в разделе «Профили SSL»
Блокировать сайты с некорректными сертификатами	Блокировка доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или выдан недоверенным центром сертификации
Проверять по списку отозванных сертификатов	Проверка сертификата сайта в списке отозванных сертификатов (CRL). Если сертификат найден в списке, сайт будет заблокирован
Блокировать сертификаты с истекшим сроком действия	Блокировка сертификатов, срок действия которых истек
Блокировать самоподписанные сертификаты	Блокировка самоподписанных сертификатов
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 — в разделе «Пользователи и устройства»

Параметр	Описание
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутренней кэш-памяти на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. **Важно!** **Количество указанных GeoIP не может быть больше 15.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов

Параметр	Описание
Адрес назначения	Списки IP-адресов назначения трафика. **Важно!** **Количество указанных GeoIP не может быть больше 15.** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов или доменов. Подробнее о работе со списками IP-адресов — в разделе «IP-адреса»
Сервисы	Сервис, для которого необходимо дешифровать трафик
Категории	Списки категорий UserGate URL filtering 4.0
Домены	Списки доменов. Доменные имена, для которых применяется правило. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена (www.example.com, а не http://www.example.com/home/). Подробнее о работе со списками URL — в разделе «Списки URL»
Время	Интервал активности правила. Вы можете добавлять необходимые временные интервалы в разделе «Календари»
Использование	Статистика срабатывания правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счетчик срабатываний, выделите правила в списке и нажмите **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к этому правилу

По умолчанию создано правило инспектирования «SSL Decrypt all for unknown users», которое необходимо для аутентификации неизвестных пользователей через Captive-портал.

Работа с внешними ICAP-серверами

ICAP (Internet Content Adaptation Protocol) — это протокол, предназначенный для передачи HTTP-сообщений на внешние серверы с целью их обработки и адаптации. Он работает поверх TCP и по своей структуре напоминает HTTP.

ICAP позволяет прокси-серверам и шлюзам безопасности перенаправлять трафик на выделенные серверы для обработки контента, например для антивирусной проверки, фильтрации или интеграции с DLP-системами.

Взаимодействие по протоколу ICAP строится по модели «клиент —сервер»:

- ICAP-клиент — это устройство, которое перехватывает HTTP-трафик (прокси-сервер или шлюз безопасности). Клиент инкапсулирует исходное HTTP-сообщение (запрос или ответ) в ICAP-запрос и отправляет его на сервер.
- ICAP-сервер — это устройство, которое принимает трафик от клиента, обрабатывает его и возвращает результат. Роль ICAP-сервера могут выполнять серверы антивирусной проверки, системы DLP или сервисы для модификации контента.

Протокол определяет два основных режима обработки трафика, которые соответствуют направлению движения данных:

- Режим модификации запроса (Request Modification, REQMOD). В этом режиме ICAP-клиент отправляет на сервер HTTP-запрос пользователя. Это актуально, например, при загрузке файла на веб-ресурс (метод POST), чтобы проверить отправляемый контент на наличие вирусов или конфиденциальных данных.
- Режим модификации ответа (Response Modification, RESPMOD). В этом режиме клиент отправляет на сервер HTTP-ответ от веб-сервера. RESPMOD используется, когда пользователь скачивает файл: ICAP-сервер проверяет загружаемый объект на вредоносный код до того, как он попадет к пользователю

Помимо основных методов REQMOD и RESPMOD, протокол поддерживает метод OPTIONS, который позволяет клиенту узнать возможности сервера (например, поддерживаемые методы) перед отправкой данных. В UserGate SWG метод OPTIONS также используется для мониторинга доступности ICAP-серверов.

При работе с внешними ICAP-серверами UserGate SWG исполняет роль ICAP-клиента, передавая HTTP-трафик на ICAP-серверы для антивирусной проверки или для проверки DLP-системами данных, передаваемых пользователями.

UserGate SWG поддерживает гибкую настройку при работе с ICAP-серверами — вы можете задать правила, согласно которым на ICAP-серверы будет направляться только выборочный трафик, или настроить работу с фермой ICAP-серверов.

Настройка работы с ICAP

Чтобы настроить работу UserGate SWG с внешними ICAP-серверами:

1. Создайте профиль ICAP-сервера.
2. Если необходимо распределять трафик на несколько серверов, вы можете создать правило балансировки трафика на ICAP-серверы.
3. Создайте правило ICAP.

Запросы или ответы будут отправляться на проверку на ICAP-серверы при срабатывании правила ICAP и наличии подходящего профиля ICAP-сервера.

Создание профиля ICAP-сервера

Чтобы создать профиль ICAP-сервера, перейдите в раздел **Настройки → Политики безопасности → ICAP-серверы,** нажмите **Добавить** и укажите необходимые параметры.

Параметр	Описание
Название	Название профиля ICAP-сервера
Описание	Описание профиля ICAP-сервера
IP-адрес	IP-адрес ICAP-сервера
Порт	TCP-порт ICAP-сервера, значение по умолчанию: 1344
Максимальный размер сообщения	Максимальный размер сообщения (в килобайтах), направляемого на ICAP-сервер. Чтобы выполнить проверку связи с сервером без отправки данных, укажите в этом поле значение 0
Период проверки соединения с ICAP-сервером	Интервал времени в секундах, через который UserGate SWG посылает запрос на ICAP-сервер для проверки его доступности.

Параметр	Описание
	Текущее состояние ICAP-сервера отображается в веб-интерфейсе с помощью цветового индикатора
Вес при балансировке	Числовое значение, определяющее относительный вес сервера при балансировке трафика. Запросы распределяются пропорционально заданным весам. Значение 0 исключает сервер из пула балансировки
Максимальное количество соединений	Максимальное количество соединений с сервером, которые могут быть установлены одновременно
Не отправлять данные, если ICAP-сервер недоступен	Отключение отправки данных на ICAP-сервер, когда он недоступен
Путь REQMOD	Настройка работы режима REQMOD: • **Включено** — включение использования режима REQMOD; • **Путь REQMOD** — указание пути в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер. Можно указать путь в следующих форматах: ◦ `/path` — путь на сервере ICAP; ◦ `icap://icap-server:port/path` — указание полного URI
Путь RESPMOD	Настройка работы режима RESPMOD: • **Включено** — включение использования режима RESPMOD; • **Путь RESPMOD** — указание пути в соответствии с требованиями, приведенными в документации на используемый ICAP-сервер. Можно указать путь в следующих форматах: ◦ `/path` — путь на сервере ICAP; ◦ `icap://icap-server:port/path` — указание полного URI
Передавать имя пользователя	Настройка передачи имени пользователя: • **Включено** — отправлять имя пользователя на ICAP-сервер. • **Кодировать в base64** — кодирование имени пользователя в base64. Может потребоваться, если имена пользователей содержат символы национальных алфавитов.

Параметр	Описание
	• **Название заголовка** — заголовок, который будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — `X-Authenticated-User`
Передавать IP-адрес клиента	Настройка передачи IP-адреса клиента: • **Включено** — оправлять IP-адрес пользователя на ICAP-сервер. • **Название заголовка** — заголовок, который будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию — `X-Client-Ip`
Передавать MAC-адрес клиента	Настройка передачи MAC-адреса клиента: • **Включено** — отправлять MAC-адрес пользователя на ICAP-сервер. • **Название заголовка** — заголовок, который будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию — `X-Client-Mac`

Создание ICAP-правила

Чтобы создать ICAP-правило, перейдите в раздел **Настройки → Политики безопасности → ICAP-правила,** нажмите **Добавить** и укажите необходимые параметры.

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Срабатывает только первое правило, в котором выполняются все указанные условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете изменить порядок правил в списке с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» в панели инструментов.

Примечание

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

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Теги	**Указание опционального тега для маркировки правила. Подробнее — в разделе «Теги»**
Описание	Описание правила
Действие	Действие правила: • **Пропустить** — не посылать данные на ICAP-сервер. Создав правило с таким действием, вы можете 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
Вставить	Выбор места расположения правила в общем списке правил
ICAP-серверы	Выбор ICAP-серверов или балансировщика ICAP-серверов, на которые UserGate SWG будет пересылать трафик. В правило можно добавить несколько серверов или балансировщиков. В этом случае при пересылке трафика будет выбран первый доступный сервер или балансировщик из списка
Источник	Зона, списки IP-адресов, списки GeoIP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Каждые пять минут UserGate SWG производит разрешение (resolution) доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи.

Параметр	Описание
	По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса. Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP-адреса и списки IP-адресов или доменов
Пользователи	Список пользователей, 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
Адрес назначения	IP-адреса, GeoIP или списки URL (веб-серверов) назначения трафика. Список URL должен включать только имена доменов. **Важно!** **Строки с символом «*» в таких списках не работают (игнорируются).** Обработка трафика происходит по следующей логике: • условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов или доменов; • условия объединяются по «И», если указаны GeoIP-адреса и списки IP-адресов или доменов
Типы контента	Система позволяет работать с видео, аудио, изображениями, исполняемыми файлами и другими типами данных. Вы можете создавать собственные группы типов контента. Подробнее о работе с типами контента — в разделе «Типы контента»
Категории	Списки категорий UserGate URL filtering
URL	Списки URL

Параметр	Описание
HTTP-метод	Тип HTTP-метода, применяемого в запросах (обычно POST или GET). При отключенной функции SSL Inspection возможно использование метода CONNECT
Сервис	Указание типа сервиса (HTTP)

Работа с несколькими ICAP-серверами

UserGate SWG поддерживает работу с несколькими серверами ICAP. В общем случае, без балансировки, данные передаются на ICAP-серверы по порядку их перечисления. В случае если ICAP-сервер не отвечает, работа UserGate SWG зависит от параметра **Действие** в правилах ICAP:

- **Пропустить** — запрос не передается 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.

Балансировку трафика на ICAP-серверы можно настроить с помощью правил балансировки нагрузки, подробнее — в разделе «Балансировка нагрузки».

ГЛОБАЛЬНЫЙ ПОРТАЛ

Общие сведения

Веб-портал, публикация через reverse-прокси, наряду с правилами DNAT и трансляции портов, позволяют опубликовать ресурсы, находящиеся внутри компании, пользователям из интернета.

При наличии публикаций внутренних ресурсов с помощью DNAT и трансляции портов, reverse-прокси, веб-портала порядок обработки правил следующий:

1. Правила DNAT и трансляции портов.

2. Правила веб-портала. Если имя узла в запросе совпало с именем узла веб-портала, и номер порта в запросе совпал с номером порта, указанного для работы веб-портала, то срабатывают правила веб-портала.

3. Правила reverse-прокси.

Веб-портал (SSL VPN)

С помощью веб-портала вы можете предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удаленных или мобильных пользователей, используя при этом только протокол HTTPS. Эта технология не требует установки специального клиента VPN, достаточно обычного веб-браузера.

> **Примечание**
> **Если на целевых HTTP-ресурсах настроена аутентификация Kerberos или NTLM, UserGate SWG может производить аутентификацию по технологии SSO (необходим настроенный LDAP-коннектор с загруженным keytab-файлом). При этом, аутентификация на самом UserGate SWG также должна быть настроена через Kerberos/NTLM. Так как UserGate SWG передает данные прозрачно, форма аутентификации при ответе сайта с ошибкой 401 (Unauthorized) не передается клиенту веб-портала.**

> **Примечание**
> **Для создания защищенного соединения с веб-серверами UserGate SWG использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. В связи с этим, перед тем, как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях `server hello` при установлении соединения.**

Для настройки веб-портала выполните следующие шаги:

1. Включите и настройте веб-портал.

2. Разрешить доступ к сервису веб-портала на необходимых зонах.В разделе **Настройки → Сеть → Зоны** разрешите сервис веб-портала для

выбранных зон (обычно зона Untrusted). Разрешение откроет доступ к порту сервиса, который был указан в настройках веб-портала.

3. Добавьте публикуемые ресурсы на веб-портал.

Настройка общих параметров веб-портала

Для включения и настройки общих параметров веб-портала перейдите в раздел **Настройки → UserGate → Настройки**, перейдите в блок Веб-портал и настройте необходимые параметры.

Параметр	Описание
Включено	Включение или отключение веб-портала
Имя хоста	Указание имени узла, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. Это имя должно определяться службами DNS в IP-адрес интерфейса UserGate SWG, входящего в зону, на которой разрешен сервис веб-портала
Порт	Указание порта TCP, который будет использоваться сервисом веб-портала. Порт вместе с именем узла образуют URL для подключения пользователей в виде `https://имя_хоста:порт`
Профиль аутентификации	Выбор профиля аутентификации пользователей для подключения к веб-порталу. Профиль аутентификации указывает метод аутентификации, например AD-коннектор или локальный пользователь. Также в профиле аутентификации вы можете указать требование использовать многофакторную аутентификацию для доступа к веб-порталу. Подробнее о профилях аутентификации — в разделе «Профили аутентификации»
Шаблон страницы аутентификации	Выбор шаблона страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Вы также можете создать свою страницу аутентификации. Подробнее — в разделе «Шаблоны страниц»
Шаблон портала	Выбор шаблона веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Вы также можете создать свой шаблон веб-портала. Подробнее — в разделе «Шаблоны страниц»

Параметр	Описание
Предлагать выбор домена AD/LDAP на странице аутентификации	Разрешить выбор домена на странице аутентификации веб-портала
Показывать CAPTCHA	При включении этой опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации веб-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе «Профили SSL»
Сертификат	Сертификат, который будет использоваться для создания HTTPS-соединения. Если выбран режим **Автоматически**, используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе «Управление сертификатами»
Аутентификация пользователя по сертификату	Если опция выбрана (PKI), система будет запрашивать у браузера пользовательский сертификат. Пользовательский сертификат должен быть добавлен в список сертификатов узла, ему должна быть назначена роль **Пользовательский сертификат** и назначен соответствующий пользователь. Подробнее о пользовательских сертификатах — в разделе «Управление сертификатами»

Добавление публикуемых ресурсов на веб-портал

Чтобы добавить на веб-портал URL внутренних ресурсов, к которым необходим доступ внешних пользователей, перейдите в раздел **Настройки → Глобальный портал → Веб-портал,** нажмите **Добавить** и укажите необходимые параметры публикуемого ресурса.

Параметр	Описание
Включено	Включение или отключение публикации
Название	Название публикации
Описание	Описание публикации
URL	URL ресурса, который необходимо опубликовать через веб-портал. Указывайте полный URL, начиная с `http://`, `https://`, `ftp://`, `ssh://` или `rdp://`

Параметр	Описание
	Важно! Для публикации терминальных серверов отключите опцию, требующую Network Level Authentication в свойствах RDP-доступа на серверах терминального доступа. Аутентификацию пользователей для доступа к серверам в этом 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 непосредственно к указанному домену. Домены прямого доступа должны быть локальными и их разрешение должно происходить через DNS-сервер, установленный внутри локальной сети. При указании домена прямого доступа нужно выбрать профиль SSL. Выбор сертификата в этом случае не является обязательным. Если сертификат не выбран, он будет сгенерирован UserGate SWG
Проверять авторизацию для RDP-сессий	Разрывать сессию RDP по завершению аутентификации на веб-портале на стороне сервера
Включить прозрачную аутентификацию	Прозрачная аутентификация позволяет аутентифицировать пользователя на опубликованном для него приложении. Для аутентификации будут использованы те же данные, что пользователь ввел при входе на веб-портал. Для успешной работы этой опции необходимо, чтобы опубликованное приложение поддерживало прозрачную аутентификацию
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о профилях SSL — в разделе «Профили SSL»
Сертификат	Сертификат, который будет использоваться для для создания HTTPS-соединения между UserGate SWG и сервером. Если выбран режим **Выбрать сертификат**, используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Подробнее о ролях сертификатов — в разделе «Управление сертификатами»
Иконка	Выбор значка для отображения публикуемого ресурса на веб-портале. Вы можете указать один из предоставленных значков, указать внешний URL, по которому доступен значок или загрузить свой значок

Параметр	Описание
Вспомогательные URL	Указание вспомогательных 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	Указание списка пользователей или группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL

Очередность публикаций на веб-портале определяет порядок отображения их пользователю. Вы можете менять очередность публикаций с помощью мыши или с помощью значков «Выше», «Ниже», «Наверх», «Вниз» внизу страницы

Публикация ресурсов с помощью reverse-прокси

UserGate SWG поддерживает публикацию веб-серверов в режиме сервера reverse-прокси. Доступ к веб-серверам и безопасность соединений с ними контролируются настраиваемыми правилами reverse-прокси.

Режим сервера reverse-прокси предоставляет следующие возможности:

- Балансировка нагрузки. Если обработку запросов к приложению выполняют несколько веб-серверов, сервер reverse-прокси может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- Переопределение URL-адресов. Сервер reverse-прокси может выполнять подмену путей и доменных имен в запросах, чтобы перенаправить их на разные веб-серверы, помогая таким образом разделить трафик для разных приложений.
- Управление доступом к веб-серверам. Сервер reverse-прокси может блокировать попытки доступа по идентификационной строке клиентского приложения (user agent) и нежелательным адресам.
- Поддержка SSL-подключения. Сервер reverse-прокси может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.

Чтобы опубликовать веб-сервер:

1. Создайте один или несколько серверов reverse-прокси.

2. Если для доступа к удаленному приложению развернуто несколько веб-серверов, создайте для них правило балансировки.

3. Создайте правила reverse-прокси, которые будут определять условия публикации веб-сервера или группы веб-серверов.

> **Важно!**
> **Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в параметрах правила.**

4. В разделе **Настройки → Сеть → Зоны** в параметрах контроля доступа той зоны, в которой необходимо разрешить доступ к внутренним ресурсам, разрешите сервис **Reverse-прокси**.

Создание сервера reverse-прокси

Чтобы создать сервер reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Серверы reverse-прокси** нажмите **Добавить**.

2. В окне **Настройка сервера reverse-прокси** укажите название, IP-адрес или FQDN и TCP-порт публикуемого веб-сервера.

3. Если необходимо, настройте остальные параметры:

- Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate SWG до публикуемого веб-сервера. Если этот флажок установлен, убедитесь, что на шаге 2 вы указали порт для защищенного соединения.

> **Примечание**
> **Для создания защищенного соединения с веб-серверами UserGate SWG использует алгоритмы шифрования GCM с повышенной устойчивостью к уязвимостям и атакам. Поэтому, перед тем как настроить передачу трафика по защищенному соединению, необходимо убедиться, что веб-сервер поддерживает алгоритмы шифрования GCM и согласует их в сообщениях «server hello» при установлении соединения.**

- Установите флажок **Проверять SSL-сертификат**, чтобы включить проверку подлинности SSL-сертификата, установленного на публикуемом веб-сервере. Доступно, если установлен флажок **HTTPS до сервера**.
- Установите флажок **Не изменять IP-адрес источника**, чтобы сохранять оригинальный IP-адрес источника в запросах. Если флажок снят, IP-адрес источника заменяется на IP-адрес UserGate SWG.

> **Важно!**
> **Если установлен флажок «Не изменять IP-адрес источника», для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UserGate SWG, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UserGate SWG или можно настроить статические маршруты через UserGate SWG для «белых» IP-адресов источников.**

4. Сохраните изменения.

Балансировка серверов reverse-прокси

Если для доступа к удаленному приложению развернуто несколько веб-серверов, вы можете распределять клиентские запросы между ними с помощью правил балансировки нагрузки.

Чтобы создать правило балансировки серверов reverse-прокси:

1. В разделе **Глобальный портал** создайте серверы reverse-прокси для удаленного приложения. Убедитесь, что в окне **Настройка сервера**

reverse-прокси для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.

2. В разделе **Настройки → Политики сети → Балансировка нагрузки** нажмите **Добавить** и выберите **Добавить балансировщик reverse--прокси**.

3. В окне **Настройка правила балансировки reverse-прокси** на вкладке **Общие** укажите название правила и включите его.

4. На вкладке **Серверы reverse-прокси** добавьте серверы, на которые будет распределяться нагрузка.

5. Сохраните изменения.

Создание правила публикации reverse-прокси

Правила публикации reverse-прокси позволяют фильтровать запросы к веб-серверам, контролировать доступ к ним и обеспечивать безопасное соединение.

Созданные правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете мышью перетаскивать правила в списке для изменения порядка применения правил.

Чтобы создать правило reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** нажмите **Добавить**.

2. В окне **Настройка правила reverse-прокси** на вкладке **Общие**:

- Включите правило и укажите его название.
- Если необходимо, укажите теги для маркировки правила. Подробнее — см. в разделе «Теги».
- В списке **Сервер reverse-прокси** выберите сервер или балансировщик reverse-прокси, которому UserGate SWG будет пересылать запросы.
- Укажите порты, на которых UserGate SWG будет слушать входящие запросы.

- Установите флажок **Использовать HTTPS**, если необходимо, чтобы обмен трафиком с клиентом проходил по защищенному соединению.
- Если флажок **Использовать HTTPS** установлен:
  - Выберите профиль SSL, поддерживающий нужные протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи.
  - Укажите сертификат веб-сервера для поддержки HTTPS-соединения.
  - Если необходимо, включите авторизацию пользователя по сертификату, выбрав значение **PKI**, и затем укажите предварительно созданный профиль клиентских сертификатов. Подробнее — см. в разделе «Профили клиентских сертификатов».
- С помощью параметра **Вставить** настройте расположение правила в списке.

> **Примечание**
> **Параметр доступен, если в списке уже есть другие правила.**

3. На вкладке **Источник** выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов, доменных имен или GeoIP-адреса (не более 15 адресов), для которых будет разрешен обмен трафиком с веб-серверами.

> **Важно!**
> **Не добавляйте в списки строки с символом «*», они будут игнорироваться.**

> **Примечание**
> **Вы также можете настроить правило, игнорирующее источники трафика в указанных зонах и с выбранными адресами. Для этого на вкладке «Источник» нужно сформировать список нежелательных зон и/или адресов и в соответствующих блоках параметров включить «Инвертировать».**

Примечание

Каждые пять минут UserGate SWG производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate SWG автоматически обновляет значение IP-адреса.

Важно!

Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменных имен; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

4. Если на шаге 2 выбраны использование HTTPS и авторизация по клиентскому сертификату, на вкладке **Пользователи**, если необходимо, сформируйте список пользователей и групп, для которых будет применяться это правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее — см. в разделе «Пользователи и группы».

5. На вкладке **Назначение** укажите IP-адреса, назначенные на интерфейсы, которые принимают входящие соединения. Этот параметр следует настраивать, когда на один интерфейс UserGate SWG назначено несколько IP-адресов либо несколько интерфейсов подключены к сети.

Примечание

Вы также можете настроить правило, игнорирующее входящие соединения на указанные адреса. Для этого на вкладке «Назначение» укажите адреса и включите «Инвертировать».

Важно!

Обработка трафика происходит по следующей логике: условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

6. На вкладке **Useragent**, если необходимо, добавьте идентификационные строки клиентских браузеров, для которых будет разрешен обмен трафиком с веб-серверами.

> **Примечание**
> **Вы также можете настроить правило, игнорирующее определенные браузеры, запрашивающие доступ к веб-серверу. Для этого на вкладке «Useragent» нужно сформировать список нежелательных браузеров и включить «Инвертировать».**

7. На вкладке **Подмена путей** настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

8. На вкладке **Доверенные браузеры** выберите созданные ранее в разделе **Настройки → Пользователи и устройства → Доверенные браузеры** подключения к серверам регистрации доверенных браузеров. Подробнее о создании подключения к серверу регистрации доверенных браузеров — в разделе «Работа с доверенными браузерами».

9. На вкладке **Обработка заголовков** установите флажки для дополнительных HTTP-заголовков, которые будут добавлены в исходный запрос. Если заголовки уже содержатся в запросе, их значения будут переписаны.

Вы можете создать правила для обработки следующих дополнительных HTTP-заголовков:

- `X-Forwarded-Host`: содержит значение заголовка Host из исходного запроса. Это значение требуется внутреннему веб-серверу для уточнения, какой контент следует вернуть клиенту, а также при журналировании и балансировке нагрузки.
- `X-Forwarded-Proto`: содержит сведения о протоколе исходного запроса, которые позволяют на стороне внутреннего веб-сервера выполнять переадресацию на безопасный ресурс либо генерировать корректные ссылки.
- `X-Forwarded-Port`: передает исходный порт подключения клиента, который необходим для генерации корректных ссылок на стороне внутреннего веб-сервера.

При передаче запроса промежуточные узлы (такие, как сервер reverse-прокси или балансировщик нагрузки) меняют значения в стандартных

заголовках запроса, обеспечивая таким образом безопасность внутренних ресурсов или правильную маршрутизацию. Но внутреннему веб-серверу для корректной обработки запроса требуется исходная информация, переданная клиентом. Например, для определения геолокации клиента или сбора статистики. Чтобы обеспечить корректную работу внутренних ресурсов, серверы reverse-прокси или другие устройства могут передавать исходные данные запроса в дополнительных HTTP-заголовках.

10. Сохраните изменения.

Подмена путей в правилах reverse-прокси

В этом разделе описан порядок работы функции подмены путей в правилах reverse-прокси.

Подмена путей в правилах reverse-прокси используется для перенаправления HTTP-запроса пользователя на иной путь. Таким образом вы можете управлять разделением трафика для разных сервисов. Например, пользователь выполнил запрос на `example.com/path1`, а сервер reverse-прокси перенаправляет запрос на `example.local/path2`.

Чтобы настроить подмену путей в правиле reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** создайте или выберите правило.

2. В окне **Настройка правила reverse-прокси** на вкладке **Подмена путей** нажмите **Добавить** и заполните поля:

   - **Изменить с** — домен и/или путь URL, которые требуется изменить. Если в поле **Изменить с** указан домен, то правило reverse-прокси будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.

   - **Изменить на** — домен и/или путь URL, на которые требуется заменить старый.

3. Сохраните правило.

При обработке HTTP-запроса сработает правило reverse-прокси, паттерн которого в поле **Изменить с** совпадет с путем URL в запросе. При срабатывании правила reverse-прокси происходит подмена пути в HTTP-запросе: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос

пользователя не попадет ни под одно правило reverse-прокси, в ответ на него будет получена ошибка: 403 Forbidden.

Условия проверки соответствия

Синтаксис HTTP-запроса представляет собой следующую последовательность: `<scheme>://<host>:<port>/<path>`.

Паттерн в поле **Изменить с** состоит из последовательности `<host>/<path>` и должен удовлетворять следующим условиям:

- `<host>` — обязательный параметр. Совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно. Все названия узлов приводятся к нижнему регистру.
- `<path>` — необязательный параметр. Без него будет выбираться любой путь. Совпадение префиксное (не строгое).
- Паттерн из поля **Изменить с** и паттерн из поля **Изменить на** должны оба либо заканчиваться символом «/», либо не содержать его в конце. В противном случае подмена путей сработает некорректно.
- Схема (`<scheme>`) запроса игнорируется и не изменяется.
- Порт (`<port>`) запроса игнорируется и не изменяется.

При совпадении запроса и исходного паттерна правило считается сработавшим.

В таблице ниже приведены примеры срабатываний паттернов.

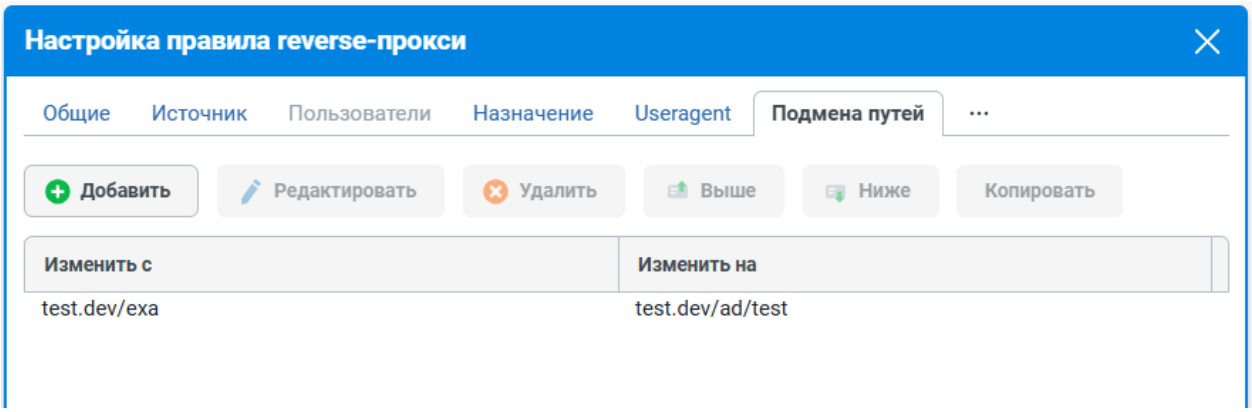
Исходный паттерн в правиле reverse-прокси	Примеры запросов, на которые правило сработает	Примеры запросов, на которые правило не сработает
test.dev	• test.dev • test.dev/ • test.dev/* • http://test.dev • test.dev:<любой порт>	• abc.com • test.develop • test.dev.lol
tesT.deV	• test.deV • tesT.deV/ • TEST.dev	• abc.com • test.develop • test.dev.lol

Исходный паттерн в правиле reverse-прокси	Примеры запросов, на которые правило сработает	Примеры запросов, на которые правило не сработает
test.dev/co	• test.dev/co* • http://test.dev/co* • test.dev:<любой порт>/co*	• test.dev.lol/co* • test.dev/kool*
http://test.dev	• http://test.dev • http://test.dev/* • http://test.dev:<любой порт> • http://test.dev:<любой порт>/ • http://test.dev:<любой порт>/*	• http://test.develop
http://test.dev/co	• http://test.dev/co* • http://test.dev:<любой порт>/co	• http://test.dev/cool*

Правила подмены путей

Рассмотрим детальнее логику работы подмены путей.

Для этого создадим правило `test.dev/exa` → `test.dev/ad/test` и сделаем несколько запросов.



1) Запрос на `test.dev/exalala`.

Параметр `path = /exalala`. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается `/exa`. Оставшаяся часть: `lala`.

При дальнейшей конвертации берется полученный остаток `lala` и добавляется к концу path паттерна из поля **Изменить на**, то есть: `/ad/test + lala`. В итоге, после преобразования, параметр path получает значение `/ad/testlala`.

Таким образом, конечный запрос будет отправлен по адресу `test.dev/ad/testlala`.

2) Запрос на `test.dev/exa/vvv`.

Параметр `path = /exa/vvv`. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается `/exa`. Оставшаяся часть: `/vvv`.

При дальнейшей конвертации берется полученный остаток `/vvv` и добавляется к концу path паттерна из поля **Изменить на**, то есть: `/ad/test + /vvv`. В итоге, после преобразования, параметр path получает значение `ad/test/vvv`.

Таким образом, конечный запрос будет отправлен по адресу `test.dev/ad/test/vvv`.

БИБЛИОТЕКИ ЭЛЕМЕНТОВ

Общие сведения

Библиотеки элементов содержит в себе все записи, адреса сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил UserGate SWG.

Первоначальные данные библиотек поставляются вместе с продуктом. Вы можете добавлять необходимые элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, обновляются автоматически при наличии специальной лицензии. Подробнее о лицензировании — в разделе «Лицензирование UserGate SWG».

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, UserGate SWG 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 UserGate SWG использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые компанией UserGate. Эти словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Подробнее о лицензии на продукт — в разделе «Лицензирование».

Наименование словаря	Описание
Соответствие списку запрещенных материалов Министерством Юстиции Российской Федерации	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции Российской Федерации
Соответствие списку запрещенных материалов республики Казахстан	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции республики Казахстан
Суицид	Морфологический словарь, содержащий перечень слов и фраз суицидальной направленности
Терроризм	Морфологический словарь, содержащий перечень слов и фраз террористической направленности
Нецензурная лексика	Морфологический словарь, содержащий перечень слов и фраз, относящихся к нецензурной лексике
Азартные игры	Морфологический словарь, содержащий перечень слов и фраз, относящихся к азартным играм
Наркотики	Морфологический словарь, содержащий перечень слов и фраз наркотической направленности

Наименование словаря	Описание
Соответствие ФЗ-436 (Защита детей)	Морфологический словарь, содержащий перечень слов и фраз тематик, нежелательных для детей
Порнография	Морфологический словарь, содержащий перечень слов и фраз порнографической направленности
Бухгалтерия (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в бухгалтерии
Маркетинг (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в маркетинге
Персональные данные (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, встречающихся в персональных данных
Финансы (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в финансах
Юридический (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в юриспруденции

Для создания собственного морфологического списка:

1. В разделе **Настройки → Библиотеки → Морфология** в блоке **Списки** морфологии нажмите **Добавить**, укажите название нового списка и его вес.

2. В блоке **Слова** нажмите **Добавить**, укажите слова или фразы с соответствующими им весами. При добавлении слов 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.

Вы можете создавать свои словари и централизованно распространять их на все устройства UserGate, имеющиеся в организации. Для создания такой базы:

1. Создайте файл с необходимыми фразами. Например, файл `list.txt` может содержать список слов в следующем формате:

```
!word1
!word2
!word3
```

```
word4 50
...
Lastword
```

Вес слова можно указать. По умолчанию он равен 100.

2. Создайте архив, содержащий этот файл. Например, ZIP-архив с именем `list.zip`.

3. Создайте файл с версией словаря. Например, файл `version.txt`, внутри него указан номер версии базы. Необходимо инкрементировать это значение при каждом обновлении морфологического словаря.

4. Разместите файлы (`list.zip` и `version.txt`) на веб-сервере.

5. Создайте морфологический список и укажите URL для обновления словаря.

На каждом устройстве UserGate создайте морфологическую базу. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. Устройство UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений.

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

При ручном вводе также можно использовать следующие символы:

Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновлений должна выполняться каждый час.

Дефис (-) — для указания диапазона значений.

Запятая (,) — в качестве разделителя значений.

Косая черта (/) — для указания шага между значениями.

> **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. Это сократит количество возможных вариантов фраз, но оставит все фразы с требуемым смыслом.**

Устройство UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется в формате md5. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Для фильтрации по морфологическому содержанию страницы создайте правило фильтрации контента, содержащее один или несколько морфологических списков.Подробнее — в разделе «Фильтрация контента».

IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил ГUserGate SWG. Первоначальный список адресов поставляется вместе с продуктом. Вы можете добавлять необходимые элементы в процессе работы. Для добавления нового списка адресов выполните следующие шаги:

Шаг	Описание
1. Создайте список.	На панели **Группы** нажмите **Добавить**: • Укажите название списка IP-адресов. • Добавьте описание списка (опционально). • Указжите уровень угрозы адресов в списке (параметр для визуального отображения, какие адреса не представляют особой угрозы, а какие лучше запретить). • Выберите тип списка (локальный или обновляемый по URL обновления)
2. Укажите адрес обновления списка (для обновляемых списков).	Укажите адрес сервера, где находится обновляемый список
3. Добавьте IP-адреса.	На панели **Адреса из выбранной группы** нажмите **Добавить** и укажите 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

Вы можете создавать свои списки IP-адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Шаг	Описание

1. Создайте файл с необходимыми IP-адресами.	Создайте 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`

2. Создайте архив, содержащий этот файл.	Поместите файл в архив zip с именем `list.zip`
3. Создайте файл с версией списка.	Создайте файл `version.txt`, внутри него укажите номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка

Шаг	Описание
4. Разместите файлы на веб-сервере.	Разместите у себя на сайте `list.zip` и `version.txt`, чтобы они были доступны для скачивания
5. Создайте список IP-адресов и укажите URL для обновления.	На каждом UserGate SWG создайте список IP-адресов. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG 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/`. Вы можете выбрать одно из предустановленных значений расписания или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями.

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется в формате md5. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

User agent браузеров

С помощью фильтрации по User agent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список User agent поставляется вместе с продуктом. Для фильтрации по типу User agent необходимо выполнить следующие действия:

Шаг	Описание
1. Создайте список Useragent.	В панели **Категории** нажмите **Добавить** и укажите название нового списка User agent
2. Добавьте необходимые User agent браузеров в новый список.	В панели **Шаблоны user agent** добавьте необходимый User agent. Список строк User agent можно найти по ссылке
3. Создайте правило фильтрации контента, содержащее один или несколько списков.	Подробнее — в разделе «Фильтрация контента»

Вы можете создавать свои списки User agent и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Шаг	Описание
1. Создайте файл с необходимыми User agent.	Создайте файл `list.txt` со списком `Useragent`.
2. Создайте архив, содержащий этот файл.	Поместите файл в архив zip с именем `list.zip`
3. Создайте файл с версией списка.	Создайте файл `version.txt`, внутри него укажите номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
4. Разместите файлы на веб-сервере.	Разместите у себя на сайте `list.zip` и `version.txt`, чтобы они были доступны для скачивания.

Шаг	Описание
5. Создайте список User agent и указать URL для обновления.	На каждом UserGate SWG создайте список User agent. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UseGate SWG будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Вы можете выбрать одно из предустановленных значений расписания или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями.

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш-сумма `list.zip`, после чего сохраняется в формате md5. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Типы контента

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа *.doc.

Существует возможность подписки на типы контента, предоставляемые разработчиками UserGate. Такие списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Подробнее о лицензии на продукт — в разделе «Лицензирование».

Для фильтрации по типу контента выполните следующие действия:

Шаг	Описание
1. Создайте список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3	В панели **Категории** нажмите **Добавить**, укажите название нового списка типа контента; опционально — описание списка и URL обновления
2. Добавьте необходимые типы контента в новый список	Добавьте необходимый тип контента в список в формате MIME. Различные типы контента и их описание доступны по ссылке. Например, для блокировки документов типа `*.doc` необходимо добавить тип контента «`application/msword`»
3. Создайте правило фильтрации контента, содержащее один или несколько списков	Подробнее — в разделе «Фильтрация контента»

Вы можете создавать свои списки типов контента и централизованно распространять их на все узлы UserGate. Для создания такого списка необходимо выполнить следующие действия:

Шаг	Описание
1. Создайте файл с необходимыми типами контента	Создать файл `list.txt` со списком типов контента
2. Создайте архив, содержащий этот файл	Поместить файл в архив zip с именем `list.zip`
3. Создайте файл с версией списка	Создать файл `version.txt`, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
4. Разместите файлы на веб-сервере	Разместить у себя на сайте `list.zip` и `version.txt`, чтобы они были доступны для скачивания

Шаг	Описание
5. Создайте список типа контента и укажите URL для обновления	На каждом UserGate SWG создайте список типа контента. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Вы можете выбрать одно из предустановленных значений расписания или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновлений должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate SWG будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется в формате md5. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Списки URL

Списки URL используются в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет ряд собственных обновляемых списков. Для использования этих списков необходима соответствующая лицензия. Подробнее о лицензировании UserGate SWG — в разделе «Лицензирование».

Наименование списка	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля
Соответствие списку запрещенных URL Министерства Юстиции РФ	Список содержит URL, запрещенные Министерством Юстиции Российской Федерации
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ
Список фишинговых сайтов	Список содержит URL фишинговых сайтов
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен по ссылке
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Список доступен по ссылке

Вы также можете создать собственные списки URL в веб-консоли или в интерфейсе командной строки UserGate SWG.

Для создания списка в веб-консоли:

1. В разделе **Настройки → Библиотеки → Списки URL** нажмите **Добавить** и задайте название и описание нового списка.

2. Выберите тип списка (локальный или обновляемый). Для обновляемого списка укажите URL обновления и настройте расписание скачивания обновлений.

3. Установите категорию создаваемого списка в поле **Чувствительность к регистру**:

- **Чувствительный к регистру** — список URL-адресов, чувствительных к регистру букв в адресе.
- **Нечувствительный к регистру** — список URL-адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах.
- **Домен** — список адресов доменов. При добавлении в этот список записи вида `http://test.ru`, она будет преобразована в запись вида `test.ru`.

> **Важно!**
> **Категория списка задается при его создании. Изменить категорию после создания списка нельзя.**

> **Примечание**
> **При использовании URL-списка ищется весь URL запроса; при использовании доменного списка — только имя узла. При сохранении URL в доменный список в процессе преобразования из него удаляется все лишнее, остается только имя узла.**

4. Добавьте необходимые записи в новый список.

В списках можно использовать специальные символы:

- * — любое количество любых символов;
- ^ — начало строки;
- $ — конец строки.

Правило фильтрации контента может содержать один или несколько списков. Подробнее — в разделе «Фильтрация контента».

> **Внимание!**
> **Спецсимволы не работают в списках исключений для блокировки рекламы. Не рекомендуется использовать спецсимволы в записях таких списков.**

Если необходимо заблокировать строго определенный адрес, используйте символы начала (^) и конца ($) строки. Например:

```
^http://domain.com/exacturl$
```

Если необходимо заблокировать адрес и все страницы внутри него, используйте символ ^ в начале строки, без символа $ в конце. Например:

```
^http://domain.com/exacturl/
```

Чтобы заблокировать домен со всеми возможными URL, укажите только имя домена без специальных символов:

```
domain.com
```

Примеры интерпретации URL-записей приведены в таблице.

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
yahoo.com или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com; mail.yahoo.com; а также: qweryahoo.com	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com; http://mail.yahoo.com;	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123;	Блокируются любые вхождения yahoo.com: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123;

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
		https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyahoo.com/	http://qwertyahoo.com/ Не блокируются вхождения типа: https://ya.ru/YAHoo.cOM	http://qwertyahoo.com/ https://ya.ru/YAHoo.cOM
^mail.yahoo.com$	Заблокирован только mail.yahoo.com	Заблокированы: http://mail.yahoo.com; https://mail.yahoo.com; а также любые ссылки на этом домене, например: http://mail.yahoo.com/personal-finance Т. е., блокируется весь домен mail.yahoo.com и все URL этого домена	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола
^mail.yahoo.com/$	Ничего не заблокировано	Заблокированы: http://mail.yahoo.com; https://mail.yahoo.com; и любые ссылки на этом домене, например: https://mail.yahoo.com/personal-finance т. к. при преобразовании списка остается только домен, слеш в этом	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
		случае удалится и реально в списке будет: ^mail.yahoo.com$ т. е. блокируется весь домен mail.yahoo.com и все URL этого домена		
^https://finance.yahoo.com/personal-finance/$	Ничего не заблокировано	Заблокированы: http://finance.yahoo.com; https//finance.yahoo.com; и любые ссылки на этом домене, например: http://finance.yahoo.com/personal-finance/ т.к. после преобразования в списке останется только: ^finance.yahoo.com$ Т. е. блокируется весь домен finance.yahoo.com и все URL этого домена	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ Не заблокируется: http://finance.yahoo.com/personal-finance/ и любое изменение регистра букв в URL: https://finance.yahoo.com/personal-financE/	Заблокируется только запрос https://finance.yahoo.com/personal-finance/ и любое изменение регистра букв в URL: https://finance.yahoo.com/Personal-financE/. Не заблокируется: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не заблокировано	Заблокированы: http://yahoo.com/12345/whatever/; https://yahoo.com/12345/whatever/;	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола	Ничего не заблокируется, поскольку URL должен начинаться с указания протокола

Пример записи	Обработка DNS-запросов	Обработка HTTP-запросов для списка доменов	Обработка HTTP-запросов для списков URL, чувствительных к регистру	Обработка HTTP-запросов для списков URL, нечувствительных к регистру
		т.к. после преобразования в списке будет: ^yahoo.com Т. е. заблокируется домен yahoo.com и все URL этого домена		

Администратор имеет возможность создавать собственные обновляемые списки и централизованно распространять их на все узлы UserGate SWG. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, `list.txt`) со списком URL в следующем формате:

```
www.site1.com/url1
www.site2.com/url2
...
www.siteend.com/urlN
```

2. Создайте архив, содержащий этот файл (например, `list.zip`).

3. Создайте файл с версией списка (например, `version.txt`). Внутри файла укажите номер версии списка (например, 3). Необходимо инкрементировать это значение при каждом обновлении списка.

4. Разместите файлы архива и версии (например, `list.zip` и `version.txt`) на веб-сервере, чтобы они были доступны для скачивания.

5. На каждом UserGate SWG создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

> **Примечание**
> **URL списка задается в формате:** `http://x.x.x.x/` **или** `ftp://x.x.x.x/`.

В свойствах списка можно настроить расписание обновления.

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

При ручном вводе также можно использовать следующие символы:

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

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в Linux можно с помощью команды:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется с расширением `.md5`. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах UserGate SWG. Первоначальный список поставляется вместе с продуктом. Вы можете добавлять необходимые элементы

в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

1. Создайте календарь.В разделе **Настройки → Библиотеки → Календари** на панели **Группы** нажмите **Добавить**, укажите название календаря и его описание.

2. Добавить временные интервалы в календарь На панели **Элементы** нажмите **Добавить** и добавьте интервал. Задайте название интервалу и укажите временные параметры.

Полосы пропускания

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую вы можете в дальнейшем использовать в правилах управления полосой пропускания. Подробнее о правилах управления полосой пропускания — в разделе «Пропускная способность».

Первоначальный список поставляется вместе с продуктом. Вы можете добавлять необходимые элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

1. Создайте полосу пропускания. В разделе **Настройки → Библиотеки → Полосы** пропускания нажмите **Добавить**, задайте название и описание полосы пропускания.

2. Укажите скорость полы пропускания в Кбит/сек.

3. Укажите значение DSCP для QoS. Это опциональный параметр. Если установлен, будет прописываться в каждый IP-пакет. Диапазон от 0 до 63.

Шаблоны страниц

С помощью шаблонов страниц вы можете настраивать отображение страниц блокировки, авторизации, предупреждений и сетевых ошибок. Список шаблонов страниц, которые поставляются с UserGate SWG, — см. в таблице ниже. Вы можете использовать эти шаблоны в качестве основы для создания пользовательских шаблонов в фирменном стиле компании или на другом языке.

По умолчанию шаблоны страниц настроены на отображение минимальной информации в стандартном оформлении. Но в HTML-коде этих шаблонов содержатся дополнительные блоки информации или интерактивных элементов, которые по умолчанию закомментированы. Вы можете раскомментировать их: например, на страницу блокировки вывести дату блокировки или форму ввода логина и пароля администратора для снятия блокировки.

Чтобы создать пользовательский шаблон страницы:

1. В разделе **Настройки → Библиотеки → Шаблоны страниц** нажмите **Добавить** и создайте шаблон страницы нужного типа.

2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.

3. Используя текстовый редактор, откройте страницу, найдите закомментированные блоки для отображения дополнительных сведений и раскомментируйте нужные.

> **Примечание**
> **Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.**

4. Импортируйте измененную страницу в созданный шаблон.

Шаблон	Описание
Blockpage (EN) и **Blockpage (RU)**	Стандартные шаблоны страницы блокировки на английском и русском языках. При необходимости страница блокировки может содержать дополнительную информацию об имени блокирующего узла и группах, в которых состоит пользователь. Для отображения на странице блокировки необходимо раскомментировать соответствующие строки в html-коде шаблона
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 для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон

Шаблон	Описание
Captive portal user auth + policy (EN) и **Captive portal user auth + policy (RU)**	выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принять правила политики доступа. При успешной авторизации пользователь получает доступ в интернет
Captive portal: email auth (EN) и **Captive portal: email auth (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе, подтвердив указанную электронную почту. Для корректной работы шаблонов необходимо настроить параметры раздела **Оповещения** в Captive-профиле
Captive portal: SMS auth (EN) и **Captive portal: SMS auth (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы шаблонов необходимо настроить параметры раздела **Оповещения** в Captive-профиле
Captive portal policy (EN) и **Captive portal policy (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принять правила политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы шаблона требуется установить метод **Принять политику** в качестве метода аутентификации в Captive-профиле
Captive portal user session (EN) и **Captive portal user session (RU)**	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps
Content warning (EN) и **Content warning (RU)**	Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием **Предупредить**
FTP client (EN) и **FTP client (RU)**	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP
SSL VPN (EN) и **(RU)**	Шаблоны на английском и русском языках для отображения страницы веб-портала
SSL VPN RDP (EN) и **(RU)**	

Шаблон	Описание
	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал
SSL VPN SSH (EN) и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал
TOTP INIT PAGE (EN) и **TOT P INIT PAGE (RU)**	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей
NETWRK ERROR PAGE (RU) и **NETWORK ERROR PAGE (EN)**	Шаблоны на русском и английском языках для отображения страницы сетевых ошибок от прокси-сервера

Категории URL

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, вы можете 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. Вы можете добавлять необходимые 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 срабатывани

Наименование	Описание
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:

1. Создайте группу категорий. В разделе **Настройки → Библиотеки → Категории URL** на панели **Группы URL категорий** нажмите **Добавить** и укажите название группы.

2. Добавьте категории. Выделите созданную группу и на панели **Категории** нажмите **Добавить**. Выберите необходимые категории из списка.

В системе определены следующие категории URL:

ID	Уровень риска	Название	Описание
0	Высокий (4)	Неизвестная тематика / Unknown	Сайты без принадлежности к какой-либо категории
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Pop-Ups	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее)
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для

ID	Уровень риска	Название	Описание
			обхождения средств веб-фильтрации и т. д.
4	Очень низкий (1)	Искусство / Arts	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т. д.
5	Очень низкий (1)	Бизнес / Business	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности
6	Очень низкий (1)	Транспорт / Transportation	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества, клубы автолюбителей и т. д.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги
10	Очень высокий (5)	Заражённые сайты / Compromised	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ

ID	Уровень риска	Название	Описание
			без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения
11	Очень низкий (1)	Компьютеры и технологии / Computers and Technology	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах
12	Средний (3)	Преступная деятельность / Criminal Activity	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств,

ID	Уровень риска	Название	Описание
			ресурсы, предлагающие эскорт-услуги
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты
15	Очень низкий (1)	Образование / Education	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости
17	Низкий (2)	Финансы / Finance	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами,

ID	Уровень риска	Название	Описание
			страховых компаниях, кредитных союзах и т. д.
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах
20	Очень низкий (1)	Правительство / Government	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским

ID	Уровень риска	Название	Описание
			оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т. д.
23	Низкий (2)	Наркотики / Illegal Drug	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний
25	Средний (3)	Военные сайты / Military	Информация о военных организациях, военной истории
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний
27	Очень низкий (1)	Новости / News	Новостные сайты: онлайн-журналы, новостные ленты и т. д.
28	Низкий (2)	Некоммерческие и неправительственные	Сайты, посвященные клубам, сообществам, союзам и

ID	Уровень риска	Название	Описание
		организации / Non-profits and NGOs	некоммерческим организациям. Значительное число данных структур созданы в образовательных или благотворительных целях
29	Низкий (2)	Нудизм / Nudity	Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие или продающие нижнее белье, интимную одежду или купальные костюмы
30	Средний (3)	Персональные сайты / Personal Sites	Персональные сайты, созданные отдельными людьми или группами лиц, блоги
31	Очень высокий (5)	Фишинг и мошенничество / Phishing and Fraud	Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных законных ресурсов, что вводит в заблуждение пользователей
32	Очень низкий (1)	Политика / Politics	Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые

ID	Уровень риска	Название	Описание
			предлагают сведения о правах и их защите
33	Очень высокий (5)	Порнография и насилие / Pornography/Sexually Explicit	Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать эротические рассказы и текстовые описания половых актов
34	Низкий (2)	Недвижимость / Real Estate	Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий
35	Низкий (2)	Религия / Religion	Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов
36	Очень низкий (1)	Рестораны и еда / Restaurants and Dining	Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина
37	Очень низкий (1)		

ID	Уровень риска	Название	Описание
		Поисковые системы и порталы / Search Engines and Portals	Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы
38	Низкий (2)	Покупки / Shopping	Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина
39	Средний (3)	Социальные сети / Social Networking	Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами
40	Очень высокий (5)	Спам-сайты / Spam Sites	Сайты, продвижение которых основано на использовании спам-рассылок
41	Очень низкий (1)	Спорт / Sports	Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги
42	Очень высокий (5)	Вредоносное ПО / Malware	Сайты, содержащие нежелательные программы, автоматически загружающиеся и

ID	Уровень риска	Название	Описание
			устанавливающиеся на ПК пользователей. Вирусы вносят изменения в систему и позволяют злоумышленникам получить данные с компьютера без ведома и согласия его владельца
43	Низкий (2)	Фондовый рынок / Stock trading	Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировкам и новостям
44	Очень низкий (1)	Переводчики / Translators	Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных ограничений, так как просмотр сайтов осуществляется с URL сайта онлайн-переводчика
45	Очень низкий (1)	Путешествия / Travel	Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описания мест назначения, реклама гостиниц и казино
46	Низкий (2)	Насилие / Violence	Сайты, содержащие изображения, текстовые описания и пропаганду физического насилия против людей, животных или организаций\сообществ.

ID	Уровень риска	Название	Описание
			Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику
47	Низкий (2)	Оружие / Weapons	Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом
48	Высокий (4)	Веб-почта / Web-based Email	Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем
49	Средний (3)	Общие / General	Сайты, которые не попадают в другие категории, например, пустые веб-страницы
50	Низкий (2)	Отдых и оздоровление / Leisure and Recreation	Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечениям и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т. д.
51	Низкий (2)	Онлайн обучение / Online training and tools	Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации

ID	Уровень риска	Название	Описание
52	Низкий (2)	Юриспруденция / Legal	Сайты юридических фирм, обсуждение и анализ юридических вопросов
53	Низкий (2)	Местные достопримечательности / Local Information	Путеводители и информация для туристов, в том числе о ресторанах и местные достопримечательности
54	Низкий (2)	Справочная информация / Reference and Research	Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации
55	Очень низкий (1)	Форумы с технической или бизнес информацией / Technical or business forums and news groups	Сайты с обсуждениями, относящимся к деловой или технической тематикам
56	Очень низкий (1)	Техническая информация / Technical information and documentation	Сайты, которые предоставляют информацию к технической документации и информации
57	Высокий (4)	Персональные хранилища / Personal Storage	Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных
58	Низкий (2)	CDNs	Сети предоставления контента
59	Низкий (2)	Нецензурная лексика / Profanity	Сайты, содержащие нецензурную лексику
60	Низкий (2)	Профессиональные социальные сети / Professional social networks	Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный

ID	Уровень риска	Название	Описание
			исключительно для бизнеса и профессионалов
61	Очень высокий (5)	Ботнеты / Botnets	Сайты, которые управляют сетями ботов через командно-контрольные центры
62	Низкий (2)	Религиозные культы / Cults	Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера
63	Низкий (2)	Мода и красота / Fashion and Beauty	Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает отзывы, сравнения, а также общую информацию, полезную потребителю
64	Низкий (2)	Поздравительные открытки / Greeting cards	Сайты, которые позволяют людям получать и отправлять поздравительные открытки
65	Очень высокий (5)	Хакерство / Hacking	Сайты, которые способствуют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию

ID	Уровень риска	Название	Описание
			вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации
66	Очень высокий (5)	Криптомайнеры / Cryptocurrency Mining	Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя
67	Очень высокий (5)	Нелегальное ПО / Illegal Software	Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей
68	Высокий (4)	Обмен картинками / Image Sharing	Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники
69	Низкий (2)	Информационная безопасность / Information Security	Сайты, которые предоставляют информацию о законной защите данных, в том числе о новых угрозах и способах борьбы с ними
70	Средний (3)	Сервисы мгновенных сообщений / Instant Messaging	Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т. п.
71	Очень низкий (1)	Сетевые ошибки / Network Errors	Сайты, которым не присвоен IP-адрес

ID	Уровень риска	Название	Описание
72	Средний (3)	Паркованные домены / Parked Domains	К паркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя сайты, находящиеся на реконструкции, папки и базовые страницы веб-серверов
73	Высокий (4)	Пиринговые сети / Peer-to-Peer	Сайты, которые позволяют осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера
74	Высокий (4)	Частные IP-адреса / Private IP Addresses	Включает наборы IP-адресов, определенные в RFC 1918
75	Низкий (2)	Школьные мошенничества / School Cheating	Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами
76	Низкий (2)	Половое воспитание / Sex Education	Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборты, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность
77	Средний (3)	Сайты сомнительного содержания / Tasteless	Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса",

ID	Уровень риска	Название	Описание
			ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными
78	Низкий (2)	Жестокое обращение с детьми / Child Abuse Images	Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми
79	Очень низкий (1)	Нетрадиционная сексуальная ориентация / Gay, Lesbian or Bisexual	Сайты, содержащие материалы о геях, лесбиянках, трансгендерах
80	Низкий (2)	Литература и книги / Literature and Books	Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии
81	Низкий (2)	Здоровое питание и диеты / Nutrition and Diet	Сайты, посвященные правильному питанию, снижению веса, диетам
82	Низкий (2)	Домашние животные / Pets and Animals	Сайты, посвященные продуктам и сервисам для домашних и других животных
84	Низкий (2)	Обновления / Updates	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
85	Средний (3)	Чат-боты искусственного интеллекта / Chat-bot AI	Сайты, предоставляющие доступ к чат-ботам искусственного интеллекта, подобным Chat GPT
97	Низкий (2)	Репутация: Низкий риск / Reputation: Low risk	Сайты с низким репутационным риском. Как правило это сайты, не имеющие известных уязвимостей, но

ID	Уровень риска	Название	Описание
			относящиеся к категориям, где риск нарушения безопасности возможен
98	Средний (3)	Репутация: Средний риск / Reputation: Medium risk	Сайты со средним репутационным риском. Как правило это сайты, которые могут содержать уязвимости и относящиеся к категориям, где риск нарушения безопасности возможен
99	Очень высокий (5)	Репутация: Высокий риск / Reputation: High risk	Сайты с высоким репутационным риском. Сайты с известными уязвимостями

Измененные категории URL

Элемент библиотеки **Измененные категория URL** позволяет администратору назначить определенным сайтам категории, отличные от категорий, назначенных техническими специалистами UserGate. Такая потребность может возникнуть в случае некорректного категорирования сайтов или в случае, если требуемый сайт не имеет назначенной ему категории. Для переопределения категории сайта выполните следующие действия:

1. Проверьте первоначальную категорию сайта. В разделе **Настройки → Библиотеки → Измененные категории URL** введите требуемый адрес сайта в строку проверки и нажмите **Проверить категорию**.

2. Назначьте новую категорию. Если полученная категория не совпадает с требуемой, нажмите **Добавить** и назначьте 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**.

Вы можете экспортировать списки сайтов с измененными категориями или импортировать любые списки сайтов и назначить им требуемые категории.

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:

1. Создайте группу почтовых адресов. В разделе **Настройки → Библиотеки → Почтовые адреса** на панели **Группы почтовых адресов** нажмите **Добавить** и укажите название группы.

2. Добавьте почтовые адреса в группу. Выделите созданную группу, на панели **Почтовые адреса** нажмите **Добавить** и добавьте необходимые почтовые адреса.

Вы можете создавать собственные обновляемые списки почтовых адресов и централизованно распространять их на все узлы UserGate. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, `list.txt`) со списком адресов.

2. Создайте архив, содержащий этот файл (например, `list.zip`).

3. Создайте файл с версией списка (например, `version.txt`). Внутри файла укажите номер версии списка (например, 3). Необходимо инкрементировать это значение при каждом обновлении списка.

4. Разместите файлы архива и версии (например, `list.zip` и `version.txt`) на веб-сервере, чтобы они были доступны для скачивания.

5. На каждом UserGate SWG создайте список адресов. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

> **Примечание**
> **URL списка задается в формате:** `http://x.x.x.x/` **или** `ftp://x.x.x.x/`.

В свойствах списка можно настроить расписание обновления.

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

При ручном вводе также можно использовать следующие символы:

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

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в Linux можно с помощью команды:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется с расширением `.md5`. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров:

1. Создайте группу телефонных номеров. В разделе **Настройки → Библиотеки → Номера телефонов** на панели **Группы телефонных номеров** нажмите **Добавить** и укажите название группы.

2. Добавьте номера телефонов в группу. Выделите созданную группу, в панели **Группа телефонных номеров** нажмите **Добавить** и добавьте необходимые номера.

Вы можете создавать собственные обновляемые списки и централизованно распространять их на все узлы UserGate. Для создания таких списков выполните следующие действия:

1. Создайте текстовый файл (например, `list.txt`) со списком номеров телефонов.

2. Создайте архив, содержащий этот файл (например, `list.zip`).

3. Создайте файл с версией списка (например, `version.txt`). Внутри файла укажите номер версии списка (например, 3). Необходимо инкрементировать это значение при каждом обновлении списка.

4. Разместите файлы архива и версии (например, `list.zip` и `version.txt`) на веб-сервере, чтобы они были доступны для скачивания.

5. На каждом UserGate SWG создайте список URL. При создании укажите тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate SWG будет проверять наличие новой версии на сайте в соответствии с настроенным расписанием скачивания обновлений.

> **Примечание**
> **URL списка задается в формате:** `http://x.x.x.x/` **или** `ftp://x.x.x.x/`.

В свойствах списка можно настроить расписание обновления.

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

При ручном вводе также можно использовать следующие символы:

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

UserGate SWG может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл `list.zip.md5`, содержащий чек-сумму файла `list.zip`. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в Linux можно с помощью команды:

```
md5sum list.zip
```

Ее вывод добавляется в файл как хэш `list.zip`, после чего сохраняется с расширением `.md5`. Например, содержимое файла `list.zip.md5`:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается два 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 в разделе **Настройки → Библиотеки → Профили оповещений** нажмите **Добавить**, выберите **Добавить профиль оповещения SMTP** и укажите необходимые параметры профиля.

Параметр	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-сервер
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP в разделе **Настройки → Библиотеки → Профили оповещений** нажмите **Добавить**, выберите **Добавить профиль оповещения SMPP** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщени
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

Параметр	Описание
	можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8

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 на сетевом устройстве.

Для создания профиля безопасности в разделе **Настройки → Библиотеки → Профили LLDP** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля LLDP
Описание	Описание профиля LLDP
Статус порта	Режим: • **Приём и передача данных LLDP** — UserGate SWG будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • **Только приём данных LLDP** — UserGate SWG не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • **Только передача данных LLDP** — UserGate SWG 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 в разделе **Настройки → Библиотеки → Профили SSL** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	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	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: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256

Параметр	Описание
	• TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256 • TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS 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

Параметр	Описание
Установка алгоритмов шифрования для стандартных протоколов	Этот 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, изменены или удалены при необходимости.

Профиль	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 (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 этого профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа к веб-консоли.**

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 в разделе **Настройки → Библиотеки → Профили пересылки SSL** нажмите **Добавить** и укажите необходимые параметры профиля.

Параметр	Описание
Название	Название профиля пересылки SSL
Описание	Описание профиля пересылки SS
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 L
GRE IP-адрес назначения	IP-адрес назначения туннеля GRE. Параметр указывается при выборе типа пересылки L3

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 **Настройки → Библиотеки → Профили BFD** нажать **Добавить** и указать необходимые параметры профиля.

Параметр	Описание
Название	Название профиля BFD
Описание	Опциональное описание профиля
Определить множитель	Множитель времени обнаружения. Локальная система рассчитывает время обнаружения неисправностей соединения как произведение множителя времени обнаружения, полученного от удалённой системы, и согласованного интервала передачи удалённой системы. Если BFD не получит управляющий пакет до истечения времени обнаружения, то считается, что произошел сбой соединения. Например, если интервал передачи равен 300 мс, а множитель — 3, то локальная система будет обнаруживать сбои только через 900 мс отсутствия приёма пакетов
Интервал приёма	Интервал приёма управляющих пакетов BFD (минимальное время, которое требуется между пакетами). Для определения интервала каждый из узлов сравнивает свой интервал передачи с интервалом приема соседа — большее из двух значений принимается в качестве интервала передачи для этого узла. Значение по умолчанию — 50 мс
Интервал передачи	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами. Значение по умолчанию — 50 мс
Время получения echo	Минимальный интервал, через который система способна принимать echo-пакеты. Значение по умолчанию — 50 мс
Время отправки echo	Минимальный интервал передачи, через который система будет способна отправлять echo-пакеты BFD. Значение по умолчанию — 50 мс
Echo режим	Включение/отключение режима передачи Echo. По умолчанию этот режим отключён. Когда функция Echo активна, поток пакетов BFD Echo передается на удалённую систему, которая возвращает их обратно по тому же маршруту пересылки. Если некоторое количество пакетов Echo-потока данных не получено, сессия объявляется нерабочей. Echo-пакеты отличаются от control-пакетов (обычный режим) тем, что пакеты имеют адрес назначения равный адресу источника. Попадая на соседнюю систему, они проходят весь обычный транзитный путь, обеспечивая

Параметр	Описание
	таким образом более полное тестирование работоспособности системы соседа. Учитывая специфику обработки и фильтрации пакетов в UserGate SWG, для работы Echo-режима BFD необходимо создавать правило межсетевого экрана с разрешением соответствующего сервиса, иначе Echo-режим работать не будет. Например, для работы в Echo-режиме с Cisco IOS нужно создать сервис с разрешением UDP src port 49152 и dst port 3785
Пассивный режим	Включение/отключение пассивного режима. При работе в пассивном режиме система ждёт управляющие пакеты от соседей и отвечает на них в случае их получения. Эта функция полезна, когда маршрутизатор выступает в роли центрального узла звездообразной сети, и требуется избежать отправки ненужных управляющих пакетов BFD. По умолчанию используется активный режим. При работе в активном режиме узел отправляет управляющие пакеты соседнему узлу. Оба узла не могут работать в пассивном режиме; хотя бы один из них (или оба) должны работать в активном режиме
Минимальное время жизни	Только для сеансов с несколькими переходами. Настройка минимального значения времени жизни (количество переходов), которое BFD будет принимать в управляющем пакете BFD. Может принимать значения от 1 до 254. Все пакеты с меньшим значением TTL будут отброшены. Установка данного значения необходима для ужесточения требований к проверке пакетов во избежание получения управляющих пакетов BFD от других сессий. Значение по умолчанию равно 254 (это означает, что ожидается только один переход между этой системой и аналогом)

Syslog-фильтры UserID агента

При использовании syslog в качестве источников событий UserGate SWG производит фильтрацию событий в соответствии с указанными syslog-фильтрами UserID агента. Фильтры syslog представляют из себя стандартные

Regexp-выражения, которые пользователь может писать и сам. В стандартной поставке представлены три вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей по протоколу SSH в журналах syslog
Unix PAM Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей посредством технологии **Pluggable Authentication Modules** (PAM) в журналах syslog
UserGate WEC Agent	Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов

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 на вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

Сценарии

Сценарии является дополнительным условием в правилах контентной фильтрации, позволяющим администратору настроить реакцию UserGate SWG на определенные события, произошедшие за некоторое время.

Примером работы сценария может быть задача по ограничению на определенное время пропускной способности для пользователя, который выбрал установленный лимит трафика.

Настройка сценариев

Для работы со сценариями необходимо:

1. Создать сценарий.
2. Применить созданный сценарий в правилах контентной фильтрации.

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

Для создания сценария нажмите **Добавить** и укажите следующие параметры:

- На вкладке **Общие**:
  - **Включено** — включение или отключение сценария.
  - **Название** — название сценария.
  - **Описание** — описание сценария.
  - **Применить для** — параметр, отвечающий за количество пользователей в правиле, к которым будет применен сценарий:
    - **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** задайте условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, укажите 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.
- **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 UserGate SWG. Проверка может осуществляться с помощью команды icmp ping, запроса DNS или выполнения HTTP GET.

Категория URL

Условием срабатывания в этом случае является совпадение указанных категорий UserGate URL в трафике пользователя.

Для настройки этого условия укажите следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выберите категории сайтов из библиотеки или создайте список с категориями сайтов из имеющихся в библиотеке элементов.

Вы можете проверить конкретный URL на соответствие той или иной категории, для этого укажите URL в строке проверки и нажмите **Проверить URL**.

Обнаружен вирус

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

Типы контента

Для настройки этого условия укажите следующие параметры:

- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария;
- **За интервал** — интервал, в течение которого будет считаться количество срабатываний.
- Выберите типы контента из библиотеки элементов или создайте собственный тип контента.

Объем трафика

Условие срабатывания сценария по объему прошедшего трафика через UserGate SWG.

Для настройки этого условия укажите следующие параметры:

- **Введите размер** — предельный объем трафика, прошедшего через UserGate SWG, при котором сработает сценарий.
- **Период** — промежуток времени за который будет посчитан объем проходящего трафика.

Например, если будет выбран объем трафика 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 от UserGate SWG.

Возможны следующие методы проверки состояния сервера:

- Ping;
- DNS;
- HTTP GET.

Метод **Ping**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — IP-адрес для выполнения ICMP ping с UserGate SWG.
- **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** — интервал времени, в течение которого клиент будет ждать ответ от сервера после успешного установления соединения.
- **Количество срабатываний** — количество срабатываний, после которых активируется условие сценария.

- **За интервал** — интервал, в течение которого будут учитываться срабатывания.

Метод **DNS**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — IP-адрес DNS-сервера, на который посылаются DNS-запросы с UserGate SWG.
- **FQDN запроса** — доменное имя сервера, которое разрешается в рамках проверки доступности.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — интервал времени, в течение которого клиент будет ждать ответ 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 будут учитываться срабатывания.

Метод **HTTP GET**.

Для настройки этого метода укажите следующие параметры:

- **Адрес** — домен для выполнения HTTP GET с UserGate SWG.
- **Шлюз** — шлюз.
- **Результат** — положительный или отрицательный. Определяет, какой результат будет ожидаться от запроса сервера. Отрицательный — нет ответа, положительный — ответ есть.
- **Тайм-аут подключения** — интервал времени, в течение которого клиент будет 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 будут учитываться срабатывания.

Теги

Тегами называются специализированные маркеры, которые могут назначаться объектам в веб-интерфейсе для удобства их отображения, группирования и фильтрации.

В UserGate SWG теги могут быть присвоены интерфейсам и всем типам правил — правилам межсетевого экрана, NAT и маршрутизации, пропускной способности, фильтрации контента, веб-безопасности, инспектирования SSL, ICAP, reverse-прокси.

В веб-консоли администратора UserGate SWG список всех созданных на устройстве тегов находится в разделе **Настройки → Библиотеки → Теги**:

Для создания нового тега нажмите **Добавить** и заполните поля настроек тега в окне свойств:

- Укажите наименование тега. Оно может иметь не более 64 символов, начинаться с символа буквы или цифры, иметь в своём составе пробел и символы: `,.()_+-:/@`.
- При необходимости для тега можно выбрать цветовую маркировку из десяти имеющихся цветов.
- Опционально добавьте описание создаваемому тегу.

Помимо библиотеки элементов теги можно создавать непосредственно в свойствах маркируемых объектов — интерфейсов или правил, выбрав в поле **Теги** опцию **Добавить новый Тег**. Откроется такое же диалоговое окно создания тега, как описано выше.

Благодаря использованию тегов объекты в веб-интерфейсе можно визуально группировать. Поддерживается фильтрация объектов в веб-интерфейсе по тегам как с помощью кнопки в меню инструментов, так и с помощью команд в строке поиска.

В разделах настроек правил или интерфейсов есть инструмент для групповой работы с тегами. При выделении сразу нескольких объектов становится

активной кнопка **Управление тегами** в панели инструментов. С помощью инструмента управления тегами можно добить и удалить теги множеству объектов одновременно.

Работа с тегами также поддерживается в интерфейсе командной строки. Подробнее о работе с тегами в CLI — в разделе «Настройка библиотек».

ДИАГНОСТИКА И МОНИТОРИНГ

Мониторинг трафика

Раздел **Мониторинг трафика** позволяет получить список всех пользовательских соединений, установленных через UserGate SWG 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 отчета требует большего количества вычислительных ресурсов устройства и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на устройство.**

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 **K** 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)

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.

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** — список фильтров, определяющих условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть по ссылке.

- **Правила** — список правил захвата пакетов. При создании правила указываются:
  - интерфейсы UserGate SWG, на которых необходимо записывать трафик;
  - фильтры, созданные ранее;
  - имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** — в этой части помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Для записи трафика:

1. Создайте фильтр для захвата пакетов. Вы также можете воспользоваться предустановленными фильтрами или записать весь трафик, не фильтруя его.

2. Создайте правило захвата, в котором укажите имя правила, имя файла, максимальный размер записываемого файла и выберите необходимые фильтры.

3. Выбрать необходимое правило и нажмите **Начать запись**. Для остановки записи нажмите **Остановить запись.**

4. В разделе **Файлы** скачайте полученный pcap-файл.

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:

Действие	Описание
Добавить в белый список	

Действие	Описание
	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 вы можете 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 выполните следующие действия:

1. Создайте фильтр для трассировки. Для этого в разделе **Диагностика и мониторинг → Сеть → Трассировка правил** нажмите **Настроить** и укажите 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.
   - **IP-адрес назначения** — IP-адрес назначения трафика.

   Фильтр необходим для ограничения вывода диагностической информации. Если его не задать, могут быть также отображены результаты обработки запросов других пользователей.

2. Запустите трассировку, нажав **Начать**.

3. Попросите пользователя обратиться к проверяемому веб-ресурсу и наблюдайте, какие правила срабатывают при открытии сайта. Будут указаны правила, которые выполняются во время обработки пользовательского запроса.

> **Примечание**
>
> **При трассировке отображаются сработавшие правила ICAP, SSL-инспекции и контентной фильтрации.**

Вы можете проверить содержание отображаемого в трассировке интернет-ресурса с помощью формы **Открыть сайт**. С помощью формы **Добавить в белый список** вы 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:

Параметр	Описание
Ping host	Узел, который необходимо проверить
TTL	Максимальное количество промежуточных узлов, которое разрешено пройти на пути к проверяемому узлу
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 узлу. Параметры команды traceroute:

Параметр	Описание
Traceroute host	Узел, 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.

Параметр	Описание
DNS-запрос (хост)	DNS имя для проверки
IP источника запроса	Один из IP-адресов устройства UserGate
DNS сервер	DNS сервер, куда отправлять запрос
Порт	UDP порт, используемый для запроса
Тип DNS-запроса	Тип запроса

LLDP-соседи

В разделе **Диагностика и мониторинг → Сеть → LLDP-соседи** отображается список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. Подробнее о настройке отправки данных по протоколу LLDP — в разделе «Настройка интерфейсов».

> **Примечание**
> **Отображение LLDP-совместимых устройств доступно, только когда в разделе «Настройки» → «Usergate» → «Настройки» включен модуль «Настройка LLDP».**

Параметр	Описание
Chassis ID	Идентификатор шасси; является обязательной TLV-записью LLDP-кадра. У каждого устройства UserGate есть только один Chassis ID. В качестве Chassis ID используется MAC-адрес интерфейса управления
SysName	Имя системы
SysDescr	Описание системы, содержит информацию об оборудовании и операционной системе устройства
Management	

Параметр	Описание
	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. TTL задаётся в разделе **Настройки → UserGate → Настройки → Модули** в поле **Настройка LLDP**

Статистика LLDP

В этом разделе отображается статистика интерфейсов, в настройках которых был указан профиль LLDP.

Параметр	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

Параметр	Описание
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

Правила оповещений

В этом разделе вы можете создавать правила оповещений для различных типов событий.

Для создания правила оповещения выполните следующие шаги:

1. Создайте один или несколько профилей оповещения. Подробнее — разделе «Профили оповещений».

2. Создайте группы получателей оповещений. Подробнее — в разделах «Почтовые адреса» и «Номера телефонов».

3. Создайте правило оповещения. В разделе **Диагностика и мониторинг → Оповещения → Правила оповещений** нажмите **Добавить** и укажите параметры правила.

Параметр	Описание
Включено	Включение или отключение правила
Название	Название правила
Описание	Описание правила

Параметр	Описание
Профиль оповещения	Выбор созданного ранее профиля 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	Указание отправителя оповещения
Тема	Указание темы оповещения
Таймаут перед повторной отправкой, секунд	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании этого правила. Параметр позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения
События	Выбор событий, для которых необходимо получать оповещения
Телефоны	Для SMPP-профиля. Указание группы номеров телефонов, на которые будут отправляться SMS-оповещения
Emails	Для SMTP-профиля. Указание группы адресов email, на которые будут отправляться почтовые оповещения

SNMP

UserGate SWG 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 устройства UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, в параметрах контроля доступа разрешите сервис SNMP.

2. Создайте правило SNMP.

Для создания правила SNMP в разделе **Диагностика и мониторинг → Оповещения → SNMP** нажмите **Добавить** и укажите параметры правила.

Параметр	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. Этот параметр необходим только для отправки трапов на сервер оповещений
Комьюнити	SNMP community — строка для идентификации устройства 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	Указание версии протокола SNMP, которая будет использоваться в правиле. Возможны варианты SNMP v2c и SNMP v3
Разрешить SNMP-запросы	Разрешение получать и обрабатывать SNMP-запросы от SNMP-менеджера
Разрешить SNMP-трапы	Разрешение на отправку SNMP-трапов на сервер, настроенный для приема оповещений
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе «Профили безопасности SNMP»
События	Выбор типов параметров, доступных для мониторинга по правилу

> **Примечание**
> **Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования — в профиле безопасности SNMP) на SNMP-менеджере должны совпадать с настройками SNMP на устройстве 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 устройства UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого перейдите в раздел **Диагностика и мониторинг → Оповещения → SNMP** и нажмите **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

Параметр	Описание
trapCoreCrush	Сбой ядра
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен
trapCoreBootstrapEnd	Загрузка сервера завершена успешно
trapDefaultGatewayChanged	Изменение шлюза по умолчанию
trapHighSessionsCounter	Таблица сессий заполнена на 90%

Параметр	Описание
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии
trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на "not_clean"
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера
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 (95%)
trapLowMemory	Высокая загрузка памяти (95%)
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов
trapRaidStatus	Изменение статуса RAID
trapPowerSupply	Первый источник питания отключен
trapCableStatus	Кабель был подключен или отключен от интерфейса
trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загруженности >=95% за 5 минут хотя бы на одном из дисковых устройств
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана
trapLDAPServerDown	Сервер LDAP недоступен
trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C

UTM-TRAPS-BINDINGS-MIB

Параметр	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. • **4** — DNS-сервер недоступен. • **5** — узел UserGate Management Center недоступен
utmCPUUsage	integer	Загруженность центрального процессора (%)

Параметр	Тип данных	Описание
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. • **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

Параметр	Тип данных	Описание
		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
utmLDAPServerAddress	string	IP-адрес LDAP-сервера
utmThermSensor	string	Название температурного сенсора
utmThermValue	integer	Значение температуры, измеренное сенсором

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается фактическое число загруженных виртуальных процессоров
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*****)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)
tcpsessionsCounter	integer	Количество активных TCP сессий на текущий момент времени. (*)
udpsessionsCounter	integer	Количество активных 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. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее

Наименование	Тип данных	Описание
		значение за последние 60 секунд. (*)
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	

Наименование	Тип данных	Описание
		Общее количество HTTP запросов. (*)
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы
haStatus	integer	Текущее состояние узла кластера
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %
memoryUsed	integer	Использование оперативной памяти; отображается в %
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %
powerSupply1Status	string	Состояние первого источника питания: • **no_power_supplies**. • **on**. • **off**
powerSupply2Status	string	Состояние второго источника питания: • **no_power_supplies**. • **on**. • **off**
raidType	string	Тип RAID массива
raidStatus	string	

Наименование	Тип данных	Описание
		Текущий статус RAID (Redundant Array of Independent Disks): • **no_raid**. • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива
diskIOUtilization	integer	Текущая утилизация диска (%)
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд

Примечание

Метрики, отмеченные в описании символом (*) не актуальны для *UGMC* и *LogAn*. Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Параметр	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber

Параметр	Тип данных	Описание
ifDescr	string	Информация об интерфейсе, которая может включать в себя название производителя, имя продукта, аппаратную версию интерфейса
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • **1** — other — неизвестный тип. • **2** — regular1822 — определён в BBN Report 1822. • **3** — hdh1822 — определён в BBN Report 1822. • **4** — ddn-x25 — определён в BBN Report 1822. • **5** — определён в стандарте канального уровня сетевой модели OSI X.25. • **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • **7** — iso88023-csmacd — определён в IEEE 802.3. • **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.

Параметр	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.

Параметр	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

Параметр	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 мультиплексирование м 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	

Параметр	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

Параметр	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

Параметр	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

Параметр	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

Параметр	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

Параметр	Тип данных	Описание
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров
ifAlias	string	Название интерфейса, заданное администратором при настройке интерфейса
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса

UTM-TEMPERATURE-MIB

Параметр	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)

Параметр	Тип данных	Описание
thermEntry	sequence	Информация о конкретном сенсоре: • thermName (string) — название сенсора. • thermValue (integer) — показание сенсора. • thermUnit (string) — единица измерения показаний сенсора

Примечание

Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание

Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учётом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

В этом разделе вы можете редактировать общие параметры SNMP-агента на устройстве. Параметры SNMP задаются для каждого узла кластера индивидуально.

Параметр	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP
SNMP локация системы	Информация о физическом расположении SNMP-агента

Параметр	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 этом разделе вы можете настраивать профили 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 на устройстве UserGate.**

Параметр	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).

Параметр	Описание
	• С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: • SHA1; • MD5; • SHA224; • SHA256; • SHA384; • SHA512
Пароль аутентификации	Пароль, используемый для аутентификации
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES
Пароль шифрования	Пароль, используемый для шифрования

ЖУРНАЛЫ И ОТЧЕТЫ

ЖУРНАЛЫ

Описание

UserGate SWG регистрирует события, возникающие в процессе его функционирования, и сохраняет их в следующих журналах:

- **Журнал событий** — содержит события, связанные с изменением параметров UserGate SWG, авторизацией пользователей, обновлениями различных списков и т. п.

- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate SWG.
- **Журнал DNS** — содержит события, связанные с DNS-трафиком.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, правил подмены портов и правил маршрутизации на основе политик (PBR). Для регистрации этих событий необходимо включить функцию журналирования в соответствующих правилах.
- **История поиска** — содержит сведения о поисковых запросах пользователей в популярных поисковых системах.
- **Агент UserID** — содержит описание событий, отражающих результат работы UserID-агента.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных отображаются в журнале событий. В случае, если узел интегрирован с UserGate Log Analyzer, записи будут отображаться в журнале событий UserGate Log Analyzer. Ротация записей журнала событий никогда не производится.

Журнал событий

Журнал событий отображает события, связанные с изменением настроек UserGate SWG, 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, старта, выключения, перезагрузки сервера и т. п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например по диапазону дат, компоненту, важности, типу события.

Вы можете выбрать для отображения только те столбцы, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** вы можете 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, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.

- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User agent браузера.

> **Примечание**
> **В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик после срабатывания всех правил на этом запросе.**
> **Если правила требуют анализа ответа от веб-сервера, то трафик ответа также будет подсчитан и учтён одинаковый, в том числе у первого сработавшего на этом запросе правила (bypass captive, decrypt). Таким образом, учитывается весь прошедший трафик и указывается одно и то же значение каждому правилу, сработавшему на этом запросе.**
> **Если анализ ответа от веб-сервера для правил не требуется, то весь остальной трафик не учитывается.**

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** выр можете 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 UserGate SWG 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.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете 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, 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.

> **Примечание**
> **В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила. Если в настройках журналирования в правиле выбрано: "Журналировать каждый пакет", то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.**
> **Если в настройках журналирования в правиле выбрано: "Журналировать начало сессии", будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.**

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете 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.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

UserID-агент

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные UserID-агентом с помощью коннектора «Microsoft Active Directory» с серверов AD. В журнале отображаются события с успешным входом в систему (идентификатор события 4624), события Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627).

Параметр	Описание
Узел	Узел UserGate, которым зафиксировано событие
Время	Время произошедшего события
Запись журнала событий конечных устройств	Ссылка на событие
Конечное устройство\сенсор	Коннектор UserID
Уровень лога	Поле «Keywords» из журнала AD
Данные	Содержание события из журнала AD
Источник журнала событий	Поле «Источник» из журнала AD
Категория журнала	

Параметр	Описание
	Код категории инцидента (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и т. д)
Категория инцидента	Поле «Тип задачи» из журнала AD
Имя компьютера	Узел Windows, на котором произошло событие
Пользователь	Поле «Пользователь» из журнала AD
Код события лога	Поле «Код события» из журнала AD (EventCode)
Идентификатор события лога	Поле «Идентификатор события» из журнала AD (EventID)
Тип события лога	Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.)
Файл журнала лога	файл журнала Windows

Syslog (Журнал)

Журнал syslog отображает события, собранные UserID-агентом с помощью коннектора «Отправитель syslog» с серверов-источников данных syslog. В журнале отображаются события входа пользователей в систему и завершения сеанса работы.

Параметр	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Запись журнала syslog	Ссылка на событие
Правило	Правило, под которое попало syslog-сообщение
Критичность	Уровень критичности события syslog
Объект	Тип процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и т. д)
Имя компьютера	Имя компьютера, на котором произошло событие
Приложение	Приложение, вызвавшее событие

Параметр	Описание
Идентификатор процесса	PID процесса, вызвавшего событие
Данные	Описание события

UserID (Журнал)

Журнал UserID содержит описания событий, отражающие результат работы UserID-агента.

Параметр	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, который вызвал событие
IP-адрес	IP-адрес узла, на котором произошло событие
Информация	Описание события

RADIUS (Журнал)

Журнал RADIUS отображает события, собранные UserID-агентом с помощью коннектора «RADIUS» из данных RADIUS accounting. В журнале отображаются события входа пользователей в систему и завершения сеанса работы.

Параметр	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Идентификатор правила	Идентификатор правила, срабатывание которого создало событие
Пользователь	Пользователь, который вызвал событие

Параметр	Описание
Группы	Строка групп, в которых состоит пользователь
Статус	Статус пользователя
IP источника	IP-адрес источника, откуда пришло сообщение
IP адрес NAS	IP-адрес NAS, авторизовавшего пользователя
IP-адрес пользователя	IP-адрес пользователя (framed ip address)

Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, очень велико, и не все поля доступны в базовом режиме просмотра. UserGate SWG предоставляет удобные способы поиска и фильтрации необходимой информации. Вы можете использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска используется графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов. Например, вы можете задать интересующий вас 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:

Ключевое слово	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:

Оператор	Описание
=	Равно. Требует полного совпадения значения поля указанному значению. Пример: `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. Пример: `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. Применимо только для полей, поддерживающих сравнения, например поля даты, portSource, portDest, statusCode и т. п. Пример: `date<='2019-03-28T20:59:59' AND statusCode=303`
>=	Больше либо равно. Значение поля должно быть больше, либо равны указанному в запросе значению. Применимо только для полей, поддерживающих сравнения, например поля даты, portSource, portDest, statusCode и т. п. Пример: `date>="2019-03-13T21:00:00" AND statusCode=200`
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Применимо только для полей, поддерживающих сравнения, например поля даты, portSource, portDest, statusCode и т. п. Пример: `date < '2019-03-28T20:59:59' AND statusCode=404`
>	Больше. Значение поля должно быть больше указанного в запросе значения. Применимо только для полей, поддерживающих сравнения, например поля даты, portSource, portDest, statusCode и т. п. Пример: `(statusCode>200 AND statusCode<300) OR (statusCode=404)`
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках. Пример: `category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')`
NOT IN	Позволяет указать несколько значений поля в запросе. Будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках. Пример: `category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')`

Оператор	Описание
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле. Этот оператор применим только к полям, в которых хранятся строковые данные. Пример: `browser ~ "Mozilla/5.0"`
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле. Этот оператор применим только к полям, в которых хранятся строковые данные. Пример: `browser !~ "Mozilla/5.0"`
MATCH	При использовании оператора `MATCH` подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON с использованием одинарных кавычек. Пример: `details MATCH '\"module\":\"threats\"'` Синтаксис запросов с использованием этого оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2 по ссылке
NOT MATCH	При использовании оператора `NOT MATCH` подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON с использованием одинарных кавычек. Пример: `details NOT MATCH '\"module\":\"threats\"'` Синтаксис запросов с использованием этого оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2 по ссылке

При составлении расширенного запроса UserGate SWG 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 UserGate SWG автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Экспорт журналов

С помощью функции экспорта журналов вы можете выгружать информацию о работе системы на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate SWG поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал трафика.
- Журнал DNS.
- Журнал UserID.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP выполняется 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 параметрах UserGate SWG указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером UserGate Log Analyzer.**

При создании правила укажите необходимые параметры для экспорта журналов.

Параметр	Описание
Название правила	Название правила экспорта журналов
Описание	Опциональное поле для описания правила
Параметры разового экспорта	Выбор диапазона экспорта журналов
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал трафика. • Журнал DNS. • UserID.

Параметр	Описание
	Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • CEF Compact. • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов
Тип сервера	SSH (SFTP), FTP, Syslog
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	

Параметр	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 журналов. Не применяется к методу отправки Syslog. Вы можете выбрать одно из предустановленных значений расписания или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>.

Параметр	Описание
	При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что экспорт журналов должен выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
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

ОТЧЕТЫ

Описание

Отчеты предназначены для получения структурированных аналитических данных о событиях, связанных с безопасностью, изменениями в конфигурации системы и активностью пользователей. Формирование и рассылка отчетов производятся в автоматическом режиме на основе предварительно настроенных правил и шаблонов.

Чтобы создать отчет:

1. Создайте правило создания отчета.

2. Запустите создание отчета вручную или дождитесь момент, когда создание отчета запустится в автоматическом режиме по указанному в правиле расписанию.

3. Получите отчет по электронной почте, если отправка была настроена в правиле, или скачайте полученный отчет в разделе **Созданные отчеты.**

> **Примечание**
> **Процесс создания отчета может продолжаться достаточно длительное время и может потреблять значительное количество вычислительных ресурсов.**

> **Примечание**
> **В отчетах по трафику (кроме отчетов веб-доступа) используются данные из компонента NetFlow. Отчеты веб-доступа по трафику используют данные из журналов (домены, URL-категории и т. п.).**

Шаблоны отчетов

С помощью шаблонов определяется внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией-разработчиком UserGate.

Полный список шаблонов доступен в разделе **Журналы и отчеты → Отчеты → Шаблоны**.

Шаблонов отчетов сгруппированы по категориям:

- **Пользовательский** — группа шаблонов по обобщенной статистике срабатывания правил отчетов.
- **Captive-портал** — группа шаблонов по событиям авторизации пользователей с помощью Captive-портала.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **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.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание и тип отображения отчета (таблица, гистограмма, пирог).

Правила отчетов

Правила отчетов создаются в разделе **Журналы и отчеты → Отчеты → Правила отчетов**.

В правиле отчета задаются параметры создаваемого отчета, а также расписание запуска генерации отчета и способы его доставки.

Параметры правила создания отчетов.

Параметр	Описание
Включено	Включение или отключение правила создания 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 (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет.

Параметр	Описание
	Важно! **Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем выше нагрузка. Для шаблонов «Подробный список всех посещенных URL» и «Подробный список всех посещенных сайтов» автоматически используется формат CSV, независимо от выбранного формата**
Количество записей	Ограничение числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей. Например, топ-20 пользователей с ошибочной авторизацией в веб-консоли
Количество в группировке (если применимо)	Ограничение 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. Это ограничение применимо только для тех шаблонов отчетов, которые содержат группирование
Пользователи	Выбор пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, отчет будет создаваться для всех пользователей
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Необходимо добавить хотя бы один шаблон
Расписание	Расписание для создания отчетов. Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что создание отчета должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений.

Параметр	Описание
	• Косая черта (/) — для указания шага между значениями
Доставка	Настройка отправки созданного отчета по электронной почте. Для отправки отчета укажите: • Профиль SMTP, который будет использован для отправки отчетов. Подробнее о настройке профилей SMTP — в разделе «Профили оповещений». • От — имя отправителя письма. • Тема письма — тема письма (subject). • Тело письма — содержимое письма. • Получатели — список получателей письма из библиотеки «Почтовые адреса»

Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять значительное количество вычислительных ресурсов. Важно учитывать загрузку ресурсов при запуске отчетов за большой интервал 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 выберите требуемое правило и нажмите «Запустить сейчас». Готовый отчет после создания будет доступен в разделе «Созданные отчеты».

Созданные отчеты

Все созданные отчеты хранятся в разделе **Журналы и отчеты → Отчеты → Созданные 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 нажмите на файл с созданным отчетом, для удаления — **Удалить**.

Для настройки времени хранения готовых отчетов (ротации) нажмите **Настроить**. Значение по умолчанию — 60 дней.

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения

UserGate SWG поддерживает работу через интерфейс командной строки (CLI).

С помощью CLI вы можете:

- просматривать конфигурацию устройства;
- выполнять диагностику работы устройства;
- настраивать параметры конфигурации устройства;
- перезагружать или выключать устройство.

Подключение к интерфейсу командной строки

К интерфейсу командной строки можно подключиться с помощью стандартных портов для монитора и клавиатуры (при наличии таких портов на устройстве), с помощью терминала через консольный порт или удаленно с помощью протокола SSH.

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

Для подключения с помощью монитора и клавиатуры:

1. Подключите монитор к разъему VGA (HDMI), клавиатуру — к разъему USB.

2. Войдите в CLI, используя имя и пароль пользователя с правами администратора (по умолчанию — Admin и usergate).

Для подключения с помощью консольного порта:

1. Подключите компьютер к устройству с помощью кабеля для консольного порта.

2. Запустите программу — эмулятор терминала, например `Putty` для Windows или `minicom` для Linux. Установите подключение через последовательный порт, указав параметры подключения: `115200`, `8 n 1`.

3. Введите логин а пароль для доступа в интерфейс (по умолчанию — Admin и usergate).

Для подключения с помощью протокола SSH:

1. Разрешите доступ для протокола CLI по SSH в параметрах зоны, к которой вы собираетесь подключаться (доступ по порту TCP 2200). Подробнее о настройке зоны в CLI — в разделе «Зоны».

2. Запустите на компьютере SSH-терминал, например `SSH` для Linux или `Putty` для Windows.

3. Укажите IP-адрес устройства, порт для подключения (по умолчанию — 2200), имя пользователя с правами администратора (по умолчанию — Admin).

Пример команды подключения для Linux: `ssh Admin@<IP-address> -p 2200`.

3. Войдите в CLI, используя пароль пользователя, указанного на предыдущем шаге.

Для подключения к CLI по SSH поддерживаются следующие алгоритмы:

- Kex: diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256;
- Public key: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-256, rsa-sha2-512, ssh-rsa;

- Ciphers: aes128-ctr, aes192-ctr, aes256-ctr;
- MAC: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-256.

Режимы работы интерфейса командной строки

CLI имеет два основных режима работы — режим диагностики и режим конфигурации.

После авторизации вы попадаете в режим диагностики.

В режиме диагностики доступны команды:

- проверки доступности сетевых ресурсов;
- просмотра статистики и информации об интерфейсах;
- просмотра информации о записях ARP;
- отслеживания пакетов по установленным правилам;
- мониторинга трафика;
- просмотра информации о маршрутах;
- просмотра состояния кластера;
- отображения системной информации;
- диагностики работы протоколов динамической маршрутизации;
- просмотра информации об авторизованных пользователях.

Приглашение командной строки в режиме диагностики имеет следующий вид:

```
Admin@nodename>
```

Настройка параметров устройства выполняется в режиме конфигурации.

Для переключения на режим конфигурации используется команда `configure`. В режиме конфигурации символ приглашения в командной строке меняется на #. Вернуться в режим просмотра можно с помощью команды `exit`.

```
Admin@nodename> configure
Admin@nodename#
Admin@nodename# exit
Admin@nodename>
```

Если система находится в состоянии до первичной инициализации, в CLI доступны команды режима диагностики и ограниченный набор команд режима конфигурации, позволяющий выполнить настройку сетевых параметров устройства. Приглашение командной строки в режиме диагностики по умолчанию имеет вид: `<user-name>@<product-type>>` (например, `Admin@SWG>`), а в режиме конфигурации — `<user-name>@<product-type>#` (например, `Admin@SWG#`). Подробнее — в разделе «Команды, доступные до первичной инициализации узла».

Если система находится в аварийном состоянии, для восстановления рабочего состояния в неё можно войти в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации устройства. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде `Admin@emergency`, в качестве пароля — пароль корневого администратора. Приглашение командной строки в режиме emergency по умолчанию имеет вид: `<user-name>@emergency@<product-type>#` (например, `Admin@emergency@SWG#`). Подробнее о режиме emergency — в разделе «Настройка устройства».

Формат команд

Команды интерфейса командной строки имеют следующий формат:

```
<action> <level> <filter> <configuration_info>
```

- `<action>` — действие, которое необходимо выполнить (`create`, `set`, `show`, `delete`).
- `<level>` — уровень контекста конфигурации. Соответствует одному из разделов структуры конфигурации в веб-интерфейсе SWG (`network`, `network-policy`, `security-policy`, `users`, `settings`, `libraries`, `logs` и т. д.).
- `<filter>` — идентификатор объекта, к которому происходит обращение для выполнения действия `<action>`.

- `<configuration_info>` — значения параметров, которые необходимо применить к объекту `<filter>`.

Поддерживается ввод команды в несколько строк (многострочный ввод). Примером таких команд могут быть команды описания правил, использующих синтаксис UPL. Для перехода на новую строку необходимо добавить символ «\» в конце строки. Начиная со второй строки ввод символа «\» необязателен. Чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@nodename# set users user example \
... name username1
... enabled on
... groups [ "Default Group" ]
...
Admin@nodename#
```

В интерфейсе командной строки поддерживается последовательное исполнение нескольких команд, вставленных из буфера обмена. Исключением являются многострочные команды, например команды, написанные с помощью синтаксиса UPL. Импортировать многострочные команды можно с помощью команды `import`.

Фильтрация вывода команд

В интерфейсе командной строки поддерживается функция фильтрации вывода команд. С помощью функции фильтрации вы можете управлять отображением результатов выполнения команд в соответствии с заданными критериями.

Фильтрация может применяться к различных типам команд просмотра, включая:

- команды отображения состояния устройства;
- команды просмотра конфигурации;
- команды просмотра системных журналов;
- команды с динамическим выводом данных (такие, как `show traffic capture` и `show network trace`).

Формат команд с фильтрацией вывода:

```
<cli-command> | grep <pattern> -f <include|exclude> -BA <Num>:<Num>
```

- `<cli-command>` — команда CLI, вывод которой нужно отфильтровать.
- `<pattern>` — искомое выражение. Поддерживается формат выражений RegExp.
- `-f <include|exclude>` — включение или исключение искомого выражения из вывода команды.
- `-BA <Num>:<Num>` — отображение строк, соседних с совпадением (<количество отображаемых строк до совпадения>`:`<количество отображаемых строк после совпадения>).

Пример фильтрации вывода команд просмотра состояния интерфейсов:

```
Admin@nodename> show network interface

+---------+-------------------+-------------+------
+-----------------------+
|   Name  |         IP        | Link status | Mode |
Zone         |
+---------+-------------------+-------------+------
+-----------------------+
| tunnel1 |  172.30.250.1/24  |     DOWN    |      | VPN for remote
access |
| tunnel2 |  172.30.255.1/24  |     DOWN    |      |  VPN for Site-to-
Site |
| tunnel3 |                   |     DOWN    |      |  VPN for Site-to-
Site |
|  port0  | 172.26.147.146/16 |    10000    | main |
MGMT         |
|  port1  | 10.150.185.119/16 |    10000    | main |        [MC]
LAN       |
|  port2  | 10.153.219.236/16 |    10000    | main |        [MC]
WAN       |
+---------+-------------------+-------------+------
+-----------------------+
Admin@nodename> show network interface | grep VPN
| tunnel1 |  172.30.250.1/24  |     DOWN    |      | VPN for remote
```

```
access |
| tunnel2 |  172.30.255.1/24  |     DOWN    |      |  VPN for Site-to-
Site |
| tunnel3 |                   |     DOWN    |      |  VPN for Site-to-
Site |
Admin@nodename> show network interface | grep VPN -f exclude
+---------+-------------------+-------------+------
+-----------------------+
|   Name  |         IP        | Link status | Mode |
Zone         |
+---------+-------------------+-------------+------
+-----------------------+
|  port0  | 172.26.147.146/16 |    10000    | main |
MGMT         |
|  port1  | 10.150.185.119/16 |    10000    | main |        [MC]
LAN       |
|  port2  | 10.153.219.236/16 |    10000    | main |        [MC]
WAN       |
+---------+-------------------+-------------+------
+-----------------------+
```

Пример фильтрации вывода команд поиска правил межсетевого экрана:

```
Admin@nodename# show network-policy firewall | grep "name\(\"VPN"
    name("VPN for remote access to Trusted and Untrusted")
    name("VPN for Site-to-Site to Trusted and Untrusted")
Admin@nodename# show network-policy firewall | grep "name\(\"VPN" -BA
4:
    src.zone = "VPN for remote access" \
    dst.zone = (Untrusted, Trusted) \
    desc("Example firewall rule which allows traffic from VPN for
remote access zone to Trusted and Untrusted zones. This is an example
rule which can be changed or deleted if necessary.") \
    enabled(false) \
    name("VPN for remote access to Trusted and Untrusted")
-----------------------------------------------
    src.zone = "VPN for Site-to-Site" \
    dst.zone = (Untrusted, Trusted) \
    desc("Example firewall rule which allows traffic from VPN for Site-
```

```
to-Site zone to Trusted and Untrusted zones. This is an example rule
which can be changed or deleted if necessary.") \
    enabled(false) \
    name("VPN for Site-to-Site to Trusted and Untrusted")
-----------------------------------------------
```

Пример фильтрации вывода команды просмотра событий журнала:

```
Admin@nodename> show logs log core static | grep ldap
2025-08-05 11:58:32.861039<0.2336.0> [critical] database:wait_tables/
1:253 'ldap_server' loaded in 0.0ms
2025-08-05 11:58:33.392739<0.3953.0> [critical] database:wait_tables/
1:253 'ldap_server' loaded in 0.0ms
2025-08-05 11:58:33.569880<0.4287.0> [critical] nagent:start_app/1:340
ldap_sync starting ...
2025-08-05 11:58:33.571394<0.4287.0> [critical] nagent:start_app/1:343
[uuid,ldap_sync] started
2025-08-05 11:59:03.889299<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
2025-08-05 11:59:12.366764<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
2025-08-05 12:00:10.162520<0.4903.0> [critical][ldap]
ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
```

Пример фильтрации вывода команды с динамическим выводом:

```
Admin@nodename> show traffic capture | grep ICMP

   92 0.305709456 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping)
request  id=0x0e30, seq=3/768, ttl=30
   93 0.305739062 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping)
reply    id=0x0e30, seq=3/768, ttl=64 (request in 92)
  706 1.329727201 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping)
request  id=0x0e30, seq=4/1024, ttl=30
  707 1.329755455 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping)
reply    id=0x0e30, seq=4/1024, ttl=64 (request in 706)
```

Горячие клавиши

В интерфейсе командной строки вы можете использовать следующие горячие клавиши:

- Tab — вызов встроенной помощи, автодополнение команды:
  - Если нажать Tab в режиме ожидания ввода, выводится полный список команд, доступных на текущем уровне.
  - Если нажать Tab на этапе ввода команды после пробела, отображается список возможных параметров команды с кратким описанием.
  - Если написать первые несколько букв команды и нажать Tab, команда будет дополнена.
- Ctrl + C — отмена ввода текущей команды.
- ↑, ↓ — прокрутка истории ввода команд.

В выводе встроенной помощи после нажатия клавиши Tab могут использоваться следующие вспомогательные символы:

- * — обязательный параметр в командах `create` и ряде других команд.
- + — опциональный параметр.
- > — вложенные параметры. После введения такого параметра появляется новый список параметров, которые можно указать.

Например:

```
Admin@nodename# set network virtual-router default
+ interfaces           List of network interfaces attached to this
virtual router
> routes               List of static network routes
```

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВОНАЧАЛЬНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла

Если устройство еще не прошло первоначальную инициализацию, в CLI доступен минимальный набор команд для настройки сетевых параметров устройства и запуска инициализации.

> **Примечание**
> **В случае сбоя в работе ядра CLI также может перейти в состояние до первичной инициализаци.**

Команды режима диагностики

В режиме диагностики доступны команды, позволяющие просмотреть:

- доступность сетевых ресурсов;
- статистику и информацию об интерфейсах;
- информацию о записях ARP;
- информацию о маршрутах;
- системную информацию.

Также в режиме диагностики можно выполнять мониторинг сетевого трафика и диагностику работы протоколов динамической маршрутизации.

Базовые команды управления устройством

Для просмотра текущих даты и времени на узле используется команда:

```
Admin@SWG> date
```

Для перезагрузки узла используется команда:

```
Admin@SWG> reboot
```

Для выключения узла используется команда:

```
Admin@SWG> shutdown
```

Для перехода в режим конфигурации узла используется команда:

```
Admin@SWG> configure
```

Для выхода из интерфейса CLI используется команда:

```
Admin@SWG> exit
```

Команды проверки доступности сетевых ресурсов

Команда	Описание

`dig`	Проверка записи DNS домена:
	`Admin@SWG> dig host <hostname> <parameters>`
	`Admin@SWG> dig host <IP-address> <parameters>`
	В команде можно использовать следующие параметры:
	• `reverse-lookup` — получение имени устройства по IP-адресу;
	• `dns` — указание IP-адреса DNS-сервера;
	• `tcp` — использование протокола TCP вместо UDP

`netcheck`	

Команда	Описание

	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры:
	• `address` — IP-адрес и порт, доменное имя узла — для проверки доступности по TCP; URL — для HTTP;
	• `dns-ip` — IP-адрес сервера DNS;
	• `dns-tcp` — использование TCP вместо UDP для DNS-запроса;
	• `check-cert` — проверка SSL-сертификата;
	• `type` — проверка доступности по:
	  ◦ `http;`
	  ◦ `tcp` (если порт не указан, то используется порт 80);
	• `data` — запрос содержимого сайта. По умолчанию запрашиваются только заголовки;
	• `timeout` — максимальный тайм-аут ожидания ответа от веб-сервера;
	• `user-agent` — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin@SWG> netcheck type tcp address <host-domain-name> data on`
	`Admin@SWG> netcheck address <host-domain-name>`

`ping`	Проверка доступности определенного узла. Можно задать следующие параметры: • `host` — IP-адрес или доменное имя узла. • `count` — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш `Ctrl + C`). • `numeric` — не определять имена. • `timestamp` — отображение временных меток. • `interval` — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • `ttl` — время жизни пакета.

Команда	Описание
	• `interface` — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения `ping`. • `mtu` — максимальный размер блока данных отправляемых пакетов. • `virtual-router` — имя виртуального маршрутизатора. `Admin@SWG> ping host <hostname> count <number>`
`traceroute`	Трассировка соединения до определенного узла. Параметры команды: • `host <ip-or-domain>` — IP-адрес или имя домена, для которого производится трассировка; • `interface <iface-name>` — интерфейс, с которого будут отправляться пакеты; • `not-map-ip` — не искать hostname для IP-адреса при отображении; • `use-icmp-echo` — использовать ICMP echo; • `port` — указать порт вместо порта по умолчанию (1 — 65535); • `min-interval` — минимальный интервал между пакетами. `Admin@SWG> raceroute host <hostname>`

Статистика и информация об интерфейсах

Для отображения информации об интерфейсах используется команда:

```
Admin@SWG> show network interface
```

Для отображения статистики определенного интерфейса и информации о нем используется следующая команда:

```
Admin@SWG> show network interface <interface-name>
```

Также доступно отображение только информации или только статистики интерфейса:

```
Admin@SWG> show network interface <interface-name> type info
Admin@SWG> show network interface <interface-name> type statistics
```

Для отображения списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов предназначена команда:

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

> **Примечание**
> **Под физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. Изменения MAC-адресов интерфейсов в настройках SWG данной командой не отображаются. Измененные настройками SWG MAC-адреса можно посмотреть командой:** `show network interface <interface-name>`.

Упорядочивание интерфейсов происходит в соответствии с номером порта в шине PCI.

Для удаления списка используется команда:

```
Admin@SWG> clear network interface-mapping
```

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенное устройство.

ARP-записи

Для просмотра информации о записях ARP используется команда:

```
Admin@SWG> show network arp
```

Для просмотра ARP-записей вы можете использовать фильтры.

Параметр	Описание
`interface`	Название интерфейса SWG
`host`	IP-адрес устройства
`mac`	MAC-адрес устройства

```
Admin@SWG> show network arp host <IP-address>
Admin@SWG> show network arp interface <interface-name>
Admin@SWG> show network arp mac <MAC-address>
```

Примечание

В режиме диагностики действия производятся с системными записями; в режиме конфигурации – со статическими ARP-записями.

Для удаления системной ARP-записи используется команда:

```
Admin@SWG> clear network arp interface <iface-name> host <ip>
```

Для удаления всех системных записей на заданном интерфейсе (можно указать несколько интерфейсов) используется команда:

```
Admin@SWG> clear network arp interfaces [ <iface-name1> <iface-name2>
… ]
```

Отслеживание пакетов

Для включения функции отслеживания пакетов используется команда:

```
Admin@SWG> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия входящих и исходящих интерфейсов, номера TCP/UDP портов источника и назначения.

Для выхода из режима отслеживания пакетов нажмите комбинацию клавиш `Ctrl + C`.

Мониторинг трафика

Для мониторинга трафика используется команда:

```
Admin@SWG> show traffic <parameters>
```

Параметры мониторинга трафика.

Параметр	Описание
`flows`	Отображение информации о входящем и исходящем потоках. Параметры фильтрации: • `source-ip` — IP-адрес источника; • `source-port` — порт источника; • `dest-ip` — IP-адрес назначения; • `dest-port` — порт назначения; • `vlan-tag` — тег VLAN; • `interface-name` — название интерфейса; • `node-name` — название узла; • `protocol` — протокол
`connections`	Отображение информации о соединениях: протокол и его номер; время жизни записи; IP-адреса источника и назначения, порты источника и назначения; IP-адреса источника и назначения, порты источника и назначения, которые ожидаются в ответе; статус сессии (UNREPLIED или ASSURED); количество переданных и принятых пакетов и байтов; зона источника; является ли эта сессия сессией известного SWG пользователя и т. п.. Возможна фильтрация по параметрам: • `protocol` — протокол; • `source-ip` — IP-адрес источника; • `dest-ip` — IP-адрес назначения; • `node-name` — название узла; • `expect` — отображение неустановленных соединений (`on/off`)

Пример команды мониторинга трафика:

```
Admin@SWG> show traffic connections dest-ip 192.168.0.100 expect on
```

Просмотр информации LLDP

Для просмотра информации, полученной по LLDP (Link Layer Discovery Protocol) используется команда:

Admin@SWG> show lldp <parameters>

Параметры фильтрации.

Параметр	Описание
`neighbors`	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • `Chassis ID` — идентификатор шасси. • `SysName` — имя системы. • `SysDescr` — описание системы, содержит информацию об оборудовании и операционной системе устройства. • `Management` — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • `Capability` — функции устройства (например, маршрутизатор, коммутатор и т. п.). • `Port ID` — идентификатор порта с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • `PortDescr` — описание порта. • `TTL` — время жизни передаваемых пакетов LLDP
`statistics`	Статистика интерфейсов, в настройках которых был указан профиль LLDP. • `Interface` — название интерфейса. • `Transmitted` — общее количество кадров LLDP, переданных через интерфейс. • `Received` — общее количество кадров LLDP, полученных на интерфейсе. • `Discarded` — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • `Unrecognized` — количество кадров LLDP с неподтвержденным содержимым, полученных на этом интерфейсе. • `Ageout` — в каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в

Параметр	Описание
	течение срока старения новых кадров не принято, информация LLDP удаляется. • `Inserted` — количество добавлений записей с информацией о соседях LLDP. • `Deleted` — количество удалений записей о соседях LLDP

Маршруты

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

```
Admin@SWG> show network route <parameters>
```

Параметры просмотра маршрутов.

Параметр	Описание
`ip`	IP-адрес, маршрут до которого необходимо отобразить
`connected`	Маршруты к сетям, которые подключены непосредственно к интерфейсам SWG. 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 выполняется с помощью команд, представленных ниже. Отображение информации OSPF:

```
Admin@SWG> show network ospf
...
Admin@SWG> show network ospf <parameter>
```

Параметр	Описание
`virtual-router`	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF: (`<vrf-name>` | `all`)
`route`	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF
`database`	Отображена информация: • Router Link States: пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны; используются для передачи информации соседним маршрутизаторам, 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, подключенных к его сегменту напрямую. • Summary Link States: пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • ASBR-Summary Link States: пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора (Autonomous System Border Router, ASBR) в других областях
`neighbor`	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора).

Параметр	Описание
	• Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором - Designated Router, DR. Если приоритеты маршрутизаторов равны, то будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например, Full/DR, Full/BDR, Full/Drother. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Доступно указание дополнительных параметров: • `interface-name` — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • `all` — отображение таблицы со всеми соседях. • `detail` — отображение подробной информации о соседях
`interface`	Отображение информации об интерфейсах OSPF. Дополнительно: • `interface-name` — отображение информации об указанном интерфейсе. • `traffic` — статистика переданных и принятых пакетов OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment)
`border-routers`	Отображение информации о пограничных маршрутизаторах

Команда для перезапуска процесса OSPF:

```
Admin@SWG> clear network ospf <parameter>
```

Параметр	Описание
`interface-name`	Название интерфейса

Параметр	Описание
`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

Для отображения таблиц BGP-маршрутизатора:

```
Admin@SWG> show network bgp
...
Admin@SWG> show network bgp <parameter>
```

Параметр	Описание
`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 определенном соседе; необходимо указание IP-адреса соседа). Дополнительные параметры, доступные при указании соседа: • `received-routes` — принятые маршруты до применения к ним входящей политики (Routemap и фильтры). • `advertised-routes` — маршруты, которые анонсируются указанному соседу
`summary`	Просмотр краткой информации о соседях

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии):

```
Admin@nodename> clear network bgp <parameter>
```

Параметры команды.

Параметр	Описание
`ip`	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации
`virtual-router`	Название виртуального маршрутизатора, которому принадлежит BGP-сосед

В случае, если на соседних устройствах поддерживается метод Route Refresh, то можно избежать полной реинициализации сессии с соседом, отправив специальное сообщение типа ROUTE REFRESH. Отправка данного сообщения позволяет обновить информацию без прерывания в маршрутизации.

Для обновления информации без обрыва сессии с соседом используется команда:

```
Admin@SWG> clear network bgp ip <neighbor-ip> soft in | out
Admin@SWG> clear network bgp virtual-router <vrf-name> ip <neighbor-ip>
soft in | out
```

Мониторинг RIP

Для отображения информации RIP из таблицы маршрутизатора по умолчанию (адрес сети, полученный по RIP; адрес Next Hop; метрика маршрута; тэг маршрута, предназначенный для разделения внутренних и внешних маршрутов; интервал времени, по истечении которого маршрут будет признан недействительным, если информация о нем не была получена) используется команда:

```
Admin@SWG> show network rip
...
Admin@SWG> show network rip <parameter>
```

Параметры команды.

Параметр	Описание
`status`	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т. п.
`virtual-router`	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить: `<vrf-name>` | `all`

Мониторинг мультикаст-трафика

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию используется команда:

```
Admin@SWG> show network mroute
...
Admin@SWG> show network mroute <parameter>
```

Параметры команды.

Параметр	Описание
`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 определенного IP-адреса; далее необходимо указать IP-адрес
`ip`	Отображение записи для определенного IP-адреса; необходимо указать IP-адрес

Мониторинг IGMP

Мониторинг работы протокола IGMP (Internet Group Management Protocol) доступен с использованием следующей команды (указание параметров является обязательным):

```
Admin@SWG> show network igmp <parameters>
```

Параметры команды.

Параметр	Описание
`virtual-router`	Выбор виртуального маршрутизатора
`statistics`	Статистика по сообщениям: • IGMP Membership Query — сообщение сервера клиенту, в котором сервер просит обновить подписку на получаемые клиентом группы иначе, сервер перестанет вещать группу/группы в данный сегмент сети. • IGMP Leave — сообщение клиента серверу; клиент сообщает, что желает убрать мультикаст-группу из списка получаемых. • IGMP Membership Report — сообщение клиента серверу; клиент желает получать трафик этой группы
`join`	Отображение информации о группах IGMP
`sources`	Отображение информации об источниках мультикаст-трафика
`groups`	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: • Общее количество групп. • Интерфейс, через который группа доступна. • Адрес группы. • Режим INCLUDE или EXCLUDE. • Таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report. • Время, в течение которого группа известна
`interface`	Отображение информации об интерфейсе, связанной с мультикаст-маршрутизацией: • Название интерфейса, его статус и адрес. • Версия IGMP. • Опрашиватель и его адрес (Querier).

Параметр	Описание
	• Таймер, который обнуляется каждый раз, как приходит сообщение Query с меньшим IP-адресом. Доступно указание: • `interface-name` — название интерфейса. • `detail` — подробная информация об интерфейсе

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды:

```
Admin@SWG> show network pim <parameter>
```

Параметры команды.

Параметр	Описание
`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`	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List)

Параметр	Описание
`rp-info`	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP
`interface`	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т.п. Также доступно указание параметров: • `interface-name` — название интерфейса. • `traffic` — статистика отправленных/полученных сообщений. • `detail` — подробная информация об интерфейсе
`group-type`	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
`secondary`	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Отображение системной информации

Для просмотра версии ПО системы используется команда:

```
Admin@SWG> show system version
```

Для отображения информации о количестве активных TCP/UDP/ICMP сессий на системе используется команда:

```
Admin@SWG> show system sessions
```

Для отображения информации о количестве активных сессий по отдельным протоколам или временным интервалам используется команда:

```
Admin@SWG> show system sessions counters [ parameters ]
```

Очистить статистику:

```
Admin@SWG> clear system sessions
```

Диагностика работы протоколов динамической маршрутизации

С помощью команд этого раздела можно просматривать события debug-логов протоколов динамической маршрутизации. Включение в debug-лог событий конкретного протокола выполняется командой debug в режиме конфигурации.

Для просмотра записей debug-лога используется команда:

```
Admin@SWG> show logs log routing <parameters>
```

Далее необходимо указать один из параметров:

Параметр	Описание
`all`	Все протоколы
`rip`	Протокол RIP
`bgp`	Протокол BGP
`igmp`	Протокол IGMP
`pim`	Протокол PIM
`ospf`	Протокол OSPF
`bfd`	Протокол BFD
`msdp`	Протокол MSDP
`mroute`	Таблица мультикаст-маршрутизации mroute
`ssmpingd`	Инструмент тестирования мультикаст-вещания ssmpingd

Для вывода событий debug-лога в консоль в реальном времени используется команда:

Просмотр системных журналов устройства

Для просмотра событий системных журналов устройства используется команда:

```
Admin@SWG> show logs log core <static | dynamic>
```

Параметры команды (static или dynamic) определяют режим отображения сообщений журналов в консоли.

Команды режима конфигурации

В режиме конфигурации доступны команды `execute` (команды, которые не относятся к настройке конфигурации устройства — ping, date, traceroute и т.п.), базовые команды настройки устройства и команды настройки сети (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, статических ARP-записей).

Команды `execute`

Команды имеют следующую структуру:

```
Admin@nodename# execute <command-name>
```

Список команд раздела `execute`.

Команда	Описание
`date`	Просмотр текущих значений даты и времени на узле: `Admin@SWG# execute date`

`dig`	Проверка записи DNS домена:
	`Admin@SWG# execute dig host <hostname> <parameters>`
	`Admin@SWG# execute dig host <IP-address> <parameters>`
	В команде можно использовать следующие параметры:
	• `reverse-lookup` — получение имени устройства по IP-адресу;
	• `dns` — указание IP-адреса DNS-сервера;
	• `tcp` — использование протокола TCP вместо UDP

`factory-reset`	Возврат устройства в первоначальное состояние (доступно в версии 7.5.0 и выше):

Команда	Описание
	`Admin@SWG# execute factory-reset` Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды

`install`	Первоначальная настройка устройства.
	
	`Admin@SWG# execute install <parameter>`
	
	• `master` — настройка устройства в качестве главного узла. Задайте логин и пароль администратора.
	• `slave` — настройка устройства в качестве дополнительного узла кластера. Укажите следующие параметры:
	  ◦ interface — интерфейса для подключения к кластеру;
	  ◦ master-ip — IP-адрес главного узла;
	  ◦ master-secret — секретный код, необходимый для подключения узла в кластер;
	  ◦ slave-ip — IP-адрес резервного узла, который будет назначен на интерфейс, используемый для подключения к кластеру. Можно указать в виде IP-адреса (например, 192.168.0.1) или в виде IP-адреса и маски подсети (например, 192.168.0.1/24). Доступно в версии 7.4.0 и выше.
	  ◦ gateway-address — IP-адрес шлюза. Шлюз необходимо указать, если узлы кластера находятся в разных подсетях.
	• `mc` — настройка устройства через UserGate Management Center. Укажите следующие параметры:
	  ◦ device-code — уникальный код устройства, используемый для подключения узла к UGMC;
	  ◦ mc-ip — IP-адрес UGMC;
	  ◦ login — задать логин администратора SWG;
	  ◦ password — задать пароль учетной записи администратора SWG

`netcheck`	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • `address` — доменное имя узла для проверки доступности по TCP или URL — для HTTP; • `dns-ip` — IP-адрес сервера DNS;

Команда	Описание

	• `dns-tcp` — использование TCP вместо UDP для DNS-запроса;
	• `check-cert` — проверка SSL-сертификата;
	• `type` — проверка доступности по:
	  ◦ `http;`
	  ◦ `tcp` (если порт не указан, то используется порт 80);
	• `data` — запрос содержимого сайта. По умолчанию запрашиваются только заголовки;
	• `timeout` — максимальный тайм-аут ожидания ответа от веб-сервера;
	• `user-agent` — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin@SWG# execute netcheck type tcp address <host-domain-name> data on`
	`Admin@SWG# execute netcheck address <host-domain-name>`

`ping`	Проверка доступности определенного узла. Можно задать следующие параметры: • `host` — IP-адрес или доменное имя узла. • `count` — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш `Ctrl + C`). • `numeric` — не определять имена. • `timestamp` — отображение временных меток. • `interval` — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • `ttl` — время жизни пакета. • `interface` — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения `ping`. • `mtu` — максимальный размер блока данных отправляемых пакетов.

Команда	Описание
	• `virtual-router` — имя виртуального маршрутизатора. `Admin@SWG# execute ping host <hostname> count <number>`
`reboot`	Перезагрузка устройства: `Admin@SWG# execute reboot`
`restore-mac`	Восстановление mac-адреса интерфейса: `Admin@SWG# execute restore-mac interface <interface-name>`
`shutdown`	Выключение устройства: `Admin@SWG# execute shutdown`
`traceroute`	Трассировка соединения до определенного узла. Параметры команды: • `host <ip-or-domain>` — IP-адрес или имя домена, для которого производится трассировка; • `interface <iface-name>` — интерфейс, с которого будут отправляться пакеты; • `not-map-ip` — не искать hostname для IP-адреса при отображении; • `use-icmp-echo` — использовать ICMP echo; • `port` — указать порт вместо порта по умолчанию (1 — 65535); • `min-interval` — минимальный интервал между пакетами. `Admin@SWG# execute traceroute host <hostname>`

Команды настройки устройства

На уровне `settings cli` настраиваются следующие параметры работы интерфейса командной строки:

- вид системного приглашения (prompt) консоли CLI;
- уровень детализации диагностики.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@SWG# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида: `Admin@nodename#`) на удобное вам.

Например, чтобы поменять вид системного приглашения на `NodeAABBCC`, выполните следующую команду:

```
Admin@SWG# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@SWG# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@SWG#
```

Чтобы задать уровень детализации диагностики используется следующая команда:

```
Admin@SWG# set settings cli log-level <off | error | debug | warning |
info>
```

Вы можете установить следующие уровни детализации:

- `off` — отключить журналирование;
- `error` — только ошибки;
- `warning` — ошибки и предупреждения;
- `info` — ошибки, предупреждения и дополнительная информация;
- `debug` — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:

```
Admin@SWG# show settings cli
```

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@SWG# set settings fastpath enabled <on/off>
```

Для просмотра настройки режима ускоренной обработки трафика используется команда:

```
Admin@SWG# show settings fastpath
```

Команды настройки сетевых параметров устройства

Настройки сетевых параметров выполняются на уровне `network`.

Настройка зон

Для создания зоны используется команда:

```
Admin@SWG# create network zone <parameter>
```

Параметры настройки зон.

Параметр	Описание
`name`	Название зоны
`dos-protection-syn`	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • `enabled` — включение/отключение защиты. • `aggregate` — суммирование пакетов: ◦ `on` — считаются все пакеты, входящие в интерфейсы данной зоны; ◦ `off` — пакеты считаются отдельно для каждого IP-адреса. • `alert-threshold` — порог уведомления. Если количество запросов превышает указанный порог, происходит запись события в системный журнал. • `drop-threshold` — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, UserGate отбрасывает пакеты и записывает это событие в системный журнал. • `excluded-ips` — список IP-адресов, которые необходимо исключить из защиты
`dos-protection-udp`	Защита зоны от сетевого флуда для протокола UDP: • `enabled` — включение/отключение защиты. • `aggregate` — суммирование пакетов: ◦ `on` — считаются все пакеты, входящие в интерфейсы данной зоны; ◦ `off` — пакеты считаются отдельно для каждого IP-адреса. • `alert-threshold` — порог уведомления. Если количество запросов превышает данный порог, то происходит запись события в системный журнал. • `drop-threshold` — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • `excluded-ips` — список IP-адресов серверов, которые необходимо исключить из защиты
`dos-protection-icmp`	Защита зоны от сетевого флуда для протокола ICMP: • `enabled` — включение/отключение защиты. • `aggregate` — суммирование пакетов: ◦ `on` — считаются все пакеты, входящие в интерфейсы данной зоны;

Параметр	Описание
	◦ `off` — пакеты считаются отдельно для каждого IP-адреса. • `alert-threshold` — порог уведомления. Если количество запросов превышает данный порог, то происходит запись события в системный журнал. • `drop-threshold` — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • `excluded-ips` — список IP-адресов серверов, которые необходимо исключить из защиты
`enabled-services`	Параметры контроля доступа зоны: • `"Any ICMP"`: разрешение использования команды ping адреса UserGate. • `SNMP`: доступ к UserGate по протоколу SNMP (UDP 161). • `response-pages`: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • `rpc`: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • `ha`: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • `VRRP`: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • `"Admin Console"`: доступ к веб-консоли управления (TCP 8001). • `DNS`: доступ к сервису DNS-прокси (TCP 53, UDP 53). • `"HTTP Proxy"`: доступ к сервису HTTP(S)-прокси (TCP 8090). • `"Authorization agent"`: доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • `"SMTP Proxy"`: сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • `"POP3 Proxy"`: сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • `"CLI over SSH"`: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.

Параметр	Описание
	• `VPN`: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • `SCADA`: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • `"REVERSE PROXY"`: сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • `"PROXY PORTAL"`: сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • `L7 DNS`: детектирование трафика DNS на уровне приложений. • `L7 NTP`: детектирование трафика NTP на уровне приложений. • `"SAML SERVER"`: выбор SAML-сервера в списке сервисов зоны и общих настройках UserGate. • `"Log Analyzer"`: сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713). • `"Dynamic routing OSPF"`: сервис динамической маршрутизации OSPF. • `"Dynamic routing BGP"`: сервис динамической маршрутизации BGP. • `"SNMP Proxy"`: сервис используется для построения распределенной системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределенной сетевой инфраструктуры). • `"SSH Proxy"`: сервис, использующийся для инициирования трафика SSH. • `Multicast`: сервис мультикастинга. • `NTP`: доступ к сервису точного времени, запущенному на сервере UserGate. • `"Dynamic routing RIP"`: сервис динамической маршрутизации RIP. • `UserID agent`: сервис для осуществления прозрачной аутентификации. В качестве источника данных аутентификации используются журналы ActiveDirectory и Syslog. • `BFD`: сервис Bidirectonal Forwarding Detection для быстрого обнаружения сетевых ошибок
`service-addresses`	

Параметр	Описание
	Указание разрешенных IP-адресов для сервисов: • `service` — выбор сервисов (список соответствует `enabled-services`); • `allowed-addresses` — разрешенные адреса: ◦ `allowed-ips` — указать разрешенные IP-адреса; ◦ `geoip` — указать код GeoIP; ◦ `ip-list` — указать заранее созданный в библиотеке элементов список IP-адресов
`antispoof-enabled`	Включение/отключение защиты от IP-спуфинга
`antispoof-negate`	При `antispoof-negate on` адреса источников, указанные в значении `ip-spoofing-networks`, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников
`geoip`	Коды GeoIP, которые используются в защите от IP-спуфинга
`ip-list`	Список IP-адресов, которые используются в защите от IP-спуфинга

Для изменения параметров зоны используется команда:

```
Admin@nodename# set network zone <zone-name> <parameters>
```

Пример изменения параметров зоны:

```
Admin@SWG# set network zone Test_zone dos-protection-syn enabled on
```

Для удаления зоны или ее параметров используется команда:

```
Admin@nodename# delete network zone <zone-name>
```

Для просмотра параметров зон используется команда:

```
Admin@SWG# show network zone
```

Настройка интерфейсов

Вы можете настроить следующие типы интерфейсов:

- bond;
- bridge;
- loopback;
- pppoe;
- vlan;
- adapter.

Для создания bond-интерфейса используется команда:

```
Admin@SWG# create network interface bond <parameters>
```

Параметры bond-интерфейса.

Параметр	Описание
enabled	Включение/отключение интерфейса
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1)
zone	Зона, которой будет принадлежать бонд-интерфейс
bonding	Дополнительные параметры бонд-интерфейса: • mode — режим работы бонда: ◦ round-robin — режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ active-backup — режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором.

Параметр	Описание
	Данная политика применяется для обеспечения отказоустойчивости). ◦ `xor` — режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). ◦ `broadcast` — режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ `802.3ad` — режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). ◦ `transmit` — режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). ◦ `load` — режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего

Параметр	Описание

	трафика распределяется последовательно (round-robin) между интерфейсами.
	• `mii-monitoring` — периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов.
	• `down-delay` — время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon.
	• `up-delay` — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon.
	• `lacp-rate` — интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:
	  ◦ `slow` — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд;
	  ◦ `fast` — запрос партнера на передачу LACPDU-пакетов каждую секунду.
	• `failover-mac` — определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения:
	  ◦ `disabled` — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.
	  ◦ `active` — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа.
	  ◦ `follow` — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Параметр	Описание

	• `xmit-hash` — определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:
	  ◦ `l2` — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad.
	  ◦ `l2-3` — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.
	  ◦ `l3-4` — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и 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
`ip-addresses`	Назначение IP-адреса для интерфейса. Адрес задается в следующем виде: `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон**

Параметр	Описание
`mac`	MAC-адрес интерфейса
`mtu`	Указание размер MTU
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение/отключения ретранслятора. • `utm-address` — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего бонд-интерфейса используется команда:

```
Admin@SWG# set network interface bond <bond-name>
```

Для удаления бонд-интерфейса или его параметров используется команда:

```
Admin@SWG# delete network interface bond <bond-name>
```

Параметры, доступные для удаления.

Параметр	Описание
`ip-addresses`	Заданный IP-адрес
`dhcp-relay server-address`	IP-адрес сервера DHCP
`bonding interface`	Интерфейсы, объединенные в бонд

Чтобы просмотреть информацию о всех бонд-интерфейсах, используйте команду:

```
Admin@SWG# show network interface bond
```

или об определенном интерфейсе:

```
Admin@SWG# show network interface bond <bond-name>
```

Для создания bridge-интерфейса используется команда:

```
Admin@nodename# create network interface bridge
```

Параметры bridge-интерфейса.

Параметр	Описание
`enabled`	Включение/отключение моста
`interface-name`	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет bridge1)
`zone`	Зона, которой будет принадлежать мост
`bridging`	Дополнительные параметры моста: • `iface-type` — режим работы интерфейса: ◦ `l2` — Layer 2 (создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security; контентная фильтрация в этом режиме работает). ◦ `l3` — Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • `interface` — интерфейсы, которые будут использованы для создания моста. • `stp` — включение/отключение использование STP (Spanning Tree Protocol) для защиты от петель. • `forward-delay` — задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP (указывается в секундах). • `max-age` — время, по истечении которого STP-соединение считается потерянным (указывается в секундах).

Параметр	Описание
	• `bypass-pair` — пара интерфейсов, которая будет использована для построения байпас-моста. Необходима поддержка оборудования ПАК UserGate
`iface-mode`	Режим назначения IP-адреса: • `dhcp` — получение динамического IP-адреса по DHCP; • `manual` — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
`ip-addresses`	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон**
`mac`	MAC-адрес интерфейса
`mtu`	Указание размера MTU
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение/отключения ретранслятора. • `utm-address` — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bridge-интерфейса используется команда:

```
Admin@SWG# set network interface bridge <bridge-name>
```

Для удаления bridge-интерфейса или его параметров используется команда:

```
Admin@SWG# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления.

Параметр	Описание
`ip-addresses`	Заданный IP-адрес
`dhcp-relay server-address`	IP-адрес сервера DHCP

Для просмотра информации о всех bridge-интерфейсах используется команда:

```
Admin@SWG# show network interface bridge
```

или об определенном интерфейсе:

```
Admin@SWG# show network interface bridge <bridge-name>
```

Для создания loopback-интерфейса используется команда:

```
Admin@SWG# create network interface loopback <parameters>
```

Параметры loopback-интерфейса.

Параметр	Описание
`enabled`	Включение/отключение интерфейса
`interface-name`	Название интерфейса
`ip-addresses`	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: `[ <ip_address/mask> ]`, маска подсети задается в десятичном виде.

Параметр	Описание
	Важно! **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон**
`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
`mac`	MAC-адрес интерфейса
`mtu`	Указание размера MTU
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение/отключения ретранслятора. • `utm-address` — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения <`ip` | `none`>). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего интерфейса используется команда:

```
Admin@SWG# set network interface loopback <interface-name>
```

Для удаления loopback-интерфейса или его параметров используется команда:

```
Admin@SWG# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления.

Параметр	Описание
`ip-addresses`	Заданный IP-адрес
`dhcp-relay`	IP-адрес сервера DHCP

Для просмотра информации о всех loopback-интерфейсах используется команда:

```
Admin@SWG# show network interface loopback
```

Об определенном интерфейсе:

```
Admin@SWG# show network interface loopback <interface-name>
```

Для создания интерфейса PPPoE используется команда:

```
Admin@SWG# create network interface pppoe
```

Параметры PPPoE-интерфейса.

Параметр	Описание
`enabled`	Включение/отключение интерфейса PPPoE
`interface-name`	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет ppp1)
`zone`	Зона, которой будет принадлежать интерфейс
`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; • `auth-type` — тип авторизации: ◦ CHAP;

Параметр	Описание
	◦ PAP; • `holdoff` — интервал времени в секундах после разрыва соединения перед повторным запуском; • `default-route` — интерфейс PPPoE в качестве маршрута по умолчанию; • `echo-interval` — интервал проверки соединения; • `echo-failure` — количество неуспешных проверок соединения, после которого SWG считает, что соединение отсутствует и разрывает его; • `providers-dns` — использование DNS-серверов, выданных провайдером; • `connection-attempts` — количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены; • `service-name` — имя сервиса необходимо прописывать в случае предоставления провайдером
`mtu`	Указание размера MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet

Для изменения существующего интерфейса PPPoE используется команда:

```
Admin@SWG# set network interface pppoe <pppoe-name>
```

Для удаления интерфейса PPPoE используется команда:

```
Admin@SWG# delete network interface pppoe <pppoe-name>
```

Для просмотра информации о всех интерфейсах PPPoE используется команда:

```
Admin@SWG# show network interface pppoe
```

Об определенном интерфейсе:

```
Admin@SWG# show network interface pppoe <pppoe-name>
```

Для создания нового VLAN-интерфейса используется команда:

```
Admin@SWG# create network interface vlan <parameters>
```

Параметры VLAN-интерфейса.

Параметр	Описание
`enabled`	Включение/отключение VLAN-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
`interface`	Физический интерфейс, на котором создается VLAN
`zone`	Зона, которой будет принадлежать интерфейс
`ip-addresses`	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде. **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон**
`mac`	MAC-адрес интерфейса

Параметр	Описание
`mtu`	Указание размера MTU
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение/отключения ретранслятора. • `utm-address` — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего VLAN-интерфейса используется команда:

```
Admin@SWG# set network interface vlan <vlan-name>
```

Для удаления VLAN-интерфейса или его параметров используется команда:

```
Admin@SWG# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления.

Параметр	Описание
`ip-addresses`	Заданный IP-адрес
`dhcp-relay server-address`	IP-адрес сервера DHCP

Для просмотра информации о всех VLAN-интерфейсах используется команда :

```
Admin@SWG# show network interface vlan
```

Об определенном интерфейсе:

```
Admin@SWG# show network interface vlan <vlan-name>
```

Настройка сетевых адаптеров

Сетевые адаптеры создать нельзя, но вы можете настраивать параметры сетевых адаптеров устройства с помощью следующей команды:

```
Admin@SWG# set network interface adapter <adapter-name>
```

Параметры сетевых адаптеров.

Параметр	Описание
`enabled`	Включение/отключение сетевого 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
`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**

Параметр	Описание
`mac`	MAC-адрес интерфейса
`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-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение/отключения ретранслятора. • `utm-address` — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения <ip | none>). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для удаления параметров адаптеров используется команда:

```
Admin@SWG# delete network interface adapter <adapter-name> <parameters>
```

Параметры, доступные для удаления.

Параметр	Описание
`ip-addresses`	Заданный IP-адрес
`dhcp-relay server-address`	IP-адрес сервера DHCP

Для просмотра параметров сетевых адаптеров используется команда:

```
Admin@SWG# show network interface adapter <adapter-name>
```

Настройка шлюзов

Для создания шлюза используется команда:

Admin@SWG# create network gateway <parameters>

Параметры шлюза.

Параметр	Описание
`enabled`	Включение/отключение шлюза
`interface`	Интерфейс, используемый для выхода в Интернет: • `port` — выбор конкретного порта (port0, port1, port2 и т. д.); • `auto` — после выбора этого параметра порт определится автоматически. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0
`virtual-router`	Виртуальный маршрутизатор, для которого настраивается шлюз
`ip`	IP-адрес шлюза
`weight`	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз)
`balancing`	Включение режима балансировки — весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами
`default`	Использование данного шлюза в качестве шлюза по умолчанию

Для изменения параметров шлюза используется команда:

```
Admin@SWG# set network gateway <gateway-name>
```

Для удаления шлюза используется команда:

```
Admin@SWG# delete network gateway <gateway-name>
```

Для просмотра информации о всех шлюзах используется команда:

```
Admin@SWG# show network gateway
```

Об определенном шлюзе:

```
Admin@SWG# show network gateway <gateway-name>
```

Настройка виртуальных маршрутизаторов

Для создания виртуального маршрутизатора используется команда:

```
Admin@SWG# create network virtual-router <parameters>
```

Параметры виртуального маршрутизатора.

Параметр	Описание
`name`	Уникальное имя виртуального маршрутизатора
`interfaces`	Интерфейсы, которые будут использованы в виртуальном маршрутизаторе. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, добавлены быть не могут; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие

`routes`	Добавление статических маршрутов.
	• `destination-ip` — IP-адрес подсети назначения. Указывается в формате `<ip/mask>`.
	• `type` — тип маршрута:
	  ◦ `unicast` — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз.
	  ◦ `unreachable` — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (type 3 code 1).
	  ◦ `prohibit` — трафик отбрасывается. Источнику отправляется ICMP-сообщение `host unreachable` (type 3 code 13).
	  ◦ `blackhole` — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
	• `enabled` — включение/отключение использования статического маршрута.
	• `gateway` — IP-адрес шлюза, через который будет доступна указанная подсеть. Этот IP-адрес должен быть доступен с устройства.

Параметр	Описание
	• `metric` — метрика маршрута. Маршрут с меньшей метрикой более приоритетен

Для изменения параметров виртуального маршрутизатора используется команда:

```
Admin@SWG# set network virtual-router <virtual-router-name>
```

Для удаления виртуального маршрутизатора или его параметров используется команда:

```
 Admin@SWG# delete network virtual-router <virtual-router-name>
<parameters>
```

Для просмотра информации о всех виртуальных маршрутизаторах используется команда:

```
 Admin@SWG# show network virtual-router
```

Об определенном виртуальном маршрутизаторе:

```
Admin@SWG# show network virtual-router <virtual-router-name>
```

Статические ARP-записи

Для добавления статических ARP-записей используется команда:

```
Admin@SWG# set network arp host <IP-address> interface <interface-name>
mac <MAC-address>
```

Параметры статических ARP-записей.

Параметр	Описание
`interface`	Название интерфейса SWG

Параметр	Описание
`host`	IP-адрес устройства
`mac`	MAC-адрес устройства

Для удаления статических ARP-записей используется команда:

```
Admin@SWG# delete network arp host <host-ip-address> interfaces [ port1
port2 ]
```

Журналирование событий протоколов маршрутизации

Команда debug позволяет включить журналирование событий протоколов маршрутизации в режиме отладки. События записываются в debug-журнал. Их просмотр также возможен в режиме диагностики консоли CLI.

Для включения журналирования конкретного протокола маршрутизации используется команда:

```
Admin@SWG# debug <protocol> <parameters>
```

Поддерживаются следующие протоколы:

Параметр	Описание
`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

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация UserGate SWG

При первоначальной инициализации UserGate SWG в интерфейсе командной строки доступны три режима конфигурации:

- Автономный (главный) узел.
- Дополнительный узел кластера.
- Управление через UserGate Management Center.

Автономный узел

Для настройки UserGate SWG в качестве автономного узла используется команда:

```
Admin@nodename# execute install master login <login-name> password
<password>
```

Необходимо задать логин и пароль администратора устройства.

Дополнительный узел кластера

Для настройки UserGate SWG в качестве дополнительного узла кластера используется команда:

```
Admin@nodename# execute install slave <parameters>
```

Дополнительные параметры настройки.

Параметр	Описание
`interface`	Интерфейс для подключения к кластеру
`slave-ip`	IP-адрес резервного узла, который будет назначен на интерфейс, использующийся для подключения к кластеру.

Параметр	Описание
	Возможные опции: • ip — IP-адрес (например, 192.168.0.1); • ip/mask — IP-адрес и маска подсети (например, 192.168.0.1/24)
`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

Управление через UserGate Management Center

Для настройки UserGate SWG с помощью UGMC используется команда:

```
Admin@nodename# execute install mc <parameters>
```

Укажите дополнительные параметры настройки.

Параметр	Описание
`login`	Логин администратора SWG
`password`	Пароль учетной записи администратора
`mc-ip`	IP-адрес сервера UGMC
`device-code`	Уникальный код устройства, использующийся для подключения узла к UGMC

КОМАНДЫ ДИАГНОСТИКИ И МОНИТОРИНГА

Команды диагностики и мониторинга

С помощью команд режима диагностики CLI вы можете просматривать информацию о системе, выполнять базовые команды управления системой, получать информацию о доступности сетевого окружения, выполнять мониторинг трафика по заданным параметрам.

Базовые команды управления

Для перезагрузки узла:

```
Admin@nodename> reboot
```

Для выключения узла:

```
Admin@nodename> shutdown
```

Для перехода в режим конфигурации CLI:

```
Admin@nodename> configure
```

Для выхода из интерфейса CLI:

```
Admin@nodename> exit
```

Команды просмотра системной информации

Для просмотра версии ПО системы:

```
Admin@nodename> show system version
```

Для просмотра количества активных сессий TCP/UDP/ICMP:

```
Admin@nodename> show system sessions
```

Для просмотра количества активных сессий по отдельным протоколам или временным интервалам:

```
Admin@nodename> show system sessions counters [ parameters ]
```

Для очистки статистики:

```
Admin@nodename> clear system sessions
```

Для просмотра текущих даты и времени на узле:

```
Admin@nodename> date
```

Команды мониторинга состояния системы

Команды мониторинга позволяют отображать состояние компонентов системы в виде временных диаграмм.

С помощью команды `show monitoring <parameters>` вы можете получить информацию о состоянии процессора, дисковой подсистемы, интерфейсов, оперативной памяти, RAID-массива, просматривать статистику по рабочей температуре устройства и по DNS- и HTTP-запросам. Например:

```
Admin@nodename> show monitoring cpu
CPU used - %
 8.00 ┤
 7.47 ┤
 6.93 ┤
 6.40 ┤
 5.87 ┤
 5.33 ┤
 4.80 ┤
 4.27 ┤
 3.73 ┤
 3.20 ┤
       09:50 22/09                    13:25 22/09
Admin@nodename>
```

При использовании команды без аргументов будет последовательно выведено состояние всех системных объектов мониторинга:

```
Admin@nodename> show monitoring
```

С помощью аргументов команды вы можете выводить информацию о каждом объекте мониторинга по отдельности.

Для мониторинга загрузки процессора:

```
Admin@nodename> show monitoring cpu
```

Для мониторинга состояния файловой системы:

```
Admin@nodename> show monitoring disk-info
```

Для мониторинга состояния RAID-массива:

```
Admin@nodename> show monitoring raid
```

Для мониторинга загрузки дисковой подсистемы операциями ввода/вывода:

```
Admin@nodename> show monitoring disk-io
```

Для мониторинга загрузки swap-раздела:

```
Admin@nodename> show monitoring swap
```

Для мониторинга загрузки интерфейсов:

```
Admin@nodename> show monitoring interface <port-name>
```

Для мониторинга загрузки оперативной памяти:

```
Admin@nodename> show monitoring memory
```

Для мониторинга рабочей температуры устройства:

```
Admin@nodename> show monitoring temperature
```

Для мониторинга состояния источников питания:

```
Admin@nodename> show monitoring power-supply
```

Для мониторинга статистики DNS-запросов:

```
Admin@nodename> show monitoring dns-requests
```

Для мониторинга статистики HTTP-запросов:

```
Admin@nodename> show monitoring http-requests
```

Команды просмотра информации об интерфейсах

Для просмотра информации обо всех имеющихся в системе интерфейсах используйте команду:

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

Вы можете просмотреть статистику и подробную информацию об определенном интерфейсе. Для этого необходимо указать в команде его название:

```
Admin@nodename> show network interface <interface-name>
```

Также вы можете вывести отдельно информацию об интерфейсе либо статистику интерфейса:

```
Admin@nodename> show network interface <interface-name> type info
Admin@nodename> show network interface <interface-name> type statistics
```

Для просмотра списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов используйте команду:

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

> **Примечание**
> **Под физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. При использовании этой команды не отображаются изменения MAC-адресов в параметрах UserGate SWG. Измененные MAC-адреса можно посмотреть с помощью команды** `show network interface <interface-name>`**.**

Сортировка интерфейсов выполняется по номеру порта PCI-шины.

Для удаления списка используйте команду:

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

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов на настроенном устройстве UserGate.

Команды проверки доступности сетевых ресурсов

Для проверки доступности узла с помощью утилиты `ping` используйте команду:

```
Admin@nodename> ping <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`host`	IP-адрес или доменное имя узла
`count`	Количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет продолжаться, пока соединение не будет прервано пользователем. Чтобы прервать отправку запросов, используйте комбинацию клавиш `Ctrl + C`
`interface`	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для отправки echo-запросов

Параметр	Описание
`interval`	Интервал времени, определяющий частоту отправки пакетов. Указывается в секундах
`mtu`	Размер MTU отправляемых пакетов
`numeric`	Не определять имя узла
`ttl`	Время жизни пакета
`timestamp`	Отображение временных меток
`virtual-router`	Имя виртуального маршрутизатора

Для трассировки соединения до определенного узла используйте команду:

```
Admin@nodename> traceroute <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`host`	IP-адрес или доменное имя узла, для которого выполняется трассировка
`interface`	Интерфейс, с которого будут отправляться пакеты
`min-interval`	Минимальный интервал между отправкой пакетов
`not-map-ip`	Не искать имя узла для IP-адреса при отображении
`port`	Указать порт вместо порта по умолчанию (1–65535)
`use-icmp-echo`	Использовать ICMP-echo

Для проверки доступности удаленного HTTP/HTTPS-сервера используйте команду:

```
Admin@nodename> netcheck <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`address`	Адрес или имя узла для проверки доступности: • доменное имя узла для проверки доступности по TCP; • URL для проверки доступности по HTTP; • IP-адрес с портом для проверки по TCP (в этом случае в параметре `type` необходимо указать `tcp`)
`type`	Протокол для проверки доступности узла: • `http`; • `tcp` (если порт не указан, используется порт 80)
`check-cert`	Проверка SSL-сертификата
`dns-ip`	IP-адрес DNS-сервера
`dns-tcp`	Использование TCP вместо UDP для DNS-запроса
`data`	Запрос содержимого сайта. По умолчанию запрашиваются только заголовки
`timeout`	Максимальный тайм-аут ожидания ответа от веб-сервера
`user-agent`	Параметр для указания типа браузера (`useragent`). На некоторых сайтах может быть разрешен доступ только через определенные браузеры. Значение параметра указывается в двойных кавычках

Для проверки записи DNS-домена используйте команду:

```
Admin@nodename> dig <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`host`	Доменное имя узла или IP-адрес для реверсивного поиска
`dns`	Указание IP-адреса DNS-сервера
`reverse-lookup`	Получение имени узла по IP-адресу
`tcp`	Использование протокола TCP вместо UDP

Для проверки принадлежности IP-адреса по текущей базе GeoIP используйте команду:

```
Admin@nodename> check-geoip ip <IP-address>
```

Команды управления ARP-записями

Для просмотра информации об ARP-записях используйте команду:

```
Admin@nodename> show network arp
```

При просмотре записей вы можете использовать дополнительные фильтры.

Параметр	Описание

`node-name`	Название узла кластера, ARP-записи которого необходимо отобразить.
	Далее необходимо указать интерфейс или IP-адрес узла:
	`Admin@nodename> show network arp node-name <node-name> interface <iface-name>`
	`Admin@nodename> show network arp node-name <node-name> host <ip>`

`interface`	Название интерфейса UserGate SWG
`host`	IP-адрес устройства
`mac`	MAC-адрес устройства

```
Admin@nodename> show network arp host <IP-address>
Admin@nodename> show network arp interface <interface-name>
Admin@nodename> show network arp mac <MAC-address>
```

ARP-записи также можно просматривать в режиме конфигурации CLI. Команды просмотра в режиме конфигурации идентичны командам режима диагностики.

> **Примечание**
> **В режиме диагностики действия выполняются с системными ARP-записями; в режиме конфигурации — со статическими.**

Вы можете добавлять статические ARP-записи в режиме конфигурации с помощью команды:

```
Admin@nodename# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`node-name`	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP- и MAC-адреса устройства
`interface`	Название интерфейса UserGate SWG
`host`	IP-адрес устройства
`mac`	MAC-адрес устройства

Команды удаления системных и статических ARP-записей имеют аналогичную структуру, отличается действие, которое необходимо выполнить:

- `clear` — удаление системных записей в режиме диагностики;
- `delete` — удаление статических записей в режиме конфигурации.

Для удаления системной ARP-записи используйте команду:

```
Admin@nodename> clear network arp interface <iface-name> host <ip>
```

Чтобы удалить запись на другом узле кластера:

```
Admin@nodename> clear network arp interface <iface-name> node-name <node-name> host <ip>
```

Чтобы удалить все системные записи на заданном интерфейсе:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> … ]
```

Для удаления всех системных записей интерфейса другого узла:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> … ] node-name <node-name>
```

Команды отслеживания пакетов

В режиме диагностики CLI вы можете отслеживать сетевые пакеты с помощью команды:

```
Admin@nodename> show network trace
```

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации CLI на уровне `network`. Подробнее — в разделе «Настройка устройства».

В выводе команды отслеживания пакетов будет отображаться следующая информация:

- IP-адреса источника и назначения;
- сетевой протокол;
- названия портов источника и назначения;
- номера TCP/UDP-портов источника и назначения.

Команда отслеживания пакетов также доступна в режиме конфигурации.

Для выхода из режима отслеживания пакетов используйте комбинацию клавиш `Ctrl + C`.

Команды мониторинга трафика

Для мониторинга трафика используйте команду:

```
Admin@nodename> show traffic
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`flows`	Отображение информации о входящем и исходящем потоках. Вы можете установить фильтрацию по параметрам: • `source-ip` — IP-адрес источника; • `source-port` — порт источника; • `dest-ip` — IP-адрес назначения; • `dest-port` — порт назначения; • `vlan-tag` — тег VLAN; • `interface-name` — название интерфейса; • `node-name` — название узла; • `protocol` —протокол
`connections`	Отображение информации о соединениях. Вы можете установить фильтрацию по параметрам: • `protocol` — протокол; • `source-ip` — IP-адрес источника; • `dest-ip` — IP-адрес назначения; • `node-name` — название узла; • `expect` — отображение неустановленных соединений

Параметр	Описание
`capture`	Отображение захвата пакетов. Вы можете установить фильтрацию по параметрам: • `count` — количество захватываемых пакетов. Значение по умолчанию — 1000. Для захвата без ограничения количества пакетов явно укажите: `count unlimited`. • `destination` — IP-адрес назначения. • `destination-port` — порт назначения. • `ipv4-protocol` — номер протокола IPv4 (0–255). • `interfaces` — название интерфейса. • `protocol` — выбор протокола. • `rule` — выбор имеющегося правила для захвата пакетов. • `source` — IP-адрес источника. • `source-port` — порт источника

Пример команды мониторинга трафика:

```
Admin@nodename> show traffic connections node-name utmcore@dineanoulwer
dest-ip 192.168.0.100 expect on
```

Команды просмотра LLDP

Вы можете просматривать информацию о сетевом окружении, полученную по LLDP (Link Layer Discovery Protocol) с помощью команды:

```
Admin@nodename> show lldp <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`neighbors`	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • `Chassis ID` — идентификатор шасси. • `SysName` — имя системы.

Параметр	Описание
	• `SysDescr` — описание системы, содержит информацию об оборудовании и операционной системе устройства. • `Management` — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • `Capability` — функции устройства (например, маршрутизатор, коммутатор и т. п.). • `Port ID` — идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • `PortDescr` — описание порта. • `TTL` — время жизни передаваемых пакетов LLDP
`statistics`	Статистика интерфейсов, в параметрах которых был указан профиль LLDP: • `Interface` — название интерфейса. • `Transmitted` — общее количество кадров LLDP, переданных через интерфейс. • `Received` — общее количество кадров LLDP, полученных на интерфейсе. • `Discarded` — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • `Unrecognized` — количество кадров LLDP с неподтвержденным содержимым, полученных на этом интерфейсе. • `Ageout` — в каждом кадре LLDP содержится информация о том, насколько долго является актуальной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется. • `Inserted` — количество добавлений записей с информацией о соседях LLDP. • `Deleted` — количество удалений записей о соседях LLDP

Примечание

Для просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на UserGate SWG: профили LLDP должны быть настроены в библиотеке элементов и активированы в настройках интерфейсов.

Мониторинг работы протоколов маршрутизации

С помощью команд этого раздела вы можете выполнять мониторинг работы протоколов маршрутизации, настроенных на UserGate SWG.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используйте команду:

```
Admin@nodename> show network route
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`ip`	IP-адрес, маршрут до которого необходимо отобразить
`node-name`	Выбор узла кластера
`connected`	Маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate SWG. Такие маршруты помечены символом «C» в списке маршрутов
`kernel`	Маршруты, добавленные администратором. Маршруты помечены символом «K» в списке маршрутов
`summary`	Количество активных подключений и записей FIB (Forwarding Information Base)
`ospf`	Маршруты, полученные с помощью протокола динамической маршрутизации OSPF. Такие маршруты помечены символом «O» в списке маршрутов
`bgp`	Маршруты, полученные с помощью протокола динамической маршрутизации BGP. Такие маршруты помечены символом «B» в списке маршрутов
`rip`	Маршруты, полученные 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

С помощью команд этого раздела вы можете выполнять диагностику протокола OSPF.

Для просмотра информации протокола OSPF используйте команду:

```
Admin@nodename> show network ospf
...
Admin@nodename> show network ospf <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`node-name`	Выбор узла кластера
`virtual-router`	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF (`<vrf-name>` | `all`)
`route`	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF
`database`	Отображение информации: • `Router Link States` — пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны. Используются для передачи информации о собственных интерфейсах и своих соседях соседним маршрутизаторам, находящимся в той же зоне. • `Network Link States` — пакеты LSA Type 2 (Network LSA) генерируются выделенным маршрутизатором (Designated Router, DR) для описания всех маршрутизаторов, подключенных к его сегменту напрямую. • `Summary Link States` — пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • `ASBR-Summary Link States` — пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора

Параметр	Описание
	(Autonomous System Border Router, ASBR) в других областях
`neighbor`	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора). • Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором (Designated Router, DR). Если приоритеты маршрутизаторов равны, будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например `Full/DR`, `Full/BDR`, `Full/Drother`. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет `Hello`. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Дополнительные параметры: • `interface-name` — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • `all` — отображение таблицы со всеми соседями. • `detail` — отображение подробной информации о соседях
`interface`	Отображение информации об интерфейсах OSPF. Дополнительные параметры: • `interface-name` — отображение информации об указанном интерфейсе. • `traffic` — статистика переданных и принятых пакетов OSPF (`Hello`, `Database Description`, `Link State Request`, `Link State Update`, `Link State Acknowledgment`)
`border-routers`	Отображение информации о пограничных маршрутизаторах

Для перезапуска процесса OSPF используйте команду:

```
Admin@nodename> clear network ospf <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`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

С помощью команд этого раздела вы можете выполнять диагностику протокола BGP.

Для просмотра таблиц BGP-маршрутизатора используйте команду:

```
Admin@nodename> show network bgp
...
Admin@nodename> show network bgp <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`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`	

Параметр	Описание
	Отображение информации о BGP-соседях. Для отображения информации об определенном соседе укажите его IP-адреса Дополнительные параметры, доступные при указании соседа: • `received-routes` — принятые маршруты до применения к ним входящей политики (`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) используйте команду:

```
Admin@nodename> clear network bgp
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`ip`	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации
`node-name`	Выбор узла кластера
`virtual-router`	Название виртуального маршрутизатора, которому принадлежит BGP-сосед

Если на соседних устройствах поддерживается метод Route Refresh, вы можете избежать полной реинициализации сессии с соседом. Для этого необходимо отправить специальное сообщения `ROUTE REFRESH`, позволяющее обновить информацию без прерывания работы маршрутизации.

Для обновления информации без обрыва сессии с соседом используйте команду:

```
Admin@nodename> clear network bgp ip <neighbor-ip> soft in | out
Admin@nodename> clear network bgp virtual-router <vrf-name> ip
<neighbor-ip> soft in | out
```

Мониторинг RIP

С помощью команд этого раздела вы можете выполнять диагностику протокола RIP.

Для просмотра информации протокола RIP из таблицы маршрутизатора по умолчанию используйте команду:

```
Admin@nodename> show network rip
...
Admin@nodename> show network rip <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`node-name`	Выбор узла кластера
`status`	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т. п.
`virtual-router`	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить (`<vrf-name>` | `all`)

Мониторинг мультикаст-трафика

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию используйте команду:

```
Admin@nodename> show network mroute
...
Admin@nodename> show network mroute <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`node-name`	Выбор узла кластера
`count`	Отображение статистики о группе и источнике
`virtual-router`	Выбор виртуального маршрутизатора (`<vrf-name>` | `all`)
`summary`	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации
`fill`	Таблица маршрутизации мультикаст-трафика
`ip`	Отображение записи для определенного IP-адреса

Мониторинг IGMP

Для мониторинга работы протокола IGMP (Internet Group Management Protocol) используйте команду:

```
Admin@nodename> show network igmp <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`node-name`	Выбор узла кластера
`virtual-router`	Выбор виртуального маршрутизатора
`statistics`	Статистика по сообщениям: • IGMP Membership Query — сообщение от сервера к клиенту с директивой обновить подписку на получаемые клиентом группы. Без обновления сервер перестанет вещать группы в данном сегменте сети. • IGMP Leave — сообщение от клиента к серверу с запросом убрать мультикаст-группу из списка получаемых. • IGMP Membership Report — сообщение от клиента к серверу с запросом получать трафик этой группы
`join`	Отображение информации о группах IGMP

Параметр	Описание
`sources`	Отображение информации об источниках мультикаст-трафика
`groups`	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: • общее количество групп; • интерфейс, через который группа доступна; • адрес группы; • режим `INCLUDE` или `EXCLUDE`; • таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report; • время, в течение которого группа известна
`interface`	Отображение информации об интерфейсе, связанном с мультикаст-маршрутизацией: • название интерфейса, его статус и адрес; • версия IGMP; • опрашиватель (IGMP querier) и его адрес; • таймер, который обнуляется каждый раз, когда приходит сообщение `Query` с меньшим IP-адресом. Дополнительные параметры: • `interface-name` — название интерфейса; • `detail` — подробная информация об интерфейсе

Мониторинг PIM

Для мониторинга работы протокола PIM (Protocol-Independent Multicast) используйте команду:

```
Admin@ndename> show network pim <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
`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 протокола PIM
`neighbor`	Информация о соседях: • интерфейс, через который была получена информация о соседе; • адрес соседа; • время, прошедшее с последнего начала работы PIM; • время, в течение которого сосед доступен; • приоритет DR
`next-hop`	Записи об адресах next-hop
`state`	Информация об известных S, G маршрутах, Incoming Interface (IIF), Outgoing Interface List (OIL)
`rp-info`	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP
`interface`	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т. п. Дополнительные параметры: • `interface-name` — название интерфейса; • `traffic` — Статистика отправленных и полученных сообщений; • `detail` — подробная информация об интерфейсе
`group-type`	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
`secondary`	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Команды мониторинга состояния кластера

Команды мониторинга состояния кластера могут быть запущены на любом из узлов, входящих в кластер. Вы можете получить информацию о текущем состоянии кластера, его узлов, режиме работы кластера и истории переключения состояний.

Для мониторинга состояния кластера используйте команду:

```
Admin@nodename> show ha-cluster state
```

Для мониторинга состояния узлов кластера используйте команду:

```
Admin@nodename> show ha-cluster tablestat
```

Для просмотра информации об истории переключения состояния кластера используйте команду:

```
Admin@nodename> show ha-cluster failover
```

Команды просмотра журналов диагностики

С помощью команд этого раздела вы можете просматривать события, содержащиеся в журналах диагностики системы, в статическом и динамическом режиме.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log core static | grep ldap
```

Подробнее о функции фильтрации вывода — в разделе «Общие положения».

Просмотр системного журнала диагностики

Для вывода всего системного журнала диагностики в консоль используйте команду:

```
Admin@nodename> show logs log core static
```

Для вывода событий системного журнала диагностики в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log core dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш `Ctrl + C`.

Просмотр журналов диагностики протоколов маршрутизации

С помощью команд этого раздела вы можете просматривать события журналов диагностики протоколов маршрутизации. Включение в журналы событий выбранного протокола выполняется командой `debug` в режиме конфигурации (подробнее — в разделе «Режим конфигурации»).

Для вывода событий журнала диагностики в консоль используется команда вида:

```
Admin@nodename> show logs log routing <parameters> <static|dynamic>
```

В команде необходимо указать протоколы, для которых будут выводиться события диагностики.

Параметр	Описание
`all-routers`	Все протоколы
`rip`	Протокол RIP
`bgp`	Протокол BGP
`igmp`	Протокол IGMP
`pim`	Протокол PIM
`ospf`	Протокол OSPF
`bfd`	Протокол BFD
`msdp`	Протокол MSDP

Параметр	Описание
`mroute`	Таблица мультикаст-маршрутизации `mroute`
`ssmpingd`	Инструмент тестирования мультикаст-вещания `ssmpingd`

Для вывода всего журнала диагностики в консоль используйте команду:

```
Admin@nodename> show logs log routing <parameters> static
```

Для вывода событий журнала диагностики в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log routing <parameters> dynamic
```

Параметры команд аналогичны параметрам, указанным ранее.

Для отключения вывода событий журнала используйте комбинацию клавиш `Ctrl + C`.

Просмотр информации об авторизованных пользователях

Для просмотра информации обо всех авторизованных пользователях используйте команду:

```
Admin@nodename> show user-auth
```

Для просмотра деталей сессии определенного пользователя используйте команду:

```
Admin@nodename> show user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (`login`), так и его IP-адрес (`ip-address`).

Для удаления сессии определенного пользователя используйте команду:

```
Admin@nodename> clear user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (`login`), так и его IP-адрес (`ip-address`).

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации интерфейса командной строки используется команда:

```
Admin@nodename> configure
```

В режиме конфигурации приглашение командной строки будет выглядеть следующим образом:

```
Admin@nodename#
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

Где:

<action> — действие, которое необходимо выполнить;

<level> — уровень контекста конфигурации, который соответствует одному из разделов структуры конфигурации в веб-интерфейсе SWG;

<filter> — идентификатор объекта, к которому происходит обращение;

<configuration_info> — значение параметров, которые необходимо применить к объекту.

Наименование	Описание
`<action>`	В режиме конфигурации доступны следующие действия: • `execute` — выполнение команд, которые не относятся к текущей конфигурации устройства (ping, date, traceroute и т. п.) Команда доступна независимо от уровня конфигурации. Подробнее — в разделе «Команды execute». • `create` — создание новых объектов. • `set` — изменение параметров объектов, включение различных параметров. • `show` — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено все, что находится глубже текущего уровня. • `delete` — удаление объекта или параметра из списка параметров. • `edit` — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображен под командной строкой. • `end` — переход на один уровень конфигурации выше. • `top` — возврат на самый верхний уровень конфигурации. • `export` — экспорт сертификатов. Подробнее — в разделе «Команды export». • `import` — импорт конфигурации. Подробнее — в разделе «Команды import». • `debug` — включение журналирования событий протоколов динамической маршрутизации в режиме отладки. Подробнее — в разделе «Команды debug». • `exit` — выход из режима конфигурации. 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 отображен под командной строкой:

Наименование	Описание

	`Admin@nodename# edit network interface`
	`Admin@nodename#`
	`Level: network interface`
	
	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` два раза:
	
	`Admin@nodename#`
	`Level: network interface`
	`Admin@nodename# end`
	`Level: network`
	`Admin@nodename# end`
	`Admin@nodename#`
	
	Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду `top`:

Наименование	Описание

	`Admin@nodename#`
	`Level: network interface`
	`Admin@nodename# top`
	`Admin@nodename#`

`<level>`	Уровни контекста конфигурации в командной строке повторяют разделы конфигурации в веб-интерфейсе UserGate SWG: • `settings` — соответствует разделу веб-интерфейса «UserGate»; • `users` — соответствует разделу веб-интерфейса «Пользователи и устройства»; • `network` — соответствует разделу веб-интерфейса «Сеть»; • `network-policy` — соответствует разделу веб-интерфейса «Политики сети»; • `security-policy` — соответствует разделу веб-интерфейса «Политики безопасности»; • `global-portal` — соответствует разделу веб-интерфейса «Глобальный портал»; • upstream-proxy — соответствует разделу веб-интерфейса «Вышестоящие прокси»; • `libraries` — соответствует разделу веб-интерфейса «Библиотеки»; • `monitoring` — соответствует разделу веб-интерфейса «Диагностика и мониторинг»
`<filter>`	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать параметры(`<configuration_info>`). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках. Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду: `Admin@nodename# show network interface adapter port0`

Наименование	Описание
	Будет отображена информация об интерфейсе port0 текущего узла SWG. 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>`	Указание параметра с аргументом. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным.
	Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки.
	Например, необходимо создать группу с именем VPN users:
	`Admin@nodename# create users group "VPN users"`
	Множественные аргументы используются для установки множества значений какого-либо параметра. Параметры записываются в квадратных скобках и разделяются пробелами.
	Например, необходимо в группу `VPN users` добавить пользователей `user1` и `user2`. Параметру `users` необходимо задать аргумент `[ user1 user2 ]`:
	`Admin@nodename# set users group "VPN users" users [ user1 user2 ]`
	Важно!
	Квадратные скобки должны быть отделены пробелами с обеих сторон

Команды execute

Команды имеют следующую структуру:

```
Admin@nodename# execute <command-name>
```

Список команд раздела `execute`.

Команда	Описание
`cache`	Очистка кэша LDAP-записей: `Admin@nodename# execute cache ldap-clear`
`check-geoip`	Проверка географической принадлежности IP-адреса по текущей базе GeoIP: `Admin@nodename# execute check-geoip ip <ip-address>`

`clear-cli-history`	Удаление истории команд интерфейса CLI. Можно удалить историю всех введенных команд интерфейса CLI или только команд в одном из режимов работы интерфейса (в режиме конфигурации или в режиме диагностики):
	`Admin@nodename# execute clear-cli-history`
	`Admin@nodename# execute clear-cli-history modes [ <configure | diagnostic> ]`

`configurate-cluster`	Генерация секретного кода, необходимого для добавления нового узла в кластер конфигурации: `Admin@nodename# execute configurate-cluster generate-secret-key <parameter>` Где: • `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;

Команда	Описание
	• `request-limit` — срок действия запроса на генерацию кода. **Важно!** **Для использования этой команды необходимо наличие лицензии на модуль** `Cluster`
`date`	Просмотр текущих значений даты и времени на узле: `Admin@nodename# execute date`

`dig`	Проверка записи DNS домена:
	
	`Admin@nodename# execute dig host <hostname> <parameters>`
	`Admin@nodename# execute dig host <IP-address> <parameters>`
	
	В команде можно использовать следующие параметры:
	
	• `reverse-lookup` — получение имени устройства по IP-адресу;
	• `dns` — указание IP-адреса DNS-сервера;
	• `tcp` — использование протокола TCP вместо UDP.

`factory-reset`	Возврат устройства в первоначальное состояние. `Admin@nodename# execute factory-reset` Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
`firewall`	Применение всех правил межсетевого экрана с обрывом текущих сессий: `Admin@nodename# execute firewall force-changes`

Команда	Описание
license	Команда регистрации продукта имеет следующую структуру: `Admin@nodename# execute license activate <pin-code>` В качестве `<pin-code>` укажите код активации продукта
logs	Команда разовой отправки журналов по имеющемуся правилу экспорта журналов: `Admin@nodename# execute logs send-once <export-log-name>`

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 и т. д.). Импортированные из МС объекты конвертируются в локальные.
	• `delete` — отключение от МС с удалением всех импортированных из МС объектов (библиотеки, правила и т. д.). Импортированные объекты, которые в настоящий момент используются, конвертируются в локальные.
	`Admin@nodename# execute mc-force-disconnect keep`
	`Admin@nodename# execute mc-force-disconnect delete`

netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • `address` — доменное имя узла для проверки доступности по TCP или URL — для HTTP; • `dns-ip` — IP-адрес сервера DNS; • `dns-tcp` — использование TCP вместо UDP для DNS-запроса;

Команда	Описание

	• `check-cert` — проверка SSL-сертификата;
	• `type` — проверка доступности по:
	  ◦ `http;`
	  ◦ `tcp` (если порт не указан, то используется порт 80);
	• `data` — запрос содержимого сайта. По умолчанию запрашиваются только заголовки;
	• `timeout` — максимальный тайм-аут ожидания ответа от веб-сервера;
	• `user-agent` — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin@nodename# execute netcheck type tcp address <host-domain-name> data on`
	`Admin@nodename# execute netcheck address <host-domain-name>`

`ping`	Проверка доступности определенного узла. Можно задать следующие параметры: • `host` — IP-адрес или доменное имя узла. • `count` — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш `Ctrl + C`). • `numeric` — не определять имена. • `timestamp` — отображение временных меток. • `interval` — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • `ttl` — время жизни пакета. • `interface` — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения `ping`. • `mtu` — максимальный размер блока данных отправляемых пакетов. • `virtual-router` — имя виртуального маршрутизатора.

Команда	Описание
	`Admin@nodename# execute ping host <hostname> count <number>`
`reboot`	Перезагрузка устройства: `Admin@nodename# execute reboot`
`restore-mac`	Восстановление mac-адреса интерфейса: `Admin@nodename# execute restore-mac interface <interface-name>`
`shutdown`	Выключение устройства: `Admin@nodename# execute shutdown`
`termination`	Закрытие сессий администраторов или пользователей: `Admin@nodename# execute termination <admin-sessions | user-sessions>` Подробнее — в разделе «Настройка сессий администраторов»
`traceroute`	Трассировка соединения до определенного узла. Параметры команды: • `host <ip-or-domain>` — IP-адрес или имя домена, для которого производится трассировка; • `interface <iface-name>` — интерфейс, с которого будут отправляться пакеты; • `not-map-ip` — не искать hostname для IP-адреса при отображении; • `use-icmp-echo` — использовать ICMP echo; • `port` — указать порт вместо порта по умолчанию (1 — 65535); • `min-interval` — минимальный интервал между пакетами.

Команда	Описание
	`Admin@nodename# execute traceroute host <hostname>`
`update`	Обновление: • `software-updates` — обновление программного обеспечения. • `libraries-updates` — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.

Часть представленных выше команд, кроме команд обновления, регистрации продукта, управления сессиями администраторов и очистки кэша, также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

```
Admin@nodename> <command-name>
```

Команды import

Импорт доступен в разделах «Настройки», «Пользователи», «Сеть», «Политики сети», «Политики безопасности», «Глобальный портал».

В разделе «Настройки» (`settings`) можно импортировать сертификаты. Подробнее — в разделе «Настройка сертификатов».

В разделах «Пользователи» (`users`), «Сеть» (`network`), «Политики сети» (`network-policy`), «Политики безопасности» (`security-policy`), «Глобальный портал» (`global-portal`) можно импортировать правила, написанные на UPL. При использовании импорта, все существующие правила будут заменены на указанные.

В разделе «Пользователи» (`users`) можно импортировать правила captive-портала. Подробнее о правилах — в разделе «Captive-портал».

В разделе «Сеть» (`network`) можно импортировать правила DNS. Подробнее — в разделе «Настройка правил DNS».

В разделе «Политики сети» (`network-policy`) можно импортировать правила межсетевого экрана, NAT и маршрутизации, пропускной способности,

балансировки нагрузки. Подробнее о правилах читайте в соответствующих разделах: «Настройка правил межсетевого экрана», «Настройка правил NAT и маршрутизации», «Настройка правил пропускной способности». «Настройка балансировки нагрузки».

В разделе «Политики безопасности» (`security-policy`) можно импортировать правила контентной фильтрации, веб-безопасности, инспектирования SSL, сценариев, ICAP-правил. О добавлении правил читайте в соответствующих разделах: «Настройка фильтрации контента», «Настройка веб-безопасности», «Настройка инспектирования SSL», «Настройка сценариев», «Настройка правил ICAP».

В разделе «Глобальный портал» (`global-portal`) можно импортировать правила веб-портала и reverse-прокси. Подробнее о создании правил — в разделах: «Настройка веб-портала» и «Настройка правил reverse-прокси».

Команды export

Команда для экспорта сертификатов.

Вы можете экспортировать сертификаты, всю цепочку сертификатов и CSR:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

Подробнее об управлении сертификатами — в разделе «Настройка сертификатов».

Команда debug

Команда debug позволяет включить журналирование событий протоколов маршрутизации в режиме отладки. События записываются в debug-лог. Их просмотр также возможен в режиме мониторинга в консоли CLI (подробнее — в разделе «Диагностика и мониторинг»).

Для включения журналирования конкретного протокола маршрутизации используется команда:

```
Admin@nodename# debug <protocol> <parameters>
```

Поддерживаются следующие протоколы:

- rip;
- ospf
- bgp;
- igmp;
- pim;
- bfd;
- msdp;
- mroute — таблица мультикаст-маршрутизации;
- ssmpingd — инструмент тестирования мультикаст-вещания.

НАСТРОЙКА УСТРОЙСТВА В CLI

Настройка общих параметров устройства

Настройка параметров работы CLI

Параметры работы интерфейса командной строки настраиваются на уровне `settings cli`.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@nodename# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида `Admin@nodename#`) на удобное вам. Например, чтобы поменять вид системного приглашения на `NodeAABBCC`, выполните следующую команду:

```
Admin@nodename# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@nodename# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@nodename#
```

Чтобы задать уровень детализации журналирования CLI используется команда:

```
Admin@nodename# set settings cli log-level
```

Вы можете установить следующие уровни детализации:

- `off` — отключить журналирование;
- `error` — только ошибки;
- `warning` — ошибки и предупреждения;
- `info` — ошибки, предупреждения и дополнительная информация;
- `debug` — максимальная детализация.

Чтобы задать уровень детализации журналирования операций экспорта и импорта конфигурации в CLI используется команда:

```
Admin@nodename# set settings cli log-level
```

Вы можете установить следующие уровни детализации:

- `off` — отключить журналирование;
- `error` — только ошибки;

- `warning` — ошибки и предупреждения;
- `info` — ошибки, предупреждения и дополнительная информация;
- `debug` — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:

```
Admin@nodename# show settings cli
```

Настройка базовых параметров устройства

Базовые параметры UserGate SWG настраиваются на уровне `settings general`.

Структура команд для настройки базовых параметров устройства:

```
Admin@nodename# set settings general <settings-module> <parameters>
```

Базовые параметры устройства сгруппированы в разделы.

Раздел	Описание

`admin-console`	Параметры консоли управления:
	• `timezone` — часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т. п.
	• `language` — язык интерфейса:
	  ◦ `ru` — русский;
	  ◦ `en` — английский.
	• `webaccess` — режим аутентификации веб-консоли:
	  ◦ `password` — аутентификация по имени и паролю;
	  ◦ `cert` — аутентификация по X.509-сертификату.
	• `uc-profile` — выбор профиля пользовательских сертификатов.
	• `web-ssl-profile` — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL».

Раздел	Описание
	• `response-pages-ssl-profile` — выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации captive-портала. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». • `api-session-lifetime` — время ожидания сеанса администратора в минутах. По истечении этого времени при вводе команды CLI, использующей API-вызовы (команды создания объектов, изменения параметров, просмотра параметров, удаления объектов или параметров), сессия администратора будет завершена сообщением Authentication session expired. Restart CLI
`server-time`	Параметры установки точного времени: • `ntp-enabled` — включение и отключение использования NTP-серверов. • `primary-ntp-server` — адрес основного NTP-сервера. • `second-ntp-server` — адрес запасного NTP-сервера. • `time` — установка времени на устройстве. Время указывается в часовом поясе UTC в формате `yyyy-mm-ddThh:mm:ss` (например, 2022-02-15T12:00:00)
`modules`	Настройка работы модулей устройства: • `proxy-port` — указание нестандартного номера порта, который будет использоваться для подключения к встроенному прокси-серверу. • `auth-captive` — указание служебного домена, который будет использоваться UserGate SWG при авторизации пользователей через captive-портал. • `logout-captive` — указание служебного домена, который будет использоваться пользователями UserGate SWG для окончания сессии. • `cert-captive` — указание служебного домена, который будет использоваться UserGate SWG при авторизации пользователей через captive-портал с помощью сертификатов. • `block-page-domain` — указание служебного домена, который будет использоваться для отображения страницы блокировки.

Раздел	Описание

	• `ftp-enabled` — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера.
	• `ftp-domain` — указание служебного домена, который будет использоваться для предоставления пользователям сервиса FTP поверх HTTP.
	• `snmp-engine-id` — настройка идентификатора SNMP устройства:
	  ◦ `length <fixed | dynamic>` — длина идентификатора. Фиксированная (не более 8 байт), только для типа `text` или динамическая (не более 27 байт).
	  ◦ `type <ip4 | ip6 | mac | text | octets>` — формат идентификатора SNMP (IPv4, IPv6, MAC-адрес, текст, октеты).
	  ◦ `value` — значение идентификатора.
	• `terminal-sever-agent` — настройка пароля для подключения агентов авторизации терминального сервера.
	• `lldp` — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения:
	  ◦ `transmit-delay` — задержка передачи. Указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например после изменения имени узла или адреса управления. Может принимать значения от 1 до 3600. Указывается в секундах.
	  ◦ `transmit-hold` — значение мультипликатора удержания. Произведение значений `transmit-delay` и `transmit-hold` определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100

`cache`	Параметры кэширования прокси-сервера: • `caching-mode` — включение или отключение режима кэширования.

Раздел	Описание
	• `exclusions` — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду: `Admin@nodename# delete settings general cache exclusions [ <URL> ]` • `max-cacheable-size` — максимальный размер объектов, которые будут кэшироваться (МБ). • `ram-size`: размер оперативной памяти, отведенный под кэширование (МБ)
`log-analyzer`	Параметры модуля сбора статистики: • `use-local-stat-server` — использование локальной службы журналирования

`proxy-portal`	Параметры предоставления доступа к внутренним ресурсам компании с помощью веб-портала:
	• `enabled` — включение или отключение использования веб-портала.
	• `hostname` — имя узла, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала.
	• `port` — порт TCP, который будет использоваться сервисом веб-портала.
	• `auth-profile` — указание профиля аутентификации, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей аутентификации».
	• `auth-template` — выбор шаблона страницы аутентификации.
	• `portal-template` — выбор шаблона веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал.
	• `enable-ldap` — выбор домена AD или LDAP на странице аутентификации:
	  ◦ `on` — показывать;
	  ◦ `off` — не показывать.

Раздел	Описание

	• `use-captcha` — показывать на странице аутентификации веб-портала код для ввода пользователем:
	  ◦ `on` — показывать;
	  ◦ `off` — не показывать.
	• `ssl-profile` — выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей SSL».
	• `certificate` — выбор сертификата, который будет использоваться для создания HTTPS-соединения.
	• `auth-mode` — выбор метода аутентификации:
	  ◦ `aaa` — аутентификация через логин и пароль локальных пользователей или аутентификация пользователей на AAA-сервере;
	  ◦ `pki` — аутентификация посредством X.509-сертификатов.
	• `user-cert-profile` — выбор профиля пользовательских сертификатов при аутентификации посредством сертификатов

`pcap`	Настройка захвата пакетов.
	Команда для настройки:
	`Admin@nodename# set settings general pcap packet-capture-mode <parameters>`
	Параметры:
	• `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 учета изменений параметров устройства: • `enabled` — включение или отключение учета изменений параметров.

Раздел	Описание
	• `event-tracker-types` — типы изменений (например, приказ, регламентные работы и т. д.). Для удаления типа изменения используется команда: `Admin@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ]`
`management-center`	Настройка агента UserGate Management Center. Команда для настройки: `Admin@nodename# set settings general management-center <parameters>` Параметры: • `enabled` — включение или отключение агента UserGate Management Center; • `mc-address` — адрес сервера UserGate Management Center; • `device-code` — уникальный код устройства для подключения устройства к UserGate Management Center

`updates-schedule`	Настройка расписания скачивания обновлений программного обеспечения и библиотек.
	Расписание для обновления программного обеспечения задается командой:
	`Admin@nodename# set settings general updates-schedule software schedule <schedule|disabled>`
	Единое расписание для скачивания обновлений библиотек задается командой:
	`Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule|disabled>`
	Расписание для скачивания обновлений отдельных библиотек задается командой:

Раздел	Описание

	`Admin@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled>`
	
	Время задается в crontab-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>.
	
	Каждое из полей может быть задано следующим образом:
	
	• Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновления программного обеспечения должна выполняться каждый час.
	• Дефис (-) — для указания диапазона значений.
	• Запятая (,) — в качестве разделителя значений.
	• Косая черта (/) — для указания шага между значениями.
	
	Команда для просмотра расписания обновлений:
	
	`Admin@nodename# show settings general updates-schedule`

`metrics-collection`	Настройка параметров передачи метрик телеметрии. • `enabled` — включение или выключение отправки метрик телеметрии. По умолчанию отправка метрик телеметрии включена. • `masking-sensitive-data` — маскирование чувствительных данных в отправляемых метриках. К чувствительным данным относятся IP-адреса, MAC-адреса, URL, адреса эл. почты и т. д. По умолчанию маскирование чувствительных данных отключено.

Управление подключаемыми модулями

Управление подключаемыми модулями устройства в CLI выполняется на уровне `settings device`.

Для управления модулями используется команда:

```
Admin@nodename# set settings device <parameters>
```

Укажите параметры команды.

Параметр	Описание

`sip`	Включение или отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT:
	`Admin@nodename# set settings device sip enabled`
	• `on`;
	• `off`.
	По умолчанию модуль выгружен.
	Для разрешения передачи медиа-трафика напрямую между конечными участниками разговора:
	`Admin@nodename# set settings device sip direct-media`
	• `on`;
	• `off`
	Важно!
	После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (нажать «Принудительно применить» в разделе «Политики сети» → «Межсетевой экран»).

Параметр	Описание
`h323`	Включение или отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • `on`; • `off`. По умолчанию модуль выгружен
`sunrpc`	Включение или отключение загрузки модуля SunRPC: • `on`; • `off`. По умолчанию модуль выгружен
`ftp-alg`	Включение или отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • `on`; • `off`. **Важно!** **Модуль нужно включать для пассивного режима работы FTP.** По умолчанию модуль выгружен
`auth-type`	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • `ah` — включение подписи; • `pass` — отключение проверки
`fw-drop-invalid`	Включение или отключение блокировки пакетов с некорректным набором параметров в полях заголовка: • `on`; • `off`. По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно

Параметр	Описание
	понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной
`fw-established`	Включение или отключение создания одного общего правила межсетевого экрана для обратных пакетов: • `on`; • `off`. По умолчанию настройка выключена
`bypass-optimization`	Включение или отключение оптимизации инспектирования SSL: • `on`; • `off`. При включённом параметре `bypass-optimization` для снижения нагрузки на прокси-сервер инспекция SSL не будет происходить, если на узле нет запрещающих правил инспектирования SSL. При этом в журнале веб-доступа при включённой опции журналирования будет присутствовать только информация уровней L3/L4. По умолчанию настройка выключена

Команда для просмотра текущих параметров:

```
Admin@nodename# show settings device
```

Настройка управления устройством

Настройка диагностики

В этом разделе вы можете управлять параметрами диагностики устройства, необходимыми службе технической поддержки для решения возможных проблем.

Параметры диагностики задаются на уровне `settings loglevel`.

С помощью следующей команды вы можете установить необходимый уровень детализации журналирования событий:

```
Admin@nodename# set settings loglevel value <off | error | warning |
info | debug>
```

- `off` — ведение журналов диагностики отключено;
- `error` — журналировать только ошибки;
- `warning` — журналировать только ошибки и предупреждения;
- `info` — журналировать только ошибки, предупреждения и дополнительную информацию;
- `debug` — журналировать все возможные события.

При журналировании на уровнях `warning`, `info` и `debug` может снижаться производительность UserGate SWG, поэтому рекомендуется устанавливать уровни `error` или `off`, если технической поддержкой UserGate не было предложено иное.

Для просмотра состояния уровня детализации диагностики используется команда:

```
Admin@nodename# show settings loglevel
```

Для включения или отключения удаленного помощника (radmin) используется команда:

```
Admin@nodename# set settings radmin enabled <on | off>
```

Для просмотра состояния удаленного помощника используется команда:

```
Admin@nodename# show settings radmin
```

Режим emergency

Если произошел сбой в работе ядра UserGate SWG, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации UserGate SWG. Обычно это учетная запись Admin. Для входа необходимо

указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Команда входа в режим emergency CLI выглядит следующим образом:

```
ssh Admin@emergency@<SWG_IP> -p 2200
```

Команда включения и отключения удаленного доступа к серверу для технической поддержки в режиме emergency:

```
Admin@emergency@SWG# set radmin-emergency enabled <on | off>
<parameters>
```

В команде указываются следующие сетевые параметры:

- interface — название интерфейса;
- ip-addr — IP-адрес интерфейса;
- gateway-address — IP-адрес шлюза.

В режиме emergency доступна команда возврата устройства в первоначальное состояние:

```
Admin@emergency@SWG# execute factory-reset
```

Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды.

Настройка получения обновлений

В этом разделе вы можете установить канал получения обновлений для устройства (стабильные версии или бета-версии).

Канал обновлений устанавливается с помощью команды:

```
Admin@nodename# set settings device-mgmt updates-channel <stable |
beta>
```

Для просмотра наличия обновлений и выбранного канала обновления используется команда:

```
Admin@nodename# show settings device-mgmt updates-channel
```

Управление резервным копированием

Правила резервного копирования создаются на уровне `settings device-mgmt`.

Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется команда:

```
Admin@nodename# create settings device-mgmt settings-backup
<parameters>
```

Параметры правил резервного копирования.

Параметр	Описание
`enabled`	Включение или отключение правила создания резервной копии устройства
`name`	Название правила резервного копирования
`description`	Описание правила резервного копирования
`type`	Выбор типа удаленного сервера для экспорта файлов: • `ssh`; • `ftp`
`address`	IP-адрес удаленного сервера
`port`	Порт сервера
`login`	Учетная запись на удаленном сервере
`password`	Пароль учетной записи
`path`	Путь на сервере, куда будут выгружены файлы
`schedule`	Расписание экспорта файлов резервных копий.

Параметр	Описание
	Время задается в crontab-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Для изменения существующего правила резервного копирования используется команда:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения, аналогичен списку параметров, доступных при создании правила.

Для удаления правила резервного копирования используется команда:

```
 Admin@nodename# delete settings device-mgmt settings-backup <rule-
name>
```

Для просмотра параметров правила резервного копирования используется команда:

```
 Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в правиле параметры (см. список параметров в таблице выше).

Экспорт параметров

Создание и настройка правил экспорта параметров устройства происходит на уровне `settings device-mgmt settings-export`.

Для создания правила экспорта параметров используется команда:

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Параметры правила экспорта.

Параметр	Описание
`enabled`	Включение или отключение правила экспорта параметров устройства
`name`	Название правила экспорта
`description`	Описание правила экспорта
`type`	Тип удаленного сервера для экспорта параметров: • `ssh`; • `ftp`
`address`	IP-адрес удаленного сервера
`port`	Порт сервера
`login`	Учетная запись на удаленном сервере
`password`	Пароль учетной записи на удаленном сервере
`path`	Путь на сервере, куда будут выгружены параметры
`schedule`	Расписание экспорта параметров. Время задается в crontab-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.

Параметр	Описание
	• Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Для изменения существующего правила экспорта параметров устройства используется команда:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения, аналогичен списку параметров, доступных при создании правила.

Для удаления правила экспорта параметров используется команда:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Для просмотра параметров правила экспорта используется команда:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в существующем правиле параметры (см. список параметров в таблице выше).

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используется команда:

```
Admin@nodename# set settings change-control config <off | log | block>
```

Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate SWG.

- `log` — активация режима отслеживания изменений конфигурации. При обнаружении изменений UserGate SWG записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- `off` — отключение режима отслеживания изменений конфигурации. Необходимо указать пароль, который был задан при активации режима отслеживания конфигурации.
- `block` — активация режима отслеживания изменений конфигурации. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate SWG записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик.

Перед активацией защиты конфигурации администратор производит настройку устройства в соответствии с требованиями организации, после чего защищает параметры от изменений (режим `log` или `block`). Любое изменение параметров через веб-интерфейс, CLI или другими способами будет приводить к журналированию и блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений используется команда:

```
Admin@nodename# show settings change-control config
```

Настройка защиты исполняемых файлов от изменения

Для настройки защиты исполняемого кода устройства от потенциального несанкционированного изменения используется команда:

```
Admin@nodename# set settings change-control code <off | log | block>
```

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate SWG.

- `log` — активация режима отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate SWG записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- `off` — отключение режима отслеживания несанкционированных изменений исполняемого кода. Необходимо указать пароль, который был задан при активации режима отслеживания исполняемого кода.
- `block` — активация режима отслеживания несанкционированных изменений исполняемого кода. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate SWG записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик. Чтобы отключить созданное правило межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов используется команда:

```
Admin@nodename# show settings change-control code
```

Настройка режима ускоренной обработки сетевого трафика

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@nodename# set settings fastpath enabled <on/off>
```

Для просмотра параметров режима ускоренной обработки трафика используется команда:

```
Admin@nodename# show settings fastpath
```

Настройка кластеров

Настройка кластера конфигурации

Кластер конфигурации настраивается на уровне `settings device-mgmt configuration-cluster`.

Для изменения параметров существующего узла кластера используется команда:

```
Admin@nodename# set settings device-mgmt configuration-cluster <node-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
`name`	Изменение имени узла кластера
`description`	Изменение описание узла кластера
`ip`	Установка IP-адреса интерфейса, входящего в зону, выделенную для кластера

Команды для удаления и отображения параметров узла кластера:

```
Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-name>
```

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

```
Admin@nodename# execute configurate-cluster generate-secret-key
```

Настройка кластера отказоустойчивости

Кластер отказоустойчивости настраивается на уровне `settings device-mgmt ha-clusters`.

Для создания кластера отказоустойчивости используется команда:

```
Admin@nodename# create settings device-mgmt ha-clusters
```

Далее необходимо задать следующие параметры:

Параметр	Описание
`enabled`	Включение/отключение кластера отказоустойчивости: • `on`, • `off`
`name`	Название кластера отказоустойчивости
`description`	Описание кластера отказоустойчивости
`nodes`	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
`delivery-mode`	Выбор режима отправки служебного трафика: • `Multicast` **— многоадресная передача сообщений синхронизации сессий и VRRP-объявлений.** • `Unicast` — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера

Параметр	Описание
`virtual-ips`	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • `ip` — задание IP-адреса для кластера отказоустойчивости (указывается в формате `IP/mask`) ; • `ha-interfaces` — задание интерфейсов для узлов кластера (указываются в формате `node-name/interface`)
`mode`	Выбор режима работы кластера: • `active-passive`: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен); • `active-active`: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
`advertise-time`	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
`master-down-timer`	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
`preemption-delay`	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
`allow-non-vip-traffic`	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
`use-vmac`	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»

Параметр	Описание
`allow-non-vip-traffic`	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
`no-preempt`	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
`heartbeat`	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
`ha-cluster-multicast-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
`session-sync`	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
`session-sync-all`	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
`vrid`	Идентификатор виртуального маршрутизатора (VRID)
`node-sync`	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
`excluded-sync-ips`	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
`unicast-sync-ip`	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`unicast-sync-port`	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и

Параметр	Описание
	резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`unicast-vrrp-ip`	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`unicast-vrrp-port`	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`track-interfaces-enabled`	Включение/отключение проверки интерфейсов
`track-interfaces`	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • `change-priority` — понизить приоритет узла кластера. • `fault` — считать узел недоступным

Пример команды создания кластера отказоустойчивости:

```
Admin@nodename#  create settings device-mgmt ha-clusters name ExampleCluster nodes [ node_1 node_2 ] mode active-passive delivery- mode multicast heartbeat [ node_1/port0 node_2/port0 ] node-sync [ node_1/port1 node_2/port1 ]
```

Команда для редактирования параметров кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters <cluster-name>
```

Команда для настройки кластера отказоустойчивости в облачной среде Yandex Cloud

```
Admin@nodename#
```

```
set settings device-mgmt ha-clusters ExampleCluster cloud service-
provider yandex-cloud yandex-cloud-settings routes new
```

Параметры для редактирования:

Параметр	Описание
`heartbeat`	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
`mode`	Выбор режима работы кластера: • `active-passive`: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен). • `active-active`: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
`name`	Название кластера отказоустойчивости
`nodes`	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
`delivery-mode`	Выбор режима отправки служебного трафика: • `Multicast` — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. • `Unicast` — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`enabled`	Включение/отключение кластера отказоустойчивости: • `on`, • `off`
`description`	Описание кластера отказоустойчивости

Параметр	Описание
`virtual-ips`	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • `ip` — задание IP-адреса для кластера отказоустойчивости (указывается в формате `IP/mask`) ; • `ha-interfaces` — задание интерфейсов для узлов кластера (указываются в формате `node-name/interface`)
`advertise-time`	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
`master-down-timer`	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
`preemption-delay`	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
`allow-non-vip-traffic`	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
`use-vmac`	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
`allow-non-vip-traffic`	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
`no-preempt`	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя

Параметр	Описание
`master-node`	Назначение мастер-узла кластера отказоустойчивости
`ha-cluster-multicast-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
`session-sync`	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
`session-sync-all`	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
`vrid`	Идентификатор виртуального маршрутизатора (VRID)
`node-sync`	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
`excluded-sync-ips`	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
`unicast-sync-ip`	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`unicast-sync-port`	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`unicast-vrrp-ip`	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера

Параметр	Описание
`unicast-vrrp-port`	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
`track-interfaces-enabled`	Включение/отключение проверки интерфейсов
`track-interfaces`	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • `change-priority` — понизить приоритет узла кластера. • `fault` — считать узел недоступным
`checkers`	Настройка диагностики узлов кластера. Проверка доступности шлюзов • `gateway-availability` — проверка доступности шлюзов: ◦ `enabled` — включение/включение/отключение проверки доступности шлюзов. Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. ◦ `action` — выбор действия в случае неудовлетворительных результатов проверки (`change-priority` — понизить приоритет узла кластера, `fault` — считать узел недоступным). ◦ `fall-count` — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ `interval-time` — регулярная проверка шлюзов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ `rise-count` — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10.

Параметр	Описание
	• `resource-availability` — проверка доступности ресурсов: ◦ `enabled` — включение/включение/отключение проверки доступности ресурсов. ◦ `action` — выбор действия в случае неудовлетворительных результатов проверки (`change-priority` — понизить приоритет узла кластера, `fault` — считать узел недоступным). ◦ `fall-count` — количество последовательных неудовлетворительных результатов проверки, после которых узел признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ `interval-time` — регулярная проверка ресурсов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ `rise-count` — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. ◦ `resources` — указание IP-адресов или FQDN тех ресурсов, доступ к которым будет проверяться
`cloud`	Параметры кластера: • `destination-prefix` — укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud. • `next-hops` — IP-адреса интерфейсов узлов кластера. • `route-table-id` — идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud

Примеры редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster
nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces
[ node_1/port3 node_2/port3 ]
...
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster
master-node utmcore@iononsteswer
```

Для удаления кластера:

```
Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- `nodes`,
- `virtual-ips`.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>
```

Настройка управления доступом к консоли UserGate SWG

Настройка управления доступом к консоли UserGate SWG выполняется на уровне `settings administrators`. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Настройка общих параметров доступа выполняется на уровне `settings administrators general`.

Для изменения параметров используется команда:

```
Admin@nodename# set settings administrators general <parameters>
```

Параметры, доступные для редактирования.

Параметр	Описание
`password`	Изменить пароля текущего администратора.
`unblock`	Разблокировать администратора.
`strong-password`	Использовать сложный пароль: • **on**. • **off**.
`num-auth-attempts`	Установить максимальное количество неверных попыток аутентификации.
`block-time`	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
`min-length`	Определить минимальную длину пароля (максимальное значение: 100 символов).
`min-uppercase`	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
`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

Учётные записи администраторов настраиваются на уровне `settings administrators administrators`.

Для создания учётной записи администратора используется команда:

```
Admin@nodename# create settings administrators administrators
<parameters>
```

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.

Параметр	Описание
`ldap-user`	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра: • **connector**: название сконфигурированного ранее LDAP-коннектора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `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"`

Параметр	Описание
	`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. • **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.

Команда для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Команда 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
```

Команда для удаления учётной записи:

```
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

Права доступа профилей администраторов настраиваются на уровне `settings administrators profiles`.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles <parameters>
```

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
	`Admin@nodename# create settings administrators profiles ... api-permissions <permission> [ object ... ]`

`webui-permissions`	Права доступа к веб-интерфейсу UserGate SWG:
	• **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`	

Параметр	Описание

	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 ... ]`

Команда для редактирования профиля:

```
Admin@nodename# set settings administrators profiles <profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Команда для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Команда для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Команда для удаления профиля администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

Просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий выполняется на уровне `settings administrators admin-sessions`.

Команда для просмотра 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

Управление сертификатами выполняется на уровне `settings certificates`.

Для импорта сертификатов используется команда:

```
Admin@nodename# import settings certificates <parameters>
```

Далее необходимо указать параметры.

Параметр	Описание
`name`	Название сертификата, которое будет отображено в списке.
`description`	Описание сертификата.
`certificate-data`	Сертификат в формате PEM.
`certificate-chain`	Цепочка сертификатов в формате PEM.
`private-key`	Приватный ключ в формате PEM.
`passphrase`	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение).
`user`	Локальный пользователь, которому будет назначен пользовательский сертификат.
`ldap-user`	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • **user**: имя пользователя в формате domain\user. • **connector**: выбор LDAP сервера.
`role`	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **ssl-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **ssl-root**: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при 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

Параметр	Описание
	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> <parameters>
```

Далее необходимо указание следующие параметры.

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.

Параметр	Описание
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
<parameters>
```

Доступные параметры.

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **ssl-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **ssl-root**: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • **ssl-cert**: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • **captive-portal**: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-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.

Параметр	Описание
	• **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.

Команда 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 прокси-сервера

Команды для просмотра и настройки параметров прокси-сервера доступны на уровне `settings proxy`.

Вы можете настроить такие параметры, как добавление заголовков HTTP — via и forwarded, а также настройки тайм-аутов на подключение к сайтам и на загрузку контента.

Для изменения параметров прокси-сервера используется команда:

```
Admin@nodename# set settings proxy <parameters>
```

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. Значение по умолчанию — 10 секунд

Параметр	Описание
`proxy_host_rfc`	Доступно: • **relaxed** — использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • **strict** — соблюдать RFC. Данный режим используется по умолчанию.

Команда для просмотра текущих параметров:

```
Admin@nodename# show settings proxy
```

Настройка работы с вышестоящими прокси-серверами

В интерфейсе командной строки настройка сценария перенаправления трафика доступна на уровне `upstream-proxy`.

Настройка состоит из следующих основных шагов:

1. Настройка подключения к вышестоящему прокси-серверу.
2. Создание профиля подключения.
3. Создание правила вышестоящего прокси.

Настройка подключения к вышестоящему прокси-серверу

Для создания подключения к вышестоящему прокси-серверу используется команда:

```
Admin@nodename# create upstream-proxy servers <parameters>
```

Параметры для настройки подключения.

Параметр	Описание
`enabled`	Подключение к вышестоящему прокси-серверу: • `on` — включено; • `off` — отключено
`name`	Название подключения к вышестоящему прокси-серверу
`description`	Описание подключения
`mode`	Тип вышестоящего прокси-сервера: • `https`; • `socks5`
`ip`	IP-адрес вышестоящего прокси-сервера
`port`	Порт вышестоящего прокси-сервера
`auth`	Аутентификация на вышестоящем прокси-сервере: • `on` — требуется; • `off` — не требуется
`user`	Логин для подключения к вышестоящему прокси-серверу
`password`	Пароль для подключения к вышестоящему прокси-серверу

Команда для редактирования параметров ранее созданного подключения к вышестоящему прокси-серверу:

```
Admin@nodename# set upstream-proxy servers <server-name> <parameters>
```

В команде редактирования можно использовать те же параметры, которые используются в команде создания подключения.

Команда для просмотра настроек ранее созданного подключения:

```
Admin@nodename# show upstream-proxy servers <server-name>
```

Команда для удаления ранее созданное подключения к вышестоящему прокси-серверу:

```
Admin@nodename# delete upstream-proxy servers <server-name>
```

Создание профиля подключения

Для создания профиля подключения к вышестоящему прокси-серверу используется команда:

```
Admin@nodename# create upstream-proxy profiles <parameters>
```

Параметры для настройки профиля.

Параметр	Описание
`enabled`	Включение/отключение профиля: • `on` — включен; • `off` — отключен
`name`	Название профиля
`description`	Описание профиля
`used-servers`	Указание вышестоящих прокси-серверов из списка ранее настроенных в системе
`http-method`	Выбор метода HTTP-запроса для проверки состояния подключения с помощью контрольного обращения к указанному URL-ресурсу: `GET`, `HEAD`, `OPTIONS`
`url-host`	Указание URL-ресурса для проверки состояния подключения через вышестоящий прокси-сервер
`check-interval`	Интервал проверки подключения в секундах
`check-timeout`	Время ожидания ответа проверки подключения в секундах

Команда для редактирования параметров ранее созданного профиля подключения к вышестоящему прокси-серверу:

```
Admin@nodename# set upstream-proxy profiles <profile-name>
```

В команде редактирования можно использовать те же параметры, которые используются в команде создания профиля.

Команда для просмотра настройки ранее созданного профиля:

```
Admin@nodename# show upstream-proxy profiles <profile-name>
```

Команда для удаления ранее созданного профиля:

```
Admin@nodename# delete upstream-proxy profiles <profile-name>
```

Создание правила вышестоящего прокси

Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе «UserGate Policy Language».

Команда для создания правила подключения к вышестоящему прокси-серверу:

```
Admin@nodename# create upstream-proxy rules <position> upl-rule
<parameters>
```

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set upstream-proxy rules <position> upl-rule
<parameters>
```

Команда для просмотра ранее созданных правил:

```
Admin@nodename# show upstream-proxy rules <position>
```

Команда для удаления ранее созданных правил:

```
Admin@nodename# delete upstream-proxy rules <position>
```

Параметры для настройки правил.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила. Например, `name("Rule 1")`
`desc`	Описание правила. Например, `desc("Rule example set via CLI")`
`proxy_profile`	Профиль подключения к вышестоящему прокси-серверу. Например, `proxy_profile(Profile1")`
`fallback_action`	Резервное действие при недоступности вышестоящего прокси-сервера: • прямое подключение — `fallback_action(direct)`; • страница блокировки — `fallback_action(blockpage)`
`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. Например, для указания зоны Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с

Параметр	Описание
	использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`time`	Настройка расписания работы правила. Для установки расписания: `time = lib.time()`; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Настройка активации лицензии и обновления ПО

Для настройки активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

Дополнительные параметры команды.

Параметр	Описание
`enabled`	Включение или отключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • `on` — включен; • `off` — отключен
`ip`	IP-адрес внешнего прокси-сервера
`port`	Порт внешнего прокси-сервера
`auth`	Аутентификация на внешнем прокси-сервере: • `on` — требуется; • `off` — не требуется
`name`	Логин на внешнем прокси-сервере
`password`	Пароль на внешнем прокси-сервере

Команда для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

Подробнее о функциональности Upstream Proxy, сценариях использования и настройках в веб-консоли администратора — в разделе «Настройка работы с вышестоящими прокси-серверами».

Настройка параметров мониторинга устройства

Настройка параметров мониторинга устройства в интерфейсе командной строки выполняется 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 — в разделе «Оповещения».

Настройка параметров SNMP устройства

Параметры SNMP устройства настраиваются на уровне `monitoring smnp-parameter`.

Для настройки параметров используется команда:

```
Admin@nodename# set monitoring snmp-parameter <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	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`. Engine ID может быть сформирован в формате: • `ip4` — IPv4. • `ipv6` — IPv6. • `mac` — MAC-адрес. • `text` — Текст. • `octets` — Октеты

Подробнее о параметрах SNMP устройства UserGate — в разделе «SNMP».

Настройка правил мониторинга по SNMP

Правила мониторинга устройства по SNMP настраиваются на уровне `monitoring snmp`.

Для создания правила используется команда:

```
Admin@nodename# create monitoring snmp <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	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`	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»

Параметр	Описание
`events`	Выбор типов параметров, доступных для мониторинга по правилу.

Команда для изменения параметров ранее созданного правила:

```
Admin@nodename# set monitoring snmp <rule-name>
```

Для работы SNMP-менеджера с UserGate SWG 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 — в разделе «Настройки сети».

Настройка профилей безопасности SNMP

Профили безопасности для аутентификации SNMP-менеджеров настраиваются на уровне `monitoring smnp-security-profile`.

Для создания профиля используется команда:

```
Admin@nodename# create monitoring snmp-security-profile <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	Описание
`name`	Название профиля безопасности SNMP
`description`	Описание профиля безопасности SNMP
`username`	Имя пользователя для аутентификации SNMP-менеджера
`auth-type`	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • `none` — без аутентификации, без шифрования. • `no-encrypt` — с аутентификацией, без шифрования. • `encrypt` — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv
`auth-alg`	

Параметр	Описание
	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

Команда для изменения параметров ранее созданного профиля:

```
Admin@nodename# set monitoring snmp-security-profile <profile-name>
```

Настройка правил оповещений

Правила оповещений настраиваются на уровне `monitoring alert-rules`.

Для создания правила оповещения используется команда:

```
Admin@nodename# create monitoring alert-rules <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	Описание
`enabled`	Включает/отключает данное правило
`name`	Название правила
`description`	Описание правила
`notification-profile`	Созданный ранее профиль оповещения

Параметр	Описание
`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

Команда для изменения параметров ранее созданного правила:

```
Admin@nodename# set monitoring alert-rules <rule-name>
```

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.

Pcap-фильтры настраиваются на уровне `monitoring pcap-filter`.

Для создания pcap-фильтра используется команда:

```
Admin@nodename# create monitoring pcap-filter <parameters>
```

Команда для изменения параметров ранее созданного фильтра:

```
Admin@nodename# set 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.

Pcap-правила настраиваются на уровне `monitoring pcap-rule`.

Для создания правила используется команда:

```
Admin@nodename# create monitoring pcap-rule <parameters>
```

Команда для изменения параметров ранее созданного правила:

```
Admin@nodename# set monitoring pcap-rule <parameters>
```

Настройка профилей клиентских сертификатов

Профили клиентских сертификатов настраиваются на уровне `settings certificate-profiles`.

Для создания профиля клиентского сертификата используется команда:

```
Admin@nodename# create settings certificate-profiles <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	Описание
`name`	Название профиля клиентского сертификата
`description`	Описание профиля
`username-field`	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • `common` — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат.

Параметр	Описание
	• `email` — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • `principal` — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, берется первый, указанный в сертификате
`certificates`	Сертификаты УЦ, назначаемые профилю
`crl`	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты, срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: • `off` — не проверять ни один сертификат. • `on` — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • `peer` — проверять только сертификат клиента. • `best-effort` — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных)
`receive-timeout`	Интервал времени, по истечении которого UserGate SWG перестает ожидать ответа от службы отзыва сертификатов

Команды для просмотра ранее созданных профилей клиентских сертификатов:

```
Admin@nodename# show settings certificate-profiles
Admin@nodename# show settings certificate-profiles <certificate-profile-name>
```

Команда для изменения параметров ранее созданного профиля:

```
Admin@nodename# set settings certificate-profiles <certificate-profile-name> <parameters>
```

Параметры, доступные для редактирования профиля, аналогичны параметрам создания профиля, рассмотренным ранее.

Команда для удаления ранее созданного профиля:

```
Admin@nodename# delete settings certificate-profiles <certificate-profile-name>
```

Настройка параметров управления телеметрией

Параметры управления телеметрией устройства настраиваются на уровне `settings telementry`.

Для редактирования параметров используется команда:

```
Admin@nodename# set settings telemetry <parameters>
```

Далее необходимо указать следующие параметры.

Параметр	Описание
`enabled`	Включение или отключение сбора телеметрии на устройстве: • `on`, • `off`. По умолчанию сбор телеметрии включен
`hide-sensitive-data`	Включение или отключение функции сокрытия персональных данных в телеметрии: • `on`, • `off`. По умолчанию функция отключена

Команда для просмотра текущих параметров:

```
Admin@nodename# show settings telemetry
```

НАСТРОЙКА СЕТЕВЫХ ПАРАМЕТРОВ

Зоны

Параметры зон настраиваются на уровне `network zone`.

Для создания новой зоны используется команда:

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

Далее необходимо указать параметры зоны.

Параметр	Описание
`name`	Название зоны
`description`	Описание зоны

`dos-protection-syn`	Защита зоны от сетевого флуда для протокола TCP (SYN-flood):
	• **enabled**: включение/отключение защиты.
	  ◦ **on**;
	  ◦ **off**.
	• **aggregate**:
	  ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны;
	  ◦ **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 устройство отбрасывает пакеты и записывает данное событие в системный журнал.

Параметр	Описание
	• **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 устройство отбрасывает пакеты и записывает данное событие в системный журнал.
	• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты

`dos-protection-icmp`	Защита зоны от сетевого флуда для протокола ICMP:
	• **enabled**: включение/отключение защиты.
	  ◦ **on**;
	  ◦ **off**.
	• **aggregate**:
	  ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны;
	  ◦ **off** — пакеты считаются отдельно для каждого IP-адреса.
	• **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 устройство отбрасывает пакеты и записывает данное событие в системный журнал.
	• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты

Параметр	Описание
`enabled-services`	Параметры контроля доступа зоны: • **"Any ICMP"**: разрешение использования команды ping адреса. • **SNMP**: доступ к устройству 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 устройством по API (TCP 4040). • **ha**: сервис, необходимый для объединения нескольких узлов в кластер (TCP 4369, TCP 9000-9100). • **VRRP**: сервис, необходимый для объединения нескольких узлов 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). • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **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. • **"SAML SERVER"**: выбор SAML-сервера в списке сервисов зоны и общих настройках устройства. • **"Log Analyzer"**: сервис анализатора журналов Log analyzer (TCP 2023 и 9713). • **"Dynamic routing OSPF"**: сервис динамической маршрутизации OSPF. • **"Dynamic routing BGP"**: сервис динамической маршрутизации BGP. • **Multicast**: сервис мультикастинга.

Параметр	Описание
	• **NTP**: доступ к сервису точного времени, запущенному на устройстве. • **"Dynamic routing RIP"**: сервис динамической маршрутизации RIP. • **UserID agent**: сервис для осуществления прозрачной аутентификации. В качестве источника данных аутентификации используются журналы ActiveDirectory и Syslog. • **BFD**: сервис Bidirectonal Forwarding Detection для быстрого обнаружения сетевых ошибок. • **"HTTPS RPC"**: доступ к API поверх HTTPS (TCP 4443)

`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

Параметр	Описание
`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
```

Команда 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`	

Параметр	Описание
	Защита зоны от сетевого флуда для протокола UDP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты
`dos-protection-icmp`	Защита зоны от сетевого флуда для протокола ICMP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты
`enabled-services`	Установленные ранее параметры контроля доступа в данной зоне
`geoip`	Коды GeoIP, которые используются в защите от IP-спуфинга
`ip-list`	Список IP-адресов, которые используются в защите от IP-спуфинга

Команда для просмотра параметров зоны:

```
Admin@nodename# show network zone <zone-name>
```

Интерфейсы

В интерфейсе командной строки можно отобразить список упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов. Команда просмотра доступна как в режиме диагностики и мониторинга, так и в режиме конфигурации.

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

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

Упорядочение интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующую команду (в режиме диагностики и мониторинга и в режиме конфигурации соответственно):

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

Admin@nodename# delete network interface-mapping
```

После добавления сетевых портов в настроенный UserGate SWG его необходимо перезагрузить — список обновится и станет доступным для отображения.

Параметры интерфейсов UserGate SWG настраиваются на уровне `network interface`.

Настройка физических сетевых интерфейсов

Физические сетевые интерфейсы (адаптеры) настраиваются на уровне `network interface adapter`.

Для отображения информации обо всех сетевых адаптерах используйте команду:

```
Admin@nodename# show network interface adapter
```

Команда для отображения информации об определенном сетевом адаптере:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Команда для изменения параметров сетевого адаптера используйте команду вида:

```
Admin@nodename# set network interface adapter <adapter-name>
<parameters>
```

В команде необходимо указать параметры сетевого адаптера.

Параметр	Описание
`enabled`	Включение или отключение сетевого интерфейса: • `on`; • `off`

Параметр	Описание
`description`	Описание сетевого интерфейса
`alias`	Псевдоним («алиас») интерфейса
`iface-type`	Тип интерфейса: • `l3` — интерфейс, работающий в режиме Layer 3. Вы можете назначить IP-адрес для интерфейса и использовать его в правилах межсетевого экрана, контентной фильтрации и других. Это стандартный режим работы интерфейса. • `mirror` — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
`iface-mode`	Режим назначения IP-адреса: • `dhcp` — получение динамического IP-адреса по DHCP; • `manual` — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
`zone`	Зона, которой будет принадлежать интерфейс
`link-info`	Настройка параметров сетевого интерфейса: • `bc_forwarding` — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • `proxy_arp`, `proxy_arp_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a–z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения.

Параметр	Описание
	Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`lldp-profile`	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе «Настройка профилей LLDP»
`ip-addresses`	Назначение IP-адреса для интерфейса. Адрес задается в виде `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.**
`mac`	MAC-адрес интерфейса
`mtu`	Размер MTU
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
`rx-ring`	Размер буфера RX ring интерфейса типа adapter
`tx-ring`	Размер буфера TX ring интерфейса типа adapter
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение или отключение ретранслятора (`on/off`).

Параметр	Описание
	• `utm-address` — IP-адрес интерфейса UserGate SWG, на который добавляется функция ретранслятора (принимает значения IP-адрес/none). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

`user-speed`	Выбор скорости интерфейса. Параметр доступен только для ПАК UserGate FG.
	Для портов 10–17 вы можете переключить скорость работы интерфейса с 10 Гбит/с на 25 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например:
	`Admin@nodename# set network interface adapter port10 user-speed 25000`
	Для портов 18–19 вы можете переключить скорость работы интерфейса со 100 Гбит/с на 40 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например:
	`Admin@nodename# set network interface adapter port18 user-speed 100000`
	Примечание
	При просмотре параметров интерфейса с помощью команды `show network interface adapter <adapter-name>` **параметр** `speed` **отображает фактическую скорость интерфейса, полученную из системы; параметр** `user-speed` **— указанную администратором скорость или значение auto для портов 0–9.**

Команда для удаления значений параметров сетевого адаптера:

```
Admin@nodename# delete network interface adapter <adapter-name>
<parameters>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Настройка VLAN-интерфейса

VLAN-интерфейсы создаются и настраиваются на уровне `network interface vlan`.

Для добавления нового VLAN-интерфейса используется команда:

```
Admin@nodename# create network interface vlan <parameters>
```

В команде необходимо указать параметры интерфейса.

Параметр	Описание
`enabled`	Включение или отключение VLAN-интерфейса: • `on`; • `off`
`description`	Описание интерфейса
`alias`	Псевдоним («алиас») интерфейса
`iface-type`	Тип интерфейса: • `l3` — Layer 3. Вы можете назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. • `mirror` — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
`iface-mode`	Режим назначения IP-адреса: • `dhcp` — получение динамического IP-адреса по DHCP; • `manual` — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса

Параметр	Описание
`tag`	Тег VLAN. Допускается создание до 4094 интерфейсов
`node-name`	Имя узла кластера, на котором создается VLAN
`interface`	Физический интерфейс, на котором создается VLAN
`zone`	Зона, которой будет принадлежать интерфейс
`link-info`	Настройка параметров сетевого интерфейса: • `bc_forwarding` — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • `proxy_arp`, `proxy_arp_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`ip-addresses`	Назначение IP-адреса для интерфейса.

Параметр	Описание
	Адрес задается в виде `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.**
`mac`	MAC-адрес интерфейса
`mtu`	Размер MTU
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение или отключение ретранслятора (`on/off`). • `utm-address` — IP-адрес интерфейса UserGate SWG, на который добавляется функция ретранслятора (принимает значения IP`-адрес/none`). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Команда для изменения параметров ранее созданного VLAN-интерфейса:

```
Admin@nodename# set network interface vlan <vlan-name> <parameters>
```

Параметры, доступные для изменения, аналогичны параметрам создания VLAN-интерфейса, кроме параметров `tag`, `node-name`, `interface` (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Команда для отображения информации обо всех VLAN-интерфейсах:

```
Admin@nodename# show network interface vlan
```

Для отображения информации об определенном интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Bond-интерфейсы создаются и настраиваются на уровне `network interface bond`.

Для создания bond-интерфейса используется команда:

```
Admin@nodename# create network interface bond <parameters>
```

В команде необходимо указать параметры интерфейса.

Параметр	Описание
`enabled`	Включение или отключение интерфейса: • `on`; • `off`
`interface-name`	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет `bond1`
`description`	Описание интерфейса
`alias`	Псевдоним («алиас») интерфейса
`node-name`	Узел кластера, на котором будет создан bond-интерфейс

Параметр	Описание
`zone`	Зона, которой будет принадлежать bond-интерфейс
`link-info`	Настройка параметров сетевого интерфейса: • `bc_forwarding` — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • `proxy_arp`, `proxy_arp_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`bonding`	Дополнительные параметры bond-интерфейса: • `aggr-mode` — режим работы bond-интерфейса: ◦ `round-robin` — режим round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости.

Параметр	Описание
	◦ `active-backup` — режим active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, если станет недоступным текущий активный интерфейс. При использовании этого режима MAC-адрес bond-интерфейса виден вовне только через один сетевой порт. Такая политика применяется для обеспечения отказоустойчивости. ◦ `xor` — режим XOR. Передача распределяется между сетевыми картами с применением формулы: «<MAC-адрес источника> XOR <MAC-адрес назначения>» по модулю <число интерфейсов>». Одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике `xmit_hash`. Политика `XOR` применяется для балансировки нагрузки и обеспечения отказоустойчивости. ◦ `broadcast` — передача на все сетевые интерфейсы. Эта политика применяется для обеспечения отказоустойчивости. ◦ `802.3ad` — режим IEEE 802.3ad. Режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Интерфейс, через который будет отправляться пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать политику `xmit_hash`. ◦ `transmit` — режим adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, другая сетевая карта получает MAC-адрес вышедшей из строя карты. ◦ `load` — режим adaptive load balancing. Включает в себя предыдущую политику, а также осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров.

Параметр	Описание

	Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт вовне, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
	• `mii-monitoring` — периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов.
	• `down-delay` — время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (`miimon`). Значение параметра должно быть кратным значениям `miimon`.
	• `up-delay` — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (`miimon`). Значение параметра должно быть кратным значениям `miimon`.
	• `lacp-rate` — интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:
	  ◦ `slow` — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.
	  ◦ `fast` — запрос партнера на передачу LACPDU-пакетов каждую секунду.
	• `failover-mac` — определение способа назначения MAC-адресов на объединенные интерфейсы в режиме active backup при переключении интерфейсов. Возможные значения:
	  ◦ `disabled` — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.
	  ◦ `active` — MAC-адрес на bond-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на bond-интерфейсе меняется во время обработки отказа.
	  ◦ `follow` — MAC-адрес на bond-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. Пока второй и последующий интерфейсы находятся в резервном режиме, этот MAC-адрес на них не устанавливается. MAC-адрес присваивается во

Параметр	Описание

	время обработки отказа. Когда резервный интерфейс становится активным, он принимает новый MAC-адрес (тот же, что присвоен bond-интерфейсу), а старому активному интерфейсу присваивается MAC-адрес, который принадлежал текущему активному интерфейсу.
	• `xmit-hash` — определение хеш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:
	  ◦ `l2` — использует только MAC-адреса для генерации хеш-суммы. При использовании этого алгоритма трафик для конкретного сетевого узла будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad.
	  ◦ `l2-3` — использует как MAC-адреса, так и IP-адреса для генерации хеш-суммы. Алгоритм совместим с IEEE 802.3ad.
	  ◦ `l3-4` — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хеш-суммы. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, в котором были отправлены, так как отправляются через разные интерфейсы.
	• `interface` — интерфейсы, которые будут объединены в bond-интерфейс

`iface-mode`	Режим назначения IP-адреса: • `dhcp` — получение динамического IP-адреса по DHCP. • `manual` — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
`iface-type`	Тип интерфейса: • `l3` — Layer 3. Вы можете назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса.

Параметр	Описание
	• `mirror` — интерфейс, работающий в режиме зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
`ip-addresses`	Назначение IP-адреса для интерфейса. Адрес задается в виде `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде **Важно!** **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.**
`mac`	MAC-адрес интерфейса
`mtu`	Размер MTU
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение или отключение ретранслятора (`on/off`). • `utm-address` — IP-адрес интерфейса UserGate SWG, на который добавляется функция ретранслятора (принимает значения IP-`адрес/none`). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Команда для изменения параметров существующего bond-интерфейса:

```
Admin@nodename# set network interface bond <bond-name> <parameters>
```

Параметры, доступные для изменения, аналогичны параметрам создания bond-интерфейса, кроме `interface-name`, `node-name` (изменение значений этих параметров недоступно).

Команда удаления bond-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.
- bonding interface — интерфейсы, объединенные в bond-интерфейс.

Команда для отображения информации обо всех bond-интерфейсах:

```
Admin@nodename# show network interface bond
```

Для отображения информации об определенном интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Настройка bridge-интерфейса

Bridge-интерфейсы создаются и настраиваются на уровне `network interface bridge`.

Для добавления нового bridge-интерфейса используется команда:

```
Admin@nodename# create network interface bridge <parameters>
```

В команде необходимо указать параметры интерфейса.

Параметр	Описание
`enabled`	Включение или отключение интерфейса: • on; • `off`
`interface-name`	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет bridge1

Параметр	Описание
`description`	Описание bridge-интерфейса
`alias`	Псевдоним («алиас») интерфейса
`node-name`	Имя узла кластера, на котором создается интерфейс
`zone`	Зона, которой будет принадлежать интерфейс
`link-info`	Настройка параметров сетевого интерфейса: • `bc_forwarding` — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • `proxy_arp`, `proxy_arp_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`bridging`	

Параметр	Описание
	Дополнительные параметры bridge-интерфейса: • `iface-type` — режим работы интерфейса: ◦ `l2` — Layer 2, создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В этом режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security и правила контентной фильтрации. ◦ `l3` — Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах. Это стандартный режим работы интерфейса. • `interface` — интерфейсы, которые будут использованы для создания моста. • `stp` — включение или отключение использование Spanning Tree Protocol (STP) для защиты от петель (`on/off`). • `forward-delay` — задержка перед переключением моста в активный режим (forwarding), в случае если включен STP (указывается в секундах). • `max-age` — время, по истечении которого STP-соединение считается потерянным (указывается в секундах). • `bypass-pair` — пара интерфейсов, которая будет использована для построения байпас-моста. Требуется поддержка оборудования ПАК UserGate
`iface-mode`	Режим назначения IP-адреса: • `dhcp` — получение динамического IP-адреса по DHCP. • `manual` — без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса
`ip-addresses`	Назначение IP-адреса для интерфейса. Адрес задается в виде `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде

Параметр	Описание
	Важно! **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.**
`mac`	MAC-адрес интерфейса
`mtu`	Размер MTU
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение или отключение ретранслятора (`on/off`). • `utm-address` — IP-адрес интерфейса UserGate SWG, на который добавляется функция ретранслятора (принимает значения IP`-адрес/none`). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Команда для изменения параметров существующего bridge-интерфейса:

```
Admin@nodename# set network interface bridge <bridge-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме `interface-name`, `node-name` (изменение значений этих параметров недоступно).

Команда для удаления bridge-интерфейса или его параметров:

```
Admin@nodename# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;

- dhcp-relay server-address — IP-адрес DHCP-сервера.

Команда для отображения информации обо всех bridge-интерфейсах:

```
Admin@nodename# show network interface bridge
```

Команда для отображения информации об определенном bridge-интерфейсе:

```
Admin@nodename# show network interface bridge <bridge-name>
```

Настройка PPPoE-интерфейса

PPPoE-интерфейсы создаются и настраиваются на уровне `network interface PPPoE`.

Для создания PPPoE-интерфейса используется команда:

```
Admin@nodename# create network interface pppoe <parameters>
```

В команде необходимо указать параметры интерфейса.

Параметр	Описание
`enabled`	Включение или отключение интерфейса: • `on`; • `off`
`interface-name`	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет ppp1
`description`	Описание интерфейса
`alias`	Псевдоним («алиас») интерфейса
`node-name`	Имя узла кластера, на котором создается интерфейс
`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_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`config`	Дополнительные параметры PPPoE-интерфейса: • `interface` — интерфейс, на котором будет создаваться PPPoE-интерфейс. • `login` — имя пользователя для соединения PPPoE. • `password` — пароль пользователя для соединения PPPoE. • `persist-connection` — автоматическое переподключение при обрыве связи.

Параметр	Описание

	• `auth-type` — тип авторизации:
	  ◦ `CHAP`;
	  ◦ `PAP`.
	• `holdoff` — интервал времени в секундах после разрыва соединения перед повторным запуском.
	• `default-route` — PPPoE-интерфейс, который будет использоваться как маршрут по умолчанию.
	• `echo-interval` — интервал проверки соединения.
	• `echo-failure` — количество неуспешных проверок соединения, по достижении которого UserGate SWG будет считать, что соединение отсутствует, и разорвет его.
	• `providers-dns` — использование DNS-серверов, выданных провайдером.
	• `connection-attempts` — количество неуспешных попыток подключения, по достижении которого попытки автосоединения будут прекращены.
	• `service-name` — имя сервиса, которое необходимо указать в случае его предоставления провайдером

`mtu`	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40

Команда для изменения параметров существующего PPPoE-интерфейса:

```
Admin@nodename# set network interface pppoe <pppoe-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме `interface-name` (изменение значения этого параметра недоступно).

Команда для удаления PPPoE-интерфейса:

```
Admin@nodename# delete network interface pppoe <pppoe-name>
```

Команда для отображения информации обо всех PPPoE-интерфейсах:

```
Admin@nodename# show network interface pppoe
```

Команда для отображения информации об определенном PPPoE-интерфейсе:

```
Admin@nodename# show network interface pppoe <pppoe-name>
```

Настройка loopback-интерфейса

Loopback-интерфейсы создаются и настраиваются на уровне `network interface loopback`.

Для создания интерфейса используется команда:

```
Admin@nodename# create network interface loopback <parameters>
```

В команде необходимо указать параметры интерфейса.

Параметр	Описание
`enabled`	Включение или отключение интерфейса: • `on`; • `off`
`interface-name`	Название интерфейса
`description`	Описание интерфейса
`alias`	Псевдоним («алиас») интерфейса
`ip-addresses`	Назначение IP-адреса для интерфейса. Адрес задается в виде `[ <ip_address/mask> ]` или `[ <ip_address/mask> <ip_address/mask> ]`, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде

Параметр	Описание
	Важно! **Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.**
`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
`lldp-profile`	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе «Настройка профилей LLDP»
`zone`	Зона, которой будет принадлежать интерфейс
`link-info`	Настройка параметров сетевого интерфейса: • `bc_forwarding` — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • `proxy_arp`, `proxy_arp_pvlan` — механизмы Proxy ARP. При указании параметра `proxy_arp` UserGate SWG будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра `proxy_arp_pvlan` UserGate SWG 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 ]` • `key` — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • `value` — значение параметра. Параметры могут принимать только целочисленные значения.

Параметр	Описание
	Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — `proxy_arp/1`; для отключения — `proxy_arp/0`. Поле `link-info` будет отображено только в случае добавления соответствующих параметров **Важно!** **Удаление заданных параметров link-info недоступно.**
`node-name`	Узел кластера, на котором будет создан интерфейс
`mac`	MAC-адрес интерфейса
`mtu`	Размер MTU
`mss`	Размер MSS: 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU – 40
`dhcp-relay`	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: • `enabled` — включение или отключение ретранслятора (`on/off`). • `utm-address` — IP-адрес интерфейса UserGate SWG, на который добавляется функция ретранслятора (принимает значения IP-`адрес/none`). • `server-address` — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Команда для изменения параметров существующего loopback-интерфейса:

```
Admin@nodename# set network interface loopback <interface-name>
<parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания loopback-интерфейса, кроме `node-name`, `interface` (изменение значений этих параметров недоступно).

Команда для удаления loopback-интерфейса или его параметров:

```
Admin@nodename# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Команда для отображения информации обо всех loopback-интерфейсах:

```
Admin@nodename# show network interface loopback
```

Команда для отображения информации об определенном loopback-интерфейсе:

```
Admin@nodename# show network interface loopback <interface-name>
```

Шлюзы

Шлюзы настраиваются на уровне `network gateway`.

Для добавления нового шлюза используется команда:

```
Admin@nodename# create network gateway
```

В команде необходимо указать параметры шлюза.

Параметр	Описание
`enabled`	Включение/отключение шлюза: • `on`; • `off`
`name`	Название шлюза
`description`	Описание шлюза
`interface`	

Параметр	Описание
	Интерфейс, использующийся для выхода в Интернет: • Выбор конкретного порта (`port0`, `port1`, `port2` итд.); • auto — после выбора этого параметра порт определится автоматически. Данная опция доступна для узлов, прошедших инициализацию
`virtual-router`	Выбор виртуального маршрутизатора, для которого настраивается шлюз
`ip`	IP-адрес шлюза
`node-name`	Выбор узла кластера, для которого настраивается шлюз
`weight`	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз)
`balancing`	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • `on`; • `off`
`default`	Использование данного шлюза в качестве шлюза по умолчанию: • `on`; • `off`

Команда для изменения 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>
```

Команда для отображения информации обо всех шлюзах:

```
Admin@nodename# show network gateway
```

Команда для отображения информации об определенном шлюзе:

```
Admin@nodename# show network gateway <gateway-name>
```

DHCP

Настройка DHCP выполняется на уровне `network dhcp`.

Для создания подсети DHCP используется команда:

```
Admin@nodename# create network dhcp
```

Далее необходимо задать следующие параметры.

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 задается 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

Параметр	Описание
`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

Команда для изменения параметров существующей DHCP-подсети:

```
Admin@nodename# set network dhcp <dhcp-name>
```

Параметры, информацию о которых можно обновить, аналогичны параметрам, доступным при создании.

Команда 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).

Команда для отображения информации обо всех созданных подсетях:

```
Admin@nodename# show network dhcp
```

Команда для отображения информации об определенной подсети DHCP:

```
Admin@nodename# show network dhcp <dhcp-name>
```

DNS-настройки

Настройка DNS находится на уровне `network dns`.

Настройка системных DNS-серверов

Системные DNS-серверы настраиваются 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> ... ]
```

Команда для удаления всего списка адресов серверов DNS:

```
 Admin@nodename# delete network dns system-dns-servers
```

Команда для удаления определённых серверов:

```
 Admin@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

Команда для отображения списка системных DNS-серверов:

```
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 команда:

```
Admin@nodename# set network dns proxy-settings
```

Далее необходимо указать параметры DNS-прокси.

Параметр	Описание
`filtering`	Фильтрация DNS-запросов: • on; • off
`caching`	Кэширование ответов DNS: • on; • off
`limit`	Ограничение количества DNS-запросов в секунду для каждого пользователя (значение по умолчанию: 100)
`max-ttl`	Максимально возможное время жизни для записей DNS
`recursive`	Осуществление рекурсивных DNS-запросов: • on; • off
`dns-timeout`	Время до следующей попытки отправления запроса на DNS-сервера (указывается в миллисекундах)
`a-aaaa-unknown`	Ответы только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS: • on; • off

Параметр	Описание
`retries`	Количество попыток DNS-запроса
`factory-defaults`	Сброс до заводских настроек значения выбранного параметра (параметры представлены в данной таблице) или всех параметров (all)

Пример команды редактирования параметров DNS-proxy:

```
Admin@nodename# set network dns proxy-settings limit 10 dns-timeout 10
```

Команда для просмотра параметров DNS-прокси:

```
Admin@nodename# show network dns proxy-settings
```

Настройка правил DNS

> **Примечание**
> **UserGate SWG не может работать в роли DNS-сервера. Предусмотрена только роль DNS-proxy. При указании в правилах DNS адреса самого UserGate SWG, возможно образование DNS-петли.**

Правила DNS настраиваются на уровне `network dns rules` с использованием UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Параметры правил DNS.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение использования правила: • enabled(yes) или enabled(true); • enabled(no) или enabled(false)
`name`	Название правила. Например: name("DNS rule example")

Параметр	Описание
`desc`	Описание правила DNS-прокси. Например: desc("DNS rule example set via CLI")
`url.domain`	Список доменов, на которые необходимо перенаправлять. Допускается использование звёздочки (*) для указания шаблона доменов. Чтобы указать список доменов: url.domain = "*.example.com"
`dns_server`	Список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены. Для указания сервера: dns_server(1.2.3.4)

Пример создания правила DNS с использованием UPL:

```
Admin@nodename# create network dns rules 1 upl-rule OK \
...url.domain = "*.example.com" \
...dns_server(1.2.3.4) \
...name("DNS rule example") \
...desc("DNS rule example description over CLI") \
...enabled(true) \
...
Admin@nodename#
Admin@nodename# show network dns rules

% ---------------- 1 ----------------
OK \
    url.domain = "*.example.com" \
    dns_server(1.2.3.4) \
    desc("DNS rule example description over CLI") \
    enabled(true) \
    id("0f83e1bb-0aa5-4f42-8eeb-9c4ffa30c04a") \
    name("DNS rule example")
```

Настройка статических записей DNS-прокси

Статические записи DNS-прокси настраиваются на уровне `network dns static-records`.

Для добавления статической DNS-записи используется команда:

```
Admin@nodename# create network dns static-records
```

Далее необходимо указать параметры записи.

Параметр	Описание
`enabled`	Включение/отключение использования статической записи: • on; • off
`name`	Название записи
`description`	Описание DNS-записи
`domain`	FQDN (Fully Qualified Name) статической записи, например www.example.com
`ips`	Список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN

Команда для отображения информации обо всех существующих статических DNS-записях

```
Admin@nodename# show network dns static-records
```

Команда для отображения информации об определённой записи:

```
Admin@nodename# show network dns static-records <static-record-name>
```

Пример создания статической записи DNS:

```
Admin@nodename# create network dns static-records name "Test DNS static
record" description "Test DNS static record description" enabled on
domain example.com ips [ 10.10.0.100 ]
Admin@nodename#
Admin@nodename# show network dns static-records

Test DNS static record
    name              : Test DNS static record
```

```
    description      : Test DNS static record description
    domain           : example.com
    ips              : 10.10.0.100
    enabled          : on
```

Команда для изменения параметров ранее созданных статических записей DNS:

```
Admin@nodename# set network dns static-records <static-record-name>
```

Список параметров, доступных для изменения, аналогичен списку команды `create`.

Пример редактирования ранее созданной статической записи DNS:

```
Admin@nodename# set network dns static-records "Test DNS static record"
ips [ 10.10.0.101 ]
Admin@nodename# show network dns static-records "Test DNS static
record"

name             : Test DNS static record
description      : Test DNS static record description
domain           : example.com
ips              : 10.10.0.100; 10.10.0.101
enabled          : on
```

Команда для удаления статической записи:

```
 Admin@nodename# delete network dns static-records <static-record-name>
```

Настройка виртуальных маршрутизаторов

Виртуальные маршрутизаторы настраиваются на уровне `network virtual-router`.

Команда для добавления нового виртуального маршрутизатора:

```
Admin@nodename# create network virtual-router <parameters>
```

Далее необходимо указать параметры виртуального маршрутизатора.

Параметр	Описание
`name`	Уникальное имя виртуального маршрутизатора
`description`	Описание виртуального маршрутизатора
`node-name`	Выбор узла, 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), бонд-интерфейсы 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
...
```

Команда для удаления виртуального маршрутизатора:

```
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 необходимо указать параметры маршрута.

Параметр	Описание
`enabled`	Включение или отключение использования статического маршрута: • on;

Параметр	Описание
	• 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 узла 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
...
```

Команда для изменения параметров созданного ранее статического маршрута:

```
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
...
```

Команда 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              : []
...
```

Команда для отображения статических маршрутов:

```
 Admin@nodename# show network virtual-router <virtual-router-name>
routes
```

Настройка OSPF

Для настройки OSPF используется команда:

```
Admin@nodename# set network virtual-router <virtual-router-name> ospf
```

Далее необходимо указать параметры OSPF.

Параметр	Описание
`enabled`	Включение или 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 устройства, 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.
	• bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке

Параметр	Описание

	элементов. Подробнее — 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. Аутентификация обычно используется для

Параметр	Описание
	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.
	◦ digest — использование MD5-хеша для ключа для аутентификации OSPF-пакетов.

Параметр	Описание
	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`	Распространение OSPF маршрутов: • connected — распространение маршрутов в непосредственно подключённые к устройству сети.

Параметр	Описание
	• kernel — распространение маршрутов, которые были добавлены администратором

Команда для отображения конфигурации OSPF в виртуальном маршрутизаторе:

```
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           : []
...
```

Команда для удаления настройки OSPF:

```
 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 команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> bgp
```

Далее необходимо указать параметры BGP.

Параметр	Описание
`enabled`	Включение/отключение OSPF-маршрутизатора: • on; • off
`router-id`	IP-адрес маршрутизатора. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору. При выключении BGP (enabled off) значение router-id может быть удалено (none)
`asn`	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе
`multiple-path`	Включение/отключение балансировки трафика на маршруты с одинаковой стоимостью: • on;

Параметр	Описание
	• off
`redistribute`	Распространение BGP маршрутов: • connected — распространение маршрутов в непосредственно подключённые к устройству 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.
	• action — действие:
	  ◦ allow — разрешить прохождение данных, попадающих под условия routemap.
	  ◦ block — запретить прохождение данных, попадающих под условия routemap.
	• next-hop — установка для отфильтрованных маршрутов значения next hop в указанный IP-адрес.
	• weight — установка для отфильтрованных маршрутов веса в указанное значение.
	• metric — установка для отфильтрованных маршрутов метрики в указанное значение.

Параметр	Описание

	• position — порядковый номер routemap в общем списке.
	• 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

`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>`

Параметр	Описание

	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.
	• ip-filter — необходимо добавить все необходимые IP-адреса при выборе фильтрации по IP-адресу. Адреса могут быть указаны в следующих форматах:
	  ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8.
	  ◦ 10.0.0.0./8:11 — маршруты, у которых первый октет 10 и префикс от 8 до 11.
	  ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13.
	• as-path-filter — необходимо добавить все необходимые номера автономных сетей при выборе фильтрации по AS пути.
	• position — порядковый номер фильтра в общем списке

`neighbors`	BGP-соседи.
	Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды:
	`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.

Параметр	Описание

	• 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 — 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.
	• 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.

Параметр	Описание
	◦ 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 команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> rip
```

Далее необходимо указать параметры RIP.

Параметр	Описание
`enabled`	Включение/отключение RIP-маршрутизатора: • on; • off

Параметр	Описание
`version`	Версия протокола RIP: • 1; • 2. Как правило, используется версия протокола 2
`metric`	Метрика RIP. По умолчанию метрика равна 1; максимальное значение — 15. Значение 16 считается бесконечным
`distance`	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические)
`originate`	Отправлять себя в качестве маршрута по умолчанию
`networks-cidr`	Указание сети в виде CIDR. Указывается в формате `<ip/mask>`
`networks-interface`	Указание сетевого интерфейса, с которого будут отправлять обновления маршрутной информации; указываются интерфейсы, принадлежащие виртуальному маршрутизатору

`redistribute`	Распространение маршрутов:
	• connected — распространение другим роутерам RIP маршрутов в непосредственно подключённые к UserGate сети:
	  ◦ <metric> — значение метрики; может принимать значения от 0 до 16;
	  ◦ off.
	• static — распространение другим маршрутизаторам статических маршрутов:
	  ◦ <metric> — значение метрики; может принимать значения от 0 до 16;
	  ◦ off.
	• kernel — распространение другим роутерам RIP маршрутов, которые были добавлены администратором:
	  ◦ <metric> — значение метрики; может принимать значения от 0 до 16;
	  ◦ off.

Параметр	Описание
	• 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 <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,

Параметр	Описание
	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 команды:

```
Admin@nodename# set network virtual-router <virtual-router-name>
multicast-router
```

Далее необходимо указать параметры мультикаст-маршрутизации.

Параметр	Описание
`enabled`	Включение или 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)

Параметр	Описание
`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:
	`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,

Параметр	Описание
	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 — 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

`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

Команда для отображения конфигурации мультикастинга в виртуальном маршрутизаторе:

```
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) выполняется на уровне `network wccp`.

Для создания сервисной группы WCCP используется команда:

```
Admin@nodename# create network wccp <parameter>
```

Далее необходимо указать параметры сервисной группы.

Параметр	Описание
`enabled`	Включение или отключение сервисной группы: • on; • off
`name`	Название сервисной группы WCCP
`description`	Описание сервисной группы
`password`	Пароль, необходимый для аутентификации устройства UserGate в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP
`fwd-type`	Способ перенаправления трафика с серверов WCCP на устройство UserGate: • l2 — используя перенаправление L2.В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес устройства UserGate. • gre — используя туннель GRE (Generic Routing Encapsulation).

Параметр	Описание
	Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и устройство 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 устройства UserGate на серверы WCCP: • l2 — используя перенаправление L2. В этом случае устройство 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 устройство UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2
`service-group`	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу
`priority`	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP
`ports`	Порты для перенаправления (порты назначения трафика). При необходимости указываются несколько портов в формате: `ports-to-redirect + [ 80 442 ]`. Важно! UserGate SWG может применять фильтрацию только для перенаправленного TCP-трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate SWG 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);

Параметр	Описание
	• udp — User Datagram Protocol (UDP)
`routers-lists`	Список IP-адресов серверов WCCP. Подробнее о создании списков IP-адресов с помощью CLI — 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. ◦ 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

Параметр	Описание
	порту — 16 бит; по IP-адресу — 32 бита; указываются в шестнадцатеричном формате

Команда 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.

Команда 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
```

Команда для удаления сервисной группы полностью или некоторых её параметров:

```
Admin@nodename# delete network wccp <service-group-name>
```

Параметры, доступные для удаления:

- `routers-lists`;
- `routers-ips`;
- `ports`.

НАСТРОЙКА РАЗДЕЛА ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Настройка групп пользователей

Группы пользователей настраиваются на уровне `users group`.

Для добавления новой группы пользователей используется команда:

```
Admin@nodename# create users group <parameter>
```

Далее необходимо указать параметры группы.

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> ... ]`)

Команда для изменения параметров группы пользователей (параметры, доступные для обновления, аналогичны с параметрами, доступными при создании группы):

```
Admin@nodename# set users group <group-name> <parameter>
```

Команда для отображения параметров группы:

```
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)
```

Команда для удаления группы пользователей или отдельных пользователей из группы:

```
Admin@nodename# delete users group <group-name>
```

Команда для удаления локальных пользователей:

```
Admin@nodename# delete users group <group-name> users [ <user1>
<user2> ... ]
```

Клманда 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 выполняется на уровне `users user`.

Команда для добавления пользователей:

```
Admin@nodename# create users user <parameter>
```

Далее необходимо указать параметры пользователей.

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

Параметр	Описание
ip-range	Диапазон IP-адресов для идентификации пользователя; пользователь всегда должен получать доступ в сеть с адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>
ip-mac	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

Команда для изменения 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
```

Команда для удаления учётной записи пользователя:

```
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

Настройка серверов аутентификации выполняется на уровне `users auth-server`.

С помощью команд этого раздела вы можете выполнить настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP

Настройка LDAP-коннектора

LDAP-коннектор настраивается на уровне `users auth-server ldap`.

Для создания LDAP-коннектора используется команда:

```
Admin@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать параметры коннектора.

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
`cache-ttl`	Время жизни записей LDAP-кэша. (Опция доступна начиная с релиза UGOS 7.1.3)
`domains`	Список доменов, которые обслуживаются указанным контроллером домена
`search-roots`	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня

Команда для редактирования информации о существующем LDAP-коннекторе:

```
 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
```

Команда для удаления LDAP-коннектора:

```
 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 выполняется на уровне `users auth-server radius`.

Для создания сервера аутентификации RADIUS используется команда:

```
Admin@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать параметры сервера.

Параметр	Описание
`name`	Имя RADIUS-сервера
`enabled`	Включение или 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 изменения параметров сервера 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
```

Команда 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+ выполняется на уровне users auth-server tacacs.

Для создания сервера аутентификации TACACS+ используется команда:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать параметры сервера.

Параметр	Описание
`name`	Имя сервера TACACS+
`enabled`	Включение или 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
```

Команда для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка сервера NTLM

Настройка сервера NTLM выполняется на уровне `users auth-server ntlm`.

Для создания сервера аутентифификации NTLM используется команда:

```
Admin@nodename# create users auth-server ntlm <parameter>
```

Далее необходимо указать параметры сервера.

Параметр	Описание
`name`	Имя NTLM-сервера
`enabled`	Включение или отключение сервера аутентификации
`description`	Описание сервера аутентификации
`domain`	IP-адрес или доменное имя сервера NLM

Команда для обновления информации о NTLM-сервере:

```
 Admin@nodename# set users auth-server ntlm <ntlm-server-name>
<parameter>
```

Команда для отображения информации о сервере NTLM:

```
Admin@nodename# show users auth-server ntlm <ntlm-server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Примеры команд для создания и редактирования сервера NTLM:

```
Admin@nodename# create users auth-server ntlm name "New NTLM server"
domain 10.10.0.12 enabled on
Admin@nodename# show users auth-server ntlm "New NTLM server"

name            : New NTLM server
enabled         : on
domain          : 10.10.0.12

Admin@nodename# set users auth-server ntlm "New NTLM server"
description "New NTLM server description"
Admin@nodename# show users auth-server ntlm "New NTLM server"

name            : New NTLM server
description     : New NTLM server description
```

```
enabled        : on
domain         : 10.10.0.12
```

Команда для удаления сервера:

```
Admin@nodename# delete users auth-servers ntlm <ntlm-server-name>
```

Настройка сервера SAML IDP

Настройка сервера SAML IDP выполняется на уровне `users auth-server saml-idp`.

Для создания сервера аутентификации SAML IDP используется команда:

```
Admin@nodename# create users auth-server saml-idp <parameter>
```

Далее необходимо указать параметры сервера.

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

Параметр	Описание
`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
```

Команда для удаления сервера:

```
 Admin@nodename# delete users auth-servers saml-idp <saml-idp-server-
name>
```

Настройка профилей аутентификации

Профили аутентификации настраиваются на уровне `users auth-profile`.

Для создания профиля аутентификации используется команда:

```
Admin@nodename# create users auth-profile <parameter>
```

Далее необходимо указать параметры профиля.

Параметр	Описание
`name`	Название профиля.
`description`	Описание профиля.
`mfa`	Указание профиля многофакторной аутентификации (если её необходимо использовать). Для указания профиль MFA должен быть создан заранее. Подробнее о создании профилей MFA с использованием интерфейса командной строки — в разделе «Настройка профилей MFA (многофакторной аутентификации)»
`idle-time`	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user

Параметр	Описание
`expiration-time`	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная авторизация пользователя на Captive-портале
`max-attempts`	Число неудачных попыток авторизации через Captive-портал до блокировки учётной записи пользователя
`lockout-time`	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации; указывается в секундах
`auth-methods`	Метод аутентификации: • `local-user-auth`: аутентификация по базе данных локально заведенных пользователей. • `policy-accept`: не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети; применяется совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • `http-basic`: аутентификация с помощью метода HTTP Basic. • `ldap`: аутентификация с использованием LDAP-коннектора. • `radius`: аутентификация с использованием RADIUS-сервера. • `tacacs`: аутентификация с использованием сервера TACACS+. • `ntlm`: аутентификация с использованием NTLM-сервера. • `saml-idp`: аутентификация с использованием сервера SAML IDP

Команда для изменения параметров 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
```

Команда для удаления профиля аутентификации:

```
Admin@nodename# delete users auth-profile <auth-profile-name>
```

Команда для удаления методов аутентификации, заданных в профиле:

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-
methods <auth-metod>
```

Настройка Captive-профилей

Captive-профили настраиваются на уровне `users captive-profiles`.

Для создания Captive-профиля используется команда:

```
Admin@nodename# create users captive-profiles <parameter>
```

Далее необходимо указать параметры профтля.

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 — 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.

Команда для изменения параметров профиля:

```
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
```

Команда для удаления профиля:

```
Admin@nodename# delete users captive-profiles <captive-profile-name>
```

Команда для 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

Правила Captive-портала настраиваются с помощью синтаксиса UPL на уровне `users captive-portal`. Подробнее о структуре команд — в разделе «UserGate Policy Language».

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 — 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, 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 — 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 — 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 — 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
`dst.zone`	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: `dst.zone = Untrusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 — 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 — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке
`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 — в разделе «Настройка категорий URL». Для указания категории URL: `category = "URL category name"`
`url`	Списки URL, для которых будет применяться правило. Для указания списка URL: `url = lib.url()`; в скобках необходимо указать название списка URL
`time`	Настройка расписания работы правила. Для установки расписания: `time = lib.time()`; в скобках необходимо указать название группы календарей.

Параметр	Описание
	Подробнее о настройке календарей — 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

Настройка терминальных серверов выполняется на уровне `users terminal-servers`.

Для создания терминального сервера используется команда:

```
Admin@nodename# create users terminal-servers <parameter>
```

Далее необходимо указать параметры сервера.

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 изменения параметров 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 узлов. Для удаления необходимо уточнить их адреса:

```
Admin@nodename# delete users terminal-servers <terminal-server-name>
hosts
```

Настройка профилей MFA (многофакторной аутентификации)

Профили MFA настраиваются на уровне `users mfa-profiles`.

Вы можете создать несколько типов профилей:

- MFA через TOTP: использование токена TOTP (Time-based One Time Password) в качестве второго фактора аутентификации.
- MFA через email: использование одноразового пароля, полученного по email, в качестве второго фактора аутентификации.
- MFA через SMS: использование одноразового пароля, полученного по SMS, в качестве второго фактора аутентификации.

Для создания профиля многофакторной аутентификации используется команда:

```
Admin@nodename# create users mfa-profiles <parameter>
```

Команда для удаления профиля многофакторной аутентификации:

```
Admin@nodename# delete users mfa-profiles <mfa-name>
```

Команда для отображения информации о всех профилях или об определённом профиле MFA:

```
Admin@nodename# show users mfa-profiles
Admin@nodename# show users mfa-profiles <mfa-name>
```

Настройка MFA через TOTP

Команда для добавления нового профиля многофакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp <parameter>
```

Далее необходимо указать параметры профиля.

Параметр	Описание
`name`	Название профиля MFA
`description`	Описание профиля MFA
`show-qr-code`	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP-клиента
`notification-profile`	Выбор профиля оповещения
`notification-sender`	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля)
`notification-subject`	Тема оповещения при использовании оповещений по email

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 (`""`)

Команда для редактирования параметров профиля многофакторной 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 многофакторной 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 многофакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp <parameter>
```

Далее необходимо указать параметры профиля.

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 многофакторной 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 многофакторной 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 многофакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp <parameter>
```

Далее необходимо указать параметры профиля.

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 многофакторной 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 многофакторной 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 команда:

```
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>
```

В качестве параметра может использоваться как имя пользователя, так и его IP-адрес.

Настройка применения политик к пользователям

Для локальных пользователей устройства 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 кэш-памяти LDAP-записей на устройстве 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 кэш-памяти используется команда:

```
Admin@nodename# execute cache ldap-clear
```

Настройка подключения к серверу регистрации доверенных браузеров

Подключение к серверу регистрации доверенных браузеров настраиваются на уровне `users trusted-browser`.

Для создания подключения используется команда:

```
Admin@nodename# create users trusted-browser <parameter>
```

Далее необходимо указать параметры подключения.

Параметр	Описание
`name`	Название подключения
`description`	Описание подключения
`url`	URL сервера регистрации доверенных браузеров, развернутого в компании
`jwt-issuer`	Параметр задается администратором в переменных среды сервера регистрации Яндекс Браузера (URL_IDP) и передается в составе токена JWT. Используется для идентификации сервера регистрации, выдавшего JWT, если в сети имеется нескольких таких серверов
`port`	Порт подключения к серверу регистрации доверенных браузеров

Параметр	Описание
`bearer-token`	Ключ доступа к серверу регистрации доверенных браузеров. Определяется администратором сервиса регистрации
`keys-update-timeout`	Интервал времени, через который UserGate SWG запрашивает у сервера регистрации доверенных браузеров набор открытых ключей в формате JWKS

Команда для изменения параметров подключения:

```
Admin@nodename# set users trusted-browser <connection-name> <parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды `create`.

Команда для просмотра параметров подключения к серверу регистрации доверенных браузеров:

```
Admin@nodenamet# show users trusted-browser <connection-name>
```

Пример создания и редактирования подключения к серверу регистрации доверенных браузеров:

```
Admin@nodename# create users trusted-browser name "Test1" description
"New enrollment host connection" url https://test1.net jwt-issuer
https://test1.net bearer-token 123321 port 8080
Admin@nodename# show users trusted-browser Test1

name                    : Test1
description             : New enrollment host connection
url                     : https://test1.net
jwt-issuer              : https://test1.net
port                    : 8080
bearer-token            : 123321
keys-update-timeout     : 600
```

Команда для удаления подключения к серверу регистрации:

```
Admin@nodename# delete users trusted-browser <connection-name>
```

Подробнее о работе с доверенными браузерами — в разделе «Работа с доверенными браузерами».

Об использовании доверенных браузеров в правилах фильтрации контента — в разделе «Настройка фильтрации контента»; в правилах reverse-прокси — в разделе «Настройка правил reverse-прокси».

НАСТРОЙКА РАЗДЕЛА ПОЛИТИКИ СЕТИ

Настройка правил межсетевого экрана

Правила межсетевого экрана настраиваются на уровне `network-policy firewall` с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила межсетевого экрана используется команда:

```
Admin@nodename# create network-policy firewall
```

Далее необходимо указать параметры правила.

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")`

Параметр	Описание
`desc`	Описание правила. Например: `desc("Firewall rule example configured in CLI")`
`reject_with`	Настройка доступна для правил с действием «Запретить»: • `reject_with(no)`. • `reject_with("host_unreach")` — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • `reject_with("tcp_rst")` — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** **При выборе действия «Посылать TCP reset» необходимо указание сервиса, использующего протокол TCP.** • reject_with("tcp_reset-both") — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
`scenario`	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: `scenario = "Example of a scenario"`. Подробнее о настройке сценариев — 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

Параметр	Описание
	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
`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 — 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 — 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 — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке
`user`	

Параметр	Описание

	Пользователи и группы пользователей, для которых применяется правило межсетевого экрана (локальные или LDAP).
	Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора).
	Примеры добавления пользователей в правило:
	`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 — 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 — 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 — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке
`time`	Настройка расписания работы правила. Для установки расписания: `time = lib.time()`; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Пример создания правила межсетевого экрана с использованием UPL:

```
Admin@nodename# create network-policy firewall 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = known \
...service = HTTP \
...rule_log(session) \
...name("Test firewall rule") \
...enabled(true)
...
Admin@nodename# show network-policy firewall 1
% ---------------- 1 ----------------
PASS \
    user = known \
    src.zone = Trusted \
    dst.zone = Untrusted \
    service = HTTP \
    rule_log(session) \
    enabled(true) \
    id("1505d309-621b-4f88-a2e4-98667c477535") \
    name("Test firewall rule")
```

Настройка правил NAT и маршрутизации

Правила NAT и маршрутизации настраиваются на уровне `network-policy nat-routing`. Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе UserGate Policy Language.

Для создания правила используется команда:

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

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set network-policy nat-routing <position> upl-rule
<parameters>
```

Команда для просмотра ранее созданных правил:

```
Admin@nodename# show network-policy nat-routing <position>
```

Команда для удаления ранее созданных правил:

```
Admin@nodename# delete network-policy nat-routing <position>
```

Подробнее о применении правил NAT — в разделе «NAT и маршрутизация».

Настройка правил NAT

При настройке правил NAT укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила NAT. Например, `name("NAT rule example")`
`desc`	Описание правила. Например, `desc("NAT rule example set via CLI")`
`nat`	Тип правила
`snat_target_ip`	IP-адрес, на который будет заменен адрес источника. Адрес указывается в кавычках. 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. Например, для указания зоны Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: `src.ip = 02:00:00:00:00:00`
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`

Параметр	Описание
`dst.zone`	Зона назначения трафика. Для указания зоны назначения трафика, например Untrusted: `dst.zone = Untrusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`dst.ip`	Добавление списков IP-адресов, доменов назначения, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов назначения используйте: `dst.ip = 02:00:00:00:00:00`

Пример создания правила NAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...nat \
...rule_log(session) \
...name("Test NAT rule") \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 1
% ---------------- 1 ----------------
OK \
    src.zone = Trusted \
    dst.zone = Untrusted \
    direction(input) \
    rule_log(session) \
    enabled(true) \
    id("0344640b-b392-4920-9853-77d85ec1338c") \
```

```
    name("Test NAT rule")\
    nat
```

Настройка правил NoNAT

При настройке правил NoNAT укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила NAT. Например, `name("NAT rule example")`
`desc`	Описание правила. Например, `desc("NAT rule example set via CLI")`
`nonat`	Тип 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. Например, указание зоны `Trusted: src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление адресов источника трафика в виде списков IP-адресов, доменов источника, или MAC-адресов. 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 — в разделе «Настройка IP-адресов».

Параметр	Описание
	Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте строку вида: `src.ip = 02:00:00:00:00:00`
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`dst.zone`	Зона назначения трафика. Например, указание зоны Untrusted: `dst.zone = Untrusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»

Пример создания правила NoNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 6 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = "testd.local\\user3" \
...rule_log(session) \
...name("NoNAT rule 1") \
...nonat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 6
% ---------------- 6 ----------------
OK \
    user = "testd.local\\user3" \
    src.zone = Trusted \
    dst.zone = Untrusted \
    rule_log(session) \
    enabled(true) \
    name("NoNAT rule 1")\
    nonat
```

Настройка правил DNAT

При настройке правил DNAT укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — включение правила
`name`	Название правила DNAT. Например, `name("DNAT rule example")`

Параметр	Описание
`desc`	Описание правила. Для описание правила используйте: `desc("DNAT rule example created via CLI")`
`dnat`	Тип правила
`snat_target_ip`	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. 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. Например, чтобы указать зону Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: `src.ip = 02:00:00:00:00:00`
`src.geoip`	Указание Geo IP источника; необходимо указать код страны. Например, `src.geoip = RU`. Коды названий стран доступны по ссылке
`user`	Список пользователей или групп, для которых применяется данное правило.

Параметр	Описание
	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`dst.zone`	Зона назначения трафика. Например, для указания зоны Untrusted: `dst.zone = Untrusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`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 NoDNAT

При настройке правил NoDNAT укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила DNAT. Например, `name("DNAT rule example")`

Параметр	Описание
`desc`	Описание правила. Например, `desc("DNAT rule example created via CLI")`
`dnat`	Тип правила
`snat_target_ip`	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. 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. Например, чтобы указать зону Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: `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

Параметр	Описание
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`dst.zone`	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: `dst.zone = Untrusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`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 7 upl-rule PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...user = known \
...rule_log(session) \
...name("NoDNAT rule") \
...nodnat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 7
% ---------------- 7 ----------------
OK \
    user = known \
    src.zone = Untrusted \
    dst.zone = Trusted \
    rule_log(session) \
    enabled(true) \
    name("NoDNAT rule")\
    nodnat
```

Настройка правил трансляции портов

При настройке правил трансляции портов укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение или отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила трансляции портов. Например, `name("Port forwarding rule example")`

Параметр	Описание
`desc`	Описание правила. Для создания описание правила используйте: `desc("Port forwarding rule example created via CLI")`
`port_mapping`	Тип правила.
`snat_target_ip`	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. 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`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: `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
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило.

Параметр	Описание
	Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`port_map`	Переназначение портов публикуемых сервисов. Для переназначения портов необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, `port_map(tcp, 2000, 2100)`. Следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами SWG: 2200, 8001, 4369, 9000-9100
`target_ip`	Адрес назначения DNAT. Например, `target_ip("1.1.1.1")`
`target_snat`	Изменение IP-адреса источника на адрес узла UserGate: • `target_snat(yes)` или `target_snat(true)`; • `target_snat(no)` или `target_snat(false)`

Пример создания правила трансляции портов с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = Untrusted \
... dst.ip = lib.network(UG_IP) \
... target_ip("10.10.0.16") \
... port_map(tcp, 2222, 23) \
... rule_log(session) \
... name(port_fw1) \
... port_mapping \
...
Admin@nodename# show network-policy nat-routing 8
% ---------------- 8 ----------------
OK \
    src.zone = Untrusted \
    dst.ip = lib.network(UG_IP) \
    target_ip("10.10.0.16") \
    port_map(tcp, 2222, 23) \
    direction(input) \
    rule_log(session) \
    enabled(true) \
    id("1af47c3f-96a3-4e65-90e3-debf169bb745") \
    name(port_fw1)\
    port_mapping
```

Настройка правил маршрутизации на основе политик

Для настройки правил маршрутизации на основе политик (policy-based routing, PBR) укажите следующие параметры.

Параметр	Описание
`PASS` `OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила

Параметр	Описание
`name`	Название правила. Например, `name("Policy-based routing rule example")`
`desc`	Описание правила. Для создания описание правила используйте: `desc("Policy-based routing rule example set via CLI")`
`route`	Тип правила.
`gateway`	Выбор одного из существующих шлюзов. Например, `gateway("1.1.1.1")`. О добавлении шлюзов с использованием интерфейса командной строки — в разделе «Настройка шлюзов»
`scenario`	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария используйте: `scenario = "Example of a scenario"`. Подробнее о настройке сценариев с использованием интерфейса командной строки — 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 — 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены.

Параметр	Описание
	Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: `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
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`dst.ip`	Добавление списков IP-адресов, 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны. Например, `dst.geoip = RU`. Коды названий стран доступны по ссылке

Пример создания и редактирования правила PBR с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule OK \
... route \
... gateway("def") \
... name("testpbr1") \
... enabled(true) \
... rule_log(session) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... service = (HTTPS, HTTP) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... user = "CN=Users1,DC=LOCAL"
Admin@nodename# show network-policy nat-routing 7
% ---------------- 7 ----------------
OK \
    user = "CN=Users1,DC=LOCAL" \
    service = (HTTPS, HTTP) \
    gateway(def) \
    direction(input) \
    rule_log(session) \
    enabled(true) \
    id("0585a95f-4707-4c11-840d-44643bc2c799") \
    name(testpbr1)\
    route
```

Настройка правил трансляции адресов сетей

При настройке правил трансляции адресов сетей (network mapping) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL

Параметр	Описание
`enabled`	Включение или отключение правила: • `enabled(yes)` или `enabled(true)` — включение правила; • `enabled(no)` или `enabled(false)` — отключение правила
`name`	Название правила. Например, `name("Network mapping rule example")`.
`desc`	Описание правила. Для создания описание правила используйте: `desc("Network mapping rule example set via CLI")`
`netmap`	Тип 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 — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: `src.ip = 02:00:00:00:00:00`

Параметр	Описание
`src.geoip`	Указание GeoIP источника; необходимо указать код страны. Например, `src.geoip = RU`. Коды названий стран доступны по ссылке
`user`	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа `Any`, `Unknown`, `Known`. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • `user = known`; • `user = user1`; • `user = "testd.local\\user2"`; • `user = (user1, "testd.local\\user2")`
`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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: `dst.ip = lib.url()`; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны. Например, `dst.geoip = RU`. Коды названий стран доступны по ссылке
`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.

Параметр	Описание
	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 трансляции адресов сетей с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = External \
... target_ip("192.168.222.0/24") \
... direction(output) \
... netmap \
... rule_log(session) \
... name(netmap1) \
...
Admin@nodename# show network-policy nat-routing 8
% ---------------- 8 ----------------
OK \
    src.zone = External \
    target_ip("192.168.222.0/24") \
    direction(output) \
    rule_log(session) \
    enabled(true) \
    id("26cbd3e8-0210-494c-9fd4-57300b47a9fe") \
    name(netmap1)\
    netmap
```

Настройка балансировки нагрузки

Правила балансировки нагрузки настраиваются на уровне `network-policy load-balancing` с использованием синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для отображения информации о всех балансировщиках используется команда:

```
Admin@nodename# show network-policy load-balancing
```

Настройка балансировщика TCP/UDP

Настройка балансировщика TPC/UDP выполняется на уровне `network-policy load-balancing tcp-udp`.

Для создания балансировщика нагрузки TCP/UDP используется команда:

```
Admin@nodename# create network-policy load-balancing tcp-udp <position>
upl-rule
```

Параметры правил балансировки нагрузки TCP/UDP.

Параметр	Описание
`OK`	Действие для создания правила с помощью UPL
`name`	Название правила балансировки. Например: `name("TCP_UDP balancer")`
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)`. • `enabled(no)` или `enabled(false)`
`desc`	Описание правила. Например: `desc("TCP_UDP balancing rule")`
`src.zone`	Зона источника трафика. Для указания зоны источника, например, Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 — 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

Параметр	Описание
	о создании и настройке списков URL с использованием интерфейса командной строки — 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. • `wlc` — weighted least connections, работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. Например: `scheduler(rr)`
`real_server`	Реальные сервера, на которые будет перенаправляться трафик. Для сервера необходимо указать: • `ip` — IP-адрес сервера. • `port` — порт сервера, на который будут перенаправлять запросы пользователей.

Параметр	Описание
	• `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 SWG 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 SWG подменяет IP-адрес источника на свой. 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-

Параметр	Описание

	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) \`

Команда для редактирования существующего правила балансировки нагрузки:

```
 Admin@nodename# set network-policy load-balancing tcp-udp <position>
upl-rule
```

Команда для отображения информации о всех правилах балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp
```

Команда 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)
```

Команда для удаления существующего балансировщика нагрузки:

```
Admin@nodename# delete network-policy load-balancing tcp-udp <position>
```

Настройка балансировщика reverse-прокси

Настройка правил балансировки reverse-прокси выполняется на уровне `network-policy load-balancing reverse-proxy`.

Для создания правила балансировки reverse-прокси используется команда:

```
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». 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
```

Команда 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)
```

Команда для удаления существующего правила балансировки нагрузки reverse-proxy:

```
Admin@nodename# delete network-policy load-balancing reverse-
proxy <position>
```

Настройка правил управления пропускной способностью

Правила управления пропускной способностью настраиваются на уровне `network-policy traffic-shaping` с использованием синтаксиса языка UPL. О структуре команд подробнее — в разделе «UserGate Policy Language».

Для создания правила управления пропускной способностью используется команда:

```
Admin@nodename# create network-policy traffic-shaping <position> upl-
rule
```

Параметры правил управления пропускной способностью.

Параметр	Описание
`OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)`. • `enabled(no)` или `enabled(false)`
`name`	Название правила пропускной способности. Например: `name("Traffic shaping rule example")`
`desc`	Описание правила. Для задания описания правила: `desc("The example of traffic shaping rule configured in CLI")`
`bandwidth_pool`	Полоса пропускания, например, `bandwidth_pool("1 Mbps")`. Подробнее о создании и настройке полос пропускания — в разделе «Настройка полос пропускания»
`scenario`	Сценарий, который должен быть активным для срабатывания правила.

Параметр	Описание
	Для указания сценария: `scenario = "Example of a scenario"`. Подробнее о настройке сценариев — 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 — 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 — 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 — в разделе «Настройка списков URL»

Параметр	Описание
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке

`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 — 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 — 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 — 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 — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке
`application`	

Параметр	Описание
	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 — в разделе «Настройка календарей»

Команда для редактирования правила управления пропускной способностью:

```
Admin@nodename# set network-policy traffic-shaping <position> upl-rule
```

Команда для просмотра всех созданных правил управления пропускной способностью:

```
Admin@nodename# show network-policy traffic-shaping
```

Команда для просмотра определенного правила управления пропускной способностью:

```
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")
```

Команда для удаления правила управления пропускной способностью:

```
Admin@nodename# delete network-policy traffic-shaping <position>
```

НАСТРОЙКА РАЗДЕЛА ПОЛИТИКИ БЕЗОПАСНОСТИ

Настройка правил фильтрации контента

Правила контентной фильтрации создаются на уровне `security-policy content-filtering` с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила контентной фильтрации используется команда:

```
Admin@nodename# create security-policy content-filtering <position>
upl-rule
```

Параметры правил контентной фильтрации.

Параметр	Описание

`PASS`
`DENY`
`WARNING`
	Действие правила контентной фильтрации:
	• `PASS` — разрешить просмотр веб-страницы;
	• `DENY` — блокировать веб-страницу;
	• `WARNING` — предупредить пользователя о том, что страница нежелательна для просмотра. Пользователь сам решает, отказаться от просмотра нет. Запись о просмотре страницы заносится в журнал

`enabled`	Включение или отключение правила: • `enabled(yes)` или `enabled(true)`; • `enabled(no)` или `enabled(false)`
`name`	Название правила контентной фильтрации. Для указания названия правила: `name("Content filtering rule example")`
`desc`	Описание правила. Например: `desc("Content filtering rule example set via CLI")`

Параметр	Описание
`rule_log`	Запись в журнал информации о трафике при срабатывании правила: • `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 — в разделе «Настройка сценариев»
`virus_usergate`	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием «Запретить»: • `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
`blockpage`	Выбор страницы блокировки; если страница не указана, используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например `DENY("Blockpage (RU)")`. Подробнее о настройке страниц блокировки — в разделе «Настройка шаблонов страниц». Вы также можете использовать внешнюю страницу, задав внешний URL: `redirect(302, "http://www.example.com")`
`src.zone`	Зона источника трафика. Для указания зоны источника, например Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов или доменов источника. Для списка IP-адресов: `src.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и

Параметр	Описание
	настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов источника: `src.ip = lib.url()`; в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке

`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 — 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 — в разделе «Зоны»
`dst.ip`	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: `dst.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: `dst.ip = lib.url()`; в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`).

Параметр	Описание
	Коды названий стран доступны по ссылке
`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 — 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 — в разделе «Настройка списков URL»
`response.header.Content-Type`	Списки типов контента, к которым будут применяться правила. Для задания списка типов контента: `response.header.Content-Type = lib.mime()`; в скобках укажите название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — 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 укажите название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка морфологи»
`request.header.User-Agent`	User agent пользовательских браузеров, для которых будет применено правило. Для указания User agent пользовательских браузеров: `request.header.User-Agent = lib.useragent()`; в скобках необходимо указать название категории User agent браузеров.

Параметр	Описание
	Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка User agent 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 (адреса страниц, с которых пользователь перешел к текущему ресурсу) 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 — 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 — в разделе «Настройка календарей»
`trusted_browser`	Проверка подлинности браузера для предоставления доступа к ресурсам. Укажите созданное ранее подключение к серверу регистрации доверенных браузеров. Например: `trusted_browser = "111"`. Подробнее о работе с доверенными браузерами — в разделе «Работа с доверенными браузерами»

Для редактирования правил контентной фильтрации используется команда:

```
Admin@nodename# set security-policy content-filtering <position> upl-rule
```

Команда для просмотра всех созданных правил контентной фильтрации:

```
Admin@nodename# show security-policy content-filtering
```

Команда для просмотра определенного правила контентной фильтрации:

```
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")
```

Команда для удаления существующего правила контентной фильтрации:

```
Admin@nodename# delete security-policy content-filtering <position>
```

Настройка правил веб-безопасности

Правила веб-безопасности создаются на уровне `security-policy safe-browsing` с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила веб-безопасности используется команда:

```
Admin@nodename# create security-policy safe-browsing <position> upl-rule
```

Параметры правил веб-безопасности.

Параметр	Описание
`OK`	Действие для создания правила с помощью UPL
`enabled`	Включение/отключение правила: • `enabled(yes)` или `enabled(true)`; • `enabled(no)` или `enabled(false)`
`name`	Название правила веб-безопасности. Например: `name("Safe browsing rule example")`
`desc`	Описание правила, например `desc("Safe browsing rule example set via CLI")`
`rule_log`	Запись в журнал информации о трафике при срабатывании правила: • `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")`.

Параметр	Описание
	О создании и настройке списков URL с использованием CLI — в разделе «Настройка списков URL»
`enable_injector`	Встраивание кода в веб страницы: • `enable_injector(yes)` или `enable_injector(true)`; • `enable_injector(no)` или `enable_injector(false)`
`custom_injector`	Встраиваемый код
`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
`social_sites_block`	Блокировка приложений социальных сетей: • `social_sites_block(yes)` или `social_sites_block(true)`; • `social_sites_block(no)` или `social_sites_block(false)`
`src.zone`	Зона источника трафика. Для указания зоны источника, например Trusted: `src.zone = Trusted`. Подробнее о настройке зон с использованием интерфейса командной строки — 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 — 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 — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке

`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 — в разделе0« 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. Для установки расписания: `time = lib.time()`; в скобках укажите название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Команда для редактирования правил веб-безопасности:

```
Admin@nodename# set security-policy safe-browsing <position> upl-rule
```

Команда для просмотра всех созданных правил веб-безопасности:

```
Admin@nodename# show security-policy safe-browsing
```

Команда для просмотра определенного правила веб-безопасности:

```
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")
```

Команда для удаления правила веб-безопасности:

```
Admin@nodename# delete security-policy safe-browsing <position>
```

Настройка правил инспектирования SSL

Правила инспектирования SSL создаются на уровне `security-policy ssl-inspection` с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила инспектирования SSL используется команда:

```
Admin@nodename# create security-policy ssl-inspection <position> upl-rule
```

Параметры правил инспектирования SSL.

Параметр	Описание
`OK` `PASS`	Действие правила инспектирования SSL: • `OK` — расшифровать; • `PASS` — не расшифровывать; • `OK ... forward` — расшифровать и переслать; `forward` указывается среди свойств правила. При настройке правила с действием «Расшифровать и переслать» необходимо указать профиль пересылки SSL. Подробнее о создании и настройке с использованием CLI профилей пересылки — 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")`

Параметр	Описание
`ssl_profile`	Профиль SSL; указывается: `ssl_profile("Default SSL profile")`. Подробнее о работе с профилями SSL через CLI — в разделе «Настройка профилей SSL»
`rule_log`	Запись в журнал информации о трафике при срабатывании правила: • `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, выдан недоверенным центром сертификации, срок действия сертификата истёк. Доступно в правилах с действием «Расшифровать»: • `block_invalid_cert(yes)` или `block_invalid_cert(true)` — включение блокировки; • `block_invalid_cert(no)` или `block_invalid_cert(false)` — отключение блокировки
`check_revoc_cert`	Проверка сертификата сайта в списке отозванных сертификатов (CRL) и блокирование доступа, если он там найден. Доступно в правилах с действием «Расшифровать»: • `check_revoc_cert(yes)` или `check_revoc_cert(true)` — включение проверки сертификата; • `check_revoc_cert(no)` или `check_revoc_cert(false)` — отключение проверки сертификата
`block_expired_cert`	Блокирование сертификатов с истёкшим сроком действия. Доступно в правилах с действием «Расшифровать»: • `block_expired_cert(yes)` или `block_expired_cert(true)` — включить блокировку сертификатов с истёкшим сроком действия; • `block_expired_cert(no)` или `block_expired_cert(false)` — отключить блокировку сертификатов с истёкшим сроком действия

Параметр	Описание
`block_self_signed_cert`	Блокировка 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 — 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 — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: `src.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов источника: `src.ip = lib.url()`; в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»

Параметр	Описание
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке
`dst.ip`	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: `dst.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: `dst.ip = lib.url()`; в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке
`service`	Тип сервиса: HTTPS, SMTPS или POP3S. Чтобы указать сервис: `service = "service name"`; для указания нескольких сервисов: `service = (service-name1, service-name2, ...)`
`category`	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: `category = lib.category()`; в скобках укажите название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки — 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 укажите название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки — в разделе «Настройка списков URL»

Параметр	Описание
`time`	Настройка расписания работы правила. Для установки расписания: `time = lib.time()`; в скобках укажите название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Команда для редактирования правил инспектирования SSL:

```
Admin@nodename# set security-policy ssl-inspection <position> upl-rule
```

Команда для просмотра параметров всех созданных правил инспектирования SSL:

```
Admin@nodename# show security-policy ssl-inspection
```

Команда для просмотра параметров определенного правила инспектирования SSL:

```
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")
```

Команда для удаления правила инспектирования SSL:

```
Admin@nodename# delete security-policy ssl-inspection <position>
```

Настройка правил ICAP

Правила ICAP создаются на уровне `security-policy icap-rules` с помощью синтаксиса UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила ICAP используется команда:

```
Admin@nodename# create security-policy icap-rules <position> upl-rule
```

Параметры правил ICAP.

Параметр	Описание
`PASS` `OK`	Действие правила ICAP: • `PASS` — пропустить. Не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • `OK` — переслать. Ппереслать 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`	

Параметр	Описание
	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, на которые устройство UserGate будет пересылать запросы; указывается в формате: `profile("Example ICAP server")`. О настройке профилей серверов ICAP через CLI — 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 — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов или доменов источника. Для списка IP-адресов: `src.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов источника: `src.ip = lib.url()`; в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке
`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 — 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.ip`	Добавление списков IP-адресов или доменов назначения. Для списка IP-адресов: `dst.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: `dst.ip = lib.url()`; в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`dst.geoip`	Указание GeoIP назначения; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке
`response.header.Content-Type`	Списки типов контента, к которым будут применяться правила. Для задания списка: `response.header.Content-Type = lib.mime()`; в скобках укажите название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — 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 укажите название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки — в разделе «Настройка категорий URL». Для указания категории URL: `category = "URL category name"`

Параметр	Описание
`url`	Списки URL, для которых будет применяться правило. Для указания списка URL: `url = lib.url()`; в скобках укажите название списка URL. Подробнее о создании и настройке списков URL — 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, ...)`

Команда для редактирования правила ICAP:

```
Admin@nodename# set security-policy icap-rules <position> upl-rule
```

Команда для просмотра параметров всех созданных правил ICAP:

```
Admin@nodename# show security-policy icap-rules
```

Команда 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")
```

Команда для удаления правила ICAP:

```
Admin@nodename# delete security-policy icap-rules <position>
```

Настройка ICAP-серверов

Профили ICAP-серверов настраиваются на уровне `security-policy icap-server`.

Для создания профиля ICAP-сервера используется команда:

```
Admin@nodename# create security-policy icap-server <parameter>
```

Параметры ICAP-сервера.

Параметр	Описание
`name`	Имя ICAP-сервера
`description`	Описание ICAP-сервера
`ip`	IP-адрес ICAP-сервера
`port`	TCP-порт ICAP-сервера; значение по умолчанию: 1344
`max-msg-size`	Максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу

Параметр	Описание
`check-icap`	Период проверки доступности сервера ICAP
`bypass`	Если эта опция включена, то устройство 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; • `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

Команда для обновления существующего профиля ICAP-сервера:

```
Admin@nodename# set security-policy icap-server <server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового профиля ICAP-сервера.

Команда для отображения информации о профиле ICAP-сервера:

```
Admin@nodename# show security-policy icap-server <server-name>
```

Команда для удаления профиля ICAP-сервера:

```
Admin@nodename# delete security-policy icap-server <server-name>
```

НАСТРОЙКА ГЛОБАЛЬНОГО ПОРТАЛА

Настройка веб-портала

Веб-портал настраивается на уровне `global-portal web-portal` с помощью синтаксиса UPL Подробнее о структуре команд — в разделе «UserGate Policy Language».

Команда для создания страницы веб-портала:

```
Admin@nodename# create global-portal web-portal <position> upl-rule
<parameters>
```

Параметры настройки закладок веб-портала.

Параметр	Описание
OK	Действие для создания правила с помощью UPL

Параметр	Описание
`enabled`	Включение или отключение правила: • `enabled(yes)` или `enabled(true)`; • `enabled(no)` или enabled(false)
`name`	Название закладки. Например: `name("Example of bookmark publishing")`
`desc`	Описание закладки. Например: `desc("Example of bookmark publishing configured in CLI")`
`url`	URL ресурса, который необходимо опубликовать через веб-портал. Необходимо указывать полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. URL указывается как `url = "http://www.example.com"`
`url.domain`	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу минуя веб-портал, подключаясь к указанному домену. Для указания домена прямого доступа: `url.domain = "example.com"`
`rdp_check_session_alive`	Разрыв сессии RDP по завершению авторизации на веб-портале: • `rdp_check_session_alive(yes)` или `rdp_check_session_alive(true)` — разрывать сессию; • `rdp_check_session_alive(no)` или `rdp_check_session_alive(false)` — не разрывать сессию
`ssl_profile`	Профиль SSL для построения защищенного канала для отображения веб-портала; указывается: `ssl_profile("SSL profile example")`
`certificate`	Сертификат, который будет использоваться для создания HTTPS-соединения. Чтобы задать сертификат: `certificate ("Certificate example")`
`icon`	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку.

Параметр	Описание
	Можно указать: • `icon("Default icon name")` — использовать штатную иконку (в скобках указывается название штатной иконки); • `icon("Icon encoded with Base64")` — использовать свою иконку. Необходимо указать содержимое файла, кодированное с использованием Base64; • `icon("http://www.icon-url-example.com")` — указать URL для использования сторонней иконки
`additional_url`	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Для указания: `additional_url("http://additional-url-example.com")`

`user`	Пользователи и группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL.
	Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора»).
	Примеры добавления пользователей в правило:
	`user = known`
	`user = "user"`
	`user = "testd.local\\user1"`
	`user = ("user", "testd.local\\user1")`

Команда для редактирования правила веб-портала:

```
Admin@nodename# set global-portal web-portal <position> upl-rule
<parameters>
```

Команда для просмотра параметров правил веб-портала:

```
Admin@nodename# show global-portal web-portal <position>
```

Пример создания правила веб-портала с использованием UPL:

```
Admin@nodename# create global-portal web-portal 1 upl-rule OK \
...user = "CN=Default Group,DC=LOCAL" \
...url = "http://www.intranet.loc" \
...name("Test web portal") \
...desc("Test web portal description") \
...enabled(true)
...
Admin@nodename# show global-portal web-portal 1
% ---------------- 1 ----------------
OK \
    user = "CN=Default Group,DC=LOCAL" \
    url = "http://www.intranet.loc" \
    icon("default.svg") \
    desc("Test web portal description") \
    enabled(true) \
    id("2fead5a1-29c3-4835-bbdb-1d0e07f84c28") \
    name("Test web portal")
```

Команда для уаления правила веб-портала:

```
Admin@nodename# delete global-portal web-portal <position>
```

Настройка правил reverse-прокси

Правила reverse-прокси настраиваются на уровне `global-portal reverse-proxy-rules` с помощью синтаксиса UPL Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания правила reverse-прокси используется команда:

```
Admin@nodename# create global-portal reverse-proxy-rules <position>
upl-rule <parameters>
```

Параметры настройки правил reverse-прокси.

Параметр	Описание
`OK`	Действие для создания правила с помощью UPL
`enabled`	Включение или 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, на который UserGate SWG будет пересылать запросы. Для указания сервера reverse-прокси: `profile("Reverse proxy server example")`
`url.port`	Порт, на котором узел UserGate SWG будет слушать входящие запросы, например, `url.port = 80`
`is_https`	Поддержка HTTPS: • `is_https(yes)` или `is_https(true)` — использовать HTTPS; • `is_https(no)` или `is_https(false)` — не использовать HTTPS
`ssl_profile`	Профиль SSL; указывается при использовании HTTPS: `ssl_profile("Default SSL profile")`. Подробнее о работе с профилями SSL через CLI — в разделе «Настройка профилей SSL»
`certificate`	Сертификат, используемый для поддержки HTTPS-соединения. Указывается при использовании HTTPS: `certificate("Certificate example")`

Параметр	Описание
`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 — в разделе «Зоны»
`src.ip`	Добавление списков IP-адресов или доменов источника. Для списка IP-адресов: `src.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов источника: `src.ip = lib.url()`; в скобках укажите название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
`src.geoip`	Указание GeoIP источника; необходимо указать код страны (например, `src.geoip = RU`). Коды названий стран доступны по ссылке ISO 3166-1

Параметр	Описание
`user`	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора»). Примеры добавления 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 устройства UserGate, доступный из сети интернет, куда адресован трафик внешних клиентов. Для списка IP-адресов: `dst.ip = lib.network()`; в скобках укажите название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для списка доменов назначения: `dst.ip = lib.url()`; в скобках укажите название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — 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
`request.header.User-Agent`	User agent пользовательских браузеров, для которых будет применено данное правило. Для указания User agent пользовательских браузеров: `request.header.User-Agent = lib.useragent()`; в скобках необходимо указать название категории User agent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Usera gent браузеров

Параметр	Описание
`rewrite_path`	Подмена домена 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 укажите: `rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2")`
`trusted_browser`	Проверка подлинности браузера для предоставления доступа к ресурсам. Укажите созданное ранее подключение к серверу регистрации доверенных браузеров. Например: `trusted_browser = "111"`. Подробнее о работе с доверенными браузерами — в разделе «Работа с доверенными браузерами»
`proxy_pass_x_forwarded`	Добавление или перезапись следующих дополнительных HTTP-заголовков: • `X-Forwarded-Host`: содержит значение заголовка Host из исходного запроса. Это значение требуется внутреннему веб-серверу для уточнения, какой контент следует вернуть клиенту, а также при журналировании и балансировке нагрузки. • `X-Forwarded-Proto`: содержит сведения о протоколе исходного запроса, которые позволяют на стороне внутреннего веб-сервера выполнять переадресацию на безопасный ресурс либо генерировать корректные ссылки. • `X-Forwarded-Port`: передает исходный порт подключения клиента, который необходим для генерации корректных ссылок на стороне внутреннего веб-сервера. Например: `proxy_pass_x_forwarded(proto, host, port)`. Подробнее о работе с дополнительными HTTP-заголовками — в разделе «Публикация ресурсов с помощью правил reverse-прокси»

Команда для редактирования правила reverse-прокси:

```
Admin@nodename# set global-portal reverse-proxy-rules <position> upl-rule <parameters>
```

Команда для просмотра параметров правила reverse-прокси:

```
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")
```

Команда для удаления правила reverse-прокси:

```
Admin@nodename# delete global-portal reverse-proxy-rules <position>
```

Настройка серверов reverse-прокси

Серверы reverse-прокси настраиваются на уровне `global-portal reverse-proxy-servers`.

Для создания сервера reverse-прокси используется команда:

```
Admin@nodename# create global-portal reverse-proxy-servers <parameter>
```

Параметры сервера reverse-прокси.

Параметр	Описание
`name`	Название сервера reverse-прокси
`description`	Описание сервера reverse-прокси
`address`	Адрес или домен публикуемого сервера
`port`	TCP-порт публикуемого сервера
`https`	Использование протокола HTTPS до публикуемого сервера: • `on` — использовать; • `off` — не использовать
`keep-source-ip`	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: • `on` — оставить оригинальный IP-адрес источника; • `off` — заменить IP-адрес источника на IP-адрес UserGate. **Важно!** **Если в пакетах сохраняется оригинальный IP-адрес источника, для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UserGate SWG, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UserGate SWG или можно настроить статические маршруты через UserGate SWG для «белых» IP-адресов источников**

Команда для редактирования параметров сервера reverse-прокси:

```
Admin@nodename# set global-portal reverse-proxy-servers <server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера reverse-прокси.

Команда для отображения информации о сервера reverse-прокси:

```
Admin@nodename# show global-portal reverse-proxy-servers <server-name>
```

Команда для удаления сервера reverse-прокси:

```
Admin@nodename# delete global-portal reverse-proxy-servers <server-
name>
```

НАСТРОЙКА БИБЛИОТЕК

Настройка библиотек (Описание)

Настройка морфологии

Списки морфологии создаются на уровне `libraries morphology`.

Для создания списка морфологии используется следующая команда:

```
Admin@nodename# create libraries morphology <parameter>
```

Параметры списка морфологии.

Параметр	Описание
`name`	Название списка морфологии
`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, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`words`	Слова и фразы, которые необходимо добавить в список. • `word` — слова и фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. • `weight` — вес слова или фразы. Если вес не задан, то автоматический устанавливается значение 100. Для добавления слов и фраз:

Параметр	Описание
	`Admin@nodename# create libraries morphology ... words new word "word or phrase" weight <weight>`

Команда для редактирования списка:

```
Admin@nodename# set libraries morphology <morphology-list-name>
<parameter>
```

Далее указываются параметры, значения которых необходимо обновить (список параметров представлен в таблице выше).

Команда для добавления в список новых слов или фраз:

```
Admin@nodename# set libraries morphology <morphology-list-name> words
new word "word or phrase" weight <weight>
```

Команда для замены слова 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>
```

Команды для удаления всего морфологического списка или отдельных слов, содержащихся в нем:

```
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 определенном списке, далее необходимо указать название интересующего морфологического списка.

Команда для просмотра содержания определенного морфологического списка:

```
Admin@nodename# show libraries morphology <morphology-list-name> words
```

Настройка IP-адресов

IP-списки создаются на уровне `libraries ip-list`.

Для создания группы IP-адресов используется команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Параметры IP-списка.

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, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>.

Параметр	Описание
	Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`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>`

Команда для редактирования списка:

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Команда для добавления в список новых адресов:

```
Admin@nodename# set libraries ip-list <ip-list-name> ips [ <ip1>
<ip2> ... ]
```

Команды для удаления всего списка адресов или IP-адресов, содержащихся в нем:

```
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
```

Команда для отображения информации об определенном списке:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Команда для просмотра содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка User agent браузеров

Списки user agent браузеров создаются на уровне

```
libraries useragents
```

.

Для создания нового списка используется команда:

```
Admin@nodename# create libraries useragents <parameter>
```

Параметры списка user agent браузеров.

Параметр	Описание
`name`	Название списка user agent
`description`	Описание списка
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений.

Параметр	Описание
	• Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`patterns`	Шаблоны User agent. Список User agent браузеров доступен по ссылке

Команда 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 User agent браузеров:

```
 Admin@nodename# set libraries useragents <useragent-list-name>
[ <useragent1> <useragent2> ... ]
```

Команды для удаления всего списка или отдельных User agent браузеров, содержащихся в нем:

```
Admin@nodename# delete libraries useragents <useragent-list-name>
Admin@nodename# delete libraries useragents <useragent-list-name>
patterns [ <useragent> ... ]
```

Команда для отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries useragents
```

Команда для отображения информации об определенном списке. Чтобы просмотреть содержание списка Useragent браузеров:

```
 Admin@nodename# show libraries useragents <useragent-list-name>
patterns
```

Настройка типов контента

Списки типов контента создаются на уровне `libraries content-types`.

Для создания нового списка типов контента используется команда:

```
Admin@nodename# create libraries content-types <parameter>
```

Параметры списка типов контента.

Параметр	Описание
`name`	Название списка типов контента
`description`	Описание списка
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`mime`	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке

Команда для редактирования списка:

```
 Admin@nodename# set libraries content-types <content-types-list-name>
<parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команда для удаления списка с типами контента:

```
Admin@nodename# delete libraries content-types <content-types-list-name>
```

Команда для удаления отдельных типов контента из списка:

```
Admin@nodename# delete libraries content-types <content-types-list-name> mime [ <mime-type> ... ]
```

Команды для отображения информации о списках типов контента:

```
Admin@nodename# show libraries content-types
Admin@nodename# show libraries content-types <content-types-list-name>
```

Команда для отображения типов контента, содержащихся в списке:

```
Admin@nodename# show libraries content-types <content-types-list-name> mime
```

Настройка списков URL

Списки URL создаются на уровне `libraries url-list`.

Для добавления нового списка URL используется команда:

```
Admin@nodename# create libraries url-list <parameter>
```

Параметры списка URL.

Параметр	Описание
`name`	Название списка URL

Параметр	Описание
`description`	Описание списка URL
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`urls`	URL, которые необходимо добавить в список
`case-sensitivity`	Чувствительность к регистру в написании адреса URL: • sensitive — чувствительно к регистру букв в адресе; • insensitive — нечувствительно к регистру букв в адресе; • domain — список адресов доменов

Команда для редактирования списка URL:

```
Admin@nodename# set libraries url-list <url-list-name> <parameter>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Команды для удаления 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> ... ]
```

Команды для просмотра информации о всех списках URL, об определенном списке URL или об адресах, входящих в определенный список:

```
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

Календари настраиваются на уровне `libraries time-sets`.

Для создания календаря используется команда:

```
Admin@nodename# create libraries time-sets <parameter>
```

Параметры календаря.

Параметр	Описание
`name`	Название календаря
`description`	Описание календаря
`time-set`	Временные интервалы. • `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.

Параметр	Описание
	◦ `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; ■ `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).

Команда для редактирования календаря:

```
Admin@nodename# set libraries time-sets <time-sets-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команда 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.

Команда для добавления 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 для удаления элемента календаря:

```
Admin@nodename# delete libraries time-sets <time-sets-name> <time-set-
type> ( <time-set-filter> )
```

Команда для отображения информации о всех календарях:

```
Admin@nodename# show libraries time-sets
```

Команда для отображения информации об определенном календаре:

```
Admin@nodename# show libraries time-sets <time-sets-name>
```

Команда 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

Полосы пропускания настраиваются на уровне `libraries bandwidth-pools`.

Для добавления новой полосы пропускания используется команда:

```
Admin@nodename# create libraries bandwidth-pools <parameter>
```

Параметры полосы пропускания.

Параметр	Описание
`name`	Название полосы пропускания
`description`	Описание полосы пропускания
`rate`	Скорость передачи данных; указывается в Кбит/с
`dscp`	Значение DSCP для QoS (при указании будет прописываться в каждый IP-пакет: принимает значения от 0 до 63)

Команда 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.

Команда для удаления полосы пропускания:

```
Admin@nodename# delete libraries bandwidth-pools <bandwidth-name>
```

Команда для отображения информации о всех полосах пропускания:

```
Admin@nodename# show libraries bandwidth-pools
```

Команда для отображения информации об определенной полосе:

```
Admin@nodename# show libraries bandwidth-pools <bandwidth-name>
```

Настройка шаблонов страниц

Шаблоны страниц настраиваются на уровне `libraries response-pages`.

Доступно создание следующих типов шаблонов страниц (<`response-page-type`>):

- `blockpage` — шаблоны страниц блокировки;
- `captiveportal-user-auth` — шаблоны страниц авторизации captive-портала;
- `captiveportal-user-session` — шаблоны страниц captive-портала, сессия пользователя;
- `content-warning` — шаблоны страниц предупреждения;
- `ftp-client` — шаблоны страниц отображения FTP поверх HTTP;
- `proxy-portal` — шаблоны страниц веб-портала;
- `pp-login-ssh` — шаблоны страниц SSH-логина веб-портала;
- `pp-login-rdp` — шаблоны страниц RDP-логина веб-портала;
- `totp-init-page` — шаблоны страниц инициализации TOTP;
- `network-error-page` — шаблоны страниц сетевых ошибок от прокси-сервера.

Для создания шаблона страницы используется команда:

```
Admin@nodename# create libraries response-pages <response-page-type>
<parameter>
```

Параметры шаблона страниц.

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; • `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

Параметр	Описание
	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 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-address>/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-address>/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;

Параметр	Описание
	• `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; • `pp-login-ssh-ru` — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. Базовые шаблоны для страницы RDP-логина веб-портала (`pp-login-rdp`): • `pp-login-rdp-en` — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал; • `pp-login-rdp-ru` — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. Базовые шаблоны для страницы инициализации TOTP (`totp-init-page`): • `totp-init-page-en` — шаблон на английском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей; • `totp-init-page-ru` — шаблон на русском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей.

Параметр	Описание
	Базовые шаблоны для страницы сетевых ошибок от прокси-сервера (`network-error-page`): • `network-error-page-en` — шаблон на английском языке для отображения страницы сетевых ошибок от прокси-сервера; • `network-error-page-ru` — шаблон на русском языке для отображения страницы сетевых ошибок от прокси-сервера
`default`	Использовать шаблон по умолчанию: • `on`; • `off`

Команда 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.

Команда для удаления шаблона страницы:

```
Admin@nodename# delete libraries response-pages <response-page-type>
<response-page-name>
```

Команда для просмотра информации о всех имеющихся шаблонах страниц:

```
Admin@nodename# show libraries response-pages
```

Команда для просмотра информации об отдельном типе шаблонов страниц:

```
Admin@nodename# show libraries response-pages <response-page-type>
```

Команда для просмотра информации об отдельном шаблоне страницы:

```
Admin@nodename# show libraries response-pages type <response-page-type> <response-page-name>
```

Настройка категорий URL

Списки категорий URL настраиваются на уровне `libraries url-categories`.

Для создания списка категорий URL используется команда:

```
Admin@nodename# create libraries url-categories <parameter>
```

Параметры списка категорий URL.

Параметр	Описание
`name`	Название списка URL-категорий
`description`	Описание списка
`categories`	Категории URL, которые необходимо добавить в список

Команда для редактирования параметров списка:

```
Admin@nodename# set libraries url-categories <list-name> <parameter>
```

Команда для добавления категорий URL в существующий список:

```
Admin@nodename# set libraries url-categories <list-name> categories [ <url-category> ... ]
```

Команда для удаления списка URL-категорий:

```
Admin@nodename# delete libraries url-categories <list-name>
```

Команда для удаления отдельных категорий из списка:

```
Admin@nodename# delete libraries url-categories <list-name> categories
[ <url-category> ... ]
```

Команда для просмотра информации о всех списках URL-категорий:

```
Admin@nodename# show libraries url-categories
```

Команда для просмотра информации об определенном списке:

```
Admin@nodename# show libraries url-categories <list-name>
```

Команда для отображения категорий URL, входящих в список:

```
Admin@nodename# show libraries url-categories <list-name> categories
```

Настройка измененных категорий URL

Настройка измененных категорий URL выполняется на уровне `overridden-url-categories`.

Для добавления новой измененной категории URL используется команда:

```
Admin@nodename# create libraries overridden-url-categories <parameter>
```

Параметры измененной категории URL.

Параметр	Описание
`domain`	Доменное имя ресурса
`description`	Описание изменяемого домена
`categories`	Новые категории сайта (можно указать не более 2-х категорий)

Команда для редактирования параметров:

```
Admin@nodename# set libraries overridden-url-categories <domain>
<parameter>
```

Команда для удаления сайта с измененными категориями:

```
Admin@nodename# delete libraries overridden-url-categories <domain>
```

Команда для отображения всего списка сайтов с измененными категориями:

```
Admin@nodename# show libraries overridden-url-categories
```

Команда для отображения информации об определенном сайте с измененными категориями URL:

```
Admin@nodename# show libraries overridden-url-categories <domain>
```

Настройка почтовых адресов

Списки почтовых адресов настраиваются на уровне `libraries email-list`.

Для создания списка почтовых адресов используется команда:

```
Admin@nodename# create libraries email-list <parameter>
```

Параметры списка почтовых адресов.

Параметр	Описание
`name`	Название списка почтовых адресов
`description`	Описание списка почтовых адресов
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, необходимо указать адрес, с которого загружаются обновления (`url`).

Параметр	Описание
	Периодичность обновления списка указывается параметром `shedule` в формате crontab. Crontab-формат: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`emails`	Почтовые адреса, которые необходимо добавить в список

Команда для редактирования информации осписке почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Команды для удаления списка или почтовых адресов из него:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails
[ <email> ... ]
```

Команды для просмотра информации о всех созданных списках, об определенных списках или для просмотра почтовых адресов, входящих в список:

```
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

Списки номеров телефонов настраиваются на уровне `libraries phone-list`.

Для создания списка телефонных номеров используется команда:

```
Admin@nodename# create libraries phone-list <parameter>
```

Параметры списка телефонных номеров.

Параметр	Описание
`name`	Название списка телефонных номеров
`description`	Описание списка телефонных номеров
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, 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> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
`phones`	Номера телефонов, которые необходимо добавить в список

Команда для редактирования информации о списке телефонных номеров:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команды для удаления списка или номеров телефонов из него:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones
[ <phone> ... ]
```

Команды для просмотра информации о всех созданных списках:

```
Admin@nodename# show libraries phone-list
```

Команда для просмотра информации об определенных списках телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Команда для просмотра номеров, содержащихся в списке:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне `libraries notification-profiles`.

Для добавления нового профиля оповещения SMTP используется команда:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Параметры профиля оповещения SMTP.

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

Параметр	Описание
	использованием SSL — 465. Уточните данное значение у администратора почтового сервера
`connection-security`	Варианты безопасности отправки почты; возможны варианты: • `none`; • `starttls`; • `ssl`
`authentication`	Включение/отключение авторизации при подключении к серверу SMTP: • `on`; • `off`
`login`	Имя учетной записи для подключения к SMTP-серверу
`password`	Пароль учетной записи для подключения к SMTP-серверу

Для создания профиля оповещения по SMS (SMPP) используется команда:

```
 Admin@nodename# create libraries notification-profiles smpp
<parameter>
```

Параметры профиля оповещения SMPP.

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

Параметр	Описание
`ssl`	Включение или отключение шифрования SSL: • `on`; • off
`login`	Имя учетной записи для подключения к SMPP-серверу
`password`	Пароль учетной 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: `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 (Сокращенный)
`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 (Сокращенный)
`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);

Параметр	Описание
	• 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`	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)

Команда для редактирования профиля оповещения:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp>
<profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Команда для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp>
<profile-name>
```

Команда для удаления правил трансляции номеров в профиле SMPP:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1¦phone2 ]
```

Команда для отображения информации обо всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

Команда для отображения информации обо всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

Команда для отображения информации об определенном профиле оповещения:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка профилей LLDP

Профили LLDP (Link Layer Discovery Protocol) настраиваются на уровне `libraries lldp-profiles`.

Для создания профиля LLDP используется команда:

```
Admin@nodename# create libraries lldp-profiles <parameter>
```

Параметры профиля LLDP.

Параметр	Описание
`name`	Название профиля LLDP
`description`	Описание профиля
`port-status`	

Параметр	Описание
	Режимы: • `rx` — только прием данных LLDP. UserGate SWG не будет отправлять информацию LLDP, но будет анализировать информацию LLDP от соседей. • `tx` — только передача данных LLDP. UserGate SWG будет отправлять информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей. • `rx-tx` — прием и передача данных LLDP. UserGate SWG будет отправлять информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.

Команда для редактирования информации о профиле:

```
Admin@nodename# set libraries lldp-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Команда для удаления профиля LLDP:

```
Admin@nodename# delete libraries lldp-profiles <profile-name>
```

Команды для отображения информации о профилях:

```
Admin@nodename# show libraries lldp-profiles
Admin@nodename# show libraries lldp-profiles <profile-name>
```

Настройка профилей SSL

Профили SSL настраиваются на уровне `libraries ssl-profiles`.

Для создания профиля SSL используется команда:

```
Admin@nodename# create libraries ssl-profiles <parameter>
```

Параметры профиля SSL.

Параметр	Описание
`name`	Название профиля SSL
`description`	Описание профиля
`min-tls-version`	Минимальная версия TLS, которая может быть использована в профиле: • `tls1`; • `tls1.1`; • `tls1.2`
`max-tls-version`	Максимальная версия TLS, которая может быть использована в 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`

Команда для редактирования информации о профиле:

```
Admin@nodename# set libraries ssl-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Команды для удаления профиля SSL полностью или для удаления отдельных алгоритмов шифрования и цифровой подписи:

```
Admin@nodename# delete libraries ssl-profiles <profile-name>
Admin@nodename# delete libraries ssl-profiles <profile-name> ssl-
ciphers [ cipher ... ]
```

Команда для отображения информации о профилях SSL:

```
Admin@nodename# show libraries ssl-profiles
Admin@nodename# show libraries ssl-profiles <profile-name>
```

Настройка профилей пересылки SSL

Профили пересылки SSL настраиваются на уровне `libraries ssl-forwarding-profiles`.

Для создания профиля пересылки используется команда:

```
Admin@nodename# create libraries ssl-forwarding-profiles <parameter>
```

Параметры профилей пересылки SSL.

Параметр	Описание
`name`	Название профиля пересылки SSL
`description`	Описание профиля пересылки

Параметр	Описание
`type`	Тип пересылки: • `l2` — при настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • `l3` — копия расшифрованного трафика передается 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 устройства 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)

Команда для редактирования параметров профилей пересылки:

```
 Admin@nodename# set libraries ssl-forwarding-profiles <profile-name>
<parameter>
```

Команда для удаления профиля:

```
 Admin@nodename# delete libraries ssl-forwarding-profiles <profile-
name>
```

Команды для отображения информации о всех имеющихся профилях или об определенном профиле пересылки:

```
Admin@nodename# show libraries ssl-forwarding-profiles
Admin@nodename# show libraries ssl-forwarding-profiles <profile-name>
```

Настройка профилей BFD

Профили BFD настраиваются на уровне `libraries bfd-profile`.

Для создания профиля BFD используется команда:

```
Admin@nodename# create libraries bfd-profile
```

Параметры профиля BFD.

Параметр	Описание
`name`	Название профиля BFD
`description`	Описание профиля
`detect-multiplier`	Множитель времени обнаружения; влияет на время обнаружения неисправностей соединения
`receive-interval`	Интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами); указывается в миллисекундах
`transmit-interval`	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами; указывается в миллисекундах
`echo-receive-interval`	Минимальный интервал, через который данная система способна принимать echo-пакеты; указывается в миллисекундах
`echo-transmit-interval`	Минимальный интервал, через который система будет способна отправлять echo-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

Команда для обновления параметров профиля BFD:

```
Admin@nodename# set libraries bfd-profile <profile-name> <parameter>
```

Команда для удаления профиля:

```
Admin@nodename# delete libraries bfd-profile <profile-name>
```

Команды для отображения информации обо всех имеющихся профилях или об определенном профиле BFD:

```
Admin@nodename# show libraries bfd-profile
Admin@nodename# show libraries bfd-profile <profile-name>
```

Настройка Syslog-фильтров UserID-агента

Syslog-фильтры UserID-агента настраиваются на уровне `libraries syslog-filters`.

Для создания syslog-фильтра используется команда:

```
Admin@nodename# create libraries syslog-filters <parameters>
```

Параметры syslog-фильтра.

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

Команда 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.

Команда для отображения информации о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Команда для удаления syslog-фильтра:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка сценариев

Сценарии настраиваются на уровне `libraries scenarios` с использованием синтаксиса UPL. Подробнее о написании правил с помощью UserGate Policy Language — в разделе «Типы правил»).

Для задания условий сценариев и их объединения используются определения (`definitions`). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слеша (как при использовании многострочного ввода).

Для создания или изменения условий сценариев используется функция `def scenario_cond`, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
<scenario_conditions>
end
```

После указания условий указываются общие свойства сценария.

Наименование	Описание
OK	Действие для создания сценария

Наименование	Описание
`scenario_cond`	Пользовательское имя определения, содержащего список условий сценария: `scenario_cond = condition_example`
`enabled`	Включение или отключение использования сценария: • `enabled(true)`; • `enabled(false)`
`name`	Имя сценария: `name("Example scenario name")`
`desc`	Описание сценария: `desc("Description for scenario created as an example")`
`trigger`	Применение: • `trigger(one_user)` — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; • `trigger(all_users)` — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила
`duration`	Задать период активности сценария; указывается в минутах
`operation_mode`	Задать режим активации сценария: • `operation_mode(all)` — сценарий сработает, если выполнятся все условия; • `operation_mode(any)` — сценарий сработает, если выполнится хотя бы одно из условий

ПримечаниеПри обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием «Объем трафика». Сценарий будет применен ко всем пользователям в течение минуты; ограничение объема трафика: 1 ГБ/день:

```
Admin@nodename# create libraries scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
```

```
... traffic_limit(1GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
...
```

Для изменения, например, объема трафика:

```
Admin@nodename# set libraries scenarios 3 upl-rule \
...def scenario_cond scenario_cond_test
...traffic_limit(2GB) \
...period(day) \
...scond_type(traffic)
...end
...OK \
...scenario_cond = scenario_cond_test
```

Типы условий, используемых при создании сценариев

Условие типа «Категория URL»

Параметры для создания или обновления условия типа «Категория URL».

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:

- `scond_type` — Тип условия: `scond_type(virus_detection)`.

Условие типа «Приложение»

Параметры для создания или редактирования условия типа «Приложение».

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 для условия «Типы контента».

Наименование	Описание
`scond_type`	Тип условия: `scond_type(mime_type)`
`response.header.Content-Type`	Тип контента: `response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST)`
`count_interval`	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): `count_interval()`
`max_event_count`	Количество срабатываний: `max_event_count()`

Условие типа «Объем трафика»

Параметры для условия «Объем трафика».

Наименование	Описание
`scond_type`	Тип условия: `scond_type(traffic)`
`traffic_limit`	Ограничение объема 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»

Параметры условия «Проверка состояния».

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 путем выполнения DNS-запроса или URL для метода HTTP GET: `url.domain = "example.ru"`
`gateway`	Название используемого шлюза: `gateway()`. **Важно!** **Шлюз должен быть предварительно создан**
`health_result`	Результат выполнения проверки: • `health_result(positive)` – положительный; • `health_result(negative)` – отрицательный
`health_request_timeout`	Тайм-аут подключения (в секундах): `health_request_timeout()`
`health_answer_timeout`	Время ожидания ответа на запрос HTTP GET (в секундах): `health_answer_timeout()`
`health_type_request`	Тип DNS-запроса: • `health_type_request(a)`; • `health_type_request(aaaa)`; • `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()`

Наименование	Описание
`max_event_count`	Количество срабатываний: `max_event_count()`

Настройка тегов

Теги настраиваются на уровне `libraries tags`.

Для создания тегов сипользуется команда:

```
Admin@nodename# create libraries tags <parameters>
```

Параметры тегов.

Параметр	Описание
`name`	Название тега
`description`	Описание тега
`color`	Выбор цветовой маркировки тега для отображения в веб-интерфейсе: • `no-color` (Значение по умолчанию); • `red`; • `orange`; • `yellow`; • `green`; • `aqua`; • `blue`; • `violet`; • `pink`; • `purple`; • `light-gray`; • `light-green`; • `light-blue`; • `black`; • `rose`; • `magenta`; • `wood`

Команда для редактирования информации о теге:

```
Admin@nodename# set libraries tags <tag-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании тега.

Команда для отображения информации о тэгах:

```
Admin@nodename# show libraries tags <tag-name>
```

Команда для удаления тега:

```
Admin@nodename# delete libraries tags <tag-name>
```

Примеры работы с тэгами в библиотеке:

```
Admin@nodename# create libraries tags name "Test tag 6" description
"Tag made with CLI" color magenta
Admin@nodename# show libraries tags

Test tag 6
    name           : Test tag 6
    description    : Tag made with CLI
    color          : magenta

Tag 5
    name           : Tag 5
    description    : Test tag #5
    color          : green

Tag 1
    name           : Tag 1
    description    : Test tag #1
    color          : no-color

Admin@nodename# show libraries tags "Test tag 6"
```

```
name           : Test tag 6
description    : Tag made with CLI
color          : magenta

Admin@nodename# set libraries tags "Test tag 6" description "Update tag
from cli"
Admin@nodename# show libraries tags "Test tag 6"

name           : Test tag 6
description    : Update tag from cli
color          : magenta

Admin@nodename# delete libraries tags "Test tag 6"
```

НАСТРОЙКА РАЗДЕЛА ЖУРНАЛЫ И ОТЧЕТЫ

Настройка экспорта журналов

Функция экспорта журналов позволяет выгружать информацию на внешние серверы для последующего анализа или обработки.

Для создания нового правила экспорта журналов используется команда:

```
Admin@nodename# create logs logs-export <parameters>
```

Параметры правила экспорта журналов.

Параметр	Описание
`enabled`	Включение или отключение правила: • on;

Параметр	Описание
	• `off`
`name`	Название правила
`description`	Описание правила
`server-type`	Тип сервера: • `ssh`; • `ftp`; • `syslog`. При выборе типа сервера доступны следующие дополнительные настройки: • `port` — порт сервера, на который следует отправлять данные. • `login` — имя учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • `password` — пароль учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • `path` — каталог на сервере для копирования файлов журналов (не применяется к методу отправки syslog). • `passive` — пассивный режим ftp. • `transport` — только для типа серверов syslog. TCP или UDP. • `protocol` — только для типа серверов syslog. RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. • `severity` — только для типа серверов syslog. Критичность. Возможны следующие значения: `alert`, `critical`, `error`, `warning`, `notice`, `info`. • `facility` — только для типа серверов syslog. Объект. Возможны следующие значения: `user-level`, `system-daemons`, `security-auth`, `log-audit`, `log-alert`, `local- (0-7)`. • `hostname` — только для типа серверов syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN). • `app-name` — только для типа серверов syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog

Параметр	Описание
`target`	IP-адрес или доменное имя сервера.
`logs`	Журналы для экспорта: • `dns` — журнал DNS; • `events` — журнал событий; • `webaccess` — журнал веб-доступа; • `traffic` — журнал трафика; • `userid` — журнал UserID. Для каждого журнала можно выбрать синтаксис выгрузки: • `cef`; • `cef-compact`; • `json`; • `cee-json`; • `off`.
`schedule`	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Crontab-формат: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set logs logs-export <log-export-rule-name>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил экспорта.

Команды для просмотра параметров созданных ранее правил экспорта:

```
Admin@nodename# show logs logs-export
Admin@nodename# show logs logs-export <log-export-rule-name>
```

Команда для удаления созданных ранее правил экспорта:

```
Admin@nodename# delete logs logs-export <log-export-rule-name>
```

Команда для настройки параметров разового экспорта журналов:

```
Admin@nodename# execute logs send-once <log-export-rule-name>
<parameters>
```

Параметр	Описание
`fresh`	Экспортировать свежие логи
`range`	Указать интервал для экспорта: • `start-export-range` — начало интервала в формате: 2022-12-31T23:59:59; • `end-export-range` — конец интервала в формате: 2022-12-31T23:59:59

Настройка отчетов

Настройка отчетов в интерфейсе командной строки выполняется в режиме конфигурации на уровне `reports`.

С помощью команд этого раздела можно просматривать имеющиеся на устройстве шаблоны отчетов, создавать и редактировать правила отчетов, просматривать ранее созданные отчеты.

Шаблоны отчетов

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией UserGate.

Для просмотра имеющихся шаблонов отчетов используется команда:

```
Admin@nodename# show reports report-templates
```

Правила отчетов

Правила отчетов задают параметры создаваемого отчета, а также расписание запуска отчетов и способы их доставки пользователям.

Для создания нового правила отчетов используется команда:

```
Admin@nodename# create reports report-rules <parameters>
```

Параметры правила отчетов.

Параметр	Описание
`enabled`	Включение/отключение правила: • `on`; • `off`
`name`	Название правила
`description`	Описание правила
`language`	Выбор языка создания отчета: • `ru`; • `en`
`time-range`	Диапазон времени в секундах, за который необходимо подготовить отчет
`format`	Выбор формата, в котором будет создан отчет: • `pdf`; • `html`
`query-limit`	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль

Параметр	Описание
`query-limit-by`	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование
`templates`	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон
`email-sender`	Отправитель письма с созданным отчетом
`email-recipients`	Список получателей письма с отчетом. Получатели должны быть добавлены в списки библиотеки «Почтовые адреса» (`email-list`)
`email-subject`	Тема письма с отчетом
`email-body`	Содержимое письма с отчетом
`smtp-profile`	Профиль SMTP, который будет использован для отправки отчетов.
`schedule`	Расписание для отправки отчетов. Crontab-формат: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set reports report-rules <report-rule-name>
<parameters>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил отчетов.

Команды для просмотра параметров созданных ранее правил отчетов:

```
Admin@nodename# show reports report-rules
Admin@nodename# show reports report-rules <report-rule-name>
```

Команда для удаления созданных ранее правил отчетов:

```
Admin@nodename# delete reports report-rules <report-rule-name>
```

Созданные отчеты

Для просмотра информации о созданных отчетах используется команда:

```
Admin@nodename# show reports generated-reports
Admin@nodename# show reports generated-reports <generated-report-name>
```

USERGATE POLICY LANGUAGE (UPL)

UserGate Policy Language (Описание)

UPL (UserGate Policy Language) — язык описания политик UserGate. Термин "политика" употребляется здесь в контексте конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента.

Правила настраиваются с использованием действий, условий и свойств.

Для каждого правила настраивается одно из действий. Действия — настройки, которые управляют обработкой транзакции (OK, WARNING, PASS, DENY, FORCE_PASS, FORCE_DENY). При настройке правил, в которых не предусмотрено указание действия (например, правила DNS, NAT и маршрутизации, пропускной способности и т.п.), необходимо указать действия PASS или OK.

Условия задаются знаками равно (=) или не равно (!=), например, зоны, адреса, GeoIP источников и назначения, сервисы, приложения и т.д.; все условия в правиле проверяются по логическому И, т.е. правило сработает, если будут выполнены все условия.

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

> **Примечание**
> **При настройке правил сначала указывается действие, потом условия и затем свойства.**

С помощью UPL в интерфейсе CLI создаются правила политик сети и безопасности для следующих разделов:

- Настройки DNS-прокси (уровень: `network dns dns-proxy dns-rules`).
- Captive-портал (уровень: `users captive-portal`).
- Межсетевой экрана (уровень: `network-policy firewall`).
- NAT и маршрутизация (уровень: `network-policy nat-routing`).
- Пропускная способность (уровень: `network-policy traffic-shaping`).
- Фильтрация контента (уровень: `security-policy content-filtering`).
- Веб-безопасность (уровень: `security-policy safe-browsing`).
- Инспектирование SSL (уровень: `security-policy ssl-inspection`).
- ICAP-правила (уровень: `security-policy icap-rules`).
- Веб-портал (уровень: `global-portal web-portal`).
- Правила reverse-прокси (уровень: `global-portal reverse-proxy-rules`).

Структура команды для создания правила:

```
Admin@nodename# create <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо создать правило.

<position> — позиция, на которую будет помещено правило.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для обновления существующего правила:

```
Admin@nodename# set <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо обновить правило.

<position> — номер правила, которое необходимо обновить.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для удаления правила:

```
Admin@nodename# delete <level> <position | all>
```

где <level> — уровень, на котором необходимо удалить правило.

<position> — номер правила, которое необходимо удалить.

<all> — удалить все правила.

Структура команды для отображения правила:

```
Admin@nodename# show <level> <position | all>
```

где <level> — раздел, правила которого нужно отобразить.

<position> — номер правила, которое необходимо отобразить.

<all> — отобразить все правила.

Пример создания правила межсетевого экрана с использованием UPL (использован многострочный ввод):

```
Admin@nodename# create network-policy firewall 1 upl-rule \
...DENY \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = known \
```

```
...service = HTTPS \
...time = lib.time("Working hours") \
...rule_log(session)\
...name("Example of firewall rule created in CLI") \
...enabled(true)
```

После создания правило 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.

В последующих статьях данного раздела можно найти более подробную информацию об общих положениях языка UPL, определениях, встроенных библиотеках, условиях, действиях, свойствах и типах правил.

Общие положения

Комментарии

Любая строка, начинающаяся с символа «**%**», является комментарием. Символ процента «%» после пробела или табуляции вводит комментарий, который продолжается до конца строки (кроме случаев, когда символ процента отображается внутри кавычек (""), как часть выражения).

Пример:

```
% Это комментарий
DENY("Too many Host headers") request.header.Host.count = 2..  % и это
тоже
```

Комментарии могут быть в любом месте файла с описанием политик.

Правила

Правило политики (rule) состоит из условий и некоторого количества действий, записанных в любом порядке. Есть также свойства (properties), которые

синтаксически выглядят как действие, но при этом активных действий не производят. Например, свойство `name` просто добавляет атрибут «имя» в правило.

Правила обычно пишутся в одной строке, но могут быть разбиты на строки с помощью специального символа — обратного слеша «`\`».

Когда правило выполняется, условие проверяется для текущей конкретной транзакции. Если условие оценивается как `True` (истина), выполняются все перечисленные действия и текущий слой заканчивается при наличии префиксов `PASS / FORCE_PASS / DENY / FORCE_DENY / WARNING / OK`. Если сработавшее правило не имеет префиксов `PASS / FORCE_PASS / DENY / FORCE_DENY / WARNING / OK`, то выполняются действия и дальше обрабатывается уже следующее правило. Если условие оценивается как `False` для этой транзакции, то дальше обрабатывается уже следующее правило.

Все условия в правиле проверяются по логическому «`И`». Другими словами, правило сработает, когда будут выполнены все условия.

В свою очередь, условие является логической комбинацией триггеров. Триггеры — это отдельные тесты, которые можно выполнить с компонентами запроса, ответа, связанными пользователями или состоянием системы.

Действия — это настройки, которые управляют обработкой транзакции. Например, запретить (*deny*) или обработать объект (изменить заголовок — *rewrite*).

Синтаксис:

```
Rule ::= (PASS | FORCE_PASS | DENY| ( DENY '(' string ')') |
FORCE_DENY | FORCE_DENY'(' string ') '| WARNING | OK)? Conditions
'\'? Actions

Conditions ::= condition '\'? Conditions

Actions ::= action '\'? Actions
```

Пример:

Запрос будет запрещен, когда сработают оба триггера:

- домен будет example.com
- время будет между 9 и 17 часами

```
DENY url.domain = "example.com" time=09:00..17:00
```

Слои

Слой (layer)— это конструкция UPL, используемая для группировки правил и принятия одного решения. Раздельные принятия решения помогают контролировать сложность политики. Это делается путем написания каждого решения в отдельном слое.

У любого правила в слое может быть префикс `PASS / FORCE_PASS / DENY / FORCE_DENY / OK / WARNING`, когда срабатывает правило с таким префиксом, все остальные правила в слое пропускаются.

В случае если сработало правило с префиксом `FORCE_PASS` или `FORCE_DENY`, то это является окончательным результатом обработки, в противном случае обработка переходит на следующий слой. После обработки всех слоев запрос будет заблокирован или пропущен в зависимости от того, что было последним — `PASS / FORCE_PASS` или `DENY / FORCE_DENY`. Если процессинг остановится на `WARNING`, будет добавлено предупреждение в тело ответа.

Префикс *OK* подразумевает остановку обработки правил в текущем слое при выполнении условий и действий (если таковые указаны). Если префикс отсутствует при выполнении условий и действий, то остановка не подразумевается.

Действия `FORCE_PASS` и `FORCE_DENY` похожи на `PASS` и `DENY`, за исключением того, что они могут быть переопределены на последующих слоях. `FORCE_DENY` и `FORCE_PASS` немедленно прекращают поверку правил как на текущем, так и на последующих слоях, и этот результат является окончательным.

Синтаксис:

```
Layer ::= '[' layer_type layer_name ']'

layer_type ::= ssl | captive| content | shaper | firewall |
safebrowsing | dns | icap | webportal | reverseproxy |
nat_routing | byod | scenarios | ipvs_server | icap_balancing |
reverseproxy_balancing

layer_name ::= string

atom ::= [a-z][0-9a-zA-Z_]+
```

`string ::= '"'` произвольная строка `'"'`

Пример 1:

```
[content "L1"]
DENY enabled(true) % по умолчанию все запрещено

[content "Devs"]
DENY group != Developers enabled(true)
%... дальше идут правила, которые будут применяться только для группы
Developers
```

Пример 2:

```
[content "Admin"]
FORCE_PASS group = Admins enabled(true)

[content "L2"]
DENY enabled(true) % по умолчанию все запрещено
```

Динамические значения

Значения «адрес запроса» (`url, url.host, url.path`), «IP-адрес источника/назначения» (`src.ip, dst.ip`), «имя пользователя» (`user`), «значения заголовков» (`request` и `response`) и «параметры запроса» (`qparam`) могут сравниваться между собой, а также использоваться в качестве аргумента в действиях (`actions`), где это предусмотрено.

Условия

Условие (condition) в языке UPL является логической комбинацией триггеров. Триггеры — это отдельные тесты, которые можно выполнить с компонентами запроса, ответа, связанными пользователями или состоянием системы. Все триггеры условия сравниваются со значениями с помощью операторов «=» и «!=». В роли значения могут выступать константные значения, такие как строки, целочисленные значения, диапазоны значений, динамические значения.

Синтаксис:

```
condition ::= condition_name   ('=' | '!=')  condition_value

condition_value ::= pattern | list

list ::= '(' ((pattern ',')* pattern)? ')'

pattern ::= word | string | integer | float | boolean| range |
condition_name

string ::= '"' произвольная строка '"'

word ::= [a-zA-Z][0-9a-zA-Z_\-]*

boolean ::= yes|no|true|false

range ::= integer .. [integer] | [integer] .. integer | float ..
[float] | [float] .. float

numeric :: = integer | range
```

http.connect

Проверка наличия *HTTP CONNECT*.

Синтаксис:

```
http.connect = yes | no | true | false
```

http.method

Проверка используемого HTTP-метода. Метод можно указывать как в кавычках, так и без.

Синтаксис:

```
http.method =   GET | CONNECT | DELETE | HEAD | POST | PUT |
TRACE | OPTIONS | TUNNEL | LINK | UNLINK | PATCH | PROPFIND |
PROPPATCH | MKCOL | COPY | MOVE | LOCK | UNLOCK | MKDIR | INDEX |
RMDIR | COPY | MOVE
```

http.request.version

Проверка версии HTTP-запроса.

Синтаксис:

```
http.request.version = 0.9 | 1.0 | 1.1
```

http.response.version

Проверка версии HTTP-ответа.

Синтаксис:

```
http.response.version = 0.9 | 1.0 | 1.1
```

http.response.code

Проверка HTTP-кода ответа. Валидные значения: 100 - 999.

Синтаксис:

```
http.response.code = NNN  %(где NNN число от 100 до 999)
```

http.request.body, http.request.body.nocase, http.response.body и http.response.body.nocase

Проверка тела запроса/ответа HTTP на содержание определенной сигнатуры.

Пример:

```
DENY http.response.body.nocase = "<title>index of" http.response.body =
">"
```

category

Проверка домена на принадлежность к определенной категории сайтов (список определенных в системе категорий смотрите в статье Категории URL). Категорию можно указать как по имени, так и по ее идентификатору. Если имя категории содержит пробелы или спецсимволы, ее необходимо указывать в кавычках.

Синтаксис:

```
category = word | string | integer | list | lib

lib ::= lib.category '(' list_libs ')'
```

```
list_libs :: = lib_name ',' list_libs

lib_name ::= word | string
```

Пример:

Запретить категории *Job Search* и *Gambling:*

```
DENY category = ("Job Search", Gambling)
```

Запретить все категории из библиотеки *Restricted cats:*

```
DENY category = lib.category("Restricted cats")
```

morphology

Проверка тела ответа морфологическими словарями.

Синтаксис:

```
morphology = word | string | list | lib

lib ::= lib.morphology '(' list_libs ')'

list_libs :: = lib_name ',' list_libs

lib_name ::= word | string
```

Пример:

Запретить контент, если сработает категория морфологии из словаря *BadWords:*

```
DENY morphology = BadWords
```

Запретить морфологические категории из библиотек **Special Words**, **BadWords**

```
DENY morphology = ("Special Words", BadWords)
DENY morphology = lib.morphology("Special Words", BadWords) %
аналогично предыдущему правилу
```

request.header.<h_name> и response.header.<h_name>

Проверка HTTP-заголовка запроса/ответа. `h_name` может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>[.base64][.nocase] = string
```

Пример:

```
DENY url="http://usergate.com" request.header.Pragma="no-cache"

PASS request.header.User-Agent = lib.useragent("Browsers")
PASS request.header.Content-Type = lib.mime("Applications")
DENY request.header.Connection.substring = "Upgrade"
```

request.header.<h_name>.substring и response.header.<h_name>.substring

Проверка HTTP-заголовка запроса/ответа на вхождение подстроки. `h_name` может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>[.base64]substring[.nocase] = string
```

Пример:

```
DENY request.header.User-Agent.substring = "curl/"
```

request.header.<h_name>.regex и response.header.<h_name>.regex

Проверка HTTP-заголовка запроса/ответа на регулярное выражение PCRE. `h_name` может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>[.base64].regex = string
```

Пример:

```
DENY("Accept only digits in content length") request.header.Content-
Length.regex != "[0-9]*"
```

request.header.<h_name>.re2 и response.header.<h_name>.re2

Проверка HTTP-заголовка запроса/ответа на регулярное выражение RE2. `h_name` может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>[.base64].re2 = string
```

Пример:

```
DENY("Accept only digits in content length") request.header.Content-
Length.re3 != "[0-9]*"
```

request.header.<h_name>.count и response.header.<h_name>.count

Проверка количества заголовков <`h_name`> в HTTP-запросе/ответе. `h_name` может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>.count = integer | range
```

Пример:

```
DENY("Too many Host headers") request.header.Host.count = 2..
```

request.header.<h_name>.length и response.header.<h_name>.length

Проверка длины значений всех заголовков <h_name> в HTTP-запросе/ответе. h_name может принимать одно из поддерживаемых значений (смотрите статью Список поддерживаемых HTTP-заголовков).

Синтаксис:

```
request.header.<h_name>.length = integer | range
```

Пример:

```
DENY("Too much Cookie data") request.header.Cookie.length = 2048..
```

request.header_names, request.header_values, response.header_values и response.header_values

Проверка имени/значения всех HTTP-заголовков запроса/ответа на значение.

Синтаксис:

```
request.header_values[.base64].regex = string

request.header_values[.base64].re2 = string

request.header_values[.base64].substring[.nocase] = string

request.header_values.count = integer | range

request.header_values.length = integer | range
```

request.x_header.<xh_name> и response.x_header.<xh_name>

Проверка HTTP-заголовка запроса/ответа на значение. xh_name — произвольный HTTP-заголовок.

Синтаксис:

```
request.x_header.<xh_name>[.base64][.nocase] = string

request.x_header.<xh_name>[.base64].regex = string
```

`request.x_header.<xh_name>[.base64].re2 = string`

`request.x_header.<xh_name>[.base64].substring[.nocase] = string`

`request.x_header.<xh_name>.count = integer | range`

`request.x_header.<xh_name>.length = integer | range`

Пример:

```
DENY url="http://usergate.com" request.x_header.Test="test1"
```

Возможны также суффиксы **length**, **count**, **regex**, **re2** как и в случае с <h_name>.

```
DENY("Too much X-Test data") request.x_header.X-Test.length = 2048..
DENY("Too much X-Test2 headers data") request.x_header.X-Test2.count =
2..
PASS request.x_header.Test.regex = "[0-9]*"
```

request.header.Cookie.<cookie_name>

Проверка заголовка запроса Cookie на значение.

Синтаксис:

`request.header.Cookie.<cookie_name>[.base64][.(nocase | substring | substring.nocase | regex | re2)] = string`

Пример:

```
DENY http.method = POST request.header.Cookie.csrf_token !=
qparam.CSRF_TOKEN enabled(true) name("Check CSRF")
```

time, day, hour, minute

Проверка соответствия текущего времени заданному условию. Если не указан суффикс `utc`, время берется локальное, иначе — по Гринвичу.

Синтаксис:

```
day[.utc] = monday | tuesday | wednesday | thursday | friday |
saturday | sunday | DD | list

time[.utc] = HH:MM | range | lib.time(<name>)

hour[.utc] = HH | range

minute[.utc] = MM | range

HH ::= 00 - 23

MM ::= 00 - 59

DD ::= 1 - 31
```

Пример:

```
PASS time = 12:00..13:00  % разрешить каждый день с 12 до 13 часов
PASS time = lib.time("Праздники") % использовать библиотеку "Праздники"
DENY day = (sunday, saturday) % запретить на выходных
DENY day = (monday, 15) hour = 9..18  % запретить каждый понедельник и
каждое 15 число месяца с 9 до 18 часов
```

Открытые интервалы учитываются по границе суток/часа.

```
PASS hour = 18.. % означает, что разрешено с 18 часов до полуночи
minute = ..10 % первые 10 минут каждого часа
```

url, url.host и url.address

Проверка url или его части на значение. Проверка использует нормализованный URI с декодированными *%*.

Синтаксис:

```
url[.(prefix | substring | suffix | regex | re2)] = string

url.host[.(prefix | substring | suffix | regex | re2)] = string

url.domain[.(prefix | substring | suffix | regex | re2)] = string

url.address = ip_address | subnet | subnet_label
```

```
url.port = [low_port]..[high_port] | port

url.path[.base64][.(prefix | substring | suffix | regex | re2)] =
string

url.is_absolute = yes | no     % полный или нет URL

prefix ::= string              % начало строки

substring ::= string           % подстрока

suffix ::= string              % окончание строки

regex ::= string               % регулярное выражение PCRE

re2 ::= string                 % регулярное выражение RE2
```

`url.address` — это, по сути, синоним `dst.ip`.

Пример:

```
DENY url.path.base64.re2 = "(?i)\bondisconnecting\W*=" enabled(true)
name("ondisconnecting (URI)")
```

qparam.<name>, qparam.values и qparam.names

Проверка значения параметров запроса. Проверка использует имена и значения параметров с декодированными *%*.

Синтаксис:

```
qparam.length = numeric          % проверить общую длину query-
параметров

qparam.count = numeric           % проверить количество query-
параметров qparam.<name>[.(length | count)] = numeric

qparam.<name>[.base64][.(nocase | substring | substring.nocase |
regex | re2)] = string

qparam.values[.base64].substring[.nocase] = string % проверить
все значения на вхождение подстроки

qparam.names[.base64].substring[.nocase] = string  % проверить
все имена на вхождение подстроки
```

```
qparam.values[.base64].regex = string              % проверить
все значения на регулярное выражение

qparam.names[.base64].regex = string               % проверить
все имена на регулярные выражения

qparam.values[.base64].re2 = string                % проверить
все значения на регулярное выражение

qparam.names[.base64].re2 = string                 % проверить
все имена на регулярные выражения numeric ::= integer | range
% число либо диапазон

regex ::= string                 % регулярное выражение PCRE

re2 ::= string                   % регулярное выражение RE2
```

Пример:

```
DENY("limit arguments total length") qparam.length =
1024..                 % total
DENY("Limit argument value length") qparam.values.length =
1024..           % for each
DENY("Limit argument name length") qparam.names.length =
1024..             % for each
DENY("Maximum number of arguments in request limited") qparam.count  =
12.. % total
DENY(""PHP injection attempt") qparam.values.base64.substring.nocase =
"${@print"
```

user и group

Проверка текущего пользователя или его группы.

Синтаксис:

```
user = word | string | known | unknown

group = word | string

user.guid = string

group.guid = string
```

`known` — используется для указания авторизованного (известного) пользователя;
`unknown` — используется для указания неавторизованного (неизвестного) пользователя.

Пример:

```
PASS user = known % разрешить известных пользователей
DENY group = "Отдел продаж" category = "Pornography/Sexually
Explicit"   % запретить категорию порно для группы "Отдел продаж"
```

src и dst

Проверка условия на IP-адрес, зону или GeoIP источника/назначения.

Синтаксис:

`src.ip = ip_address | subnet | subnet_label | list | lib`

`dst.ip = ip_address | subnet | subnet_label | list | lib`

`src.zone = integer | zone_name`

`dst.zone = integer | zone_name`

`src.geoip = iso3166 | list`

`dst.geoip = iso3166 | list`

`src.mac = mac_address | list`

`dst.mac = mac_address | list`

`lib ::= lib.(network | url) '(' list_libs ')'`

`list_libs :: = lib_name ',' list_libs`

`lib_name ::= word | string`

`iso3166 ::= [A-Z][A-Z]`

`url.address` — это, по сути, синоним `dst.ip`.

scenario

Проверка активности определенного сценария.

Синтаксис:

`scenario = string | word | list`

Пример:

```
DENY scenario = Torrents  desc("Запретить, если активен сценарий
Torrents")
```

virus_heuristic и virus_usergate

Проверка тела ответа на вирусы.

Синтаксис:

`virus_heuristic = yes | no | true | false  % (по умолчанию false)`

`virus_usergate = yes | no | true | false  % (по умолчанию false)`

`heuristic` — эвристический анализатор (медленный);
`usergate` — проверка по хэшам (быстрый).

bridge_vlan_filter

Фильтрация трафика по VLAN-тегам для интерфейса в режиме моста (bridge).

Синтаксис:

`bridge_vlan_filter '='|'!=' list | number | number..number`

Пример:

```
DENY bridge_vlan_filter = (10, 100..200)  desc("Запретить трафик по
VLAN-тегам")
```

service

Детектирование трафика определенного сервиса для межсетевого экрана.

Синтаксис:

`service = string | word | list`

Пример:

```
DENY service = POP3  desc("Запретить сервис POP3")
```

envelope_from и envelope_to

Проверка email-адреса отправителя/адресата сообщения.

Синтаксис:

`envelope_from '='|'!='' string | list`

`envelope_to '='|'!='' string | list`

Пример:

```
PASS envelope_from = "Email froup from" envelope_to = "Email froup to"
service = SMTP mark_hdr(Subject) enabled(true) name("Mail Pass Rule")
```

response_time

Проверка времени ответа в миллисекундах.

Синтаксис:

`response_time = integer`

Встроенные библиотеки

Библиотеки (`lib`) — это элементы языка UPL, которые служат для доступа к встроенным и пользовательским библиотекам. Как правило, это достаточно

большие списки, которые неудобно описывать через определения `def`. Обращение к библиотекам происходит по их именам.

Синтаксис:

```
library ::= lib.<url | morphology | category | useragent | mime |
network | time | applicationgroup | servicegroup>(list_names)

list_names ::= name list_names

name ::= word | string
```

`url` — список URL;
`morphology` — список морфологических словарей;
`category` — группа категорий;
`useragent` — список юзерагентов;
`mime` — список типов контента;
`network` — список сетей/IP-адресов;
`time` — библиотека с промежутками времени.

Пример:

```
DENY src.ip = lib.network("Bad ips", "Test ips")
DENY dst.ip = lib.network("Bad ips")
DENY dst.ip = lib.url("Bad urls") % в данном случае домены будут
резолвиться в ip-адреса

DENY morphology = lib.morphology("Porno words", "Bad words")
DENY category = lib.category("Restricted categories") category =
lib.category(Productivity)

PASS request.header.User-Agent = lib.useragent("Browsers")
PASS request.header.Content-Type = lib.mime(Applications)
DENY time = lib.time(Weekends)
```

Свойства

Свойства (`properties`) — это некие атрибуты правила, например, `name` или `enabled`. Они используются для предоставления

дополнительной информации в процессе обработки правил.
Синтаксис свойств точно такой же, как у действий.

Синтаксис:

```
property = prop_name | prop_name '(' list_params ')'

prop_name ::= name | desc | id | rule_log | enabled | scenario

list_params ::= value ',' list_params
```

name и desc

Атрибуты *имя* и *описание* для правила.

Синтаксис:

```
Name ::= name '(' string|word ')'

Description ::= desc '(' string ')'
```

Пример:

```
DENY hour = 9..18 category = News name("Запретить News")
desc("Запретить категорию News в рабочее время")
```

enabled

Атрибут, который включает или выключает работу правила.

Синтаксис:

```
Enable ::= enabled '(' boolean ')'

boolean ::= yes | no | true | false       % (по умолчанию false)
```

rule_log

Устанавливает атрибут журналирования правила.
Значение `session` действительно только для правил межсетевого экрана, защиты от dos-атак и пропускной способности.

Синтаксис:

```
Logging ::= rule_log '(' boolean | session ')'

LoggingFwRule ::= rule_log '(' boolean , interval,  burst')'

boolean ::= yes | no | true | false         % (по умолчанию no)

interval ::= "integer/[s,m,h,d]"

burst ::= integer
```

`interval` — среднее число пакетов, попадающих под условие `limit` в единицу времени (`1/s, 1/m, 1/h, 1/d)` , `default = 3/h`;
`burst` — максимальное число пакетов, попадающих в под условие `limit` за один раз (`default = 5`).

profile

Устанавливает профиль правила.

Синтаксис:

```
Profile ::= profile '(' string | word | list ')'
```

certificate

Сертификат, используемый для поддержки HTTPS-соединения. Действительно только для правил reverse-прокси.

Синтаксис:

```
CertAuthEnabled ::= cert_auth_enabled '(' boolean ')'

Certificate ::= certificate '(' certificate_name ')'

certificate_name ::= string | word
```

gateway

Шлюз. Имя одного из существующих шлюзов. Действительно только для правил NAT и маршрутизации, и для условий сценария «Проверка состояния».

Синтаксис:

```
Gateway ::= gateway '(' string | word ')'
```

Свойства правил межсетевого экрана

reject_with

Устанавливает способ, с помощью которого будет блокироваться трафик. Действительно только для правил межсетевого экрана.

Синтаксис:

```
Reject ::= reject_with '(' "tcp-reset-both" | "tcp-rst" | "host-unreach" ')'
```

fragmented

Проверка на фрагментацию пакетов. Действительно только для правил межсетевого экрана.

Синтаксис:

```
Fragmented ::= fragmented '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

`yes` — проверяются только фрагментированные пакеты;
`no` — проверяются только нефрагментированные пакеты;
—, если свойство *fragmented* не указано, то будут проверяться все пакеты.

Свойства правил инспектирования SSL

block_invalid_cert

Блокирование сайтов с некорректными сертификатами. Действительно только для правил инспектирования SSL.

Синтаксис:

```
InvalidCertificate ::= block_invalid_cert '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

check_revoc_cert

Проверка по списку отозванных сертификатов. Действительно только для правил инспектирования SSL.

Синтаксис:

```
ChekRevocation ::= check_revoc_cert '(' boolean ')'

boolean ::= yes | no | true | false
```

block_expired_cert

Блокировка сертификатов с истекшим сроком действия. Действительно только для правил инспектирования SSL.

Синтаксис:

```
ExpiredCertificate ::= block_expired_cert '(' boolean ')'

boolean ::= yes | no | true | false
```

block_self_signed_cert

Блокировка самоподписанных сертификатов. Действительно только для правил инспектирования SSL.

Синтаксис:

```
SelfSignedCertificate ::= block_self_signed_cert '(' boolean ')'

boolean ::= yes | no | true | false
```

ssl_profile

Профиль SSL. Действительно только для правил инспектирования SSL, reverse-прокси, веб-портала.

Синтаксис:

```
SslProfile ::= ssl_profile '(' string | word ')'
```

ssl_forward_profile

Профиль пересылки SSL. Действительно только для правил инспектирования SSL.

Синтаксис:

```
SslForwardProfile ::= ssl_forward_profile '(' string | word ')'

profile_id ::= integer
```

Свойства правил пропускной способности

bandwidth_pool

Полоса пропускания. Действительно только для правил пропускной способности.

Синтаксис:

```
BandwidthPool ::= bandwidth_pool '(' bandwidth ')'
```

```
bandwidth ::= "100 Kbps" | "512 kbps" | "1 Mbps" | "2 Mbps" | "5 Mbps" | "10 Mbps" | "20 Mbps" | "50 Mbps" | "100 Mbps"
```

Пример:

```
scenario = "Сценарий обнаружения torrent" bandwidth_pool("1 Mbps") enable(true) name("Пропускная способность torrent")
```

Свойства правил NAT и маршрутизации

target_ip

Адрес назначения DNAT, если задано действие `dnat` или `port_mapping`.

Новая IP-сеть/маска, если задано действие `netmap`.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

```
TargetIp ::= target_ip '(' ipv4 | ipv4_with_mask ')'
```

Пример:

```
PASS target_ip("192.168.1.20") dnat
```

target_snat

Включение SNAT. При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

```
TargetSnat ::= target_snat '(' boolean ')'

boolean ::= yes | no | true | false
```

snat_target_ip

SNAT IP (внешний адрес). Явно указывает IP-адрес, на который будет заменен адрес источника при подмене адресов пакетов.

Действительно только для правил NAT и маршрутизации.

Синтаксис:

```
SnatTargetIp ::= snat_target_ip '(' ip_address ')'
```

port_map

Порт-форвардинг. Переопределение портов публикуемых сервисов. Действительно только для правил NAT и маршрутизации.

Синтаксис:

```
PortMap ::= port_map '(' protocol, port_from, port_to ')'

protocol ::= tcp | udp | smtp | smpts

port_from ::= integer

port_to ::= integer
```

`port_from` — номер TCP/UDP-порта, на который пользователи шлют запросы; `port_to` — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.

direction

Направление подмены сетей. Действительно только для правил NAT и маршрутизации.

Синтаксис:

```
Direction ::= direction '(' input | ouput ')'
```

`input` — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике;

`ouput` — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике.

Свойства правил DNS-прокси

dns_server

Список IP-адресов DNS-серверов. Действительно только для правил DNS-прокси.

Синтаксис:

```
DnsServer ::= dns_server '(' ip_address | ip_address_list ')'
```

Свойства правил reverse-прокси

cert_auth_enabled

Аутентификация по сертификату. Действительно только для правил reverse-прокси.

Синтаксис:

```
CertAuthEnabled ::= cert_auth_enabled '(' boolean ')'

boolean ::= yes | no | true | false
```

is_https

Включение поддержки HTTPS. Действительно только для правил reverse-прокси.

Синтаксис:

```
IsHttps ::= is_https '(' boolean ')'

boolean ::= yes | no | true | false
```

rewrite_path

Подмена путей. Действительно только для правил reverse-прокси.

Синтаксис:

```
RewritePath ::= rewrite_path '(' path_from, path_to ')'
```

`path_from` — изменить с (домен и/или путь URL, которые требуется изменить);
`path_to` — изменить на (домен и/или путь URL, на которые требуется заменить старые).

Свойства правил веб-портала

icon

Иконка, которая будет отображаться на веб-портале для данной закладки. Действительно только для правил веб-портала.

Синтаксис:

```
Icon ::= icon '(' string | word ')'
```

additional_url

Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей.

Действительно только для правил веб-портала.

Синтаксис:

```
AdditionalUrl ::= additional_url '(' string | word | list ')'
```

rdp_check_session_alive

Проверка авторизации для RDP-сессий. Действительно только для правил веб-портала.

Синтаксис:

```
RdpCheckSessionAlive ::= rdp_check_session_alive '(' boolean ')'

boolean ::= yes | no | true | false
```

transparent_auth

Включение прозрачной аутентификации пользователя. Действительно только для правил веб-портала.

Синтаксис:

```
TansparentAuth ::= transparent_auth '(' boolean ')'
```

```
boolean ::= yes | no | true | false
```

Свойства правил веб-безопасности (Safe browsing)

enable_adblock

Блокировка рекламы.

Синтаксис:

```
EnableAdblock ::= enable_adblock '(' boolean ')'

boolean ::= yes | no | true | false
```

url_list_exclusions

URL-список сайтов исключений, для которых блокировать рекламу не требуется.

Синтаксис:

```
UrlListExclusions ::= url_list_exclusions '(' list_libs ')'

list_libs :: = lib_name ',' list_libs

lib_name ::= word | string
```

enable_injector

Позволяет вставить произвольный код во все веб-страницы.

Синтаксис:

```
EnableInjector ::= enable_injector '(' boolean ')'

boolean ::= yes | no | true | false
```

custom_injector

Код инжектора.

Синтаксис:

```
CustomInjector ::= custom_injector '(' string ')'
```

safe_search

Функция безопасного поиска.

Синтаксис:

```
SafeSearch ::= safe_search '(' boolean ')'

boolean ::= yes | no | true | false
```

search_history_logging

Запись в журнал поисковых запросов пользователей.

Синтаксис:

```
SearchHistoryLogging ::= search_history_logging '(' boolean ')'

boolean ::= yes | no | true | false
```

social_sites_block

Блокировка приложения в популярных социальных сетях.

Синтаксис:

```
SocialSitesBlock ::= social_sites_block '(' boolean ')'

boolean ::= yes | no | true | false
```

Свойства правил сценариев

trigger

Тип срабатывания сценария. Действительно только для правил сценариев.

Синтаксис:

```
Trigger ::= trigger '(' trigger_type ')'

trigger_type ::= all_users | one_user
```

duration

Продолжительность. Время в минутах, в течение которого сценарий будет активным после его активации. Действительно только для правил сценариев.

Синтаксис:

```
Duration ::= duration '(' integer ')'
```

operation_mode

Сценарий срабатывает при совпадении одного или всех условий.

Синтаксис:

OperationMode ::= operation_mode '(' mode ')'

```
mode ::= all | any
```

Свойства условий сценария

scond_type

Тип условий сценария. Действительно только для условий сценария.

Синтаксис:

```
SCondType ::= scond_type '(' type ')'
```


```
SCondType ::= scond_type '(' type ')'
```


count_interval

Количество срабатываний. Действительно только для условий сценария «Категория URL» (`url_category`), «Приложение» (`app`), «Тип контента» (`mime_type`) и «Проверка состояния» (`health_check`).

Синтаксис:

```
CountInterval ::= count_interval '(' integer ')'
```

max_event_count

Интервал времени в минутах, за который было обнаружено `count_interval` срабатываний. Действительно только для условий сценария «Категория URL» (`url_category`), «Приложение» (`app`), «Тип контента» (`mime_type`) и «Проверка состояния» (`health_check`).

Синтаксис:

```
MaxEventCount ::= max_event_count '(' integer ')'
```

packet_size

Размер пакета. Размер пакета в трафике пользователя превысил указанное значение. Действительно только для условий сценария «Размер пакета» (`net_packet_size`).

Синтаксис:

```
PacketSize ::= packet_size '(' size ')'
```

```
size ::= integer | integer KB | integer MB | integer GB
```

64 — размер в байтах;
2MB — размер в мегабайтах.

traffic_limit

Объем трафика. Действительно только для условий сценария «Ограничение трафика» (`traffic`).

Синтаксис:

```
TrafficLimit ::= traffic_limit '(' size ')'
```

```
size ::= integer | integer KB | integer MB | integer GB
```

period

Период времени. Действительно только для условий сценария «Ограничение трафика» (`traffic`).

Синтаксис:

```
Period ::= period '(' time_period ')'
```

```
time_period ::= minute | hour | day | week | month
```

health_check_method

Метод проверки. Действительно только для условий сценария «Проверка состояния» (`health_check`).

Синтаксис:

```
CheckMethod ::= health_check_method '(' method ')'
```

```
method ::= ping | dns | get
```

health_result

Результат. Действительно только для условий сценария «Проверка состояния» (`health_check`).

Синтаксис:

```
esult ::= health_result '(' result ')'
```

```
result ::= positive | negative
```

health_request_timeout

Тайм-аут подключения (сек). Действительно только для условий сценария «Проверка состояния» (`health_check`).

Синтаксис:

```
RequestTimeout ::= health_request_timeout '(' integer ')'
```

health_answer_timeout

Тайм-аут ответа (сек). Действительно только для условий сценария «Проверка состояния» (`health_check`), «Метод проверки HTTP GET» (`get`).

Синтаксис:

```
ut ::= health_answer_timeout '(' integer ')'
```

health_type_request

Тип DNS-запроса. Действительно только для условий сценария «Проверка состояния» (`health_check`), «Метод проверки DNS» (`dns`).

Синтаксис:

```
TypeRequest ::= health_type_request '(' type_name ')'
```

```
type_name ::= word | string
```

Свойства правил балансировки нагрузки

scheduler

Метод балансировки. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

`Scheduler ::= scheduler '(' balancing_type ')'`

`balancing_type ::= wrr | rr | lc | wlc`

`wrr` — Weighted round robin;

`rr` — Round robin;

`lc` — Least connections;

`wlc` — Weighted least connections.

real_server

Реальные серверы. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

`RealServer ::= real_server '(' mode, ipv4[:port], weight ')'`

`mode ::= gate | masq | masq_snat`

`port ::= integer`

`weight ::= integer`

`gate – шлюз;`

`masq` — маскарадинг;

`masq_snat` — маскарадинг с подменой IP-адреса источника (SNAT).

Пример:

```
OK \
        url.address = 172.168.13.100 \
        url.port = 10000 \
        service = tcp \
        scheduler(wlc) \
        real_server(masq_snat, 172.168.13.11:10000, 50) \
        ipvs_fallback(gate, 172.168.13.12)
        monitor_kind(ping) \
        monitor_interval(60) \
```

```
        monitor_timeout(60) \
        monitor_failurecount(10) \
        enabled(true) \
        name("TCP/UPD load balancing")
```

ipvs_fallback

Аварийный режим сервера. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
IpvsFallback ::= ipvs_fallback '(' mode, ipv4[:port] ')'

mode ::= gate | masq | masq_snat

port ::= integer
```

monitor_kind

Режим. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorKind ::= monitor_kind '(' kind ')'

kind ::= ping | connect | negotiate
```

monitor_service

Сервис. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorService ::= monitor_service '(' service ')'

service ::= http | dns
```

monitor_request

Запрос. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorRequest ::= monitor_request '(' string ')'
```

monitor_response

Ожидаемый ответ. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorResponse ::= monitor_response '(' string ')'
```

monitor_interval

Интервал проверки. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorInterval ::= monitor_interval '(' integer ')'
```

monitor_timeout

Время ожидания. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorTimeout ::= monitor_timeout '(' integer ')'
```

monitor_failurecount

Число неудачных попыток. Действительно только для правил балансировки нагрузки TCP/UDP.

Синтаксис:

```
MonitorFailurecount ::= monitor_failurecount '(' integer ')'
```

Действия

Действие (`action`) — это то, что будет выполнено,
если условия в правиле истинны. В качестве параметров могут использоваться константные значения, или динамические значение там, где это предусмотрено.

Синтаксис:

```
action = action_name | action_name '(' list_params ')'

action_name ::= warning | log_message | append | delete | set |
replace | encrypt | inc|dec | reset | redirect | encrypt_body_url
| decrypt_path | body_inject | set_cookie_token | body_replace |
lookup_and_auth | encode_cookie | decode_cookie | sma | nat |
dnat | route | port_mapping | netmap | forward | ignore |
action_label

action_label ::= 'action'.<action_label_name>

action_label_name ::= atom

list_params ::= value ',' list_params
```

warning

Действия, которые разрешаются без выхода из обработки правил на текущем слое. `warning` ставит отметку о том, что необходимо вставить код с предупреждением в тело ответа.

Пример:

```
[L1]
category = lib.category(Productivity) warning
DENY user = user1
```

log_message

Записать сообщения в журнал.

Пример:

```
DENY category = lib.category(Productivity) log_message("Deny porno")
```

append

Добавить заголовок к HTTP-запросу/ответу. Список поддерживаемых заголовков приведен в Приложении.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Синтаксис:

```
append([request | response,] <headername>, value)
```

`headername` — см. в Приложении.
`value ::= string | numeric | condition_name.`

set

Переписать значение конкретному HTTP-заголовку. Список поддерживаемых заголовков см. в Приложении.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Синтаксис:

```
set([request | response,] <headername>, value)
```

`headername` — см. в Приложении.
`value ::= string | numeric | condition_name.`

delete

Удалить HTTP-заголовок. Список поддерживаемых заголовков см. в Приложении.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Синтаксис:

```
delete([request | response,] <headername>)
```

`headername` — см. в Приложении.

replace

Модифицировать значение HTTP-заголовка. Список поддерживаемых заголовков см. в Приложении.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Синтаксис:

`replace([request | response,] <headername>, regex, value)`

`regex ::= string` % регулярное выражение

`value ::= string | condition_name`

`headername` — см. в Приложении.

Пример 1:

Добавить заголовок Referer:

```
PASS append(Referer, "http://example.com") enabled(true)
```

Удалить заголовок:

```
PASS delete(Referer)
```

Переписать заголовок:

```
PASS set(request, Cache-Control, no-cache)
```

Модифицировать заголовок Location:

```
PASS response.header.Location.count = 1.. replace(response, Location,
"http://example.com", url.host) enabled(true)
```

Пример 2:

```
define action delete_referer
    log_message("Referer header deleted")
    delete(request, Referer)
end
```

encrypt

Шифровать часть пути в HTTP-заголовке. Список поддерживаемых заголовков см. в Приложении.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

```
encrypt([request | response,] <headername>, <url>[, <user_key>[,
<add_ip>]])
```

`url ::= string` % часть url для фильтрации

`user_key ::= string` % пользовательский ключ шифрования (необязательный параметр)

`add_ip ::= boolean` % добавлять ли IP к ключу шифрования (логическое значение, необязательный параметр)

`boolean ::= yes | no | true | false`

headername — см. в Приложении.

encrypt_body_url

Шифровать часть пути в ссылках тела ответа.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

```
encrypt_body_url(<url>[, <user_key>[, <add_ip>]])
```

`url ::= string` % часть url для фильтрации

`user_key ::= string` % пользовательский ключ шифрования (необязательный параметр)

`add_ip ::= boolean` % добавлять ли IP к ключу шифрования (логическое значение, необязательный параметр)

```
boolean ::= yes | no | true | false
```

decrypt_path

Дешифровать часть пути запроса.

Первый параметр может быть опущен, если заголовок относится к одной группе `request` или `response`.

Ключ шифрования и флаг "Использовать IP как часть ключа шифрования" — необязательные параметры.

Синтаксис:

```
decrypt_path(<path>[, <user_key>[, <add_ip>]])

path ::= string              % часть пути для фильтрации

user_key ::= string          % пользовательский ключ шифрования
(необязательный параметр)

add_ip ::= boolean           % добавлять ли IP к ключу шифрования
(логическое значение, необязательный параметр)

boolean ::= yes | no | true | false
```

Пример:

Шифровать все относительные пути в заголовке *Location* и теле ответа, и дешифровать путь запроса:

```
decrypt_path("/", "User_Key", true) enabled(true) name("Path decode")
http.response.code = 302 encrypt(Location, "/", "User_Key", true)
enabled(true) name("Encrypt Location header")
encrypt_body_url("/", "User_Key", true) enabled(true) name("Encrypt all
relative URL")
```

body_inject

Вставить скрипт в тело ответа.

Синтаксис:

```
body_inject(inject_text)
```

`inject_text ::= string`

set_cookie_token

Добавить в ответ заголовок 'Set-Cookie' со сгенерированным токеном.

Синтаксис:

`set_cookie_token(cookie_name, parameter, expires_date)`

`cookie_name ::= string`

`parameter ::= string`

`expires_date ::= [DD_]HH:MM` % время которое будет прибавлено к текущему времени

Пример:

Реализация CSRF защиты:

```
DENY http.method = POST request.header.Referer.substring = "/login.php"
qparam.UCSRF_TOKEN != request.header.Cookie.ucsrf_token enabled(true)
name("Check CSRF")
url.path.prefix = "/login.php" set_cookie_token(ucsrf_token, "path=/",
01_00:00) body_inject("<script language='JavaScript'>
    var tokenName = 'UCSRF_TOKEN';

    document.addEventListener('DOMContentLoaded', function()
    {
        var t_res = document.cookie.match(/ucsrf_token=(.+?)(;|$)/);
        var tokenValue = t_res ? t_res[1] : '';

        var forms = document.getElementsByTagName('form');
        for(i=0; i<forms.length; i++)
        {
            var html = forms[i].innerHTML;
            html += '<input type=hidden name=' + tokenName + ' value='
+ tokenValue + ' />';
            forms[i].innerHTML = html;
        }
```

```
    });
</script>") enabled(true) name("Inject")
```

encode_cookie

Шифровать значения Cookie в заголовке *Set-Cookie* с заданным именем.

Синтаксис:

`encode_cookie(cookie_name[, condition_name][, user_kry_string][, f_encrypt])`

`cookie_name ::= string`

`condition_name` % условие используемое для кодирования (по умолчанию src.ip)

`user_kry_string ::= string` % пользовательский ключ шифрования (по умолчанию "")

`f_encrypt := true` % необходимо шифрование (по умолчанию false)

decode_cookie

Дешифровать токен в заголовке Cookie с заданным именем.

Синтаксис:

`decode_cookie(cookie_name[, condition_key][, user_kry_string][, f_decript])`

`cookie_name ::= string`

`condition_name` % условие используемое для декодирования (по умолчанию src.ip)

`user_kry_string ::= string` % пользовательский ключ шифрования (по умолчанию "")

`f_encrypt := true` % необходимо шифрование (по умолчанию false)

Пример:

Шифрование и дешифрование Cookie с именем *security:*

```
response.header.Set-Cookie.count != 0 encode_cookie("security", src.ip,
true) enabled(true) name("encode_cookie")
request.header.Cookie.count != 0 decode_cookie("security", src.ip,
true) enabled(true) name("decode_cookie")
```

body_replace

Модифицировать тело ответа. Выполняется не более двух (первых) модификаций для каждого ответа.

Синтаксис:

`body_replace(<regex>, <value>)`

`regex ::= string` % регулярное выражение

`value ::= string`

Пример:

```
PASS \
body_replace("(\\+7|8)[\\s(]?(\\d\{3})[\\s)]?(\\d\{3})[\\s-]?(\\d\{2})
[\\s-]?(\\d\{2})", "+\\1 (\\2) \\3-XX-XX") \
body_replace("(\\w{1})[\\w\.]*(\\w{1})@([\\w]+)\\.([\\w]+)", "\\1***\
\2@\\3.\\4") \
enabled(true) \
name("Replace mail and phone")
```

lookup_and_auth

Аутентифицировать пользователя. В случае если IP не указан, запрос маркируется имением пользователя.

Синтаксис:

`lookup_and_auth(<user_login>[, <ip_address>[, <session_timeout>]])`

`user_login ::= string | condition_name` % Логин аутентификации

`ip_address ::= string | condition_name` % IP адрес

`session_timeout ::= integer` % тайм-аут сессии, по умолчанию 0.

Пример:

```
lookup_and_auth(request.x_header.X-Authenticated-User,
request.x_header.X-Forwarded-For, 300) enabled(true) name("User
authentication")
lookup_and_auth(request.x_header.X-Authenticated-User) enabled(true)
name("Mark request")
```

redirect

При блокировке перенаправить пользователя на адрес, который указан в редиректе.

Синтаксис:

`Redirect ::= redirect(RespCode[, RedirectText], Url)`

`RespCode ::= 301 | 302 | 305 | 307`

`RedirectText ::= string`

`Url ::= string`

Пример:

```
DENY src.zone = Trusted redirect(302, "Custom test (Moved)", "https://
block.captive/block")
DENY src.zone = Untrusted redirect(302, "https://block.captive/block")
```

inc и dec

Используются для изменения значения переменных, объявленных как `def var`.

Синтаксис:

`inc(var.<var_name>, integer)`

`dec(var.<var_name>, integer)`

Пример:

На каждый `http.response.code = 500` увеличивается значение `rps` на 1. Если превысили 10 таких запросов за 5 минут, блокируем дальнейшие ответы. Через 5 минут переменная *rps* будет сброшена в 0:

```
def var rps
    init = 0
    window = 00:05
    key = src.ip
end

http.response.code = 500 var.rps=..10 inc(var.rps, 1) enabled(true)

PASS var.rps = 5 log_message("Warning!") enabled(true)

DENY var.rps=11.. log_message("Too many 500 errors!") enabled(true)
```

reset

Сбросить значения переменных, объявленных как `init` в `def var`, в начальное значение.

Синтаксис:

`reset(var.<var_name>)`

sma

Используются для подсчета среднего значения в окне времени, которое определяется в переменной как `window` в `def var`.

Синтаксис:

`sma(var.<var_name>, integer)`

Пример:

Блокируются запросы, когда среднее время запроса за 30-секундный интервал превысит 2 секунды:

```
def var avg_time
    init = 0
    window = 00:00:30
    key = src.ip
end

src.zone = Untrusted sma(var.avg_time, response_time) enabled(true)
name("sma")
DENY src.zone = Untrusted var.avg_time = 2000.. enabled(true) name("sma
res")
```

nat

NAT — подмена сетевых IP-адресов.

Пример:

```
PASS src.zone = Trusted dst.zone = Untrusted nat
```

dnat

DNAT — подмена IP-адреса назначения.

Пример:

```
PASS dnat target_ip("192.168.1.20")
```

port_mapping

Порт-форвардинг — перенаправление трафика на указанный IP-адрес с изменением номера порта публикуемого сервиса.

Пример:

```
PASS port_mapping target_ip("192.168.1.20") port_map(tcp, 2000, 2001)
```

netmap

Network mapping — позволяет произвести замену IP-адресов источника или назначения одной сети на другую.

Пример:

```
PASS netmap target_ip("192.168.32.0/24") direction(output)
```

route

Policy-based routing — позволяет маршрутизировать IP-пакеты на основе расширенной информации, например, сервисов, MAC-адресов или серверов (IP-адресов).

SNAT IP — Адрес, на который будет заменен адрес источника для трафика NAT.

Пример:

```
PASS service = HTTP route getway(Шлюз1)
```

ignore

Игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации.

Пример:

```
OK profile("Example ICAP server") enabled(true) name("ICAP rule")
ignore
```

forward

Переслать. В случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL.

Пример:

```
OK url = lib.url(ZAPRET_INFO_BLACK_LIST_DOMAIN)ssl_profile("Default SSL
profile") ssl_forward_profile("Forward SSL profile") enabled(false)
name("Decrypt rule") forward
```

Типы правил

Правила контентной фильтрации

Префиксы

Имя	Описание
PASS	Разрешение посещения.
DENY	Блокировка веб-страницы.
WARNING	Предупреждение пользователя о том, что страница нежелательна для посещения.

Условия

src.zone, src.geoip, src.ip.

dst.zone, dst.geoip, dst.ip.

category, morphology, scenario, time, url, user.

request.header.Referer — Список URL, в котором указаны рефереры для текущей страницы.
request.header.User-Agent — User agent пользовательских браузеров.
response.header.Content-Type — Списки типов контента.
http.method — Метод, используемый в HTTP-запросах.

Свойства

name, desc, enabled, rule_log, virus_heuristic.

Пример

```
[content "Content Rules"]
 % ---------------- 1 --- "Content Rules" --------------
PASS \
    url = lib.url("Education institutions") \
    src.zone = Trusted \
    desc("Content filtering rule which allows access to the list of
URLs. This is an example rule which can be changed or deleted if
necessary.") \
    rule_log(yes) \
    enabled(true) \
    name("Example white list")
% ---------------- 2 --- "Content Rules" --------------
DENY("Blockpage (EN)") \
    url = lib.url("Education institutions") \
    dst.zone = Untrusted \
    rule_log(yes) \
    enabled(false) \
    name("Example block RU RKN by URL list")
% ---------------- 3 --- "Content Rules" --------------
DENY \
    url = lib.network("Private IPs") \
    morphology = lib.morphology(Drugs) \
    src.zone = Trusted \
    time = lib.time(Weekdays) \
    rule_log(yes) \
    redirect(302, "https://bing.com") \
    enabled(false) \
    name("Example redirect to safesearch engines")
```

Правила межсетевого экрана

Префиксы

Имя	Описание
PASS	Разрешение трафика.

Имя	Описание
DENY	Блокировка трафика.

Условия

src.zone, src.geoip, src.ip.

dst.zone, dst.geoip, dst.ip.

service, scenario, time, url, user, hip_profile.

Свойства

name, desc, enabled, rule_log, reject_with.

Пример

```
[firewall "Firewall rules"]
% ---------------- 1 ----------------
DENY \
    scenario = "Example torrent detection scenario" \
    dst.zone = Untrusted \
    dst.ip = lib.network("Botnets IP list") \
    rule_log(session) \
    reject_with("host-unreach") \
    enabled(true) \
    name("Example block RU RKN by IP list")
```

Правила NAT и маршрутизации

Префиксы

Имя	Описание
OK	Всегда OK.

Тип правила определяется действием (Action):

- **nat — правило NAT;**
- **dnat — правило DNAT;**
- **port_mapping — правило порт-форвардинга;**

- **netmap — правило Network mapping;**
- **route — правило policy-based.**

Условия

src.zone, src.geoip, src.ip, src.mac.

dst.zone, dst.geoip, dst.ip.

service, scenario, time, url, user.

Свойства

name, desc, enabled, rule_log, direction, target_ip, target_snat, snat_target_ip,

port_map, gateway.

Пример

```
[nat_routing "NAT and Routing Rules"]
% ---------------- 1 ----------------
OK \
    src.zone = Trusted \
    service = (HTTP, HTTPS) \
    snat_target_ip("192.168.13.210") \
    rule_log(session) \
    enabled(true) \
    name("NAT Rule")\
    nat
% ---------------- 2 ----------------
OK \
    src.zone = Management \
    dst.ip = (lib.network("Private IPs"), lib.url("Microsoft Windows
Internet checker")) \
    target_ip("171.168.1.1") \
    target_snat(yes) \
    snat_target_ip("192.168.1.1") \
    enabled(true) \
    name("DNAY Rule")\
    dnat
% ---------------- 3 ----------------
```

```
OK \
    target_ip("172.168.1.1") \
    snat_target_ip("192.168.1.1") \
    port_map(tcp, 2000, 2000) \
    enabled(true) \
    name("Port-forwarding Rule")\
    port_mapping
% ---------------- 4 ----------------
OK \
    user = example \
    scenario = "Example torrent detection scenario" \
    gateway(My) \
    enabled(true) \
    name("Policy-base Rule")\
    route
% ---------------- 5 ----------------
OK \
    dst.geoip = (RW, SO) \
    target_ip("172.168.1.1") \
    direction(input) \
    enabled(true) \
    name("Network mapping Rule")\
    netmap
```

Правила Captive-портала

Префиксы

Имя	Описание
PASS	Не использовать аутентификацию.
OK	Использовать Captive-профиль.

Условия

src.zone, src.geoip, src.ip.

dst.zone, dst.geoip, dst.ip.

time, url, category.

Свойства

name, desc, enabled, rule_log, profile.

Пример

```
[captive "Captive Rules"]
% ---------------- 1 ----------------
PASS \
    category = lib.category(Threats) \
    url = lib.url("Microsoft Windows Internet checker") \
    time = lib.time(Weekends) \
    rule_log(yes) \
    enabled(true) \
    name("Skip auth for Microsoft Internet checker")
% ---------------- 2 ----------------
OK \
    src.zone = Trusted \
    profile("Example Captive profile") \
    enabled(true) \
    name("Example Captive portal")
```

Правила инспектирования SSL

Префиксы

Имя	Описание
PASS	Не расшифровывать передаваемые данные.
OK	Расшифровать передаваемые данные.

Пересылка определяется действием (Action):

- **forward — в случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL (ssl_forward_profile).**

Условия

src.zone, src.geoip, src.ip,

dst.geoip, dst.ip,

time, service, user, category.

Свойства

name, desc, enabled, rule_log, ssl_profile, ssl_forward_profile.

block_invalid_cert, check_revoc_cert, block_expired_cert, block_self_signed_cert.

Пример

```
[ssl "Decrypt Rules"]
% ---------------- 1 ----------------
PASS \
    category = (Finance, "Information Security") \
    rule_log(yes) \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example DO NOT Decrypt rule for Finance and Security sites")
% ---------------- 2 ----------------
OK \
    category = lib.category(Threats) \
    rule_log(yes) \
    block_invalid_cert(yes) \
    check_revoc_cert(yes) \
    block_expired_cert(yes) \
    block_self_signed_cert(yes) \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example decrypt rule for parental control")
% ---------------- 3 ----------------
OK \
    url = lib.url("Default SSL profile") \
    rule_log(yes) \
    ssl_profile("Default SSL profile") \
    ssl_forward_profile("SSL forward profile") \
    enabled(false) \
    name("Example decrypt RU RKN")\
    forward
```

DNS-правила

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

url.domain.

Свойства

name, desc, enabled, dns_server.

Пример

```
[dns "DNS Rules"]
% ---------------- 1 ----------------
OK \
    url.domain = "*.example.com" \
    dns_server(1.2.3.4) \
    enabled(true) \
    name("Dns rule")
```

ICAP-правила

Префиксы

Имя	Описание
PASS	Пропуск. Не посылать данные на ICAP-сервер.
OK	Пересылка данных на ICAP-сервер.

Действие (Action):

- **ignore — игнорировать ответ от ICAP-сервера.**

Условия

src.zone, src.geoip, src.ip.

dst.zone, dst.geoip, dst.ip.

url, category, user, service, http.method, response.header.Content-Type.

Свойства

name, desc, enabled, rule_log, profile.

Правила reverse-прокси

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

src.zone, src.geoip, src.ip, src.mac.

dst.zone, dst.geoip, dst.ip.

user, request.header.User-Agent, url.port.

Свойства

name, desc, enabled, rule_log, profile,
certificate, cert_auth_enabled, is_https, ssl_profile,

rewrite_path.

Пример

```
[reverseproxy "Reverse proxy Rules"]
% ---------------- 1 ----------------
OK \
    url.port = 80 \
    src.zone = Untrusted \
    desc("Example reverse proxy rule. This is an example rule which can
```

```
be changed or deleted if necessary. ") \
    profile("Example reverse proxy server") \
    rewrite_path("example.com/path1", "example.local/path1") \
    enabled(true) \
    name("Example reverse proxy rule")
```

Правила веб-безопасности

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

src.zone, src.geoip, src.ip, src.mac.

dst.zone, dst.geoip, dst.ip.

time, user,

Свойства

name, desc, enabled, rule_log.

enable_adblock, safe_search, search_history_logging, social_sites_block, enable_injector,

custom_injector, url_list_exclusions.

Пример

```
[safebrowsing "Safe browsing Rules"]
% ---------------- 1 ----------------
OK \
    rule_log(yes) \
    enable_adblock(yes) \
    safe_search(yes) \
    search_history_logging(yes) \
    social_sites_block(yes) \
    enable_injector(yes) \
```

```
    custom_injector(code) \
    url_list_exclusions(FISHING_BLACK_LIST) \
    desc("Safebrowsing rule for all users. This is an example rule
which can be changed or deleted if necessary.") \
    enabled(false) \
    name("Example safebrowsing")
```

Правила пропускной способности

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

src.zone, src.geoip, src.ip, src.mac.

dst.zone, dst.geoip, dst.ip.

time, user application, service, scenario,

Свойства

name, desc, enabled, rule_log, bandwidth_pool.

Пример

```
[shaper "Shaper Rules"]
% ---------------- 1 ----------------
OK \
    scenario = "Example torrent detection scenario" \
    service = "HTTP Proxy" \
    rule_log(session) \
    bandwidth_pool("1 Mbps") \
    enabled(true) \
    name("Example Bandwidth rule")
% ---------------- 2 ----------------
OK \
    scenario = "Example torrent detection scenario" \
```

```
    src.zone = Trusted \
    application = lib.category("Coin Miners", Business) \
    rule_log(yes, "3/h", 5) \
    bandwidth_pool("100 Kbps") \
    enabled(true) \
    name("Example torrent shaper")
```

Правила веб-портала

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

url, user, url.domain.

Свойства

name, desc, enabled.

icon, ssl_profile, certificate, additional_url, rdp_check_session_alive, transparent_auth.

Пример

```
[webportal "Web portal Rules"]
% ---------------- 1 ----------------
OK \
    user = "CN=Default Group,DC=LOCAL" \
    url = "http://www.intranet.loc" \
    icon("default.svg") \
    rdp_check_session_alive(yes) \
    transparent_auth(yes) \
    certificate("CA (Default)") \
    ssl_profile("Default SSL profile") \
    enabled(false) \
    name("Example http application published via web portal")
```

Правила сценариев

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

scenario_cond.

Свойства

name, desc, enabled.

operation_mode, trigger, duration.

Условия сценария

Категория URL (url_category)

Условия

category

Свойства

count_interval, max_event_count, scond_type

Обнаружение вируса (virus_detection)

Свойства

scond_type

Тип котента (mime_type)

Условия

response.header.Content-Type

Свойства

count_interval, max_event_count, scond_type

Размер пакета (net_packet_size)

Свойства

packet_size, scond_type

Сессий с одного IP (sessions_per_ip)

Свойства

sessions_limit, scond_type

Объем трафика (traffic)

Свойства

traffic_limit, period, scond_type

Проверка состояния (health_check)

Условия

url.address, url.domain

Свойства

health_check_method, health_result, health_request_timeout, health_type_request, health_answer_timeout, count_interval, max_event_count, scond_type

Пример

```
[scenarios "Scenario Rules"]
% ---------------- 1 ----------------
def scenario_cond example_scenario_define
    category = (lib.category(Threats), "Advertisements & Pop-Ups")
count_interval(10) max_event_count(3) scond_type(url_category)
    scond_type(virus_detection)
```

```
    application = lib.category(Threats) count_interval(2)
max_event_count(1) scond_type(app)
    ips_tl(medium) scond_type(ips)
    response.header.Content-Type = lib.mime("Java script")
count_interval(0) max_event_count(0) scond_type(mime_type)
    packet_size(200MB) scond_type(net_packet_size)
    sessions_limit(50) scond_type(sessions_per_ip)
    traffic_limit(2GB) period(hour) scond_type(traffic)
    url.address = "192.168.100.100" url.domain = "example.com"
health_check_method(dns) \
        health_result(negative) health_request_timeout(4)
health_type_request(a) \
        count_interval(5) max_event_count(3) scond_type(health_check)
    url.domain = "example.com" health_check_method(get) \
        health_result(negative) health_request_timeout(5)
health_answer_timeout(10) \
        count_interval(0) max_event_count(0) scond_type(health_check)
end
OK \
    scenario_cond = example_scenario_define \
    operation_mode(all) \
    trigger(one_user) \
    duration(5) \
    enabled(false) \
    name("Example torrent detection scenario")
```

Правила балансировки нагрузки TCP/UDP

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

src.zone, src.geoip, src.ip, src.mac.

service, url.address, url.port.

Свойства

name, desc, enabled.

scheduler, real_server, ipvs_fallback

monitor_kind, monitor_service, monitor_request, monitor_response, monitor_interval,

monitor_timeout, monitor_failurecount

Пример

```
[ipvs_server "TCP/UDP load balancing Rules"]
% ---------------- 1 ----------------
OK \
    src.geoip = RW \
    url.address = 192.168.1.100 \
    url.port = 80 \
    service = tcp \
    scheduler(rr) \
    real_server(gate, 1.1.1.1:80, 50) \
    ipvs_fallback(masq_snat, 8.8.8.8:10000) \
    monitor_kind(negotiate) \
    monitor_service(http) \
    monitor_request("example.com") \
    monitor_interval(60) \
    monitor_timeout(60) \
    monitor_failurecount(10) \
    enabled(true) \
    name("TCP load balancing")
```

Правила балансировки ICAP

Префиксы

Имя	Описание
OK	Всегда OK.

Свойства

name, desc, enabled, profile.

Пример

```
[icap_balancing "ICAP load balancing Rules"]
% ---------------- 1 ----------------
OK \
    profile("Example ICAP server") \
    enabled(true) \
    name("ICAP load balancing")
```

Правила балансировки reverse-прокси

Префиксы

Имя	Описание
OK	Всегда OK.

Свойства

name, desc, enabled, profile.

Пример

```
[reverseproxy_balancing "Reverse proxy load balancing Rules"]
% ---------------- 1 ----------------
OK \
    profile("Example reverse proxy server") \
    enabled(true) \
    name("Reverse-proxy load balancing")
```

Список поддерживаемых HTTP-заголовков

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Accept	Request	✔	✔	✔
Accept-Charset	Request	✔	✔	✔
Accept-Encoding	Request	✔	✔	✔
Accept-Language	Request	✔	✔	✔
Accept-Ranges	Response	✔	✔	✔
Age	Response			
Allow	Request/ Response	✔	✔	✔
Authorization	Request			
Cache-Control	Request/ Response	✔	✔	✔
Client-IP	Request	✔	✔	
Connection	Request/ Response		✔	
Content-Encoding	Request/ Response		✔	
Content-Language	Request/ Response		✔	
Content-Length	Request/ Response			
Content-Location	Request/ Response		✔	✔
Content-Range	Request/ Response			
Content-Type	Request/ Response			
Cookie	Request	✔	✔	✔
Date				

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
	Request/ Response			
ETag	Response	✔	✔	
Expect	Request	✔		
Expires	Request/ Response		✔	✔
From	Request	✔	✔	
Host	Request			
If-Match	Request	✔		
If-Modified-Since	Request			
If-None-Match	Request	✔		
If-Range	Request			
If-Unmodified-Since	Request			
Last-Modified	Request/ Response			
Location	Response	✔	✔	
Max-Forwards	Request			
Meter	Request/ Response		✔	✔
Pragma	Request/ Response		✔	✔
Proxy-Authenticate	Response	✔		
Proxy-Authorization	Request	✔		
Proxy-Connection	Request	✔		
Range	Request	✔	✔	
Referer	Request	✔	✔	

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Retry-After	Response	✔	✔	
Server	Response	✔	✔	
Set-Cookie	Response	✔	✔	✔
TE	Request	✔		
Trailer	Request/ Response		✔	
Transfer-Encoding	Request/ Response		✔	
Upgrade	Request/ Response		✔	
User-Agent	Request	✔	✔	
Vary	Response	✔	✔	✔
Via	Request/ Response	✔	✔	✔
Warning	Request/ Response	✔	✔	✔
WWW-Authenticate	Response			

Определения

В файлах политик определения (`def`) служат для объединения наборов условий или действий. Каждое определение должно иметь уникальное пользовательское имя, по которому к нему можно обратиться из правил.

def condition

Наборы условий. Все условия в одной строке проверяются по логическому *И*. Перевод строки означает логическое *ИЛИ*. Символ экранирования — обратный слеш «****» в конце строки позволяет перенести условие по *И* на следующую строку.

Синтаксис:

```
def condition label_name

    conditions

end

conditions ::= condition '\'? [conditions]

condition ::= name '=' value

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+
```

def scenario_cond

Список условий сценария. Каждое условие сценария обычно пишется в одной строке, но при необходимости условие может быть разбито на строки с помощью специального символа — обратного слеша «****».

Синтаксис:

```
def scenario_cond label_name

    scenario_conditions

end

scenario_conditions ::= Conditions '\'? Properties

Conditions ::= condition '\'? Conditions

Properties ::= property '\'? Properties

scenario_cond ::= name '=' value

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+
```

def var

Определение переменных. Служит для подсчета некоторых событий за определенный интервал времени. Для изменения значения предназначены действия `inc` и `dec`.

Синтаксис:

```
def var label_name

    init ::= integer

    window ::= time

    key ::= condition_name | condition_list

end

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

condition_list ::= '(' condition_name , condition_list ')'
```

init — это начальное значение переменной, к которому она вернется по истечении времени *window*;

key — поле или список полей, по которым группируются значения переменной (необязательный параметр).

ДАШБОРД

Работа с дашбордами и виджетами

В UserGate SWG можно отслеживать текущее состояние устройства, объемы трафика, проходящего через него, статус лицензии и различные статистические данные, связанные с сетевой безопасностью. Эти данные представлены в виде виджетов на странице **Дашборды**. Вы можете настраивать виджеты в соответствии с вашими требованиями.

> **Примечание**
> **Просмотр и изменение дашбордов доступны, если в профиле доступа вашей учетной записи настроены соответствующие разрешения.**

Вы можете добавлять новые дашборды, переименовывать их и удалять, выбирать нужные виджеты из поставляемых с продуктом коллекций, изменять состав виджетов на дашбордах, их расположение и размер. По умолчанию созданы дашборды с виджетами NOC (Network Operation Center) и SOC (Security Operation Center).

В зависимости от типа данных виджеты поделены на три коллекции:

- **Центр управления сетью**;
- **Центр управления безопасностью**;
- **Группа VPN**.

В виджетах из коллекций **Центр управления безопасностью** и **Группа VPN** в графическом виде представлены данные из журналов UserGate SWG. Поэтому, чтобы данные отображались в виджете, необходимо настроить соответствующие правила и включить для них журналирование событий. Например, если настроена сеть VPN и ведется запись соответствующих событий, вы сможете отслеживать статистику по виджетам из коллекции **Группа VPN**.

По умолчанию в виджете отображаются данные за последний час. Вы можете изменить период для каждого из виджетов, выбрав предустановленный вариант в верхней правой части виджета. В виджетах с графиками также можно выделить часть периода, чтобы подробнее ознакомиться с определенной частью графика. Возвращение к исходному масштабу выполняется по двойному нажатию левой кнопкой мыши.

Настройка виджета

Для некоторых виджетов вы можете фильтровать данные и настраивать способ их отображения. Если настройка доступна, в правом верхнем углу виджета отображается значок шестеренки.

Чтобы настроить виджет:

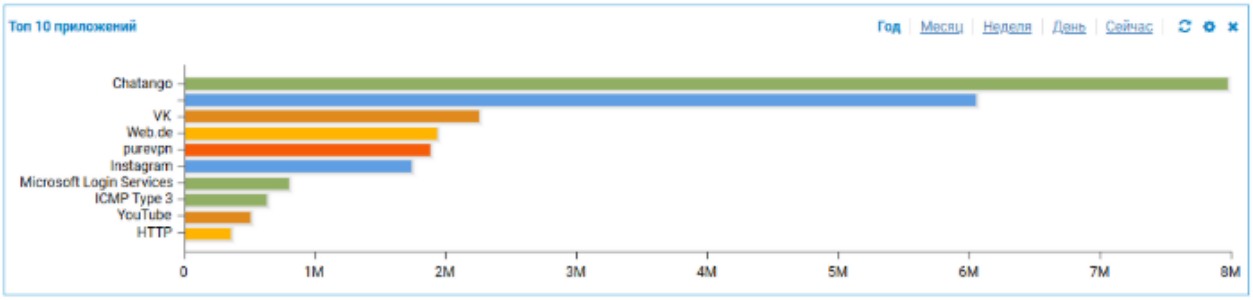
1. Нажмите на значок шестеренки в правом верхнем углу нужного виджета.
2. В окне **Настройка виджета** выполните одно или несколько действий (в зависимости от типа виджета набор параметров может отличаться):
    - измените название виджета;
    - укажите максимальное количество записей, которые будут отображаться в виджете;

- выберите, по какому значению будут сгруппированы данные в виджете;
- выберите, в виде какой диаграммы или таблицы будут представлены данные;
- с помощью SQL-запроса настройте фильтрацию данных, отображаемых в виджете;
- добавьте описание виджета.

1. Нажмите **Сохранить**.

Пример фильтрации данных в виджете

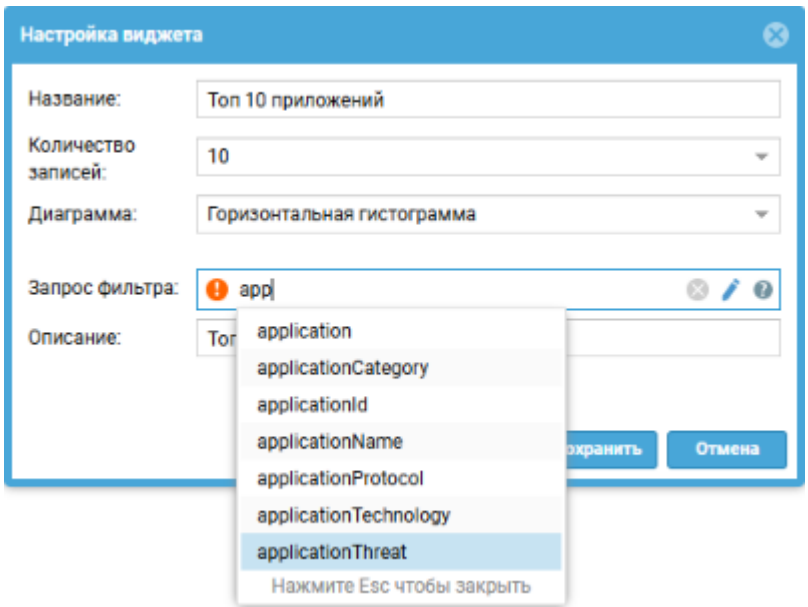
На дашборд добавлен виджет **Топ-10 приложений**, в котором по умолчанию представлены разные приложения, в том числе не представляющие угрозы.



Чтобы по виджету можно было отслеживать только опасные приложения, необходимо в окне **Настройка виджета** в поле **Запрос фильтра** настроить дополнительную фильтрацию данных с помощью SQL-запроса.

В SQL-запросах используется тот же синтаксис, что и в журналах для поиска и фильтрации данных. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации «Поиск и фильтрация данных». Значения параметров собираются из событий в журнале.

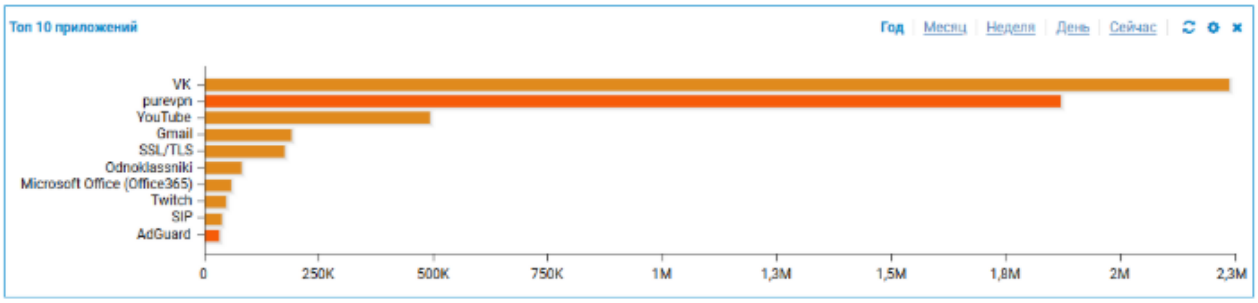
При вводе запроса в поле отображается список доступных операторов, параметров и их значений, из которых можно сформировать нужный запрос.



Запрос на фильтрацию опасных и очень опасных приложений выглядит следующим образом:

```
applicationThreat in (high, 'very high')
```

После завершения настройки и обновления данных в виджете будут представлены только опасные и очень опасные приложения.



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Раздел технической поддержки

Раздел технической поддержки на сайте компании содержит дополнительную информацию по настройке устройства. Здесь же вы можете оставить заявку на решение возникшей проблемы с оборудованием.

Аварийные ситуации

Сбои в работе устройства могут возникнуть при некорректной установке обновлений программного обеспечения.

Для профилактики аварийных ситуаций:

1. Перед установкой обновления сделайте резервную копию устройства. Подробнее — в разделе «Управление резервным копированием».

2. Во время установки обновления создайте точку восстановления системы. Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении устройства:

1. Восстановите предыдущую стабильную версию ПО. Подробнее — в разделе «Обновление ПО».

2. Обратитесь в службу технической поддержки в зависимости от уровня вашего сервисного контракта:

- Premium-поддержка: позвоните по выделенному телефону для экстренной помощи.
- Brilliant-поддержка: свяжитесь с вашим выделенным техническим специалистом.
- Базовая поддержка: обратитесь за квалифицированной помощью на странице поддержки.

ПРИЛОЖЕНИЯ

Требования к сетевому окружению

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate SWG)	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.
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверам технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного	Синхронизация времени.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			времени)/ Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного 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.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и	Сервис, необходимый для работы кластера

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			последующие узлы)	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 SWG до UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG SWG до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Связь с UserGate Log Analyzer	TCP	9713	Входящий (от LogAn к UG SWG)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer.
		2023		Построение SSH-туннеля

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			Входящий (от LogAn к UG SWG)	для обмена данными с помощью полученных ключей.
Подключение конечных устройств с установленным ПО UserGate Client	TCP	4045	Входящий (от конечного устройства на UG SWG)	Подключение конечных устройств и приём телеметрии для проверки комплаенса.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 – для LDAP и 636 - для LDAP over SSL).
Captive-портал и страница блокировки	TCP	443, 8043	Входящий (от браузера клиента на UG SWG)	Отображение страницы авторизации Captive-портала и страницы блокировки.
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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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 SWG)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UG SWG)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.
Прокси-агент	UDP	8090	Входящий (от агента на UG SWG)	Доступ к серверу UserGate, необходимый для работы прокси-агента, предоставляющего доступ в Интернет пользовател

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				ям, 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 электронну ю почту.
ICAP	TCP	1344	Исходящий (до серверов ICAP)	Сервис работы с серверами ICAP.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)/ Входящий (UserGate выступает в качестве DHCP-сервера)	Сервис службы DHCP.
BGP	TCP	179	Исходящий (передача информации соседним BGP-маршрутизат орам)/ Входящий (получение информации от соседних BGP-	Сервис динамическо й маршрутиза ции BGP.

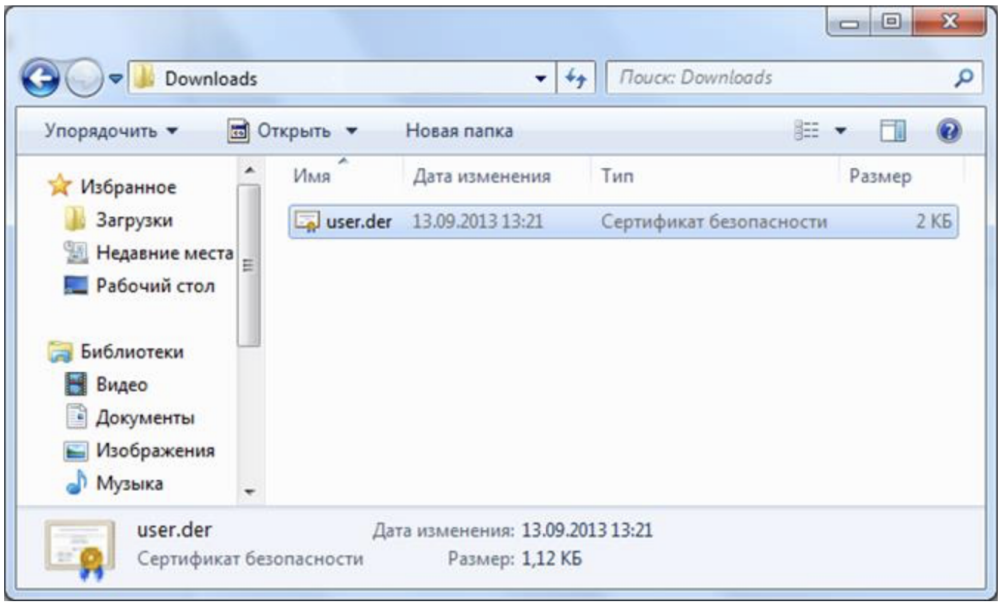
Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			маршрутизаторов)	
OSPF	89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам / Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF.
RIP	UDP	520	Исходящий (распространение соседним маршрутизаторам 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.

Установка сертификата локального удостоверяющего центра

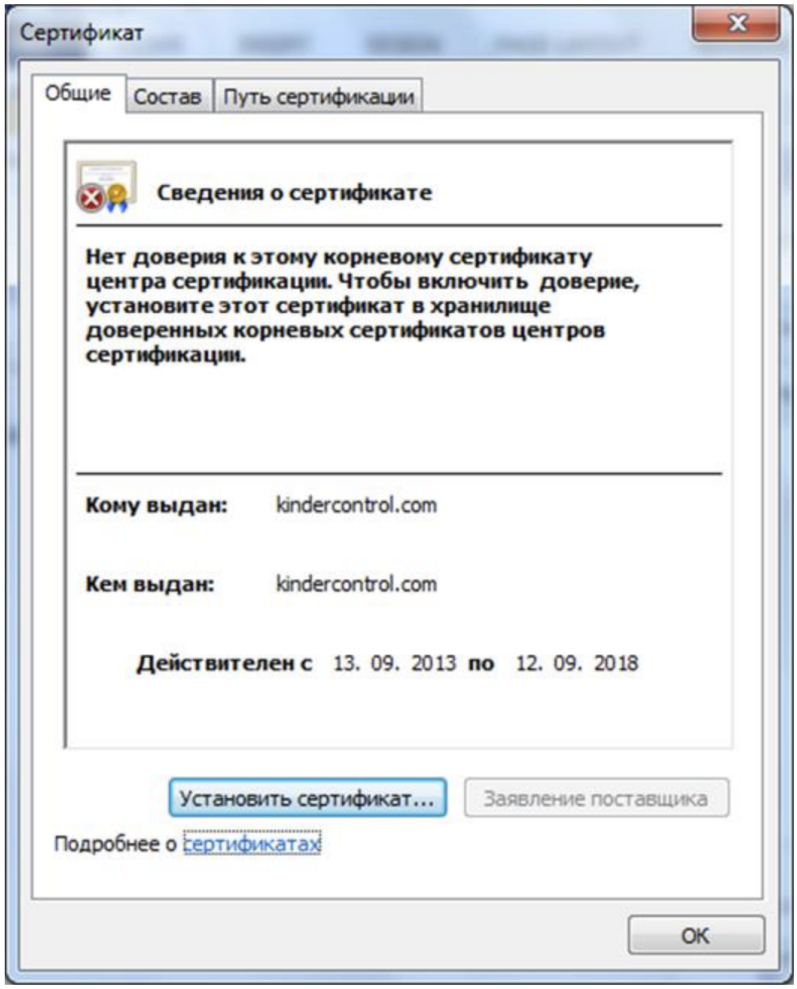
Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

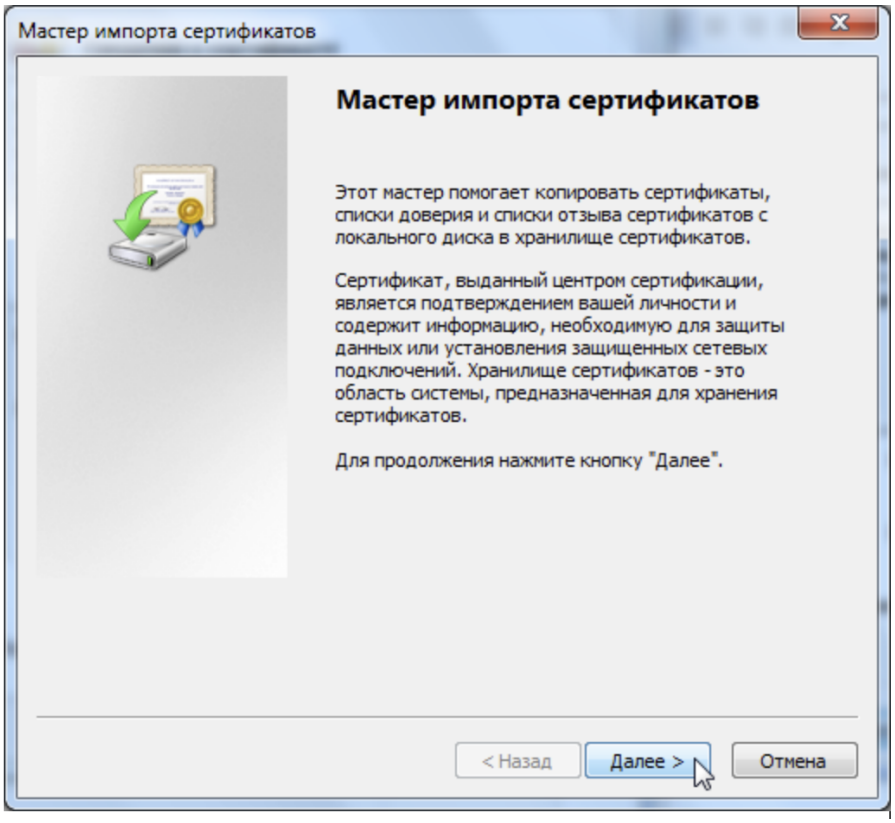
Откройте папку, куда вы скачали pem-сертификат, переименуйте его в `user.der` и дважды нажмите на него:



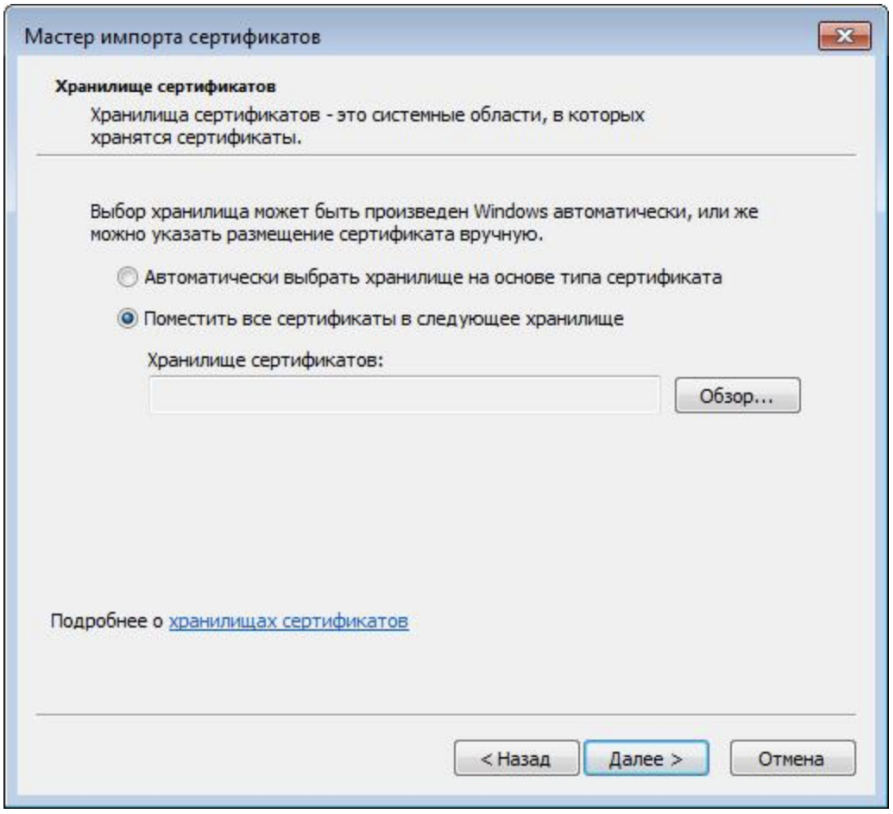
Откроется информация о сертификате. Нажмите **Установить сертификат**:



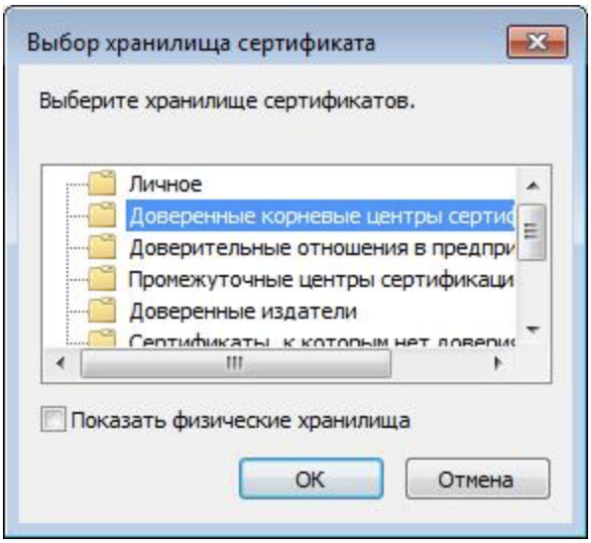
Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:



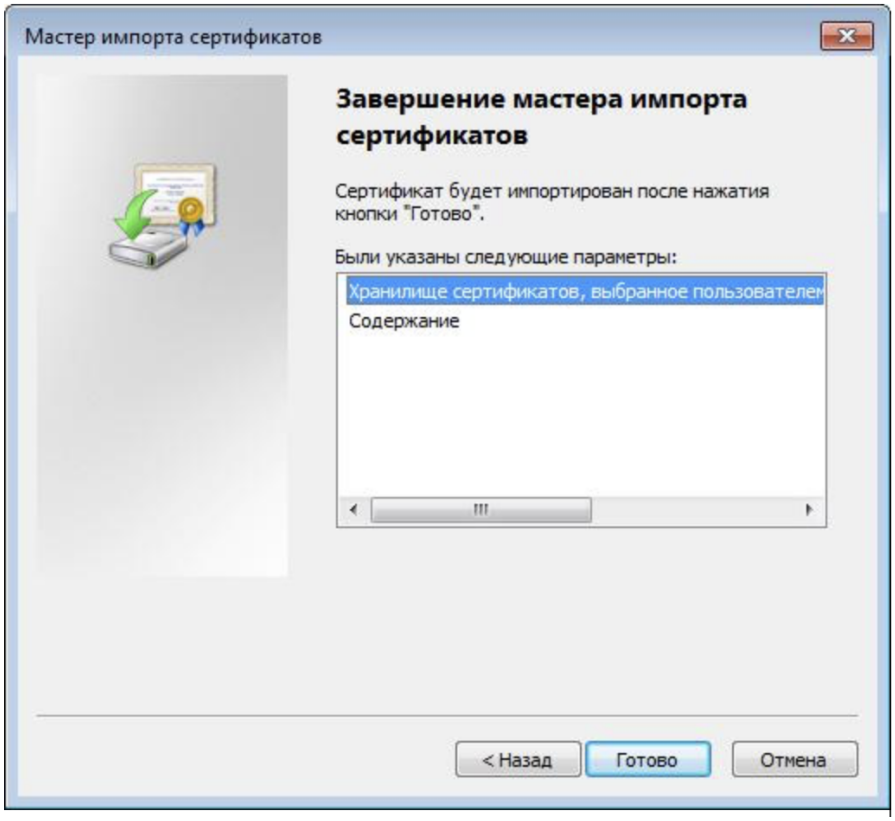
Выберите хранилище сертификата и нажмите **Обзор**:



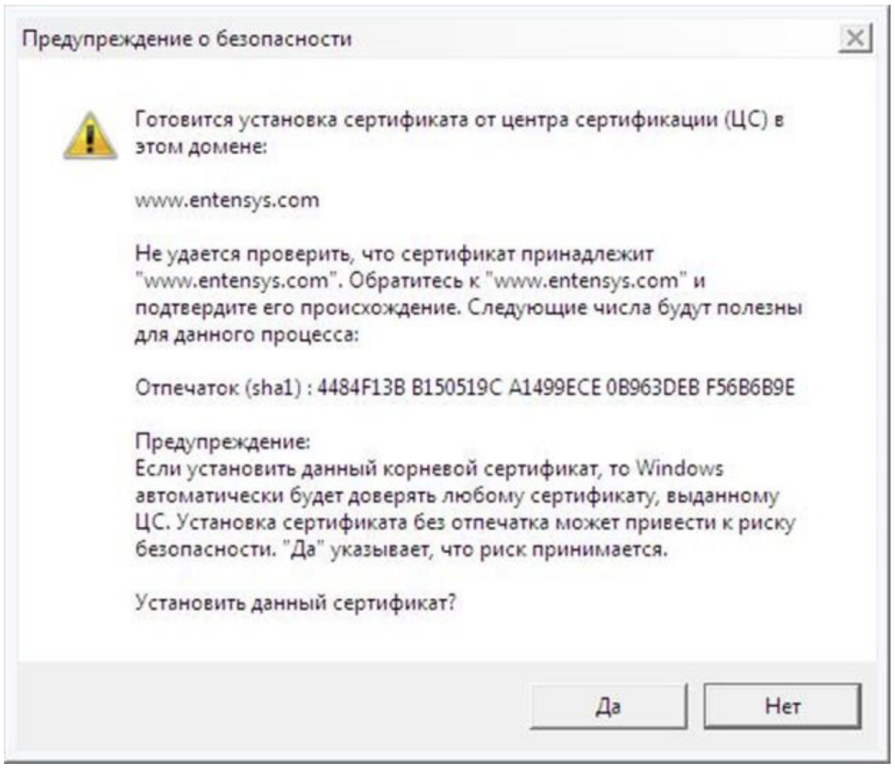
Выберите **Доверенные корневые центры сертификации** и нажмите **OK**:



Нажмите **Готово**:



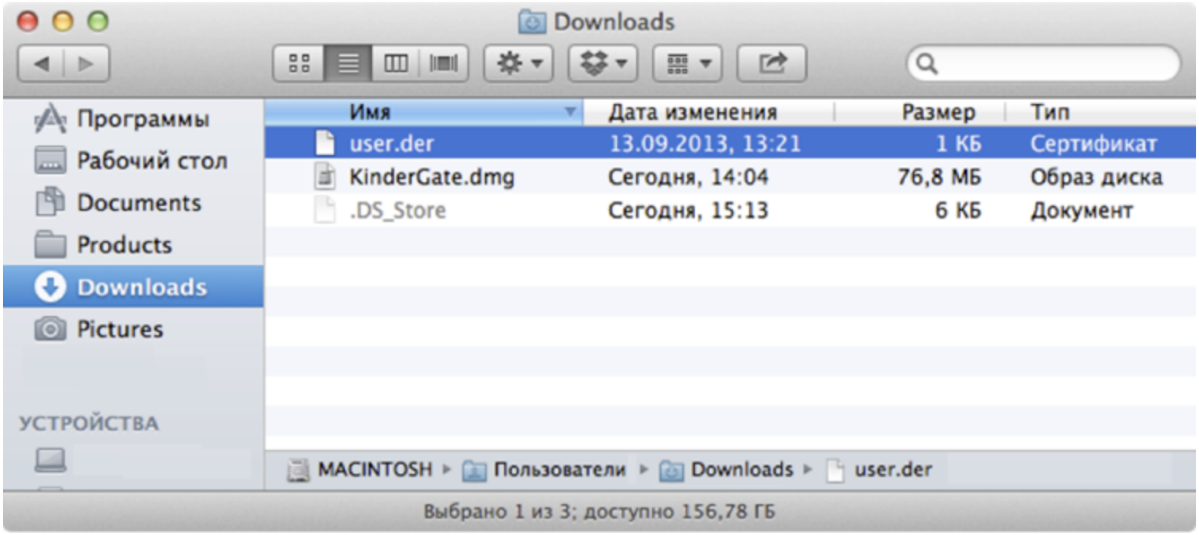
Когда появится предупреждение системы безопасности, нажмите **Да**:



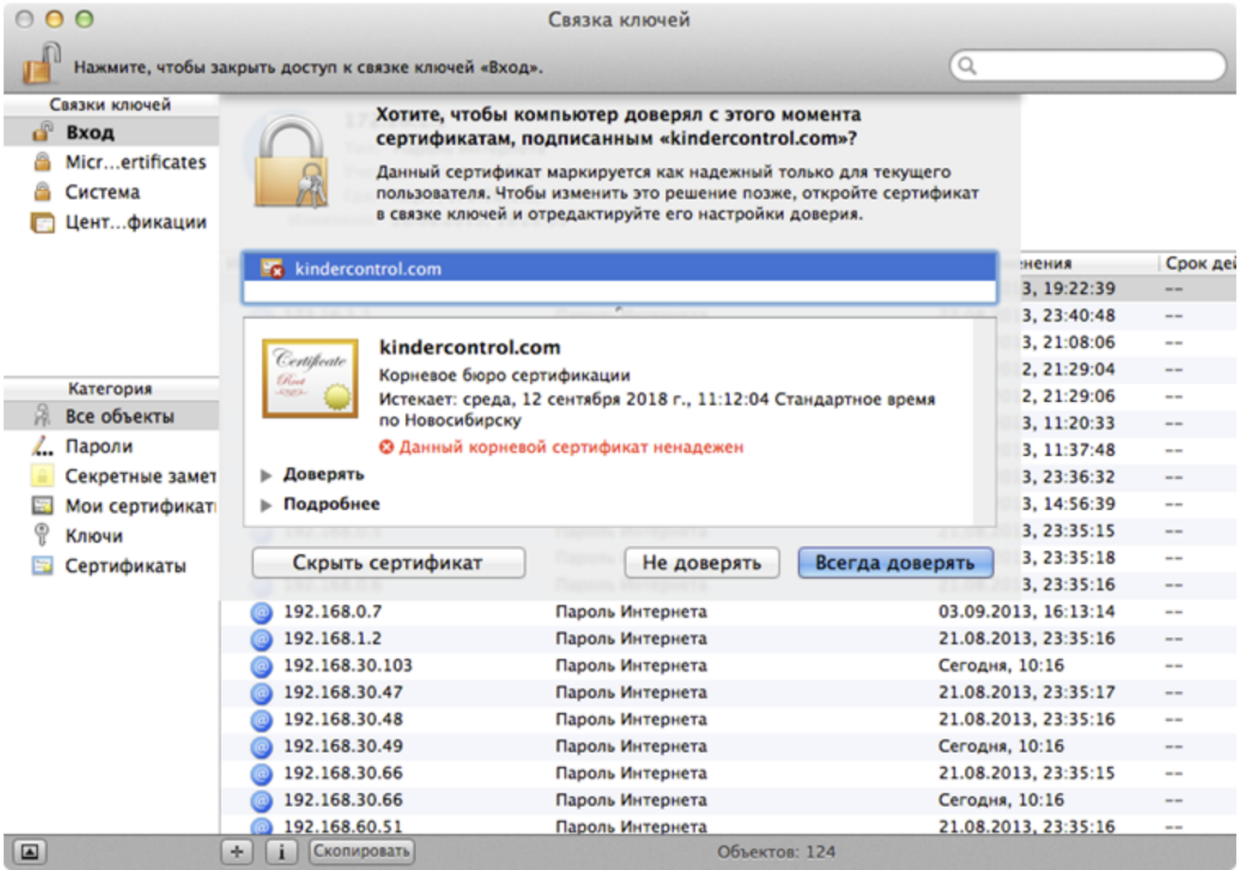
Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в macOSX

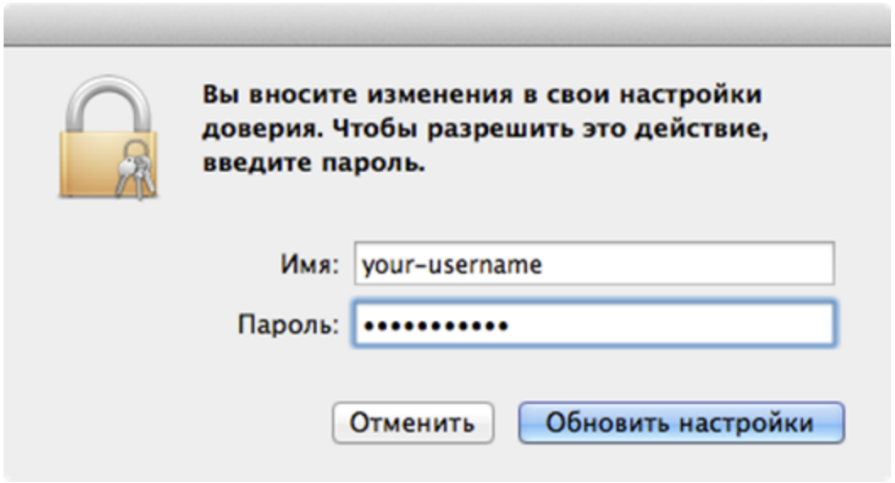
Перейдите в папку, куда вы скачали pem-сертификат и дважды нажмите на него:



Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:



Введите свой пароль для подтверждения данной операции:

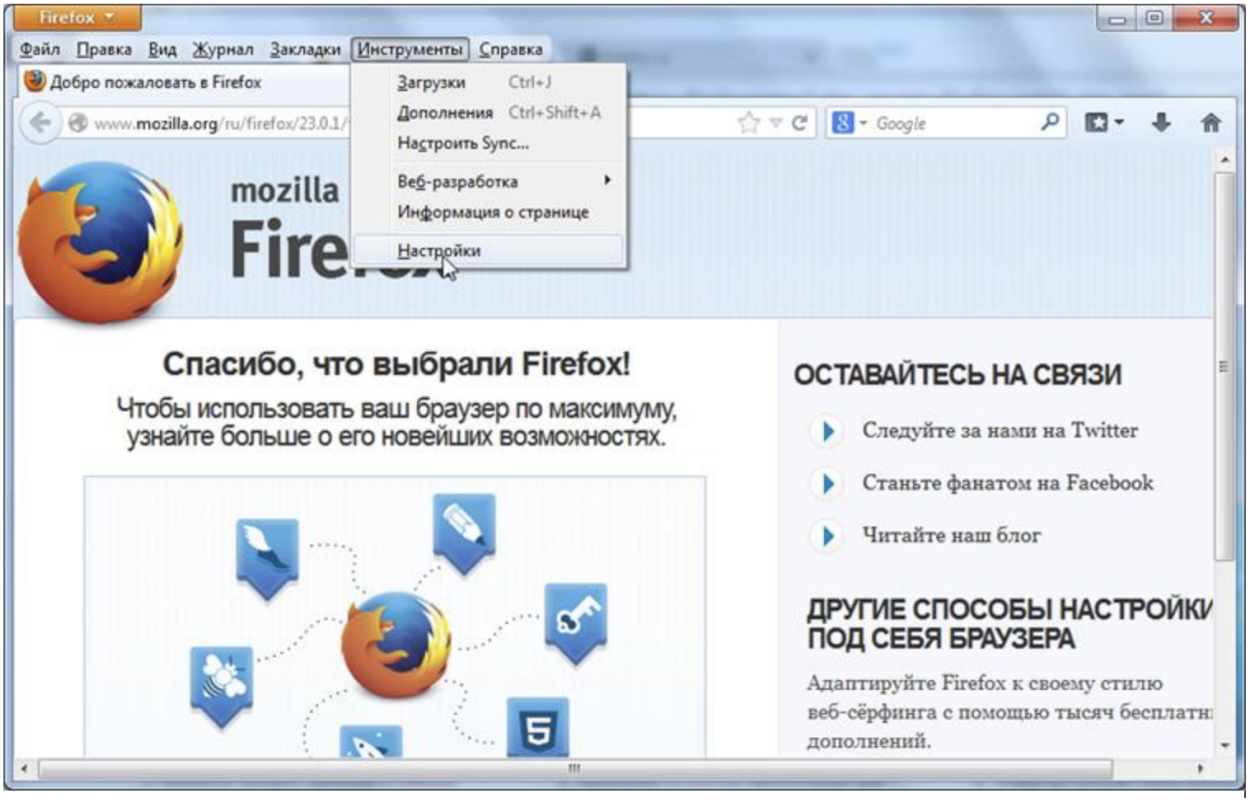


Сертификат установлен.

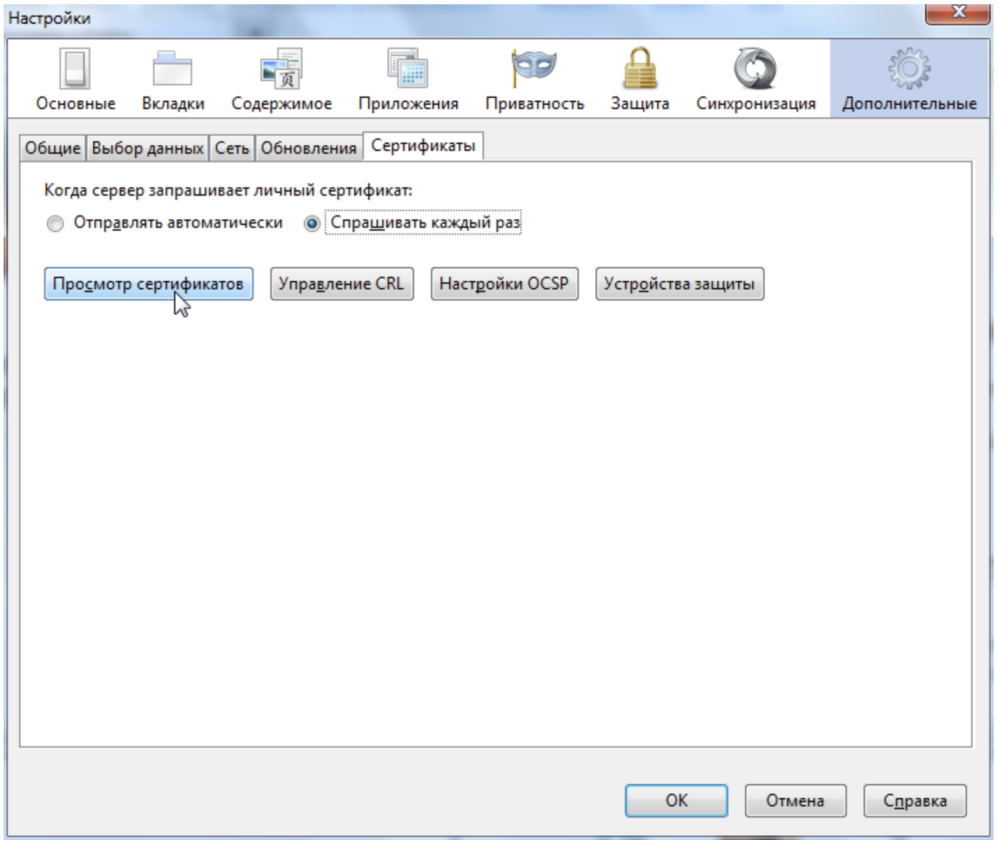
Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется одинаково для всех операционных систем. Рассмотрим установку на примере ОС Windows.

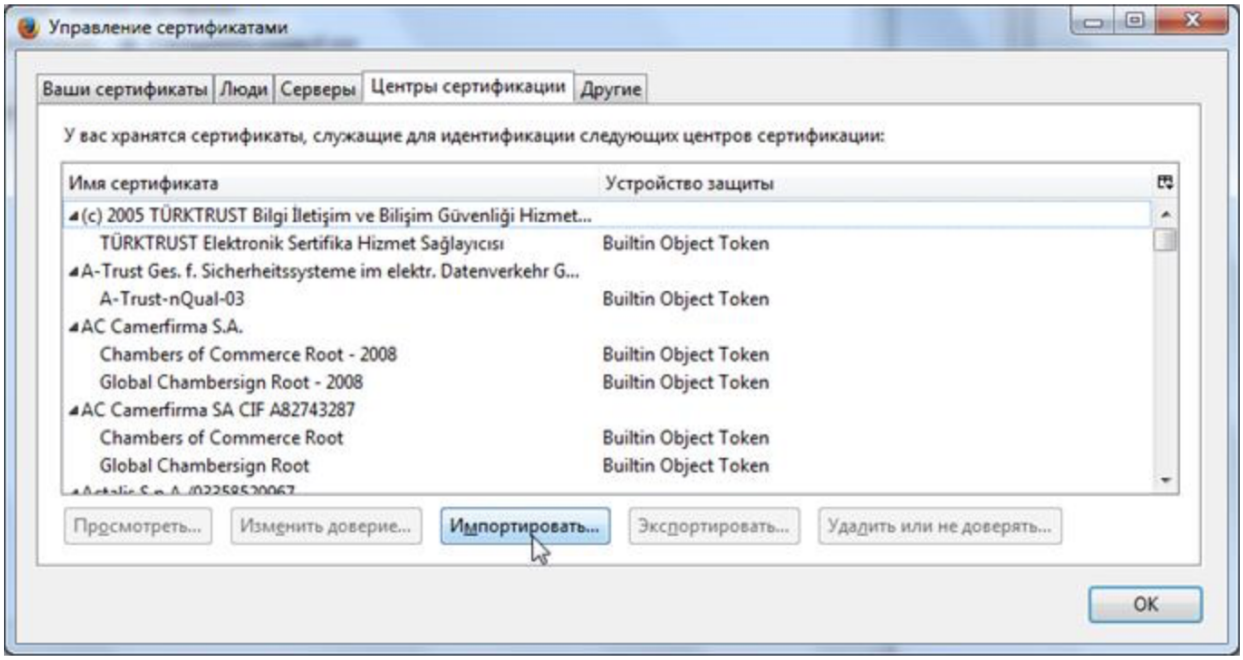
Откройте настройки браузера Firefox (**Инструменты → Настройки**):

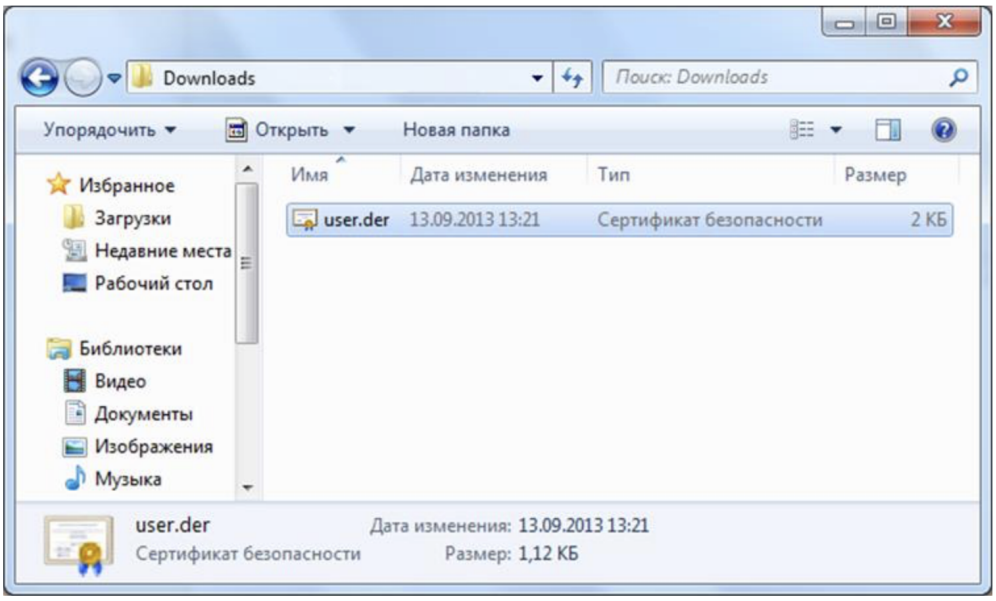


Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите **Просмотр сертификатов**:

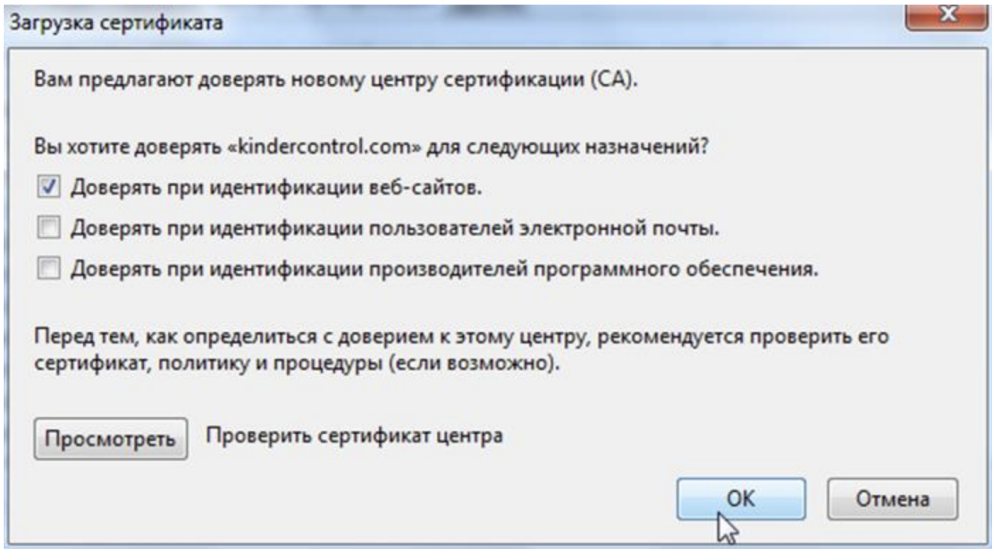


Нажмите **Импортировать** и укажите путь к скачанному PEM-сертификату:





Установите флажок **Доверять при идентификации веб-сайтов** и нажмите **OK**:



Установка сертификата завершена.

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.	SWG
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 1 — информационные;

Тип поля	Название поля	Описание	Пример значения
			• 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
	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.	SWG
	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 устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было	{"id": 39,"name":"Social

Тип поля	Название поля	Описание	Пример значения
		создано событие, например, причина блокировки сайта.	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 содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com

Тип поля	Название поля	Описание	Пример значения
	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 индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted

Тип поля	Название поля	Описание	Пример значения
	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
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	cn1Label		Packets sent

Тип поля	Название поля	Описание	Пример значения
		Поле используется для указания количества переданных пакетов в направлении источник — назначение.	
	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**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate

Тип поля	Название поля	Описание	Пример значения
	Device Product	Тип продукта.	SWG
	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 устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id": 39,"name":"Social Networking","threat _level":3}

Тип поля	Название поля	Описание	Пример значения
	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 содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/

Тип поля	Название поля	Описание	Пример значения
	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 индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone

Тип поля	Название поля	Описание	Пример значения
	cs3	Название зоны назначения.	Untrusted
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Computers & Technology
	cn1Label	Поле указывает исходный ответ сервера.	Response
	cn1	Код ответа HTTP.	302

Примечание

Общее правило для компактного формата — значения некоторых полей обрезаются по длине до 80 символов. Например, список url-категорий, url, имя пользователя, имя правила, имя зоны, и т.д.

Формат журнала DNS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	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

Тип поля	Название поля	Описание	Пример значения
			уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	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

Тип поля	Название поля	Описание	Пример значения
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS об ычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего пра вила.	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	Source Country

Тип поля	Название поля	Описание	Пример значения
		указания страны источника.	
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	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

Тип поля	Название поля	Описание	Пример значения
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала DNS **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	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
	act	Действие, принятое устройством в соответствии с	block

Тип поля	Название поля	Описание	Пример значения
		настроенными политиками.	
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS об

Тип поля	Название поля	Описание	Пример значения
			ычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего пра вила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Поле используется для указания передаваемых данных.	Data
	cs4	Передаваемые данные.	{"question": [{"domain":"google.com","type":"A","class":"IN"}], "answer": [{"domain":"google.com","type":"TXT","class":"IN","ttl": 5,"data":"Blocked"}, {"domain":"google.com","type":"A","class

Тип поля	Название поля	Описание	Пример значения
			":"IN","ttl": 5,"data":"10.10.0.1"}] }
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21

Тип поля	Название поля	Описание	Пример значения
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1		

Тип поля	Название поля	Описание	Пример значения
		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent

Тип поля	Название поля	Описание	Пример значения
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный

Тип поля	Название поля	Описание	Пример значения
			уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08

Тип поля	Название поля	Описание	Пример значения
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)

Тип поля	Название поля	Описание	Пример значения
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted

Формат журнала 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.	SWG
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	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: 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-1-5-21-3795870133-5220325-21257

Тип поля	Название поля	Описание	Пример значения
			45684-513} % {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 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

Тип поля	Название поля	Описание	Пример значения
			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 соб ытия журнала Windows (Система\Безопас ность\Приложени е и т. д.).	logEventType
	cn3	Тип события журнала Windows.	4
	cs1Label	Поле используется для указания идентификатора конечного устройства — источника события.	endpointId

Тип поля	Название поля	Описание	Пример значения
	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
	cs4	Категория события.	Group Membership
	cs5Label	Поле используется для указания файла журнала Windows.	logFile
	cs5	Файл журнала Windows	Security

Тип поля	Название поля	Описание	Пример значения
	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}\\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-1-5-21-3795870133-5220325-21257

Тип поля	Название поля	Описание	Пример значения
			45684-572}\\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.	SWG
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: • 0 — emergencies; • 1 — alerts; • 2 — critical; • 3 — errors; • 4 — warnings; • 5 — notifications; • 6 — informational; • 7 — debugging.
CEF [расширение]	**rt**	Время, когда было получено событие:	1701085036026

Тип поля	Название поля	Описание	Пример значения
		миллисекунды с 1 января 1970 года.	
	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	Поле используется для указания имени устройства, на котором произошло событие.	Hostname
	cs1	Имя компьютера, на котором произошло событие.	node1

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для указания приложения, вызвавшего событ ие.	Tag
	cs2	Приложение, вызвавшее событ ие.	org.gnome.Shell.desktop
	cs3Label	Поле используется для указания идентификатора процесса события.	ProcessID
	cs3	PID процесса вызвавшего событие.	3036
	cs4Label	Поле используется для указания срабатывания правила.	Rule
	cs4	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages

Формат журнала RADIUS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	Source	Название журнала.	radius
	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	Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
	suser	Имя пользователя.	Unknown, если пользователь неизвестен.
	src_ip	IP-адрес источника, откуда пришло сообщение.	192.168.57.4
	dst	IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
	dvc	IP-адрес пользователя (fra med ip address).	192.168.57.29
	cs1Label	Поле используется для указания группы, в которой состоит пользователь.	user groups

Тип поля	Название поля	Описание	Пример значения
	cs1	Строка групп в которых состоит пользователь.	test_group

Формат журнала UserID

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	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-1-5-21-3795870133-5220

Тип поля	Название поля	Описание	Пример значения
			325-2125745684-512"], "user_sid":"S-1-5-21-3795870133-5220325-2125745684-1103","login":"user1","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 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
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

Название поля	Описание	Пример значения
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-1-5-21-3795870133-5220325-2125745684-512}\r\n\t\t% {S-1-5-21-3795870133-5220325-2125745684-572}\r\n\t\t% {S-1-5-64-10}\r\n\t\t% {S-1-16-12288}\r\n\r\nThe subject fields indicate the 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).

Название поля	Описание	Пример значения
		\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-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t% {S-1-5-32-544}\\r\\n\\t\\t% {S-1-5-32-555}\\r\\n\\t\\t% {S-1-5-32-545}\\r\\n\\t\\t% {S-1-5-32-554}\\r\\n\\t\\t% {S-1-5-2}\\r\\n\\t\\t%{S-1-5-11} \\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t% {S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t% {S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t% {S-1-16-12288}']
error	Код ошибки из журнала AD, которая произошла при получении данных.	0
status	Описание ошибки из журнала AD, которая	

Название поля	Описание	Пример значения
	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	Тип источника события syslog. Например, user-level messages. Подробнее о значениях syslog facility смотрите в RFC 5424.	1
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

Название поля		Описание	Пример значения
app_name		Приложение, вызвавшее событие.	org.gnome.Shell.desktop
process_id		PID процесса, вызвавшего событие.	3036
data		Описание события.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"console.assert\", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
rule	**guid**	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages
	type	Тип сработавшего правила.	

Описание журнала RADIUS

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
event_type	Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
action	Действие, принятое устройством в соответствии с настроенными политиками.	login
src_ip	IP-адрес источника, откуда пришло сообщение.	192.168.57.4

Название поля		Описание	Пример значения
nas_ip		IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
framed_ip		IP-адрес пользователя.	192.168.57.29
rule	**guid**	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
user	**guid**	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name	Имя пользователя.	user_name
	groups	Название группы, в которой состоит пользователь.	test_group

Описание журнала UserID

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons	Причина, по которой было создано событие.	{\"user_groups_sids\": [\"S-1-5-21-3795870133-5220325-2125745684-513\", \"S-1-5-21-3795870133-5220325-2125745684-512\", \"S-1-5-21-3795870133-5220325-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-5220325-2125745684-1103\",\"login\": \"user1\",\"domain\":\"DEV\", \"event_id\":4624}

Название поля			Описание	Пример значения
action			Действие, принятое устройством в соответствии с настроенными политиками.	login
src_ip			IPv4 источника события.	10.10.0.11
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name		Название правила, срабатывание которого вызвало событие.	dev.local
	type		Тип сработавшего правила.	syslog
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name		Имя пользователя.	user1
	groups	**guid**	Уникальный идентификатор группы, в которой состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local

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).

Наименование	Описание
3	Список IP-адресов доступных шлюзов.
6	Список DNS-серверов.
7	Список лог-серверов (MIT-LCS UDP).
9	Список LPR-серверов (RFC 1179).
13	Размер загрузочного образа для клиентов.
15	Имя домена.
16	Swap-сервер.
17	Путь корневого каталога для клиента.
18	Путь расширений BOOTP.
19	Применение пересылки IP-датаграмм.
20	Использование маршрутизации удаленного источника.
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.

Наименование	Описание
36	Необходимость использования инкапсуляции данных Ethernet.
37	Значение TTL для TCP-пакетов.
38	Интервал отправки контрольных пакетов TCP (TCP keep-alive).
40	Домен NIS.
41	Список серверов NIS.
42	Список серверов времени NTP.
44	Список IP-адресов серверов NetBIOS.
45	Список IP-адресов серверов рассылки датаграмм NetBIOS.
46	Тип узла NetBIOS.
47	Область NetBIOS.
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).

Наименование	Описание
69	Список серверов SMTP.
70	Список серверов POP3.
71	Список серверов NNTP.
74	Список серверов IRC.
77	Класс пользователя.
80	Опция позволяет получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
93	Архитектура системы клиента DHCP.
94	Идентификатор сетевого интерфейса клиента DHCP.
97	Идентификатор клиента на основе UUID/GUID.
119	Список поиска DNS.
120	Список серверов SIP.
121	Список бесклассовых статических маршрутов.
125	Указание информации о поставщике.
255	Конец списка опций; обязательно должен присутствовать последним.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Криптомайнеры
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения
	Мода и красота
	Отдых и оздоровление

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
	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 преимуществ использования отдельных	Ненависть и нетерпимость

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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
Личная и немодерируемая информация.	Персональные сайты

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги	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 продукции и табачных изделий	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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
Преступления-клевета, экстремизм	Преступная деятельность

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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; реклама табака и изделий из него	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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