UserGate

UserGate WAF 7.6.x
Руководство администратора

Оглавление

ВВЕДЕНИЕ

Общие сведения

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

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

Основные функции UserGate WAF:

- Анализ, фильтрация, модификация и блокирование трафика HTTP/HTTPS версии 0.9, 1.0, 1.1.
- Межсетевой экран с возможностью блокировки по IP-адресам, узлам и GeoIP.
- Создание правил анализа HTTP-трафика (WAF-правил) с использованием языка UPL (UserGate Policy Language).
- Использование наборов объектов (например, групп IP-адресов, URL, номеров телефонов) при создании WAF-правил.
- Детальный анализ результатов срабатывания WAF-правил. в разделе «Атаки» в веб-консоли.
- Автоматическая выгрузка журналов сработавших WAF-правил на удаленный сервер по SSH, FTP, syslog.

Инструменты базовой диагностики сети.

- Публикация внутренних веб-сервисов через UserGate WAF с помощью правил.

ЛИЦЕНЗИРОВАНИЕ

Лицензирование UserGate WAF

Для работы UserGate WAF необходимо приобрести базовую лицензию, которая предоставляет доступ к основным функциям устройства. Дополнительно лицензируемые модули дают право на использование расширенных функций и на получение обновлений программного обеспечения.

Базовая лицензия

Лицензирование UserGate WAF выполняется по параметрам производительности платформы.

В процессе активации базовой лицензии проверяется следующее:

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

При попытке регистрации некорректного оборудования с помощью ключа с ограничением по производительности появится ошибка: «Конфигурация сервера не соответствует лицензированным характеристикам, например увеличено число ядер процессора».

> **Примечание**
>
> **Если виртуальная машина зарегистрирована с помощью корректного ключа, а в дальнейшем в нее будут добавлены дополнительные ядра, то активным в виртуальной машине будет только лицензированное количество ядер.**

> **Примечание**
>
> **Базовая лицензия на продукт является бессрочной (обновления ПО и библиотек не включены). Базовая лицензия включает в себя модуль Security Update (SU) сроком на один год.**

Дополнительно лицензируемые модули

Модуль	Описание
Security Updates (SU)	Модуль SU дает право на получение обновлений: • ПО WAF; • модулей экспертизы от UserGate; ◦ Защита от известных атак из списка «OWASP top 10»; ◦ User-Agent. Действует один год, по истечении этого срока: • Базовые функциональности ПО продолжают работать без изменений и ограничений. • Перестает обновляться ПО. В качестве обновления может быть скачана и установлена только версия, которая была актуальна в момент окончания срока действия ключа. • Перестают обновляться базы экспертизы. Полученные ранее базы экспертизы продолжают работать. Для дальнейшего получения обновлений необходимо продлить лицензию на модуль SU
Cluster	Модуль включает лицензию на работу устройств UserGate в режиме «кластер». Срок действия лицензии 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 все в порядке устройство будет работать в штатном режиме. При успешной проверке в журналах отображается запись об этом событии.

Если серверы лицензирования недоступны, делается 14 попыток подключения с интервалом в 120 секунд. В случае неуспеха попытки прекращаются на сутки, после чего снова следуют 14 попыток подключения к серверу активации. В случае если в период действия лицензии не удается подключиться к серверу активации, лицензия блокируется в связи с истечением срока действия (модули, лицензия которых просрочена, перестают работать). При каждой ошибке подключения к серверу активации в журналы заносится сообщение об ошибке.

Порядок действий при онлайн-активации

Для регистрации устройства:

1. В веб-консоли администратора устройства выберите раздел **Дашборды** и перейдите на вкладку **NOC**.

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.

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 администратора устройства выберите раздел **Дашборды** и перейдите на вкладку **NOC**.

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 на вкладке **NOC** 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».

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Общие сведения

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

Развертывание виртуального образа

UserGate WAF 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 4-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 посмотреть 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. Настройте параметры виртуальной машины. В зависимости от ожидаемой нагрузки увеличьте размер оперативной памяти виртуальной машины. Рекомендованное минимальное значение — 12 ГБ.

4. 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 более.

Для систем виртуализации QEMU-KVM размер системной области по умолчанию, составляет 8 ГБ. Система, при первом запуске, сама определит наличие дополнительного диска и расширит свои системные разделы.

Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:

```
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 **Factory reset**. Система UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в четвертом пункте.

UserGate поставляется с четырьмя интерфейсами, назначенными в зоны:

- **Management** — первый интерфейс виртуальной машины;
- **Trusted** — второй интерфейс виртуальной машины;

- **Untrusted** — третий интерфейс виртуальной машины;
- **DMZ** — четвертый интерфейс виртуальной машины.

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
```

При первоначальном старте, после сброса в первоначальное состояние (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.

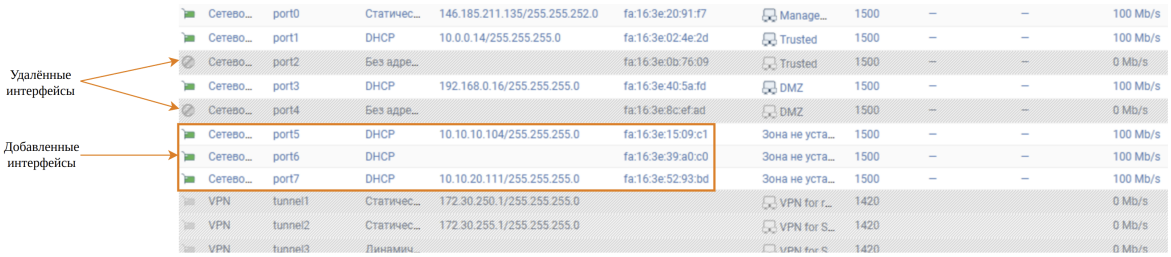
```
Admin@canntoralcti> show network interface-mapping

+-----------+----------------------+
| 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 |
+-----------+----------------------+
```

- Удалённые 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 рестарта 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 происходят при первом запуске в виртуальной среде пользователя. При подготовке пользователями собственного виртуального образа устройства UserGate для разворачивания его 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 настроек склонированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие vm источника.

Оптимизация производительности сетевых интерфейсов на основе virtio

Для оптимизации производительности сетевых интерфейсов на основе virtio в средах виртуализации KVM, oVirt, zVirt рекомендуется на гипервизоре включать режим Multi Queues и устанавливать 8 очередей на сетевой интерфейс.

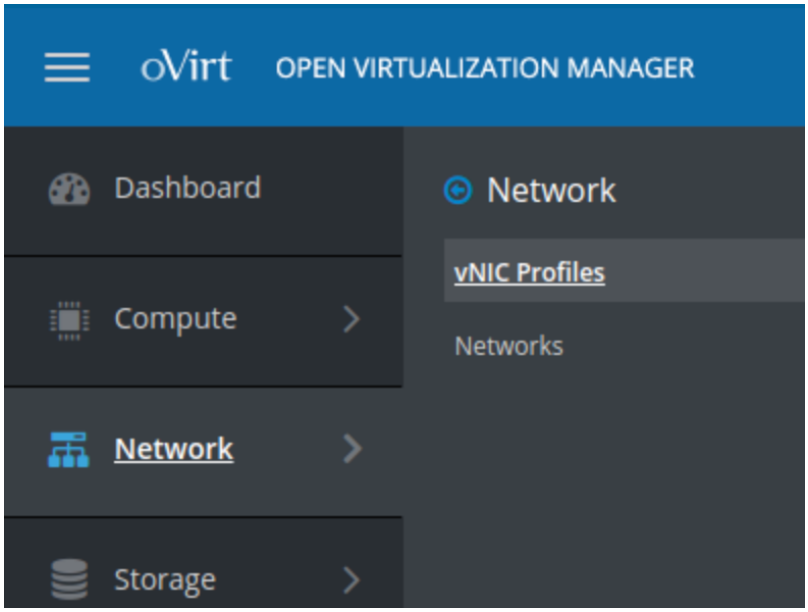
Например, в случае платформы OVirt (см. документацию oVirt), для того чтобы выставить 8 очередей для vNIC, необходимо подключиться к CLI гипервизора и ввести команду:

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

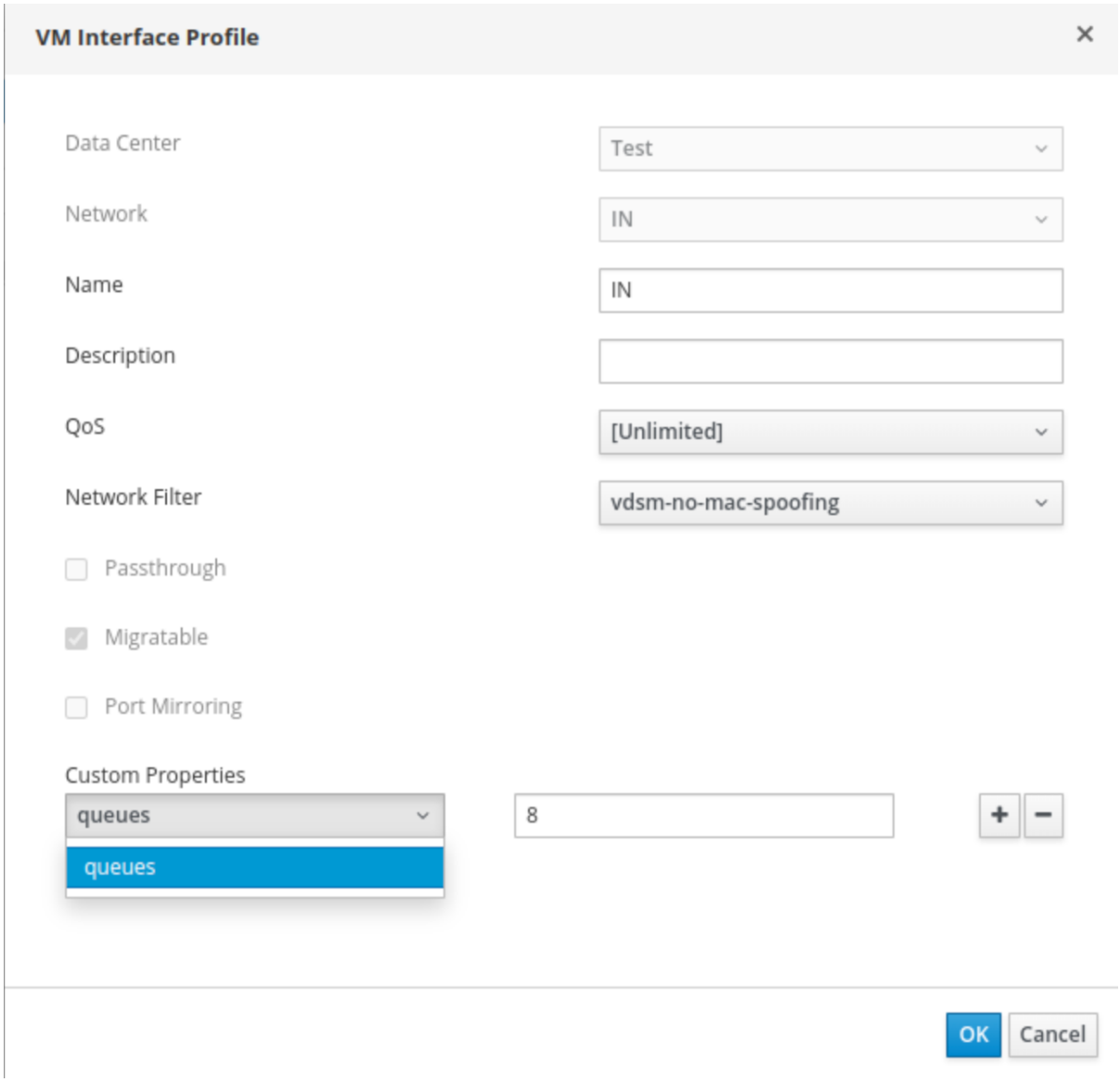
Вместо параметра `other-nic-properties` нужно вставить список существующих кастомизированных правил (если есть). Посмотреть, существуют ли такие правила, можно командой:

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

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



Выбрать редактирование профиля сетевых карт, назначенного для WAF, в выпадающем списке **Custom Properties** выбрать **queues**, после чего ввести нужное количество очередей.



Требования к сетевому окружению

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

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

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

- Обеспечение репликации настроек — порты TCP 4369, TCP 9000-9100;

- Сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности — в таблице ниже.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate WAF)	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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
NTP	UDP	123	Исходящий (до сервера точного времени)/ Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного времени)	Синхронизация времени.
DNS	TCP/UDP	53	Входящий (от клиентов к серверу UserGate, если он выступает в качестве DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Резерв для кластера	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Резерв для UserGate Management Center	TCP	9712	Исходящий (от UG WAF до UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG WAF до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Резерв для UserGate Log Analyzer	TCP	9713	Входящий (от LogAn к UG WAF)	Первоначальная установка связи и обмен ключами шифрования с сервером

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				UserGate Log Analyzer.
		2023	Входящий (от LogAn к UG WAF)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP	Для версий 6.1.x: 1269 (передача данных на LogAn 6.1.x), 22699 (передача данных на LogAn 7.x.x) Для версий 7.0.x: 22699 (передача данных на LogAn 6.1.x), 22711 (передача данных на LogAn 7.x.x, с использованием SSL)	Исходящий (от UG WAF к LogAn)	Передача журналов и телеметрии на сервер LogAn.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 – для LDAP и 636 - для LDAP over SSL).
Kerberos	TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей по протоколу Kerberos.
NTLM	TCP	445	Исходящий (на сервер	Аутентификация

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			аутентификации NTLM)	пользователей по протоколу NTLM.
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
Агент терминального сервиса	UDP	1812, 1813	Входящий (от агента на UG WAF)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UG WAF)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
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.

Подключение к UserGate WAF

Интерфейс `port0` настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка выполняется 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, то для доступа к CLI необходимо использовать в качестве логина `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 WAF. После загрузки в консоли WAF будет указан полученный интерфейсом IP-адрес. Подключитесь к веб-консоли устройства по адресу: https://<WAF_IP_address>:8001 для дальнейшей активации продукта. • **Статический IP-адрес**. Включите UserGate WAF. Используя CLI, назначьте необходимый IP-адрес на интерфейс `port0`. Произведите первоначальную инициализацию в интерфейсе командной строки или подключитесь к веб-консоли UserGate WAF по указанному адресу (он должен иметь вид: https://<WAF_IP_address>:8001). Подробнее об использовании CLI — в разделе «Интерфейс командной строки»
2. Выберите язык	
3. Задайте пароль	
4. Настройте зоны, IP-адреса интерфейсов, подключите UserGate WAF 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
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 → Консоль администратора → Настройки** в секции **Серверы DNS** укажите IP-адреса DNS-серверов вашего провайдера или серверов, используемых в вашей организации. Подробнее об управлении DNS — в разделе «Общие настройки»

Шаг	Описание
7. Настройте время сервера	В разделе **Настройки → Консоль администратора → Настройки → Настройка времени сервера** настройте синхронизацию времени с серверами NTP.
8. Зарегистрируйте WAF	В разделе **Дашборды** на вкладке **NOC** в виджете **Лицензия** н ажмите **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 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»
10. Если необходимо, создайте дополнительных администраторов	В разделе **Настройки → Консоль администратора → Администраторы** создайте дополнительных администраторов системы, наделите их необходимыми полномочиями (ролями).

После выполнения этих шагов UserGate WAF готов к работе. Для более детальной настройки обратитесь к необходимым главам руководства администратора.

Автоматизация развертывания UserGate WAF с помощью Cloud-init

Cloud-init — индустриальный стандарт для кросс-платформенной инициализации виртуальных машин (инстансов) в облачных сервисах провайдеров. UserGate WAF 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 об использовании CLI — в разделе «Интерфейс командной строки».

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

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

Оба файла можно объединить в один файл, используя 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 WAF:

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

- Через подключаемый ISO-диск. Диск должен содержать 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:

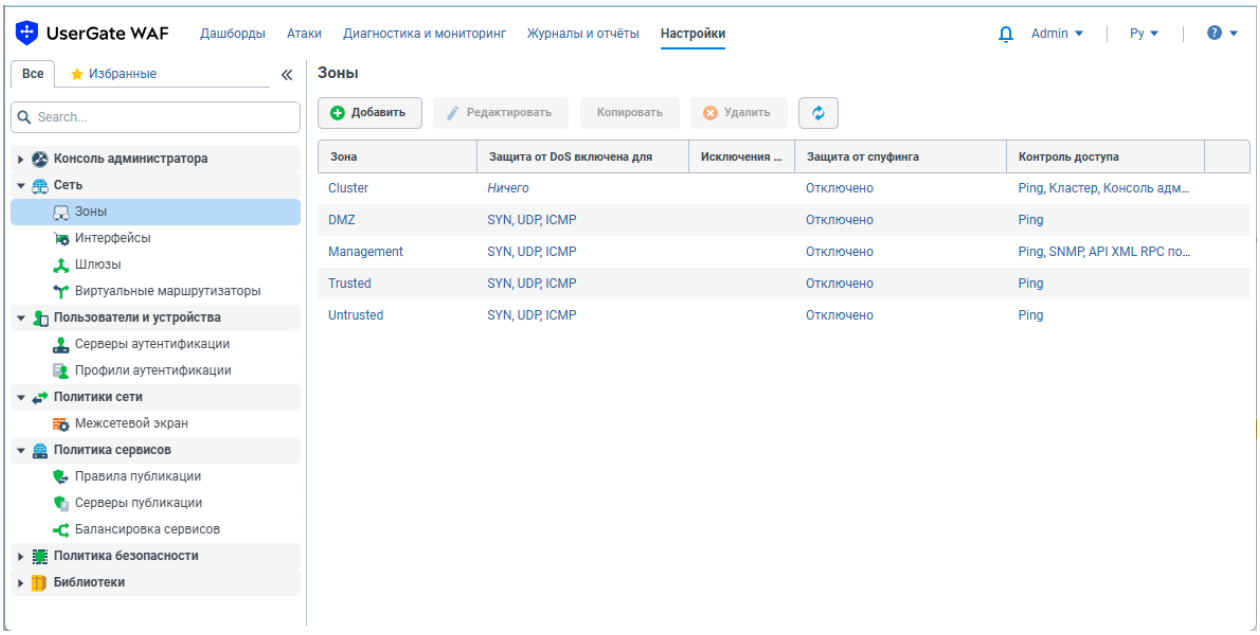
```
mkisofs -joliet -rock -volid "cidata" -output nocloud.iso meta-data
user-data vendor-data
```

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

ВЕБ-КОНСОЛЬ

Веб-консоль Usergate WAF

Все действия вы можете выполнять в веб-консоли, доступной после входа в UserGate WAF.



Главное меню

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

- **Дашборды** — страница со статистическими данными о состоянии устройства и результатах его работы, представленными в виде таблиц, списков и графиков. При входе в UserGate WAF эта страница открывается по умолчанию. Подробнее о дашбордах — в разделе «Работа с дашбордами и виджетами».
- **Атаки** — страница для отслеживания и анализа атак. Подробнее об атаках — в разделе «Просмотр обнаруженных атак».
- **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 и настройки экспорта журналов. Подробнее о журналах — в разделе «Журналы».
- **Настройки** — страница для настройки устройства и политики безопасности.

Прочие элементы управления

Также в верхней панели находятся следующие элементы управления:

- Центр уведомлений — содержит список уведомлений об изменениях в конфигурации устройства (таких как, изменения в WAF-профилях или в правилах публикации веб-сервисов).
- Логин вашей учетной записи — раскрывает меню для смены пароля учетной записи, выбора темы оформления веб-консоли, 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 веб-консоли.
- 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 веб-консоли

Все страницы, кроме страницы **Дашборды**, состоят из рабочей области и боковой панели. Содержимое и вид рабочей области зависят от выбранной страницы, информация может отображаться в виде таблицы, виджетов или блоков параметров. Боковая панель содержит список разделов, предоставляющих доступ к различным возможностям UserGate WAF, 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.

НАСТРОЙКА УСТРОЙСТВА

Настройка общих параметров

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

Блок параметров	Параметр	Описание
Настройки интерфейса	**Часовой пояс**	Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения времени и даты, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-консоли устройства по умолчанию
	Режим аутентификации веб-консоли	Доступны следующие режимы аутентификации: • **По имени и паролю**. Вход администратора в веб-консоль по логину и паролю учетной записи. • **По X.509-сертификату**. Вход администратора в веб-консоль по цифровому сертификату. Этот сертификат должен быть подписан сертификатом удостоверяющего центра, обеспечивающим

Блок параметров	Параметр	Описание
		доступ к веб-консоли, и установлен в браузере. При включении режима отключается аутентификация по логину и паролю, к ней можно вернуться с помощью команд CLI. • **Профиль клиентского сертификата.** Вход администратора в веб-консоль по сертификату инфраструктуры открытых ключей (PKI). Проверка подлинности этого сертификата выполняется с помощью профиля клиентского сертификата, обеспечивая тем самым безопасность сетевого соединения
	Профиль SSL для веб-консоли	Профиль SSL, с использованием которого создается защищенный канал для доступа к веб-консоли
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-консоли должна завершаться его сессия. Также необходимо включить параметр **Автоматическое закрытие сессии по таймеру**
	Автоматическое закрытие сессии по таймеру	При включенном параметре сессия администратора будет завершаться по истечении таймера автоматического закрытия сессии

Блок параметров	Параметр	Описание
		По умолчанию параметр отключен
Настройка времени сервера	**Использовать NTP**	При включенном параметре для синхронизации времени на устройстве будут использоваться NTP-серверы из указанного списка
	Основной NTP-сервер	Адрес основного сервера точного времени. Значение по умолчанию — **pool.ntp.org**
	Запасной NTP-сервер	Адрес запасного сервера точного времени
	Время на сервере (UTC)	Время на сервере UserGate WAF в часовом поясе UTC
Обновления ПО	**Канал обновлений**	Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate. Вы можете выбрать **Стабильные** (стабильные версии ПО) или **Бета** (версии ПО для бета-тестирования). Если настроена интеграция с UserGate Management Center, параметр примет значение **Management Center** и будет недоступен для изменения
	Обновления	Проверка наличия обновлений UGOS в репозитории UserGate. После проверки вы можете вручную загрузить и установить доступные обновления. В процессе установки обновл

Блок параметров	Параметр	Описание
		ения UGOS вы можете создать точку восстановления. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню после установки обновления UGOS
	Офлайн-обновление	Загрузка файла обновления UGOS офлайн
Обновления библиотек	**Обновления**	Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate. После проверки вы можете вручную обновить необходимые библиотеки
	Расписание автоматических обновлений	Настройка расписания автоматического обновления библиотек. При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0–59> <часы: 0–23> <дни месяца: 1–31> <месяцы: 1–12> <дни недели: 0–6, где 0 — воскресенье>. Для ручного ввода вы можете использовать следующие символы: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.

Блок параметров	Параметр	Описание
		• 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 выбранной библиотеки будет применено ко всем библиотекам в списке. **Примечание** **В целях уменьшения нагрузки на систему рекомендуется настраивать расписание автоматического обновления только для используемых библиотек**
Модули	**Настройка LLDP**	Настройка использования LLDP-протокола канального уровня, с помощью которого UserGate WAF обменивается данными с соседними устройствами в локальной сети. Для настройки доступны следующие параметры: • **Transmit delay** — интервал отправки LLDP-пакетов (от 1 до 3600 секунд). Изменяя этот

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

Блок параметров	Параметр	Описание
	Код устройства	Уникальный код UserGate WAF для интеграции с внешним сервером UserGate Log Analyzer или UserGate SIEM
Агент UserGate Management Center	**Настройка агента**	Настройка агента для интеграции с UserGate Management Center (UGMC). Для настройки доступны следующие параметры: • **Включено** — управление состоянием подключения UserGate WAF к UGMC. • **Адрес сервера UserGate Management Center** — адрес сервера UGMC в формате IPv4-адреса или FQDN (возможно использование IDN-адреса). • **Код устройства** — идентификатор UserGate WAF для подключения к UGMC
Серверы DNS	**Системные DNS-серверы**	Настройка IP-адресов DNS-серверов

Управление устройством

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

- параметры диагностики;
- операции с сервером;
- резервное копирование;
- экспорт и импорт настроек.

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 диагностики

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

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** — перезагрузка WAF. • **Выключить** — выключение WAF
Проверка лицензии и обновлений вышестоящим прокси-сервером	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО WAF. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate. При наличии обновлений в разделе **Управление устройством → Операции с сервером** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя WAF.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния WAF, как это описано в разделе «Системные утилиты». Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее

Наименование	Описание
	состояние устройства в случае возникновения каких-либо проблем во время применения обновлений
Шаг 2. Установить обновления	В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки WAF будет перезагружен

Управление резервным копированием

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

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе **Управление устройством → Управление резервным копированием** нажать **Создание резервной копии**. Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где: *PRODUCT* — тип продукта: WAF, LogAn, MC; *NODE-NAME* — имя узла UserGate; *DATE* — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки **Остановить**. Запись о создании резервной копии отобразится в журнале событий устройства

Для восстановления состояния устройства необходимо выполнить следующие действия:

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

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

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе **Управление устройством → Управление резервным копированием** нажать кнопку **Добавить**, указать имя и описание правила
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки. Путь на сервере должен уже существовать. Сама система несуществующие папки не создаст! В случае использование SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать **Настроить SSH-ключ** и указать **Сгенерировать ключи** или **Импортировать ключ**. **Важно!** При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей **/home/user/.ssh/** в файле **authorized_keys**. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка **Проверить соединение**); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. **Важно!** Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)

Наименование	Описание
	Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

Экспорт и импорт настроек

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

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

- Настройки DNS.
- Настройки всех интерфейсов.
- Настройки шлюзов.
- Настройки виртуальных маршрутизаторов (VRF).
- Настройки зон.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Экспорт → Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит текущие настройки сервера под именем

Наименование	Описание
	utm-utmcore@nodename_version-YYYYMMDD_HHMMSS.bin, где: nodename — имя узла WAF version — версия UGOS YYYYMMDD_HHMMSS — время выгрузки настроек в часовом поясе UTC, например: utm-utmcore@heashostatot_6.1.1.10462R-1_20210511_095942

Для применения созданных ранее настроек необходимо выполнить следующие действия:

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

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

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе **Управление устройством → Экспорт и импорт настроек** нажать кнопку **Добавить**, указать имя и описание правила
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль/Подтверждение пароля** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде:

Наименование	Описание
	(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа

Управление доступом к веб-консоли UserGate WAF

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

> **Примечание**
>
> **При первоначальной настройке UserGate WAF создается локальный суперпользователь Admin.**

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

Наименование	Описание
Шаг 1. Создать профиль доступа администратора.	В разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки

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

При создании профиля доступа администратора необходимо указать следующие параметры:

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

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

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

Для настройки этих параметров необходимо:

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

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

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

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

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Подробнее о настройке контроля доступа к зонам — в разделе «Настройка зон».

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

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

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

Наименование	Описание
	`openssl req -x509 -subj '/C=RU/ST=Moscow/O=MyCompany /CN=ca.mycompany.com' -newkey rsa:2048 -keyout ca-key.pem -out ca.pem -nodes` `openssl rsa -in ca-key.pem -out ca-key.pem` В файле ca-key.pem будет находиться приватный ключ сертификата, в ca.pem — публичный ключ. Импортировать публичный ключ в UserGate WAF
Шаг 3. Создать сертификаты для учетных записей администраторов.	С помощью средств сторонних утилит (например, openssl) создать сертификаты для каждого из администраторов. Необходимо, чтобы поле сертификата **Common name** в точности совпадало с именем учетной записи администратора, как она была создана в UserGate WAF. Для openssl и пользователя Administrator54 команды будут следующими: `openssl req -subj '/C=RU/ST=Moscow/O=MyCompany /CN=Administrator54' -out admin.csr -newkey rsa:2048 -keyout admin-key.pem -nodes`
Шаг 4. Подписать сертификаты администраторов, созданным на шаге 2 сертификатом удостоверяющего центра.	С помощью средств сторонних утилит (например, openssl) подписать сертификаты администраторов сертификатом удостоверяющего центра веб-консоли. Для openssl команды будут следующими: `openssl x509 -req -days 9999 -CA ca.pem -CAkey ca-key.pem -set_serial 1 -in admin.csr -out admin.pem` `openssl pkcs12 -export -in admin.pem -inkey admin-key.pem -out admin.p12 -name 'Administrator54 client certificate'` Файл admin.p12 содержит подписанный сертификат администратора
Шаг 5. Добавить подписанные сертификаты в ОС, с которой администраторы	Добавить подписанные сертификаты администраторов (admin.p12 в нашем примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой

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

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

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

Управление сертификатами

Общие сведения

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

Для выполнения данных функций UserGate WAF использует различные типы сертификатов:

Наименование	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate WAF
SSL инспектирование	Сертификат класса удостоверяющего центра. Он используется для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS трафика. Например, при перехвате HTTPS-трафика сайта yahoo.com оригинальный сертификат, выданный: Subject name = yahoo.com

Наименование	Описание
	Issuer name = VeriSign Class 3 Secure Server CA — G3, подменяется на Subject name = yahoo.com Issuer name = компания, как она указана в сертификате центра сертификации, заведенного в UserGate WAF
SSL инспектирование (пр омежуточный)	Промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата
SSL инспектирование (кор невой)	Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата
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 WAF с сервером SSO SAML IDP. Подробно о настройке работы UserGate WAF с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства

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

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

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку **Создать** в разделе **Сертификаты**
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Страна** — страна, в которой выписывается сертификат.

Наименование	Описание
	• **Область или штат** — область или штат, в котором выписывается сертификат. • **Город** — город, в котором выписывается сертификат. • **Название организации** — название организации, для которой выписывается сертификат. • **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • **E-mail** — email вашей компании
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в UserGate WAF. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата (SSL веб-консоли, инспектирование SSL, УЦ для авторизации в веб-консоли). В случае, если вы выбрали SSL веб-консоли, UserGate WAF перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. Сертификат инспектирования SSL начинает работать немедленно после того, как его выбрали

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

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в приложении «Установка сертификата локального удостоверяющего центра». • **Экспорт CSR** — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности UserGate не разрешает экспорт приватных ключей сертификатов.

Примечание

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

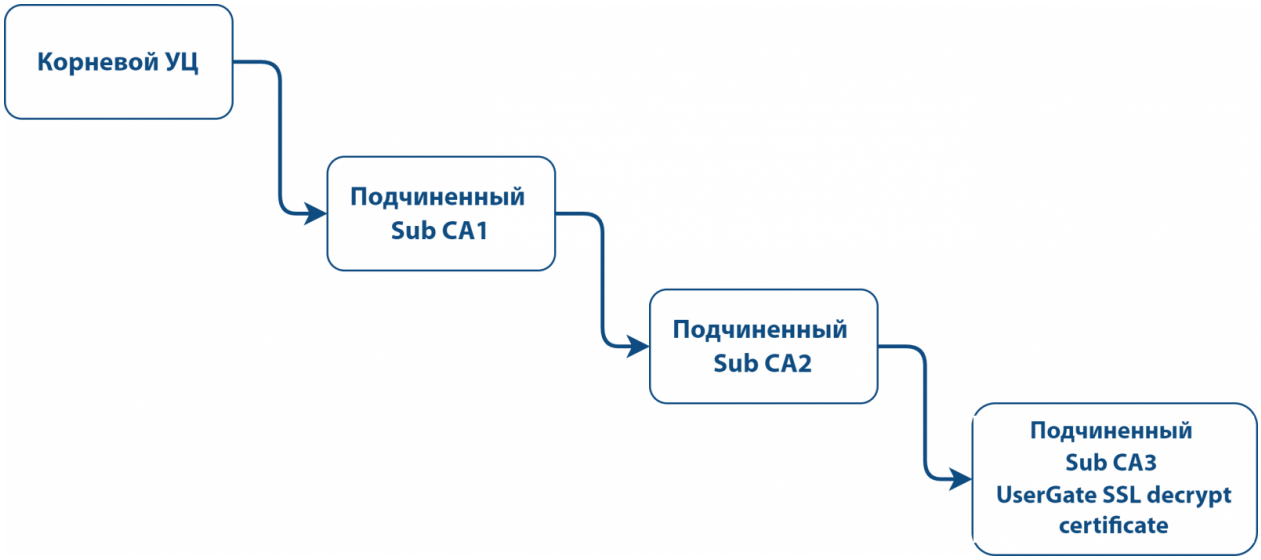
Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку **Импорт**
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Файл сертификата**: загрузите файл, содержащий данные сертификата. • **Приватный ключ**: загрузите файл, содержащий приватный ключ сертификата. • **Пароль** для приватного ключа, если таковой требуется. • **Цепочка сертификатов** – файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле

Использование корпоративного УЦ для создания сертификата инспектирования SSL

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

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



Пример структуры корпоративного УЦ

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

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

1. Сертификат класса удостоверяющего центра (CA):
    - В расширении X509v3 Basic Constraints (RFC 5280) сертификата должен быть атрибут CA:TRUE.

- В разделе **Консоль администратора → Сертификаты** такие сертификаты помечаются иконкой **Файл сертификата УЦ** слева от названия сертификата.

1. Ограничение использования сертификата не установлено или в его назначении в явном виде указаны атрибуты **Digital signature** и **Certificate signing**.

   - В сертификате не использованы никакие атрибуты расширения X509v3 Key Usage (RFC 5280).
     - В разделе **Консоль администратора → Сертификаты** в столбце **Назначение сертификата** для такого сертификата будет указано **Отсутствует**.
   - Если в сертификате используется расширение X509v3 Key Usage, то для инспектирования SSL обязательно должны присутствовать атрибуты digitalSignature и keyCertSign.
     - В разделе **Консоль администратора → Сертификаты** в столбце **Назначение сертификата** для такого сертификата будет указано **Digital signature** и **Certificate signing**.

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

Для выполнения этой задачи следует выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать CSR-запрос на создание сертификата в UserGate WAF.	Нажать на кнопку **Создать → Новый CSR**. Заполнить необходимые поля и создать CSR. Будет создан приватный ключ и файл запроса. С помощью кнопки **Экспорт** скачать файл запроса
Шаг 2. Создать сертификат на основе подготовленного CSR.	В Microsoft CA создать сертификат на основе полученного на предыдущем шаге CSR-файла с помощью утилиты certreq: certreq.exe -submit -attrib "CertificateTemplate:SubCA" HTTPS_csr.pem или с помощью веб-консоли Microsoft CA, указав в качестве шаблона «Подчиненный центр сертификации». Обратитесь к документации Microsoft за более подробной

Наименование	Описание
	информацией. По окончании процедуры вы получите сертификат (публичный ключ), подписанный УЦ Sub CA2
Шаг 3. Скачать полученный сертификат.	Из веб-консоли Microsoft CA скачать созданный сертификат (публичный ключ)
Шаг 4. Загрузить сертификат в созданный ранее CSR.	В UserGate WAF выбрать созданный ранее CSR и нажать кнопку **Редактировать**. Загрузить файл сертификата и нажать **Сохранить**
Шаг 5. Указать тип сертификата – инспектирование SSL.	В UserGate WAF выбрать созданный ранее CSR и нажать кнопку **Редактировать**. В поле **Используется** указать **SSL инспектирование**
Шаг 6. Скачать сертификаты для промежуточных УЦ (Sub CA1 и Sub CA2).	В веб-консоли Microsoft CA выбрать и скачать сертификаты (публичные ключи) для УЦ Sub CA1 и Sub CA2
Шаг 7. Загрузить сертификаты Sub CA1 и Sub CA2 в UserGate WAF.	С помощью кнопки **Импорт** загрузить скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2
Шаг 8. Установить тип — инспектирование SSL (промежуточный) для сертификатов Sub CA1 и Sub CA2.	В UserGate выбрать загруженные сертификаты и нажать кнопку **Редактировать**. Указать в поле **Используется** — **Инспектирование SSL (промежуточный)** для обоих сертификатов
Шаг 9. Загрузить сертификат Root CA в UserGate (опционально).	С помощью кнопки **Импорт** загрузить корневой сертификат организации в UserGate WAF. С помощью кнопки **Редактировать** указать в поле **Используется** — **Инспектирование SSL (корневой)**

Профили клиентских сертификатов

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

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

При выборе режима аутентификации посредством сертификатов (PKI) указывается сконфигурированный ранее профиль клиентского сертификата, который в дальнейшем можно будет использовать в настройках reverse-прокси.

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

Наименование	Описание
Название	Название профиля клиентских сертификатов
Описание	Опциональное описание профиля
Получать имя пользователя из	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • **Common-name** — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • **Subject altname email** — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name). • **Principal name** — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько электронных адресов, берется первый, указанный в сертификате
Сертификаты УЦ	Сертификаты УЦ, назначаемые профилю. Список сертификатов удостоверяющих центров. Используется для валидации предоставленного клиентом сертификата. Сертификат клиента проверяется на валидность для каждого сертификата УЦ из списка. Перебор списка идет сверху вниз
Проверка отозванных сертификатов	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты,

Наименование	Описание
	срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: • **Не проверять** — не проверять ни один сертификат. • **Вся цепочка** — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. • **Сертификат пользователя** — проверять только сертификат клиента. • **Считать валидным, если статус неизвестен** — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных)
Тайм-аут проверки	Интервал времени, по истечению которого UserGate WAF перестает ожидать ответа от службы списков отзыва сертификатов

Системные утилиты

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

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

Наименование	Описание
UGOS WAF	Загрузка UserGate WAF с выводом диагностической информации о загрузке в последовательный порт
UGOS WAF (failsafe)	Загрузка UserGate WAF в упрощённом видеорежиме

Наименование	Описание
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор)
Restore previous version	Раздел доступен после обновления или создания резервной копии

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

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление
Expand data partition	Увеличение раздела для хранения данных. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate WAF. **Важно!** Для расширения системного раздела с сохранением данных и параметров UserGate WAF необходимо средствами гипервизора добавить **новый** диск и затем выполнить операцию **Expand data partition**, как описано в разделе «Расширение системного раздела»
Create backup	Создать полную копию диска UserGate WAF на внешний USB носитель. **Важно!** Перед созданием резервной копии USB носитель будет отформатирован
Restore from backup	Восстановление UserGate WAF с внешнего USB носителя
Factory reset	Сброс состояния UserGate WAF. Версия ПО останется той, которая была установлена при запуске команды. Все данные и настройки будут утеряны
Exit	Выход и перезагрузка устройства

Расширение системного раздела

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

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

Примечание

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

Кластеризация и отказоустойчивость

Для построения отказоустойчивого решения UserGate WAF необходимо настроить два типа кластеров — кластер конфигурации и кластер отказоустойчивости:

- **Кластер конфигурации.** Узлы, объединенные в одну общую схему, «видят» друг друга и синхронизируют свою конфигурацию, поддерживая таким образом 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. При этом часть параметров для каждого из узлов кластера остается уникальной, например параметры сетевых интерфейсов, шлюзов, маршрутов и диагностики.
- **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). Вы можете собрать несколько кластеров отказоустойчивости. Например, если в кластер конфигурации добавлены узлы A, B, C и D, на их основе можно создать два кластера отказоустойчивости — A-B и C-D.

> **Важно!**
> **Работа устройств UserGate в режимах кластера конфигурации и кластера отказоустойчивости доступна, если в используемую лицензию включен модуль** `Cluster`.

Настройка кластера конфигурации

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

Чтобы настроить кластер конфигурации:

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

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

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

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

4. В окне **Свойства интерфейса**:

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

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

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

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

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

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

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

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

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

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

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

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

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.

О кластере отказоустойчивости

В режиме работы кластера «активный — пассивный» одно из устройств 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.**

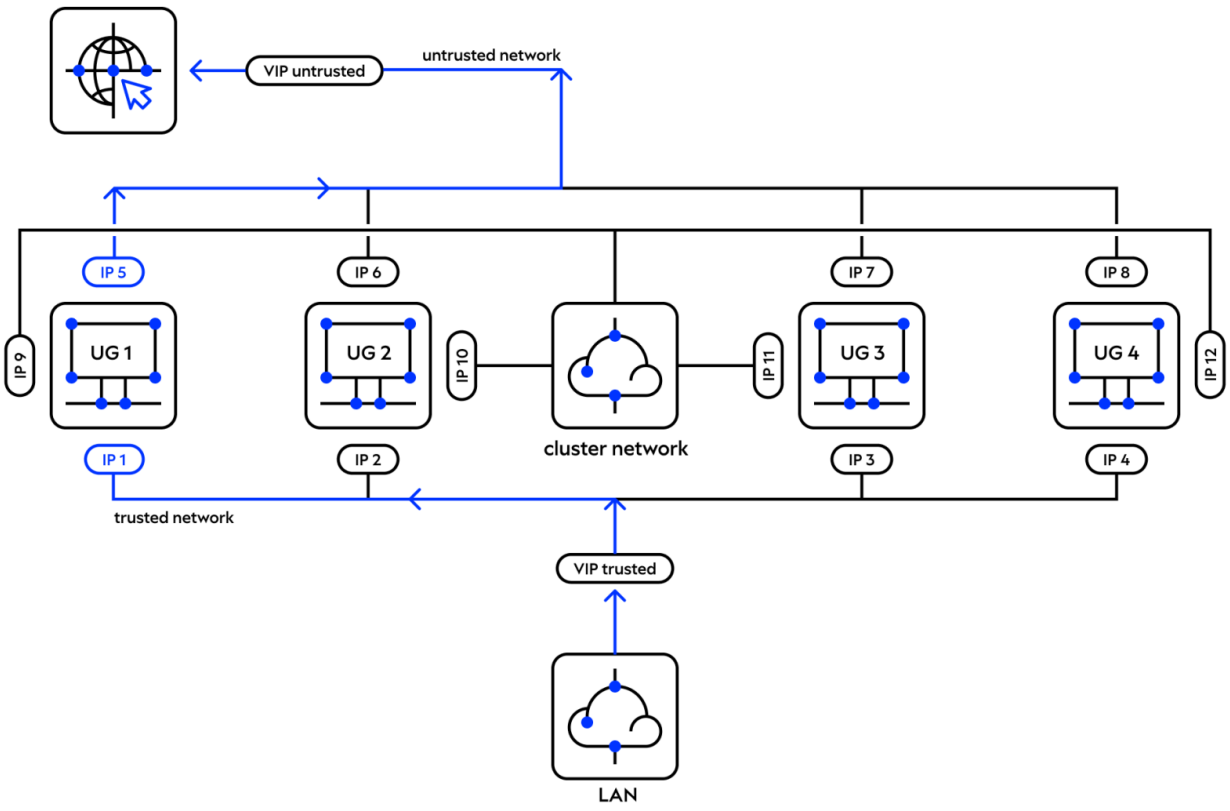
- **Сбой в работе ПО UserGate WAF.**

> **Примечание**
>
> **Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на резервный узел при переключении, устройству UserGate WAF посылается служебное оповещение GARP (Gratuitous ARP), извещающее сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается UserGate WAF 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`.



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** и введите название 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 вы установите 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.

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

8. 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.

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 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 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.

Параметр	Описание
	• **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
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

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

Вы можете настроить кластер отказоустойчивости UserGate WAF 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.
- 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 WAF, 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 WAF и объедините их в кластер конфигурации.

   ПримечаниеСервис 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 WAF 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** разрешит 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** и введите название кластера.

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**.

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

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.

НАСТРОЙКА СЕТИ

Настройка сетевых зон

Под сетевой зоной в UserGate WAF понимается логическое объединение сетевых интерфейсов. Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например можно создать зону для локальной сети (LAN) или зону интерфейсов управления (Management).

По умолчанию в UserGate WAF предусмотрены следующие сетевые зоны:

- **Management** — для доверенных сетей, из которых разрешено администрирование устройства.
- **Trusted** — для внутренних доверенных сегментов сети (например, LAN).
- **Untrusted** — для внешних недоверенных сетей (например, интернет).
- **DMZ** — для сегментов сети, содержащих публичные сервисы (демилитаризованная зона).

Вы можете изменять параметры этих сетевых зон, а также добавлять новые зоны (не больше 255 зон). Кроме того, вы можете управлять доступом к сервисам устройства для подключенных к зоне клиентов.

В свойствах зоны можно управлять доступом к следующим сервисам UserGate WAF.

Сервис	Назначение
Ping	Проверка доступности UserGate WAF с помощью утилиты `ping`. Подробнее — в разделе «Диагностика и мониторинг»
SNMP	Доступ к устройству по SNMP-протоколу (порт UDP 161). Подробнее — в разделе «Оповещения»
API XML RPC поверх HTTP	Доступ к API по протоколу HTTP (порт TCP 4443)
API XML RPC поверх HTTPS	Защищенный доступ к API по протоколу HTTPS (порт TCP 4443)
Кластер	

Сервис	Назначение
	Объединение нескольких узлов UserGate WAF в кластер (TCP 4369, TCP 9000-9100). Подробнее — в разделе «Кластеризация и отказоустойчивость»
VRRP	Объединение нескольких узлов UserGate WAF в отказоустойчивый кластер (IP-протокол 112). Подробнее — в разделе «Кластеризация и отказоустойчивость»
Консоль администрирования	Доступ к веб-консоли управления (порт TCP 8001)
CLI по SSH	Доступ к интерфейсу командной строки для управления сервером устройства (порт TCP 2200)
Reverse-прокси	Публикация внутренних ресурсов. Подробнее — в разделе «Публикация веб-ресурсов»
Log Analyzer/SIEM	Отправка журналов событий на сервер UserGate Log Analyzer или UserGate SIEM
SNMP-прокси	Построение распределенной системы мониторинга и регулирования нагрузки
NTP-сервис	Доступ к службе точного времени на сервере UserGate WAF

Для работы сервисов необходимо разрешить соответствующие порты и протоколы в сетевой инфраструктуре организации. Подробнее — в разделе «Требования к сетевому окружению».

Вы также можете включать защиту от DoS-атак и защиту от IP-спуфинга для каждой зоны. Кроме того, в свойствах зоны вы можете ограничить количество активных сессий для одного IP-адреса. Это позволит снизить нагрузку на инфраструктуру организации при DDoS-атаках, предотвратить злоупотребление ресурсами и обеспечить их доступность для всех пользователей.

Чтобы добавить сетевую зону:

1. В разделе **Настройки → Сеть → Зоны** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
   - Укажите название и при необходимости описание зоны.

- При необходимости укажите параметры защиты сетевой зоны от DoS-атак для протоколов TCP (SYN-флуд), UDP, ICMP соответственно:
  - Установите флажок **Включено** для включения защиты.
  - При необходимости установите флажок **Агрегировать** для суммарного подсчета всех входящих пакетов. Если флажок не установлен, пакеты учитываются отдельно для каждого IP-адреса.
  - В поле **Порог уведомления** укажите количество запросов с одного IP-адреса, при превышении которого в системном журнале будет сгенерирована запись о событии.

    Рекомендованное значение — 3000 пакетов/сек.
  - В поле **Порог отбрасывания пакетов** укажите количество запросов с одного IP-адреса, при превышении которого будут отброшены пакеты, поступившие с этого IP-адреса, с регистрацией события в системном журнале.

    Рекомендованное значение — 6000 пакетов/сек. Для протокола UDP необходимо увеличить это значение, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN.
  - При необходимости в блоке параметров **Исключения защиты от DoS** добавьте IP-адреса узлов, к которым не следует применять ограничения. Это может понадобиться, например, для серверов IP-телефонии, генерирующих интенсивный поток UDP-пакетов.

> **Примечание**
>
> **Рекомендуется включать защиту от DoS-атак для каждой сетевой зоны.**

3. При необходимости на вкладке **Контроль доступа** укажите сервисы, которые будут доступны подключенным к зоне клиентам.

> **Важно!**
>
> **Не рекомендуется разрешать доступ к сервисам для зон, подключенных к недоверенным сетям (например, к интернету).**

> **Примечание**
> **Вы можете дополнительно ограничить доступ к каждому сервису, указав разрешенные диапазоны IP-адресов или географические регионы (GeoIP).**

4. При необходимости на вкладке **Защита от IP-спуфинга** включите защиту и укажите для зоны разрешенные диапазоны IP-адресов или географические регионы (GeoIP). Сетевые пакеты, поступающие с IP-адресов, не входящих в разрешенный список, будут отброшены.

При включении инвертирования (соответствует логическому отрицанию) указанные диапазоны IP-адресов будут запрещены для сетевой зоны.

> **Примечание**
> **Например, для зоны Untrusted вы можете указать диапазоны «серых» IP-адресов (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) и установить флажок «Инвертировать».**

5. При необходимости на вкладке **Ограничение сессий** включите ограничение и укажите максимальное количество активных сессий для одного IP-адреса.

> **Примечание**
> **В блоке параметров «Исключения» вы можете добавить список IP-адресов, для которых ограничение не будет действовать.**

6. Нажмите **Сохранить**.

Настройка интерфейсов

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

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

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
- Назначить зону интерфейсу.
- Назначить профиль Netflow для отправки статистических данных на Netflow коллектор.
- Назначить Алиас/Псевдоним — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.
- Изменить физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
- Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:
- VLAN.
- Бонд.
- Мост.
- Loopback.

Создание интерфейса VLAN

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

Наименование	Описание
Включено	Включает VLAN
Название	

Наименование	Описание
	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN
Описание	Опциональное описание интерфейса
Тип интерфейса	Указать тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов
Имя узла	Имя узла в кластере, на котором создается данный VLAN
Интерфейс	Физический интерфейс, на котором создается VLAN
Зона	Зона, которой принадлежит VLAN
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. Подробнее об этом — в разделе «Профили Netflow»
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. **Важно!** Значение параметра не может содержать символы кириллицы
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает бонд
Название	Название бонда
Имя узла	Узел кластера UserGate WAF, на котором будет создан бонд
Зона	Зона, к которой принадлежит бонд
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. Подробнее об этом — в разделе «Профили Netflow»
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. **Важно!** Значение параметра не может содержать символы кириллицы
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **XOR.** Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости.

Наименование	Описание
	• **IEEE 802.3ad** — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • **Adaptive transmit load balancing.** Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям

Наименование	Описание
	miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • **Follow** — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • **Layer 2** — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.

Наименование	Описание
	• **Layer 3+4** — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS

Создание моста (bridge)

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

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

image3

Рисунок 4 Использование моста

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

При выборе режима Layer 2 создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой.

Внимание!

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

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

Если мост создается в ПАК UserGate WAF, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить 2 интерфейса в байпас-мост. Байпас-мост автоматически переключает два выбранных интерфейса в режим байпас (закорачивает их, пропуская весь трафик мимо WAF) в случаях если:

- Электропитание ПАК UserGate WAF отключено.
- Система внутренней диагностики обнаружила проблему в работе ПО UserGate WAF. Тайм-аут срабатывания при обнаружении проблемы — 10 секунд.

Управление работой байпас-реле сетевых портов возможно через интерфейс PMC. Подробнее об этом — в разделе «Команды управления платформой» руководства по интерфейсу командной строки PMC.

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

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

Наименование	Описание
Включено	Включает интерфейс мост
Название	Название интерфейса
Имя узла	Узел кластера UserGate WAF, на котором создать интерфейс мост
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2
Зона	Зона, к которой принадлежит интерфейс мост

Наименование	Описание
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. Подробнее об этом — в разделе «Профили Netflow»
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. **Важно!** Значение параметра не может содержать символы кириллицы
Интерфейсы моста	Два интерфейса, которые будут использованы для построения моста
Интерфейсы байпас моста	Пара интерфейсов, которые можно использовать для построения байпас моста. Требуется поддержка оборудования ПАК UserGate WAF
STP (Spanning Tree Protocol)	Включает использование STP для защиты сети от петель
Forward delay	Задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP
Maximum age	Время, по истечении которого STP-соединение считается потерянным
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS

Интерфейс loopback

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

Параметр	Описание
Включено	Включает интерфейс
Название	Название интерфейса в виде loopbackN, где N — целое число

Параметр	Описание
Описание	Опциональное описание интерфейса
Имя узла	Выбор узла кластера UserGate WAF, на котором создается интерфейс
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2
Зона	Зона, к которой принадлежит интерфейс
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. Подробнее об этом — в разделе «Профили Netflow»
Профиль LLDP	Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol (LLDP)
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. **Важно!** Значение параметра не может содержать символы кириллицы
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS

Настройка шлюзов

Для подключения UserGate WAF к интернету 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 WAF, 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 WAF 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 WAF 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 WAF 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 WAF 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 WAF 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.

Виртуальные маршрутизаторы

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

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

Каждый виртуальный маршрутизатор имеет свою собственную таблицу маршрутизации.

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

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

Виртуальные маршрутизаторы имеют следующие ограничения:

- Следующие сервисы могут быть использованы только в Виртуальном маршрутизаторе по умолчанию:
    - DNS.
    - Авторизация.
    - Любой сетевой трафик, генерируемый самим устройством — проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS сообщений, SNMP трапов и т.п.
- Зоны глобальны, то есть настройки зоны, и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

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

Для добавления виртуального маршрутизатора необходимо выполнить следующие действия:

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

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

Наименование	Описание
Шаг 1. Создать виртуальный маршрутизатор.	В разделе **Сеть → Виртуальные маршрутизаторы** нажмите добавить и задайте имя и описание нового виртуального маршрутизатора. Укажите имя узла, на котором создается данный виртуальный маршрутизатор при наличии кластера

Наименование	Описание
Шаг 2. Добавить интерфейсы в созданный виртуальный маршрутизатор.	На вкладке **Интерфейсы** укажите интерфейсы, которые должны быть помещены в данный виртуальный маршрутизатор. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, не могут быть добавлены; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, и другие
Шаг 3. Добавить статические маршруты (опционально).	Добавьте маршруты (кроме маршрута по умолчанию), которые будут применены к трафику в этом виртуальном маршрутизаторе. Подробнее об этом — в разделе «Статические маршруты». Маршрут по умолчанию добавляется в разделе **Сеть → Шлюзы**. Подробнее о настройке шлюзов — в разделе «Настройка шлюзов»

Статические маршруты

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

Для добавления маршрута необходимо выполнить следующие шаги:

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

Наименование	Описание
	• **Unreachable** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • **Prohibit** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13)
Шаг 4. Указать адрес назначения.	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32
Шаг 5. Указать шлюз.	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с UserGate WAF
Шаг 6. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UserGate WAF сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов
Шаг 7. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько

ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Серверы аутентификации

Серверы аутентификации — это внешние источники учетных записей пользователей, например, LDAP-сервер, или серверы, производящие аутентификацию для UserGate WAF, например, RADIUS, TACACS+, SAML. Система поддерживает следующие типы серверов аутентификации:

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

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.

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

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации
Название	Название сервера аутентификации
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то UserGate WAF получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate WAF будет использовать резервный В случае недоступности части контроллеров домена с площадки, где работает UserGate WAF, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену
Срок жизни LDAP-кэша	Срок жизни LDAP-кэша (от 1 до 48 часов). Новый срок жизни применяется к новым записям, добавляемым в LDAP-кэш после того, как администратор его установит. (Доступно начиная с релиза UGOS 7.1.3)
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов

Наименование	Описание
	или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена
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. Подробно об аутентификации Kerberos и создании keytab-файла — в разделе «Метод аутентификации Kerberos»

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

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

Настройка LDAP-коннектора завершена.

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

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть UserGate WAF выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate WAF 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 WAF, поэтому, если пользователи не были заведены в UserGate WAF предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только

пользователей типа **Known** (успешно прошедших аутентификацию на сервере RADIUS) или **Unknown** (не прошедших авторизацию).

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

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

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

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При авторизации через TACACS+ UserGate WAF 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 WAF, поэтому, если пользователи не были заведены в WAF предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

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

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации

Наименование	Описание
Название сервера	Название сервера аутентификации
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации
Адрес	IP-адрес сервера TACACS+
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет авторизовать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю, единожды авторизовавшись в системе SSO, прозрачно проходить авторизацию на всех ресурсах, поддерживающих аутентификацию SAML. UserGate WAF может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в UserGate WAF поэтому, если не настроено подключение к домену AD с помощью LDAP-коннектора, в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере SAML) или **Unknown** (не прошедших аутентификацию).

Для использования авторизации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
Создать DNS-записи для UserGate WAF.	На контроллере домена создать DNS-запись, соответствующую UserGate WAF, для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate WAF, подключенного в сеть **Trusted**

Наименование	Описание
Настроить DNS-серверы на UserGate WAF.	В параметрах UserGate WAF в качестве системных DNS-серверов указать IP-адреса контроллеров домена
Настроить сервер SAML IDP.	Добавить на сервере SAML IDP запись о сервис-провайдере UserGate WAF, указывая созданное на шаге 1 FQDN имя
Создать сервер аутентификации пользователей SAML IDP.	Создать в UserGate WAF сервер аутентификации пользователей SAML IDP

Для создания сервера аутентификации пользователей SAML IDP необходимо в разделе **Пользователи и устройства → Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации
Название сервера	Название сервера аутентификации
Описание	Описание сервера аутентификации
SAML metadata URL	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку **Загрузить** происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера аутентификации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации
Сертификат SAML IDP	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: • Создать новый сертификат из скачанного — если при настройке был использован метод загрузки xml-файла, то сертификат автоматически создается и ему назначается роль SAML IDP. Подробнее об этом — в разделе «Управление сертификатами». • Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе **Сертификаты**, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP.

Наименование	Описание
	• Не использовать сертификат
Single sign-on URL	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации
Single sign-on binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты **POST** и **Redirect**. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации
Single logout URL	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации
Single logout binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты **POST** и **Redirect**. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации

Сервер аутентификации NTLM

Аутентификация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации с помощью NTLM UserGate WAF работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в Интернет.

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

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Настроить синхронизацию времени с контроллером домена.	В параметрах UserGate WAF включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена
Создать DNS-запись для UserGate WAF.	На контроллере домена создать DNS-записи, соответствующие UserGate WAF для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate WAF, подключенного в сеть **Trusted**
Добавить NTLM-сервер.	В разделе **Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить NTLM-сервер** и указать название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена
Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate WAF 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 WAF 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
Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в **Панель управления → Свойства браузера → Безопасность**, выберите зону **Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя** и установите **Автоматический вход в сеть с текущем именем пользователя и паролем** (**Control panel → Internet options → Security**, выберите зону **Internet → Custom level → User Authentication → Logon** и установите **Automatic logon with current name and password**). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites)

Метод аутентификации Kerberos

Аутентификация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации через Kerberos WAF работает с контроллерами домена, которые выполняют проверку пользователя, получающего доступ в Интернет.

Аутентификация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для авторизации с помощью Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Создать DNS-записи для UserGate WAF.	На контроллере домена создать DNS-записи, соответствующие UserGate WAF, для использования в качестве доменов для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc В качестве IP-адреса укажите адрес интерфейса UserGate WAF, подключенного в сеть **Trusted**. **Важно!** Для корректной работы создайте записи типа A, не используйте CNAME-записи
Создать пользователя для UserGate WAF.	Создать пользователя в домене AD, например, kerb@domain.loc с опцией **password never expires**. Установите пароль пользователю kerb. **Важно!** Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb. **Важно!** Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись
Создать keytab-файл.	На контроллере домена, создать keytab файл, выполнив следующую команду **из-под администратора** (команда в одну строку!): ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab Введите пароль пользователя kerb. **Важно!** Команда чувствительна к регистру букв. В данном примере:

Наименование	Описание
	auth.domain.loc — DNS-запись, созданная для сервера UserGate на шаге 1 DOMAIN.LOC — Kerberos realm domain, обязательно большими буквами! kerb@DOMAIN.LOC — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена
Настроить синхронизацию времени с контроллером домена.	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена
Создать LDAP-коннектор и загрузить в него keytab-файл.	Создать сервер аутентификации типа LDAP-коннектор и загрузить полученный на предыдущем шаге keytab-файл. **Важно!** Не используйте в качестве пользователя для LDAP-коннектора, пользователя, созданного ранее для работы Kerberos. Необходимо использовать отдельную учетную запись. Подробно о настройке LDAP-коннектора — в разделе «LDAP-коннектор»
Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени UserGate, созданного на шаге 3
Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в **Панель управления → Свойства браузера → Безопасность**, выберите зону **Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя** и установите **Автоматический вход в сеть с текущем именем пользователя и паролем** (**Control panel → Internet options → Security**, выберите зону **Internet → Custom level → User Authentication → Logon** и установите **Automatic logon with current name and password**). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites)

Профили аутентификации

Профиль аутентификации позволяет указать набор способов и параметров авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах UserGate WAF. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства → Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Время бездействия до отключения	Данный параметр определяет, через сколько секунд UserGate WAF переведет пользователя из **Known users** в **Unknown users** при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя)
Время жизни аутентифицированного пользователя	Данный параметр определяет, через сколько секунд UserGate WAF переведет пользователя из **Known users** в **Unknown users**. По происшествии указанного времени пользователю потребуется повторно авторизоваться на Captive-портале
Число неудачных попыток аутентификации (локальные пользователи)	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя
Время блокировки локального пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например, сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, то они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов аутентификации, таких как: • **Локальный пользователь** — аутентификация по базе данных локально заведенных пользователей. • **Принять политику** — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип аутентификации необходимо применять совместно с профилем

Наименование	Описание
	Captive-портала, в котором используется страница авторизации Captive portal policy. • **HTTP Basic** — аутентификация с помощью устаревшего метода HTTP Basic.

ПОЛИТИКИ СЕТИ

Межсетевой экран

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

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

Примечание

Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Примечание

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

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

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

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

Наименование	Описание
Включено	Включает или отключает правило
Название	Название правила
Описание	Описание правила
Действие	**Запретить**: блокирует трафик. **Разрешить**: разрешает трафик
Отбросить и	Настройка данного параметра доступна для правил, блокирующих трафик (выбрано действие **Запретить**). Параметр может принимать одно из следующих значений: • **Не выбран**. • **Посылать ICMP host unreachable**: блокировка трафика с отправкой ICMP-сообщения. • **Посылать TCP reset**: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** При выборе действия **Посылать TCP reset** необходимо указание сервиса (вкладка **Сервис**), использующего протокол TCP. • **Посылать TCP reset в обе стороны**: блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования.

Наименование	Описание
	• **Журналировать все сетевые пакеты**. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • **Нет**. В этом случае информация не будет записываться
Применить правило к	Применимость правила: • Все пакеты. • Только фрагментированные пакеты. • Только нефрагментированные пакеты
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки имен доменов источника трафика. **Важно!** Строки с символом '*' в списках имен доменов не работают (игнорируются). Каждые 5 минут WAF производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни WAF автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки имен доменов назначения трафика. **Важно!** Строки с символом '*' в списках имен доменов не работают (игнорируются). Каждые 5 минут WAF производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни WAF автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов
Время	Интервалы времени, когда правило активно
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счетчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счетчики**
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п

НАСТРОЙКА ПУБЛИКАЦИИ ВЕБ-СЕРВИСОВ

Публикация веб-сервисов

UserGate WAF поддерживает публикацию веб-сервисов. Доступ к веб-сервисам и безопасность соединений с ними контролируются настраиваемыми правилами публикации.

Режим публикации предоставляет следующие возможности:

- **Балансировка нагрузки**. Если обработку запросов к веб-сервису выполняют несколько веб-серверов, UserGate WAF может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- **Подмена путей**. UserGate WAF может выполнять подмену путей и доменных имен в запросах, помогая таким образом разделить трафик для разных веб-сервисов.
- **Управление доступом к веб-серверам**. UserGate WAF может блокировать попытки доступа по идентификационной строке клиентского приложения (useragent) и нежелательным адресам.
- **Поддержка SSL-подключения**. UserGate WAF может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.
- **Сигнатурный анализ трафика**. Правила публикации с подключенными профилями безопасности защищают веб-сервисы от атак и других угроз безопасности. Подробнее — в разделе «Настройка параметров безопасности WAF».
- **Фильтрация WebSocket-трафика**. UserGate WAF поддерживает обмен трафиком по протоколу WebSocket и обеспечивает безопасность установления WebSocket-соединений. Подробнее — в разделе «Защита WebSocket-соединений».
- **Определение реального IP-адреса источника запроса**. UserGate WAF может анализировать заголовки HTTP-запросов, чтобы определить реальный IP-адрес. Подробнее — в разделе «Настройка функции определения реального IP-адреса».
- **Фильтрация трафика**, закодированного по стандарту Base64. Подробнее — в разделе «Фильтрация закодированного трафика».

Чтобы опубликовать веб-сервис:

1. Создайте один или несколько серверов публикации.

2. Если для доступа к веб-сервису используются несколько серверов, создайте для них правило балансировки.

3. Создайте правила публикации, которые будут определять условия публикации веб-сервисов выбранным сервером или балансировщиком.

> **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 публикации

Чтобы создать сервер публикации:

1. В разделе **Политика сервисов → Серверы публикации** нажмите **Добавить**.

2. В окне **Настройка сервера публикации** укажите название, IP-адрес или FQDN и TCP-порт сервера публикации.

3. Если необходимо, настройте остальные параметры:

- Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate WAF до сервера публикации. Если этот флажок установлен, убедитесь, что на шаге 2 вы указали порт для защищенного соединения.
- Установите флажок **Проверять SSL-сертификат**, чтобы включить проверку подлинности SSL-сертификата, установленного на сервере публикации. 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 WAF.

> **Важно!**
> **Если установлен флажок «Не изменять IP-адрес источника», для корректной работы необходимо настроить маршрутизацию таким образом, чтобы сервер публикации отвечал через тот же сетевой интерфейс UserGate WAF, с которого приходят запросы клиентов. Для этого на сервере публикации в качестве шлюза по умолчанию можно указать UserGate WAF или можно настроить статические маршруты через UserGate WAF для «белых» IP-адресов источников.**

4. Сохраните изменения.

Балансировка нагрузки на серверы публикации

Если для доступа к веб-сервису развернуто несколько серверов публикации, вы можете распределять клиентские запросы между ними с помощью правил балансировки нагрузки.

Чтобы создать правило балансировки серверов публикации:

1. В разделе **Политика сервисов → Серверы публикации** создайте серверы публикации веб-сервисов. Убедитесь, что в окне **Настройка сервера публикации** для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.

2. В разделе **Политика сервисов → Балансировка сервисов** нажмите **Добавить**.

3. В окне **Настройка правила балансировки сервисов** на вкладке **Общие** укажите название правила и включите его.

4. На вкладке **Серверы публикации** добавьте серверы, на которые будет распределяться нагрузка.

5. Сохраните изменения.

Создание правила публикации

Правила публикации позволяют фильтровать запросы к веб-сервисам, 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 публикации:

1. В разделе **Настройки → Политика сервисов → Правила публикации** нажмите **Добавить**.

2. В окне **Настройка правила публикации** на вкладке **Общие**:

   - Включите правило и укажите его название.
   - В списке **Сервер публикации** выберите сервер публикации или балансировщик, которому UserGate WAF будет пересылать запросы.
   - Укажите порты, на которых UserGate WAF 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, и сертификат сервера публикации для поддержки HTTPS-соединения.
   - С помощью параметра **Вставить** настройте расположение правила в списке.

     ПримечаниеПараметр 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 серверами публикации.

> **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 WAF выполняет разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate WAF автоматически обновляет значение IP-адреса.

Важно!

Обработка трафика происходит по следующей логике: условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов и/или доменов; условия объединяются по «И», если указаны GeoIP и списки IP-адресов и/или доменов.

4. На вкладке **Назначение** укажите IP-адреса, назначенные на интерфейсы, которые принимают входящие соединения. Этот параметр следует настраивать, когда на один интерфейс UserGate WAF 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.

5. На вкладке **Профили безопасности**, если необходимо, включите защиту веб-сервисов и WebSocket-соединений. Подробнее об этом — в разделах

«Настройка параметров безопасности WAF» и «Защита WebSocket-соединений».

6. На вкладке **Веб-сервисы** нажмите **Добавить** и укажите путь к одному или нескольким веб-сервисам, запросы к которым будет обрабатывать правило.

> **Примечание**
>
> **Формат записи: `<host>/<path>`, где `<host>` — обязательный параметр (совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно; все названия узлов приводятся к нижнему регистру.), а `<path>` — необязательный, без которого будет выбираться любой путь (совпадение префиксное, не строгое). При указании пути для `<host>` в качестве маски можно использовать символ *. Например, запись `*.example.org` соответствует как `www.example.org`, так и `www.sub.example.org`.**

> **Важно!**
>
> **Следует указывать те веб-сервисы, публикацию которых обеспечивает сервер, выбранный на шаге 2. В противном случае правило сработает некорректно.**

7. На вкладке **Useragent**, если необходимо, добавьте идентификационные строки клиентских браузеров, для которых будет разрешен обмен трафиком с веб-сервисами.

> **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».**

8. На вкладке **Подмена путей**, если необходимо, настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

9. Сохраните изменения.

Подмена путей в правилах публикации

Подмена путей в правилах публикации используется для модификации HTTP-запроса пользователя. Правило публикации обрабатывает запрос, выполняя в нем подмену пути, и передает модифицированный запрос на указанный сервер публикации. Веб-сервис, доступ к которому контролируется этим сервером публикации, получает и обрабатывает модифицированный запрос и возвращает соответствующий ответ. Таким образом вы можете управлять разделением трафика для разных сервисов.

Чтобы настроить подмену путей в правиле публикации:

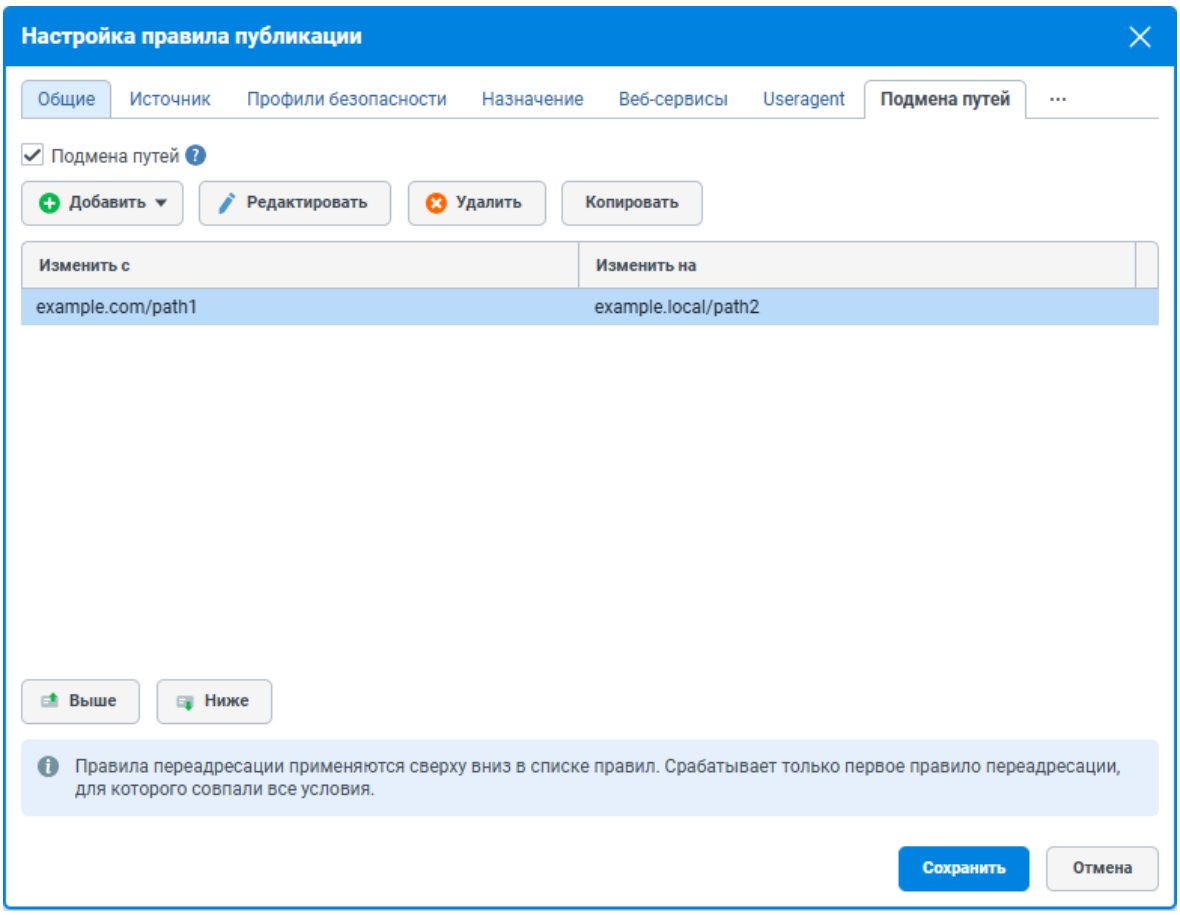
1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте или выберите правило.

2. В окне **Настройка правила публикации** на вкладке **Подмена путей** установите флажок **Подмена путей**.

3. Нажмите **Добавить** и укажите пути подмены одним или двумя способами:

   - **Пути для подмены**. Заполните вручную поля, где:
     - **Изменить с** — домен и/или путь URL, который требуется изменить.
     - **Изменить на** — домен и/или путь URL, на который требуется заменить старый.
   - **Веб-сервисы**. В качестве домена и/или пути URL, который требуется изменить, выберите веб-сервис, указанный на вкладке **Веб-сервисы**, и в поле **Изменить на** укажите для него соответствующий домен и/или путь URL, на который требуется его заменить.

> **Примечание**
>
> **Вы можете настраивать подмену путей и для кириллических доменов.**



4. Сохраните правило.

При обработке HTTP-запроса правило публикации сработает, если путь, указанный на вкладке **Веб-сервисы**, совпадет с путем URL в HTTP-запросе. Затем происходит подмена пути в HTTP-запросе, если она предусмотрена сработавшим правилом: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос пользователя не попадет ни под одно правило публикации, 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.

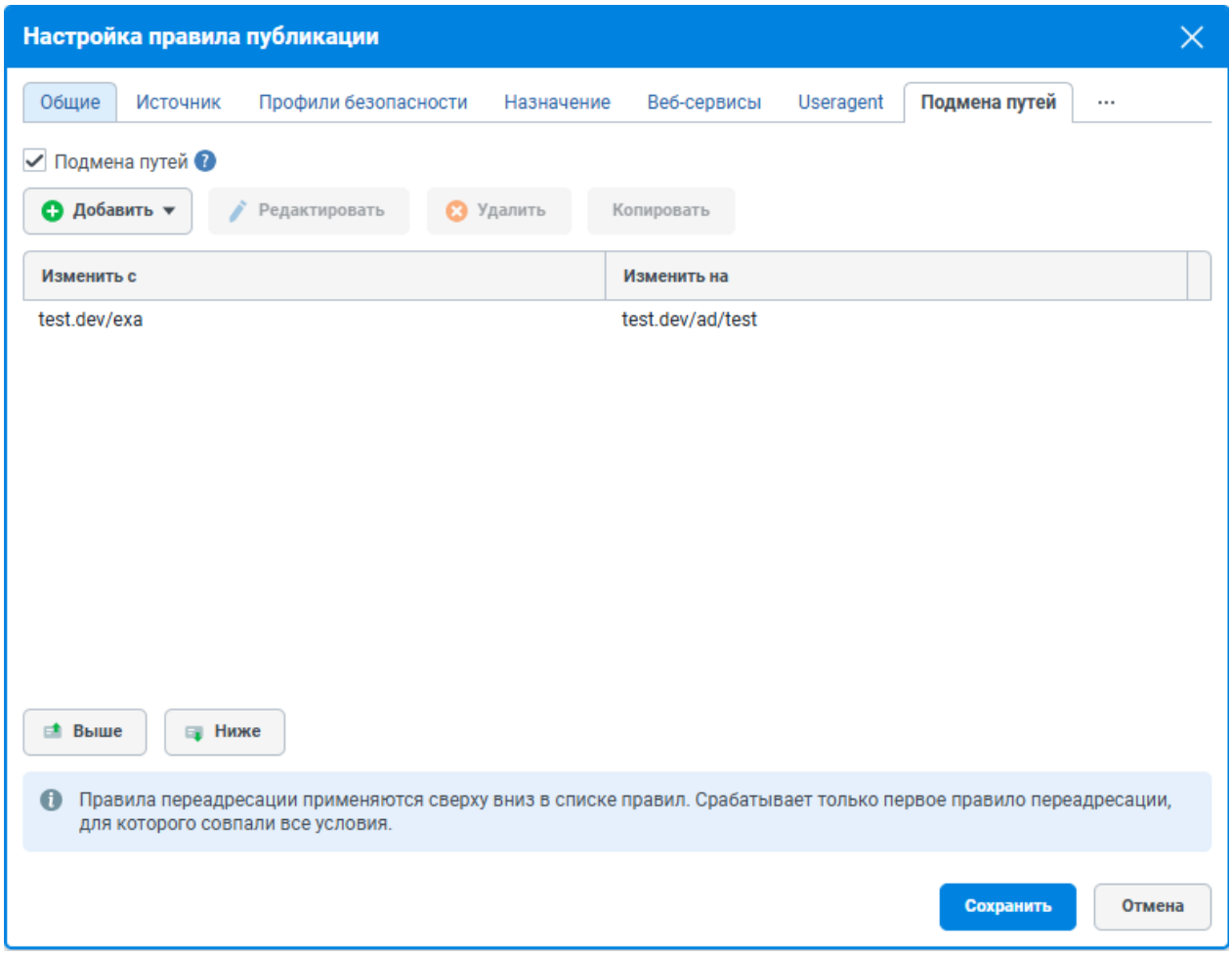
Исходный паттерн в правиле публикации	Примеры запросов, на которые правило сработает	Примеры запросов, на которые правило не сработает
test.dev	• test.dev • test.dev/ • test.dev/* • http://test.dev • test.dev:<любой порт>	• abc.com • test.develop • test.dev.lol
tesT.deV	• test.deV • tesT.deV/ • TEST.dev	• abc.com • test.develop • test.dev.lol
test.dev/co	• test.dev/co* • http://test.dev/co* • test.dev:<любой порт>/co*	• test.dev.lol/co* • test.dev/kool*
http://test.dev	• http://test.dev • http://test.dev/* • http://test.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/cool*

Исходный паттерн в правиле публикации	Примеры запросов, на которые правило сработает	Примеры запросов, на которые правило не сработает
	• http://test.dev:<любой порт>/co	

Примеры срабатывания 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`.

Настройка определения реального IP-адреса

Когда между веб-клиентом и узлом WAF находятся прокси-серверы, балансировщики нагрузки или другие сетевые узлы, в запросах, проходящих через них, IP-адрес источника (веб-клиента, отправившего исходный запрос), заменяется собственным IP-адресом такого сетевого узла. Для корректного определения реального IP-адреса источника прокси-серверы или балансировщики могут передавать его в специальных HTTP-заголовках, таких как `X-Real-IP`, `X-Forwarded-For` или пользовательские заголовки.

В UserGate WAF есть возможность определения реального IP-адреса источника запроса по таким HTTP-заголовкам. Данные, полученные из заголовков `X-Real-IP` и `X-Forwarded-For`, а также из пользовательских заголовков, можно использовать для выявления потенциальных угроз, контроля доступа на основе IP-адресов и анализа данных о посетителях сайта.

Алгоритм обработки заголовков X-Real-IP и пользовательских заголовков

HTTP-заголовок `X-Real-IP` или пользовательский заголовок используется для указания IP-адреса веб-клиента, отправившего исходный запрос. Серверные приложения могут использовать этот заголовок для журналирования или определения местоположения пользователя. Если прокси-сервер, балансировщик или другой сетевой узел передает запрос дальше, этот заголовок может перезаписываться следующим сервером в цепочке.

Если в параметрах правила публикации выбрана обработка заголовка `X-Real-IP` или пользовательского заголовка, алгоритм обработки этих заголовков выглядит следующим образом:

1. При получении HTTP-запроса UserGate WAF проверяет запрос на наличие заголовка (`X-Real-IP` или пользовательского заголовка).

2. Если заголовок не найден в запросе, UserGate WAF добавляет его и в качестве реального IP-адреса указывает IP-адрес сетевого узла, передавшего запрос.

3. Если заголовок найден, но не содержит значения, UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос, и добавляет его в заголовок.

4. Если заголовок найден и содержит значение, UserGate WAF выполняет поиск IP-адреса сетевого узла, передавшего запрос, в списке доверенных источников:

- Если IP-адрес сетевого узла не является доверенным, UserGate WAF заменяет значение в заголовке на этот IP-адрес и принимает его в качестве реального IP-адреса.
- Если IP-адрес сетевого узла является доверенным, значение в заголовке проверяется на соответствие формату IPv4/IPv6:
  - если формат корректный, UserGate WAF принимает значение, указанное в заголовке, в качестве реального IP-адреса;
  - если формат некорректный, UserGate WAF заменяет значение в заголовке на IP-адрес сетевого узла, передавшего запрос, и принимает его в качестве реального IP-адреса.

5. После обработки запроса значение заголовка, принятое как реальный IP-адрес, сохраняется в записях журнала веб-доступа, а обработанные запросы передаются на анализ и дальнейшую обработку в соответствии с правилами и политикой безопасности в UserGate WAF. При срабатывании правила публикации в записях журнала срабатывания также сохраняется значение реального IP-адреса.

Алгоритм обработки заголовка X-Forwarded-For

HTTP-заголовок `X-Forwarded-For` содержит список IP-адресов, через которые прошел запрос. IP-адрес веб-клиента, отправившего исходный запрос, добавляется в начало списка, а каждый следующий узел добавляет свой IP-

адрес в конец списка. Этот заголовок полезен для отслеживания реального происхождения запроса, особенно в многослойных сетевых конфигурациях.

Пример заголовка:

```
X-Forwarded-For: 203.0.113.42, 192.168.1.1, 10.0.0.1
```

Где:

- 203.0.113.42 — IP-адрес веб-клиента, отправившего исходный запрос;
- 192.168.1.1 — IP-адрес первого сетевого узла;
- 10.0.0.1 — IP-адрес второго сетевого узла.

Если в параметрах правила публикации выбрана обработка заголовка `X-Forwarded-For`, алгоритм обработки этих заголовков выглядит следующим образом:

1. При получении HTTP-запроса UserGate WAF проверяет запрос на наличие заголовка.

2. Если заголовок не найден, UserGate WAF добавляет его и в качестве реального IP-адреса указывает IP-адрес сетевого узла, передавшего запрос.

3. Если заголовок найден, но не содержит значений, UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос, и добавляет его в заголовок.

4. Если заголовок содержит значения и рекурсивный режим выключен, UserGate WAF проверят формат первого значения (в примере это `203.0.113.42`) на соответствие формату IPv4/IPv6:

   - Если формат корректный, UserGate WAF принимает этот IP-адрес в качестве реального IP-адреса.
   - Если формат некорректный, UserGate WAF принимает IP-адрес сетевого узла, передавшего запрос, в качестве реального IP-адреса.

5. Если заголовок содержит значения и рекурсивный режим включен, UserGate WAF выполняет поиск доверенного IP-адреса, последовательно проверяя значения в заголовке:

- Если первый IP-адрес (в примере это `203.0.113.42`) найден в списке доверенных источников, UserGate WAF принимает этот IP-адрес в качестве реального IP-адреса.
- Если доверенный IP-адрес не является первым значением в списке (в примере это `192.168.1.1`), UserGate WAF проверяет стоящий перед ним в списке IP-адрес (в примере это `203.0.113.42`) на соответствие формату IPv4/IPv6:
    - Если этот IP-адрес прошел проверку, UserGate WAF принимает его в качестве реального IP-адреса.
    - Если этот IP-адрес не прошел проверку, UserGate WAF в качестве реального IP-адреса принимает следующий после него в списке доверенный IP-адрес (в примере это `192.168.1.1`).
- Если ни одно из значений в заголовке не является доверенным IP-адресом, UserGate WAF проверяет последнее значение в заголовке на соответствие формату IPv4/IPv6 и в случае успешной проверки принимает последнее значение (в примере это `10.0.0.1`) в качестве реального IP-адреса. В противном случае UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос.

6. После обработки запроса значение заголовка, принятое как реальный IP-адрес, сохраняется в записях журнала веб-доступа, а обработанные запросы передаются на анализ и дальнейшую обработку в соответствии с правилами и политиками безопасности в UserGate WAF. При срабатывании правила публикации в записях журнала срабатывания также сохраняется значение реального IP-адреса.

Настройка функции определения реального IP-адреса источника запроса

Чтобы настроить функцию определения реального IP-адреса:

1. В разделе **Настройки → Политика сервисов → Правила публикации** выберите правило, которое необходимо настроить, и нажмите **Редактировать**.

2. В окне **Настройка правила публикации** на вкладке **Реальный IP** установите флажок **Получать реальный IP**.

3. Выберите заголовок, из которого будет извлекаться адрес источника запроса:

- **X-Real-IP**.
- **X-Forwarded-For**. При выборе этого заголовка:
  - Если необходимо, установите флажок **Рекурсивный режим**, чтобы анализировать цепочку IP-адресов в заголовке.
  - Установите флажок **Добавлять IP-адрес реверс-прокси**, если вы хотите, чтобы адрес прокси-сервера UserGate WAF был добавлен в список IP-адресов в заголовке.
- **Пользовательский заголовок**. При выборе этого заголовка укажите его название.

4. Если необходимо, в блоке **Доверенные источники** укажите списки адресов или сетей доверенных источников запроса, например прокси-серверов и балансировщиков.

5. Сохраните изменения.

> **Примечание**
>
> **Сведения о реальных IP-адресах могут отображаться в разделах «Атаки» и «Журналы и отчеты» → «Журнал веб-доступа».**

Балансировка нагрузки

UserGate WAF может выполнять балансировку нагрузки на серверы публикации.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов. Чтобы настроить балансировку, необходимо в разделе **Политика сервисов → Балансировка сервисов** создать правила балансировки.

Балансировщик позволяет распределить нагрузку на внутренние серверы или ферму серверов публикации и может быть использован в правилах публикации.

Для создания балансировщика необходимо в разделе **Политика сервисов → Балансировка сервисов** нажать **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило
Название	Название правила балансировки
Описание	Описание правила балансировки
Серверы публикации	Выбрать серверы публикации, на которые будет распределяться нагрузка. Более подробно о публикации с помощью правил — в разделе «Публикация веб-сервисов»

НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ

Настройка параметров безопасности WAF

Параметры и уровень защиты веб-трафика в UserGate WAF определяются политикой безопасности. Настроенная политика безопасности позволяет UserGate WAF обнаруживать и блокировать различные угрозы, включая наиболее опасные атаки из списка OWASP Top 10.

Основными элементами политики безопасности являются:

- **WAF-правило** — представляет собой выражение, содержащее условия обнаружения угроз безопасности. WAF-правило обеспечивает защиту веб-трафика от различных атак и может сработать как на запрос к веб-ресурсу, так и на его ответ. При срабатывания WAF-правила выполняется назначенное действие. WAF-правила бывают системными и пользовательскими.
- **Слой** — конструкция, предназначенная для группировки WAF-правил по типам атак с целью принятия одного решения по результатам проверки веб-трафика. Слои бывают системными и персональными.

- **WAF-профиль** — это набор системных и/или персональных слоев. WAF-профиль с настроенными слоями определяет политику безопасности, в соответствии с которой выполняется защита вашего веб-сервиса.

Алгоритм настройки и применения политики безопасности следующий:

1. Убедитесь, что лицензия UserGate WAF `Security Updates` активирована. Подробнее о лицензии — в разделе «Лицензирование UserGate WAF».

2. Создайте WAF-профиль, включите необходимые слои с WAF-правилами и, если необходимо, настройте параметры слоев. Подробнее — в разделе «Создание WAF-профиля».

3. Если необходимо, настройте WAF-правила в каждом слое, чтобы выполнять только необходимые проверки веб-трафика. Подробнее — в разделе «Настройка системных WAF-правил».

4. Подключите WAF-профиль в правиле публикации, настроенном на проверку трафика соответствующего веб-сервиса. Подробнее — в разделе «Подключение WAF-профиля в правиле публикации».

Правило публикации с подключенным WAF-профилем будет проверять веб-трафик на наличие угроз выбранному веб-сервису. При срабатывании WAF-правила, для которого включено журналирование, UserGate WAF записывает информацию об обнаружении атаки или другого события ИБ. Эти сведения доступны для просмотра и анализа в разделе **Атаки**. Подробнее — в разделе «Просмотр обнаруженных атак».

Работа с WAF-профилями

WAF-профиль необходим для настройки наборов слоев с WAF-правилами. По умолчанию WAF-профиль создается с выключенными слоями. В зависимости от того, какой уровень защиты следует обеспечить вашему веб-сервису, необходимо включить и настроить нужные слои.

В WAF-профиле могут использоваться как персональные слои с пользовательскими правилами, так и системные слои, содержащие правила от экспертов UserGate.

Вы можете создавать WAF-профили, копировать и удалять. Созданные WAF-профили отображаются в разделе **Настройки → Политика безопасности → WAF-профили**.

Создание WAF-профиля

Чтобы создать WAF-профиль:

1. В разделе **Политика безопасности → WAF-профили** нажмите **Добавить**.

2. Введите название WAF-профиля.

3. В блоке **WAF-слои** в списке системных слоев включите нужные слои. В счетчике активных правил под названием слоя отобразится количество включенных правил.

> **Примечание**
>
> **После сохранения WAF-профиля включенные слои автоматически поднимаются наверх в своих группах. Порядок в таком случается определяется так: первый в списке включенный слой поднимается на первое место, на второе место поднимается следующий по списку включенный слой и так далее. В рамках одной группы вы можете перемещать слои по списку, чтобы таким образом настроить очередность проверки трафика системными WAF-правилами.**

4. Если необходимо, настройте каждый из включенных системных слоев. Подробнее — в разделе «Настройка системного слоя».

5. Если необходимо, добавьте и включите персональные слои с пользовательскими WAF-правилами. Подробнее — в разделе «Создание персонального слоя и пользовательских WAF-правил». Пользовательские правила имеют приоритет перед системными правилами, включенными в этом WAF-профиле.

6. Сохраните изменения.

Теперь созданный WAF-профиль можно подключить в правиле публикации.

Подключение WAF-профиля в правиле публикации

Чтобы подключить WAF-профиль в правиле публикации и начать проверку трафика в соответствии с настроенной политикой безопасности:

1. В разделе **Политика сервисов → Правила публикации** создайте или выберите правило публикации. Подробнее — в разделе «Публикация веб-сервисов».

2. На вкладке **Профили безопасности** установите флажок **Включить защиту веб-приложений (WAF)** и выберите из списка нужный WAF-профиль.

> **Примечание**
>
> **Если нужного профиля нет в списке, вы можете создать его, нажав в конце списка на «Создать и выбрать новый объект».**

3. Завершите настройку других параметров правила публикации и сохраните изменения.

Правило публикации настроено на защиту веб-сервера, указанного в его параметрах.

Настройка системного слоя

Системные слои создаются компанией UserGate и содержат правила, сгруппированные по типам атак. Настройка системного слоя выполняется в рамках выбранного WAF-профиля. Выключение всего слоя исключает из проверки все WAF-правила, входящие в него. Если слой включен, параметры слоя влияют на то, какие WAF-правила, входящие в него, будут участвовать в проверке веб-трафика.

Для настройки доступны следующие параметры системного слоя:

- Технологии защиты. Системные WAF-правила защищают веб-сервисы, разработанные на базе различных технологий. Например, `Outlook Web Access` или `MySQL`. Удаление технологии защиты из слоя исключает из проверки WAF-правила, связанные с этой технологией. Таким образом можно настроить политику безопасности с учетом используемых в вашем веб-сервисе технологий.

- Уровень защиты, установленный в WAF-правиле (низкий, средний, высокий). Например, вы можете установить уровень защиты только «высокий», тогда в слое останутся активными только правила, обеспечивающие защиту этого уровня. Прочие правила, с уровнями защиты «низкий» и «средний», будут выключены.

- Дополнительная конфигурация параметров отдельных правил. Выбранные таким образом значения параметров системных WAF-правил будут более приоритетными, чем те, которые изначально назначены в глобальном

списке правил. Подробнее — в разделе «Настройка системных WAF-правил».

Чтобы настроить системный слой:

1. Выберите WAF-профиль и нажмите **Редактировать**.

2. В окне **WAF-профиль** в блоке **WAF-слои** выберите из списка слой и нажмите на его название.

3. В окне **Свойства системного слоя** настройте нужные параметры, включая параметры WAF-правил.

4. Сохраните изменения.

Создание персонального слоя и пользовательских WAF-правил

Чтобы более гибко управлять политикой безопасности, вы можете создавать персональные слои, содержащие пользовательские WAF-правила, написанные на языке UserGate Policy Language (UPL). Созданные персональные слои отображаются в разделе **Политика безопасности → Персональные слои**. Вы можете просматривать и редактировать их, выполнять поиск по названию слоя.

Чтобы создать персональный слой:

1. В разделе **Персональные слои** нажмите **Добавить**.

> **Примечание**
>
> **Вы также можете создать персональный слой при создании или изменении WAF-профиля, нажав в окне свойств профиля кнопку «Добавить персональный слой».**

2. В окне **Свойства персонального слоя** укажите название.

3. В области **Редактирование выражения** введите UPL-выражение, содержащее правила проверки трафика. Подробнее о синтаксисе написания UPL-правил — в разделе «UserGate Policy Language».

> **Примечание**
> **Область представляет собой встроенный редактор с подсветкой ключевых слов и выражений и проверкой синтаксиса UPL.**

4. Если необходимо, включите журналирование пользовательского правила. Для этого в области редактирования UPL-выражения добавьте свойство `"rule_log(true)"`.

5. Нажмите **Проверить выражение** и, если необходимо, внесите исправления.

6. Сохраните изменения.

Созданный персональный слой автоматически добавится во все WAF-профили и будет по умолчанию выключен. Чтобы UserGate WAF выполнял проверку веб-трафика с помощью пользовательских WAF-правил, при настройке WAF-профиля необходимо включить нужные персональные слои и затем подключить этот WAF-профиль в правило публикации. Подробнее о настройке и подключении WAF-профилей — в разделе «Работа с WAF-профилями».

Работа с системными WAF-правилами

UserGate WAF поставляется с набором системных WAF-правил, обеспечивающих защиту веб-трафика от различных атак. Системные WAF-правила загружаются с серверов UserGate автоматически после активации лицензии и затем регулярно обновляются и дополняются командой экспертов UserGate.

> **Важно!**
> **Для получения регулярных обновлений системных WAF-правил вам необходимо обладать лицензией на модуль `Security Updates`.**

> **Примечание**
> **При обновлении экспертизы все системные WAF-правила как в WAF-профилях, так и в глобальном списке переводятся в режим журналирования – их действие устанавливается как `No action`. Журналирование включается автоматически, чтобы администратор мог проанализировать поведение новых версий правил перед включением блокировки.**

Системные WAF-правила группируются в системные слои, которые также формируются разработчиками решения. Критерием группировки WAF-правил в слои являются следующие типы атак:

- Abuse of Functionality;
- Authentication/Authorization Attacks;
- Buffer Overflow;
- Command Execution;
- Denial of Service;
- Detection Evasion;
- Directory Indexing;
- HTTP Parser Attack;
- HTTP Response Splitting;
- Information Leakage;
- LDAP Injection attempt;
- SQL-injection;
- Malicious File Upload;
- Microsoft OWA;
- Other Application Attacks;
- Path Traversal;
- Predictable Resource Location;
- Remote File Include;
- Server Side Code Injection;
- Session Hijacking;
- Trojan/Backdoor/Spyware;
- Vulnerability Scan;
- XPath Injection;

- Cross site scripting (XSS);
- XML External Entity (XXE).

Все системные WAF-правила отображаются в разделе **Политика безопасности → Глобальные правила**. Вы можете просматривать сведения о WAF-правилах (например, в каком слое они находятся, какое выбрано действие или профиль ответа), изменять их параметры, выполнять поиск и сортировку.

О действиях в WAF-правилах

При срабатывании WAF-правила выполняется одно из назначенных действий:

- `No action` — при срабатывании правила система фиксирует событие (если включено журналирование), но не предпринимает действий в отношении трафика.
- `Pass` — все правила, расположенные в слое под сработавшим правилом, пропускаются, и происходит переход к проверке WAF-правилами следующего слоя (при его наличии). Если следующего слоя нет, проверка завершается пропуском запроса или ответа.
- `Deny` — все правила, расположенные в слое под сработавшим правилом, пропускаются, и происходит переход к проверке WAF-правилами следующего слоя (при его наличии). Если следующего слоя нет, проверка завершается блокированием запроса или ответа.
- `Force deny` — является окончательным результатом обработки, и перехода к проверке WAF-правилами следующего слоя не происходит. Проверка завершается блокированием запроса или ответа.
- `Force pass` — является окончательным результатом обработки, и перехода к проверке WAF-правилами следующего слоя не происходит. Проверка завершается пропуском запроса или ответа.

Таким образом, приоритет force-действий выше, что следует учитывать, настраивая последовательность слоев.

Поиск системных WAF-правил

Для быстрого поиска в глобальном списке WAF-правил предусмотрены фильтр и сортировка по параметрам.

Важно!

При формировании поискового запроса рекомендуется для одного параметра WAF-правила указывать одно значение. В противном случае результаты поиска могут быть неверными. Пример корректного запроса: `technology = "PHP"`. **Пример некорректного запроса:** `technology = "PHP" AND technology = "WordPress"`.

Для фильтрации используются следующие параметры WAF-правила.

Название параметра в веб-консоли	Параметр	Описание
Уровень угрозы	`threatLevel`	Уровень угрозы, от которой защищает WAF-правило: • 1: низкий; • 2: средний; • 3: высокий
ID правила	`ruleId`	Идентификатор WAF-правила
Название	`name`	Название WAF-правила
Ссылка	`reference`	Ссылки на внешние ресурсы с описаниями уязвимостей
Время последнего обновления	`lastUpdate`	Время последнего обновления правила на серверах UserGate
Профиль ответа	`responseProfile`	Название профиля ответа
Системный слой	`systemLayer`	Системный слой, к которому относится WAF-правило
Пакет	`package`	Название пакета экспертизы, в который входит данное WAF-правило
Действие	`action`	Действие правила: `No action`, `Pass`, `Deny`, `Force deny`, `Force pass`

Настройка системных WAF-правил

В веб-консоли UserGate WAF вы можете настраивать системные WAF-правила двумя способами:

- через настройку WAF-профиля;
- через глобальный список системных WAF-правил.

Для изменения доступны следующие параметры системного WAF-правила:

- Включение или выключение WAF-правила.
- Исключения к WAF-правилу. Подробнее об исключениях — в разделе «Настройка исключений для WAF-правил».
- Журналирование событий, связанных с работой WAF-правила.

> **Примечание**
> **По умолчанию журналирование событий включено во всех системных WAF-правилах.**

- Действия, которое будет выполнено при срабатывании WAF-правила.
- Профиль ответа, который вернется в ответ на клиентский запрос, если блокирующее WAF-правило сработает. Подробнее о профилях ответа — в разделе «Профили ответа».
- Отмена всех изменений и возвращение значений параметров правила к изначальным.

Настройка системного WAF-правила в WAF-профиле

При настройке системного WAF-правила в профиле WAF параметры правила изменяются только в этом профиле и имеют более высокий приоритет, чем параметры в глобальном списке правил. Например, если в профиле `Example profile` для правила `Rule1` действие `No Action` заменено на `Pass`, это значение сохранится, даже если в глобальном списке для `Rule1` будет выбрано действие `Force pass`.

Чтобы изменить параметры системного WAF-правила в WAF-профиле:

1. В разделе **WAF-профили** создайте по кнопке **Добавить** или выберите из списка WAF-профиль.

2. В окне **WAF-профиль** в блоке **WAF-слои** в одной из групп системных слоев выберите системный слой и нажмите на его название.

3. В окне **Свойства системного слоя** в секции **Правила** нажмите **Настройка правил**.

4. В окне **Настройка правил** выберите WAF-правило и нажмите **Переопределить**.

5. В окне **Переопределение правил** измените нужные параметры.

6. Сохраните все изменения.

> **Примечание**
> **Вы также можете изменить параметры сразу нескольких нескольких WAF-правил. Для этого в окне «Настройка правил» нужно выбрать несколько WAF-правил, затем нажать «Переопределить», в окне «Переопределение правил» изменить нужные параметры и сохранить изменения.**

Настройка системного WAF-правила в глобальном списке

При настройке системного WAF-правила через глобальный список параметры WAF-правила изменятся только в тех WAF-профилях, в которых не выполнялась настройка этого правила.

Чтобы изменить параметры системного WAF-правила через глобальный список:

1. В разделе **Глобальные правила** выберите нужное WAF-правило и нажмите **Редактировать**.

2. В окне **Редактирование правил** измените нужные параметры.

3. Сохраните изменения.

> **Примечание**
> **Вы также можете изменить параметры сразу нескольких нескольких WAF-правил. Для этого в глобальном списке нужно выбрать несколько WAF-правил, затем нажать «Редактировать», в окне «Редактирование правил» изменить нужные параметры и сохранить изменения.**

Восстановление значений по умолчанию

При настройке политики безопасности может понадобиться восстановить исходные состояния отдельных элементов. В зависимости от того, значения параметров какого элемента нужно вернуть к исходным, необходимо перейти в одно из следующих окон и нажать **Восстановить значения по умолчанию**:

- В окне **WAF-профиль** — чтобы вернуть значения по умолчанию для всех системных слоев в WAF-профиле.
- В окне **Свойства системного слоя** — чтобы сбросить в первоначальное состояние выставленные технологии и уровни защиты этого слоя.
- В окне **Свойства системного слоя**, нажав **Настройка правил** — чтобы восстановить исходное состояния выбранных правил в WAF-профиле
- В разделе **Глобальные правила** — чтобы восстановить исходное состояния выбранных правил в глобальном списке.

Настройка исключений для WAF-правил

По умолчанию блокирующие WAF-правила применяются ко всем запросам и ответам, содержащим значения, соответствующие условиям WAF-правила. Вы можете настроить исключения, чтобы скорректировать работу WAF-правил.

Исключения помогут предотвратить ложные срабатывания и обеспечить гибкое управление обработкой трафика. Например, они позволяют игнорировать легитимный трафик от систем мониторинга, партнерских API и доверенных поисковых ботов (Googlebot, YandexBot), а также запросы с надежными реферерами или специфическими заголовками `Accept` от внутренних систем.

Исключения задаются условиями, при выполнении которых WAF-правило пропускает запрос или ответ без обработки. Если для WAF-правила есть исключение, оно проверяется в первую очередь. Если WAF-правило содержит несколько исключений, достаточно срабатывания любого исключения, чтобы прекратить обработку.

Для создания исключений используются UPL-условия и логические операторы, аналогичные операторам фильтрации данных. Подробнее о UPL-условиях и операторах — в разделах «Условия» и «Поиск и фильтрация данных».

Вы можете настраивать исключения по следующим условиям.

Условие	Описание
`http.method`	Проверка HTTP-метода
`src.ip`	Проверка IP-адреса
`http.request.body.re2`	Проверка тела HTTP-запроса
`http.response.body.re2`	Проверка тела HTTP-ответа
`http.request.body`, `http.request.body.nocase`	Проверка тела HTTP-запроса
`http.response.body`, `http.response.body.nocase`	Проверка тела HTTP-ответа
`request.header.Host`	Проверка HTTP-заголовка запроса `Host`
`url.path`	Проверка URL
`request.header.User-Agent`	Проверка заголовка `useragent`
`request.header.Referer`	Проверка запроса на доверенные рефереры
`request.header.Accept`	Проверка заголовка `Accept`
`request.header.Cookie`	Проверка заголовка запроса `Cookie` на значение
`qparam`	Проверка значения параметров запроса
`upl.condition`	Поле для произвольного исключения, написанного на языке UPL. Выражения записываются в поле значений через пробел, который работает как логическое «И»

Создание исключения

Чтобы создать исключение:

1. В разделе **Настройки → Политика безопасности → Исключения** нажмите **Добавить**.

2. В окне **Свойства исключения** укажите название исключения.

3. Если необходимо вести запись сработавших исключений, установите флажок **Журналирование**.

4. Выберите из списка условие, затем выберите доступный для него логический оператор и укажите одно или несколько значений.

> **Примечание**
> **Вы можете добавить несколько условий в одно исключение. В этом случае исключение сработает, если при проверке запроса или ответа выполнены все указанные условия.**

5. Сохраните изменения.

Исключение создано. Чтобы оно сработало, его следует применить к выбранным WAF-правилам.

Применение исключений

Созданные исключения можно применить к WAF-правилам двумя способами:

- **Через настройку WAF-профиля.** Исключения, добавленные в WAF-правила через настройку WAF-профиля, применяются только в рамках этого профиля. Таким образом, для одного WAF-правила, включенного в несколько WAF-профилей, можно применить собственный набор исключений в каждом из этих профилей. Если к WAF-правилу уже были применены исключения, их набор будет изменен только в выбранном WAF-профиле.
- **Через настройку WAF-правила, выбранного в общем списке WAF-правил.** Исключения, добавленные в WAF-правило через общий список WAF-правил, применяются только в тех WAF-профилях, использующих это WAF-правило, в которые не были добавлены исключения через настройку WAF-профиля.

Чтобы применить исключения через настройку WAF-профиля:

1. В разделе **Настройки → Политика безопасности → WAF-профили** выберите WAF-профиль.

2. В окне **WAF-профиль** нажмите название слоя с WAF-правилами, к которым требуется применить исключения.

3. В окне свойств слоя в секции **Правила** нажмите **Настройка правил**.

4. В окне **Настройка правил** выберите WAF-правило и нажмите **Переопределить**.

5. В окне **Переопределение правил** в секции **Исключения** в колонке **Доступны** выберите одно или несколько предварительно созданных исключений и нажмите значок плюса.

6. Сохраните изменения.

Примечание

Вы также можете применить исключения сразу к нескольким WAF-правилам. Для этого в окне «Настройка правил» нужно выбрать несколько WAF-правил и затем нажать «Переопределить». В секции «Исключения» необходимо выбрать «Перезаписать», после чего станет доступным добавление исключений. После сохранения изменений добавленные исключения применятся ко всем выбранным WAF-правилам. Если в блок «Выбранные» не добавлено ни одно исключение, но выбрана перезапись исключений, все ранее добавленные исключения будут удалены из выбранных WAF-правил.

Чтобы применить исключения через настройку WAF-правила:

1. В разделе **Настройки → Политика безопасности → Правила** выберите WAF-правило и нажмите **Редактировать**.

2. В окне **Редактирование правил** в секции **Исключения** в колонке **Доступны** выберите одно или несколько предварительно созданных исключений и нажмите значок плюса.

3. Сохраните изменения.

Примечание

Вы также можете применить исключения сразу к нескольким WAF-правилам. Для этого в списке нужно выбрать несколько WAF-правил и затем нажать «Редактировать». В секции «Исключения» необходимо выбрать «Перезаписать», после чего станет доступным добавление исключений. После сохранения изменений добавленные исключения применятся ко всем выбранным WAF-правилам. Если в блок «Выбранные» не добавлено ни одно исключение, но выбрана перезапись исключений, все ранее добавленные исключения будут удалены из выбранных WAF-правил.

Примененные исключения отобразятся в свойствах WAF-правила в общем списке WAF-правил в столбце **Исключения**.

Информация о сработавших исключениях доступна на странице атак: для WAF-правил со сработавшим исключением в столбце **Действие** отображается значение **No action**, а в столбце **Исключения** появляется соответствующий значок. При наведении на него курсора отображается название сработавшего исключения. Подробнее о просмотре информации о сработавших WAF-правилах — в разделе «Просмотр обнаруженных атак».

Работа с заголовком X-Request-Id

`X-Request-Id` — вспомогательный опциональный заголовок HTTP, который содержит уникальный идентификатор запроса. Этот идентификатор позволяет трассировать отдельные HTTP-запросы при решении проблем в работе веб-сервисов.

Значение идентификатора запроса является случайным, не содержит никакой персональной информации о пользователе и генерируется для каждого отдельного HTTP-запроса, что исключает опасность нарушения приватности пользователя.

В UserGate WAF идентификатор запроса используется для корреляции HTTP-запросов и записей журнала веб-доступа и журнала срабатывания правил WAF в рамках одного соединения. Функциональность доступна в версии 7.4.0 и выше.

UserGate WAF проверяет приходящие HTTP-запросы на наличие заголовка `X-Request-Id` и значения идентификатора запроса. Если заголовок `X-Request-Id` отсутствует, UserGate WAF добавляет его в запрос и генерирует уникальное значение идентификатора запроса. Если HTTP-запрос приходит в UserGate WAF с уже существующим заголовком `X-Request-Id`, то UserGate WAF заменяет его значение на собственное сгенерированное уникальное значение.

Далее запрос передается на анализ и дальнейшую обработку в соответствии с правилами и политиками безопасности в UserGate WAF. Значение идентификатора запроса сохраняется в записях журнала веб-доступа.

При срабатывании правила WAF клиенту возвращается ответ с идентификатором запроса в качестве значения заголовка `X-Request-Id`. В записях журнала срабатывания сохраняется значение идентификатора запроса.

В веб-интерфейсе администратора в разделе **Атаки**, а также в разделе **Журналы и отчеты** на вкладке **Журнал веб-доступа** есть колонка

Идентификатор запроса, где отображается значение этого индикатора. Поддерживается функция фильтрации событий в журнале по идентификатору запроса.

Фильтрация закодированного трафика

Двоичные данные могут передаваться в закодированном виде через каналы, предназначенные только для передачи текста. С помощью стандарта кодирования Base64 любой файл преобразуется в строку текста и передается по протоколам, поддерживающим только текстовый формат. Стандарт Base64 используется например для кодирования вложений электронной почты или для встраивания графических, видео- или аудиоданных в веб-разработке.

Некоторые атаки на веб-приложения также используют стандарт кодирования Base64 для обхода фильтров межсетевых экранов, в том числе используется многократное кодирование, затрудняющее анализ исходных данных. Например, в случае SQL-внедрения выполняется кодирование SQL-запроса в Base64, чтобы обойти сигнатурный анализ. Как правило, эти данные передаются в параметрах URL, cookies и заголовках HTTP-запросов.

В UserGate WAF вы можете использовать правила публикации для декодирования и фильтрации таких данных.

Поддерживается декодирование следующих элементов HTTP-запроса:

- путь из URL;
- значения Cookies;
- значения в заголовках HTTP-запросов;
- тело запроса/ тело ответа, если в заголовке content type указан MIME-тип `application/x-www-form-urlencoded` (начиная с версии 7.6.0);
- параметры из тела POST-запроса или из URL GET-запроса.

Чтобы настроить фильтрацию закодированного трафика:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте правило. Подробнее о создании и настройке правила публикации — в разделе «Публикация веб-сервисов».

2. В окне **Настройка правила публикации** на вкладке **Профили безопасности** установите флажок **Включить защиту веб-приложений**

(WAF) и выберите WAF-профиль, в соответствии с которым декодированные данные будут подвергаться сигнатурному анализу. После выбора WAF-профиля станет доступной вкладка **Base64**.

3. На вкладке **Base64** установите флажки для тех элементов клиентского запроса, которые следует декодировать.

4. Укажите количество итераций декодирования для многократно закодированных данных. Максимальное значение — 5.

5. Сохраните изменения.

При срабатывании правила публикации будет выполнена попытка декодирования выбранных элементов HTTP-запроса, а в записях журнала событий сохранится информация об изменении состояния декодированных параметров.

Профили ответа

В соответствии с политикой безопасности WAF-правила могут блокировать подозрительные запросы к защищаемым веб-сервисам. С помощью профилей ответа вы можете настроить, какой ответ будет возвращен клиенту при срабатывании блокирующего WAF-правила:

- страница блокировки с указанием кода состояния HTTP;
- сообщение о разрыве соединения;
- переадресация на другой ресурс.

Чтобы создать профиль ответа:

1. На странице **Настройки** в разделе **Политика безопасности → Профили ответа** нажмите **Добавить.**

2. В окне **Свойства профилей ответа** укажите название профиля.

3. Выберите нужный тип политики и настройте для него необходимые параметры:

   - **TCP RST**. Выберите этот тип политики, чтобы при срабатывании блокирующего WAF-правила выполнялся разрыв соединения.

- **Переадресация**. Укажите ссылку для перенаправления запроса, трехзначный код состояния HTTP и, если необходимо, добавьте текст ответа.

> **Примечание**
> **Трехзначный код состояния HTTP для переадресации должен начинаться с цифры 3. Например, 302. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду.**

- **Шаблон страницы**. В списке **Страница блокировки** выберите шаблон страницы из списка (либо оставьте выбранный по умолчанию), укажите трехзначный код состояния HTTP и, если необходимо, добавьте текст ответа. Подробнее о создании шаблона страницы — в разделе «Шаблоны страниц».

> **Примечание**
> **Трехзначный код состояния HTTP для блокировки должен начинаться с цифр 1, 2, 4 или 5. Например, 403. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду.**

4. Сохраните изменения.

Чтобы добавить созданный профиль ответа в WAF-правило:

1. На странице **Настройки** в разделе **Политика безопасности → Глобальные правила** выберите правило, которому назначено действие **Deny** или **Force deny**, и нажмите **Редактировать**.

2. В окне **Редактирование правил** в списке **Профили ответа** выберите нужный профиль и сохраните изменения.

> **Примечание**
> **Вы также можете добавить профиль ответа в WAF-правило при создании или изменении WAF-профиля. Подробнее о настройке WAF-профилей — в разделе «Настройки безопасности WAF».**

Защита WebSocket-соединений

UserGate WAF может контролировать безопасность установления соединений по протоколу WebSocket.

Протокол WebSocket обеспечивает двунаправленную связь между клиентом и сервером в реальном времени и позволяет поддерживать постоянное соединение, по которому данные могут передаваться в обе стороны без необходимости повторных запросов от клиента. Принцип работы протокола WebSocket следующий:

1. Установление соединения. Клиент отправляет HTTP-запрос на «рукопожатие» (handshake-запрос) серверу, предлагая установить WebSocket-соединение. Если сервер поддерживает протокол WebSocket, он возвращает подтверждающий ответ, и соединение переключается с HTTP на WebSocket.

2. Двунаправленный обмен данными. После успешного подключения клиент и сервер могут свободно отправлять данные друг другу в любое время без дополнительного подтверждения.

3. Закрытие соединения. Соединение может быть закрыто по инициативе клиента или сервера с отправкой кода закрытия и возможного описания причины.

В UserGate WAF правила установления WebSocket-соединений определяются WebSocket-профилем, который позволяет настроить:

- Блокирование любого WebSocket-трафика, который приходит в UserGate WAF.
- Проверку целостности handshake-запроса.
- Проверку наличия заголовка Origin — HTTP-заголовка, который браузеры автоматически добавляют в запрос при установке WebSocket-соединения. Заголовок Origin содержит URL источника, который инициирует соединение.
- Списки значений заголовков запроса (Origin, Sec-WebSocket-Extensions, Sec-WebSocket-Protocols), на основании которых UserGate WAF будет устанавливать WebSocket-соединение с доверенными источниками или игнорировать запросы, поступающие из нежелательных источников.

- Журналирование событий, связанных с установлением WebSocket-соединений. Подробнее — в разделе «Журнал WebSocket».

Настройка WebSocket-профиля для блокирования всего WebSocket-трафика

Чтобы создать WebSocket-профиль, блокирующий весь WebSocket-трафик:

1. В разделе **Настройки → Политика безопасности → WebSocket-профили** нажмите **Добавить**.

2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** установите флажок **Блокировать WebSocket-трафик**.

3. Если необходимо, включите журналирование событий

4. Сохраните изменения.

Чтобы начать блокирование трафика в соответствии с настроенным WebSocket-профилем, его нужно выбрать в качестве профиля безопасности в правиле публикации.

Настройка WebSocket-профиля для фильтрации WebSocket-соединений

Чтобы создать WebSocket-профиль, фильтрующий WebSocket-соединения:

1. В разделе **Настройки → Политика безопасности → WebSocket-профили** нажмите **Добавить**.

2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** укажите название профиля.

3. Настройте один или несколько параметров фильтрации WebSocket-соединений:

   - На вкладке **Общие** включите проверку целостности запроса, установив соответствующий флажок.

   - На вкладке **Источники** установите флажок **Учитывать Origin**, нажмите **Создать и добавить новый объект** и создайте список URL источников, с которыми разрешается устанавливать WebSocket-соединение.

> **Примечание**
> **Вы также можете настроить WebSocket-профиль, игнорирующий источники, запрашивающие WebSocket-соединение. Для этого на вкладке «Источники» нужно сформировать список нежелательных источников либо добавить предустановленные списки и включить «Инвертировать».**

- На вкладке **Расширения и протоколы** установите флажки **Учитывать Sec-WebSocket-Extensions** и **Учитывать Sec-WebSocket-Protocols** и добавьте списки разрешенных расширений и субпротоколов, которые указываются в заголовках Sec-WebSocket-Extensions и Sec-WebSocket-Protocols. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные значения.

> **Примечание**
> **Вы также можете настроить WebSocket-профиль на игнорирование WebSocket-соединений по запросам, в заголовках которых найдены расширения и субпротоколы из добавленных списков. Для этого на вкладке «Расширения и протоколы» нужно добавить списки нежелательных расширений и субпротоколов и включить «Инвертировать».**

4. Если необходимо, на вкладке **Общие** включите журналирование событий.

5. Сохраните изменения.

Чтобы начать фильтрацию WebSocket-соединений в соответствии с настроенным WebSocket-профилем, его нужно выбрать в качестве профиля безопасности в правиле публикации.

Создание списков расширений и субпротоколов для WebSocket-соединений

Handshake-запрос может содержать в том числе следующие заголовки:

- Sec-WebSocket-Protocol — содержит набор субпротоколов, которые клиент будет использовать при передаче данных.

- Sec-WebSocket-Extensions — содержит дополнительные расширения WebSocket-протокола, которые поддерживает браузер. Например, может быть указан метод сжатия передаваемых данных.

Вы можете создавать списки расширений и субпротоколов и использовать их в WebSocket-профиле для фильтрации WebSocket-соединений.

Чтобы создать список расширений:

1. В разделе **Настройки → Библиотеки → WebSocket-расширения** нажмите **Добавить** и укажите название списка.
2. Выберите тип списка:
   - **Локальный**, если список будет поддерживаться вручную.
   - **Обновляемый**, если список будет загружаться из внешнего источника. В этом случае укажите URL источника и настройте расписание автоматических обновлений списка.
3. Сохраните список.

Чтобы создать список субпротоколов:

1. В разделе **Настройки → Библиотеки → WebSocket-протоколы** нажмите **Добавить** и укажите название списка.
2. Выберите тип списка:
   - **Локальный**, если список будет поддерживаться вручную.
   - **Обновляемый**, если список будет загружаться из внешнего источника. В этом случае укажите URL источника и настройте расписание автоматических обновлений списка.
3. Сохраните список.

О настройке расписания обновлений списков

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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа».

Подключение WebSocket-профиля в правиле reverse-прокси

Чтобы подключить WebSocket-профиль в правиле reverse-прокси:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте или выберите из списка правило. Подробнее — в разделе «Публикация веб-сервисов».

2. В окне **Настройка правила публикации** на вкладке **Профили безопасности** установите флажок **Включить защиту WebSocket-соединений** и выберите нужный WebSocket-профиль.

3. Сохраните изменения.

Обработка дополнительных HTTP-заголовков

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.

В UserGate WAF вы можете использовать правила публикации 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.

Чтобы настроить обработку дополнительных HTTP-заголовков:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте правило. Подробнее об этом — в разделе «Публикация веб-сервисов».

2. В окне **Настройка правила публикации** на вкладке **Обработка заголовков** установите флажки для тех заголовков, которые будут добавлены в исходный запрос. Если заголовки уже содержатся в запросе, их значения будут переписаны.

3. Сохраните изменения.

БИБЛИОТЕКИ ЭЛЕМЕНТОВ

Описание

Данный большой раздел содержит в себе все записи, адреса сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил в UserGate WAF.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому

что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Подробнее о лицензии на продукт — в разделе «Лицензирование».

IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил UserGate WAF. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели **Группы** нажать на кнопку **Добавить**, дать название списку IP-адресов
Шаг 2. Указать адрес обновления списка (не обязательно).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе
Шаг 3. Добавить IP-адреса.	На панели **Адреса из выбранной группы** нажать на кнопку **Добавить** и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

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

Наименование	Описание
	`x.x.x.x` `y.y.y.y` `z.z.z.z`
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом UserGate WAF создать список IP-адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание** **URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.** Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое

Наименование	Описание
	из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Useragent браузеров

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список Useragent.	В панели **Категории** нажать на кнопку **Добавить** и задать название нового списка Useragent, опционально, описание списка и URL обновления
Шаг 2. Добавить необходимые Useragent браузеров в новый список.	В панели **Шаблоны useragent** добавить необходимый Useragent. Исчерпывающий список строк Useragent представлен тут: http://www.useragentstring.com/pages/useragentstring.php
Шаг 3. Создать UPL-правило, содержащее один или несколько списков.	Подробнее о персональных слоях — в разделе «Настройка параметров безопасности WAF»

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл **list.txt** со списком **Useragent**
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом UserGate WAF создать список Useragent. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов.

Наименование	Описание
	• Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Списки URL

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

Наименование	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля
Соответствие списку запрещенных URL Министерства Юстиции РФ	Данный список содержит URL, запрещенные Министерством Юстиции Российской Федерации
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ
Список фишинговых сайтов	Данный список содержит URL фишинговых сайтов
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В разделе **Библиотеки → Списки URL** нажать на кнопку **Добавить**, задать название нового списка.

Наименование	Описание
	Выбрать **Тип** списка — **Локальный** или **Обновляемый**. Для обновляемого списка указать **URL обновления** и настроить **Расписание скачивания обновлений**. Установить категорию создаваемого списка в поле **Чувствительность к регистру**: • **Чувствительный к регистру** — список URL адресов, чувствительных к регистру букв в адресе. • **Нечувствительный к регистру** — список URL адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах. • **Домен** — список адресов доменов для использования в правилах DNS-фильтрации. Категория списка задается при его создании. Изменить категорию после создания списка нельзя
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «$» и «*»: «*» — любое количество любых символов «^» — начало строки «$» — конец строки Символы «?» и «#» не могут быть использованы
Шаг 3. Создать UPL-правило, содержащее один или несколько списков.	Подробнее о персональных слоях — в разделе «Настройка параметров безопасности WAF»

Если URL-запись начинается с http://, «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

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

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

^http://domain.com/exacturl$

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

^http://domain.com/exacturl/

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

domain.com

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com mail.yahoo.com а также: qweryahoo.com	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyahoo.com/
^mail.yahoo.com$	Заблокирован только mail.yahoo.com	Заблокированы только: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/$	Ничего не заблокировано	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/$	Ничего не заблокировано	Заблокирован только: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не заблокировано	Заблокированы: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

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

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл **list.txt** со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания
Шаг 5. Создать список и указать URL для обновления.	На каждом UserGate WAF создать список URL. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание** **URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.** Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную.

Наименование	Описание
	При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах WAF. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему

элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели **Группы** нажать на кнопку **Добавить**, указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели **Элементы** нажать на кнопку **Добавить** и добавить интервал. Дать название интервалу и указать время.

Шаблоны страниц

С помощью шаблонов страниц вы можете настраивать вид страницы блокировки или страницы сетевых ошибок.

Шаблон страницы блокировки предназначен для настройки ответа, который возвращается клиенту, чей запрос был заблокирован WAF-правилом. Подробнее об этом — в разделе «Профили ответа».

Шаблон страницы сетевых ошибок предназначен для отображения информации об ошибках в работе сервера публикации.

Чтобы создать шаблон страницы:

1. На странице **Настройки** в разделе **Библиотеки → Шаблоны страниц** нажмите **Добавить** и выберите, шаблон какой страницы вы хотите создать.

2. В окне **Свойства шаблона страницы** укажите его название, выберите стандартный шаблон на нужном языке и, если необходимо, назначьте его шаблоном по умолчанию.

> **Примечание**
>
> **Чтобы применить созданный шаблон страницы сетевых ошибок, его нужно назначить шаблоном по умолчанию.**

3. Сохраните изменения.

По умолчанию шаблоны страниц настроены на отображение минимальной информации в стандартном оформлении. Вы можете использовать их в качестве

основы для создания пользовательских шаблонов в фирменном стиле компании, на другом языке или с дополнительными блоками информации.

Чтобы создать пользовательский шаблон страницы:

1. Добавьте новый 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 и внесите нужные изменения.

> **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.

Теперь, чтобы использовать пользовательский шаблон страницы блокировки, необходимо создать профиль ответа с этим шаблоном и затем этот профиль выбрать в параметрах блокирующих WAF-правил. Чтобы использовать пользовательский шаблон страниц сетевых ошибок, его достаточно назначить шаблоном по умолчанию.

Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели **Группы почтовых адресов** нажать на кнопку **Добавить**, дать название группе
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу, в панели **Почтовые адреса** нажать на кнопку **Добавить** и добавить необходимые почтовые адреса

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все устройства UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл **list.txt** со списком почтовых адресов
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом UserGate WAF создать список адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего).

Наименование	Описание
	• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели **Группы телефонных номеров** нажать на кнопку **Добавить**, дать название группе
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу, в панели **Группа телефонных номеров** нажать на кнопку **Добавить** и добавить необходимые номера

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл **list.txt** со списком номеров
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate WAF создать список адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего).

Наименование	Описание
	• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP: доставка сообщений по электронной почте.
- SMPP: доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля SMTP-сообщений необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN SMTP-сервера, который будет использоваться для отсылки почтовых сообщений
Порт	TCP-порт, используемый SMTP-сервером. Обычно для SMTP-протокола используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL
Авторизация	Включает авторизацию при подключении к SMTP-серверу
Логин	Имя учетной записи для подключения к SMTP-серверу
Пароль	Пароль учетной записи для подключения к SMTP-серверу

Для создания профиля SMPP-сообщений необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN SMPP-сервера, который будет использоваться для отсылки SMS-сообщений
Порт	TCP-порт TCP, используемый SMPP-сервером. Обычно для SMPP-протокола 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

Наименование	Описание
	можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8

Профили Netflow

Netflow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

UserGate WAF может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс UserGate WAF, необходимо выполнить следующие действия:

1. Создать профиль Netflow.
2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.

Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили Netflow** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля Netflow
Описание	Описание профиля Netflow
IP-адрес Netflow коллектора	IP-адрес сервера, куда сенсор будет отправлять статистику
Порт Netflow коллектора	UDP-порт, на котором коллектор будет принимать статистику

Наименование	Описание
Версия протокола	Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе
Таймаут активного потока (сек)	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд
Таймаут неактивного потока (сек.)	Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд
Количество потоков	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения
Отправлять информацию NAT	Отправлять информацию о NAT преобразованиях в статистику Netflow
Частота отправки шаблона (пакетов)	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов
Период отправки старого шаблона (сек.)	Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд

Профили LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

Наименование	Описание
Название	Название профиля LLDP
Описание	Описание профиля LLDP
Статус порта	Режим: • **Приём и передача данных LLDP** — NGFW будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • **Только приём данных LLDP** — NGFW не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • **Только передача данных LLDP** — NGFW будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей

Профили SSL

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в настройках веб-консоли, в настройках правил reverse-прокси.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля SSL
Описание	Описание профиля SSL
Протоколы SSL	**Минимальная версия TLS** — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. **Максимальная версия TLS** — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем
Наборы алгоритмов шифрования	Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и

Наименование	Описание
	подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • 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

Наименование	Описание
	• TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS GOST2012256 WITH 28147 CNT IMIT • TLS GOSTR341001 WITH 28147 CNT IMIT • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле **Выберите протокол для установки алгоритмов** необходимые версии протоколов TLS, нажать на кнопку **Применить**, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили SSL:

Наименование	Описание
Default SSL profile	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется

Наименование	Описание
Default SSL profile (GOST)	Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов, например, для веб-портала. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется
Default SSL profile (web console)	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль. **Важно!** Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!

ДИАГНОСТИКА И МОНИТОРИНГ

Мониторинг трафика

Раздел **Мониторинг трафика** позволяет получить список всех пользовательских соединений, установленных через UserGate WAF 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 для выбранного из списка IP-адреса источника.

> **Примечание**
>
> **Процесс построения данного отчета требует большего количества вычислительных ресурсов UserGate WAF и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на узел.**

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.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

Захват пакетов

Раздел **Захват пакетов** позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, wireshark. Это бывает необходимо для диагностирования сетевых проблем.

Раздел состоит из трех частей:

- **Фильтры** — здесь определяются условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть по ссылке http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.
- **Правила** — в правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** — сюда помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Чтобы записать трафик, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимый фильтр	Опционально. Можно воспользоваться предустановленными фильтрами или писать весь трафик, не фильтруя его
Шаг 2. Создать правило	Создать правило, в котором указать имя правила, имя файла, максимальный размер записываемого файла и необходимые фильтры
Шаг 3. Выбрать необходимое правило и начать запись	Выбрать необходимое правило и нажать на кнопку **Начать запись**. По окончании прекратить запись, нажав на кнопку **О становить запись**
Шаг 4. В разделе **Файлы**, скачать полученный файл	Скачать pcap-файл для анализа

Ping

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации
Счетчик	Количество повторов
Показывать timestamp	Добавляет timestamp в вывод команды
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена

Traceroute

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить
Использовать ICMP	Использовать ICMP-протокол для выполнения команды traceroute. Если не указано, то используется UDP-протокол
Интерфейс	С какого сетевого интерфейса выполнять команду
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена

Запрос DNS

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS-имя для проверки
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS-сервер, куда посылать запрос
Порт	UDP-порт, используемый для запроса
Тип DNS-запроса	Тип запроса

LLDP-соседи

Данный раздел отображает список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP.

Наименование	Описание
Chassis ID	

Наименование	Описание
	Идентификатор шасси; является обязательной TLV-записью LLDP-кадра. У каждого устройства UserGate есть только один Chassis ID. В качестве Chassis ID используется MAC-адрес интерфейса управления
SysName	Имя системы
SysDescr	Описание системы, содержит информацию об оборудовании и операционной системе устройства
Management	Адрес соседнего устройства. Содержит информацию: • IP-адреса интерфейса управления (IPv4 и IPv6). • Номер интерфейса указанного адреса управления
Capability	Функции устройства (например, маршрутизатор, коммутатор и т.п.)
Port ID	Идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit); является обязательной TLV-записью LLDP-кадра. В качестве идентификатора используется MAC-адрес интерфейса
PortDescr	Описание порта
TTL	Время жизни передаваемых пакетов LLDP; является обязательной TLV-записью LLDP-кадра. TTL задаётся в разделе **Консоль администратора → Настройки → Модули** в поле **Настройка LLDP**

Статистика LLDP

Данная вкладка отображает статистику интерфейсов, в настройках которых был указан профиль LLDP. Отображается следующая информация:

Наименование	Описание
Interface	Название интерфейса
Transmitted	Общее количество кадров LLDP, переданных через интерфейсе

Наименование	Описание
Received	Общее количество кадров LLDP, полученных на интерфейсе
Discarded	Число полученных на этом интерфейсе кадров LLDP, которые были отброшены
Unrecognized	Количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе
Ageout	В каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется
Inserted	Количество добавлений записей с информацией о соседях LLDP
Deleted	Количество удалений записей о соседях LLDP

ОПОВЕЩЕНИЯ

Правила оповещений

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или отправке пароля пользователю по SMS. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения	Подробнее об этом — в разделе «Профили оповещений»
Шаг 2. Создать группы получателей оповещений	Подробнее об этом — в разделах «Почтовые адреса» и «Номера телефонов»
Шаг 3. Создать правило оповещения	Во вкладке **Диагностика и мониторинг** в разделе **Оповещения → Правила оповещений** добавить правило

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило
Название	Название правила
Описание	Описание правила
Профиль оповещения	Созданный ранее профиль оповещения. Для SMPP-профилей появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде электронных адресов
От	От кого будет приходить оповещение
Тема	Тема оповещения
Таймаут перед повторной отправкой, секунд	Укажите 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
События	Укажите события, для которых необходимо получать оповещения
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения

SNMP

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.

2. Создать правило SNMP.

Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

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. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений
Комьюнити	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на SNMP-сервере. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию
Версия	Указывает версию SNMP-протокола, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе «Профили безопасности SNMP»

Параметр	Описание
События	Выбор типов параметров, доступных для мониторинга по правилу

> **Примечание**
> **Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования — в профиле безопасности SNMP) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.**

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Актуальные mib-файлы UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого необходимо перейти на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения → SNMP** нажать **Скачать MIB**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.
- UTM-TEMPERATURE-MIB.

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен

Наименование	Описание
trapCoreBootstrapEnd	Загрузка сервера завершена успешно
trapDefaultGatewayChanged	Изменение шлюза по умолчанию
trapHighSessionsCounter	Таблица сессий заполнена на 90%
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии
trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на "not_clean"
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера
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).

Наименование	Описание
	Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий
utmSessionsMax	integer	Максимальное количество активных сессий
utmUsers	integer	Количество активных пользователей на данный момент
utmUsersMax	integer	Максимальное количество активных пользователей
utmDataPartionFSStatus	integer	Состояние файловой системы. • **0** — clean. • **1** — not clean
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • **0** — master-узел. • **1** — slave-узел. • **3** — fault
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • **1** — связь с узлом потеряна. • **2** — HTTP прокси-сервер недоступен. • **3** — ни один из шлюзов недоступен. • **4** — DNS-сервер недоступен.

Наименование	Тип данных	Описание
		• **5** — узел UserGate Management Center недоступен
utmCPUUsage	integer	Загруженность центрального процессора (%)
utmMemory	integer	Использование оперативной памяти (%)
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%)
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • **no_raid**. • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • **no_raid** • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из

Наименование	Тип данных	Описание
		дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • **2** — partialDegraded — полный или частичный выход из строя одного из дисков. • **3** — failed — не работает из-за наличия ошибки. • **4** — offline — диск не доступен для RAID-контроллера
utmPowerSupply	integer	Количество источников питания: • **1** — один блок питания. • **2** — два блока питания
utmPowerSupplyStatus	integer	Состояние источника питания: • **no_power_supplies**. • **0** — off. • **1** — on
utmCSCIfName	string	Название интерфейса
utmCSCStatus	integer	Статус сетевого адаптера: • **1** — кабель подключен. • **2** — кабель не подключен
utmDiskIOUtilization	integer	Текущая утилизация диска (%)
utmLDAPServerName	string	Название LDAP-сервера
utmLDAPServerAddress	string	IP-адрес LDAP-сервера
utmThermSensor	string	

Наименование	Тип данных	Описание
		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. (*)

Наименование	Тип данных	Описание
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 60 секунд. (*)
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)

Наименование	Тип данных	Описание
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	Общее количество HTTP запросов. (*)
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы
haStatus	integer	Текущее состояние узла кластера
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %
memoryUsed	integer	Использование оперативной памяти; отображается в %
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %
powerSupply1Status	string	Состояние первого источника питания: • **no_power_supplies**. • **on**. • **off**
powerSupply2Status	string	Состояние второго источника питания: • **no_power_supplies**.

Наименование	Тип данных	Описание
		• **on**. • **off**
raidType	string	Тип RAID массива
raidStatus	string	Текущий статус RAID (Redundant Array of Independent Disks): • **no_raid**. • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива
diskIOUtilization	integer	Текущая утилизация диска (%)
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд

Примечание

Метрики, отмеченные в описании символом (*) не актуальны для *UGMC* и *LogAn*.

Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов

Наименование	Тип данных	Описание
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber
ifDescr	string	Описание интерфейса
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • **1** — other — неизвестный тип. • **2** — regular1822 — определён в BBN Report 1822. • **3** — hdh1822 — определён в BBN Report 1822. • **4** — ddn-x25 — определён в BBN Report 1822. • **5** — определён в стандарте канального уровня сетевой модели OSI X.25. • **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • **7** — iso88023-csmacd — определён в IEEE 802.3. • **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.

Наименование	Тип данных	Описание
		• **10** — iso88026-man — определён в стандарте ISO 88026 "MAN". • **11** — starLan — определён в стандарте IEEE 802.3e. • **12** — proteon-10Mbit — Proteon 10 Mbit • **13** — proteon-80Mbit — Proteon 80 Mbit. • **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM. • **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1 • **19** — e1 — европейский аналог T1. • **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции.

Наименование	Тип данных	Описание
		• **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • **22** — propPointToPointSerial — определён в стандарте RFC1213. • **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • **27** — nsip — XNS over IP — предназначен для использования в разнообразных

Наименование	Тип данных	Описание
		средах передачи данных. • **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **29** — ultra — ULTRA Technologies. • **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **32** — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду
ifPhysAddress	string	

Наименование	Тип данных	Описание
		Физический адрес интерфейса (MAC-адрес)
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • **1** — up — готов для передачи пакетов. • **2** — down — не работает. • **3** — testing — в режиме тестирования; рабочие пакеты не могут быть переданы
ifOperStatus	integer	Текущий статус работы интерфейса: • **1** — up — интерфейс готов для передачи пакетов. • **2** — down — интерфейс не может передавать пакеты данных. • **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. • **4** — unknown — интерфейс находится в неизвестном состоянии. • **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. • **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего

Наименование	Тип данных	Описание
		компонента, обычно аппаратного. • **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки
fInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке

Наименование	Тип данных	Описание
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передачи. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок
ifOutQLen	gauge32	Длина выходной очереди (в пакетах)
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки

Наименование	Тип данных	Описание
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости
ifHCOutOctets	counter64	Смысл одинаков со смыслом объекта **ifOutOctets** — количество байтов, переданное данным

Наименование	Тип данных	Описание
		интерфейсом, включая служебные; используется счётчик большей ёмкости
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutUcastPkts** — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutMulticastPkts** — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости
ifHCOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutBroadcastPkts** — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • **1** — enabled — включено. • **2** — disabled — отключено
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с

Наименование	Тип данных	Описание
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров
ifAlias	string	Название интерфейса, заданное администратором
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса

UTM-TEMPERATURE-MIB

Наименование	Тип данных	Описание
termNumber	integer	Количество температурных сенсоров на данной платформе
thermLowerThreshold	integer	Нижний предел рабочей температуры
thermUpperThreshold	integer	Верхний предел рабочей температуры
thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry)
thermEntry	sequence	

Наименование	Тип данных	Описание
		Информация о конкретном сенсоре: • thermName (string) — название сенсора. • thermValue (integer) — показание сенсора. • thermUnit (string) — единица измерения показаний сенсора

Примечание

Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание

Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учётом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

Данный раздел используется для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP. Параметры SNMP задаются для каждого узла индивидуально.

Наименование	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP
SNMP локация системы	Информация о физическом расположении SNMP-агента

Наименование	Описание
SNMP описание системы	Описание системы
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как **фиксированная** (не более 8 байт) или **динамическая** (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**. Engine ID может быть сформирован в формате: • IPv4 (ip4). • IPv6 (ipv6). • MAC-адрес (mac). • Текст (text). • Октеты (octets)

Профили безопасности SNMP

В данном разделе производиться настройка профилей безопасности для аутентификации SNMPv3-менеджера.

> **Примечание**
> **Настройки аутентификации для SNMP v3 (имя пользователя, пароль, тип и алгоритм аутентификации, алгоритм и пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate**

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

Описание

UserGate WAF журналирует все события, происходящие во время его работы, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением параметров устройства, например, авторизацией администраторов или обновлением библиотек.
- **Журнал веб-доступа** — подробные сведения о веб-запросах, обработанных UserGate WAF.
- **Журнал WebSocket** — данные об установленных и заблокированных WebSocket-соединениях.

- **Журнал трафика** — подробные сведения о срабатываниях правил межсетевого экрана. Для регистрации срабатываний правила необходимо включить журналирование в свойствах этого правила.

В разделе **Журналы и отчеты → Журналы** вы можете управлять данными журналов: просматривать эти данные, фильтровать их, скачивать в CSV-файл, а также экспортировать на внешние серверы.

> **Примечание**
>
> **При настроенной интеграции с UserGate Log Analyzer или UserGate SIEM журналы UserGate WAF хранятся и обрабатываются в базе данных внешнего сервера.**

UserGate WAF автоматически освобождает дисковое пространство путем ротации журналов. По мере заполнения выделенного объема диска старые записи перезаписываются новыми (кроме журнала событий). Уведомления об этом фиксируются в журнале событий, записи которого не ротируются.

Журнал событий

Журнал событий отображает события, связанные с изменением настроек WAF, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал веб-доступа

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL в настройках которых включено журналирование. Отображается следующая информация:

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Useragent браузера.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал WebSocket

Если для сервера reverse-прокси настроены правила, фильтрующие WebSocket-соединения, вы можете отслеживать события, связанные с установленными или заблокированными WebSocket-соединениями. Результаты фильтрации WebSocket-соединений отображаются на странице **Журнал WebSocket**. Запись событий в журнал ведется для правил reverse-прокси, в которых разрешено журналирование этих событий.

Чтобы разрешить запись событий в журнал WebSocket:

1. В разделе **Настройки → Политика безопасности → WebSocket-профили** выберите WebSocket-профиль или настройте новый. Подробнее — в разделе «Защита WebSocket-соединений».

2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** установите флажок **Включить журналирование** и сохраните изменения.

3. Убедитесь, что WebSocket-профиль с включенным журналированием подключен в правиле reverse-прокси.

На странице **Журнал WebSocket** можно настроить сортировку и отображение данных с помощью меню, которое вызывается из заголовка любого столбца. Вы также можете просмотреть подробную информацию о событии, дважды нажав на нужную запись.

Для поиска событий записи могут быть отфильтрованы по различным критериям, например по зоне источника, действию или дате.

С помощью кнопки **Экспортировать в CSV** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал трафика

Журнал трафика отображает события срабатывания правил WAF, в настройках которых включено журналирование. Отображается следующая информация:

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.
- Байт отправлено/получено.
- Пакетов отправлено/получено.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Экспорт журналов

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate WAF поддерживает выгрузку следующих журналов:

- журнал событий;
- журнал веб-доступа;
- журнал WebSocket;
- журнал трафика;
- атаки.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Параметр	Описание
Название правила	Название правила экспорта журналов
Описание	Опциональное поле для описания правила
Параметры разового экспорта	Выбор диапазона экспорта журналов. Опция доступна в версии ПО 7.2.0 и выше

Параметр	Описание
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • **Журнал событий**; • **Журнал веб-доступа**; • **Журнал трафика**; • **Журнал WebSocket** (доступно начиная с версии ПО 7.4.1); • **Атаки**. 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 — в разделе «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.

Параметр	Описание
	• **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
Объект	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 узла, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN)
Название приложения	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	

Параметр	Описание
	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • **Ежедневно**; • **Еженедельно**; • **Ежемесячно**; • **Каждые ... часов**; • **Каждые ... минут**; • **Задать вручную**. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день

Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. UserGate WAF предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31

Наименование	Описание
	будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date<='2019-03-28T20:59:59' AND statusCode=303
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date>="2019-03-13T21:00:00" AND statusCode=200
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404)
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, которые не содержат указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')

Наименование	Описание
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax

При составлении расширенного запроса UserGate WAF 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 WAF автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Описание форматов журналов

Экспорт журналов в формате CEF

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	events
	Origin	Модуль, в котором произошло событие	admin_console
	Severity	Важность события	Может принимать значения: • 1 — информационные; • 4 — предупреждения; • 7 — ошибки; • 10 — критичные
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство,	wafcore@ersthetatica

Тип поля	Название поля	Описание	Пример значения
		генерирующее это событие	
	act	Тип события	login_successful
	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	WAF
	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

Тип поля	Название поля	Описание	Пример значения
			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	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта	{"id": 39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня	TCP.
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	username
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535

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
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.)	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении	40

Тип поля	Название поля	Описание	Пример значения
		назначение — источник	
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания 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 указания 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)

Тип поля	Название поля	Описание	Пример значения
	cs6Label	Поле указывает, было ли содержимое расшифровано	Decrypted
	cs6	Статус расшифрования: расшифровано или нет	true, false
	flexString1Label	Поле используется для указания типа контента	Media type
	flexString1	Тип контента	text/html
	flexString2Label	Поле используется для указания категории запрашиваемого URL-адреса	URL Categories
	flexString2	Категория URL	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества переданных	Packets received

Тип поля	Название поля	Описание	Пример значения
		пакетов в направлении назначение — источник	
	cn2	Количество переданных пакетов в направлении назначение — источник	1
	cn3Label	Поле используется для указания исходного ответа сервера	Response
	cn3	Код ответа HTTP	302

Формат журнала веб-доступа **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	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**		1652344423822

Тип поля	Название поля	Описание	Пример значения
		Время, когда было получено событие: миллисекунды с 1 января 1970 года	
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня	TCP.
	src	IPv4-адрес 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	GET

Тип поля	Название поля	Описание	Пример значения
		доступа к URL-адресу (POST, GET и т.п.)	
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	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,	Default Allow

Тип поля	Название поля	Описание	Пример значения
		срабатывание которого вызвало событие	
	cs2Label	Поле используется для указания зоны источника	SrcZone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для указания зоны назначения	DstZone
	cs3	Название зоны назначения	Untrusted
	flexString1Label	Поле используется для указания категории запрашиваемого URL-адреса	URLCats
	flexString1	Категория URL	Computers & Technology
	cn1Label	Поле используется для указания исходного ответа 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, имя правила, имя зоны.

Формат журнала WebSocket (версия 7.4.1 и выше)

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	NGFW
	Device Version	Версия продукта	7
	Source	Тип журнала	websocket
	Origin	Источник события	log
	Severity	Уровень опасности	Не используется. Поле передается с пустыми данными
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1759728622455
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
	act	Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
	reason	Информация о причине возникновения события	{"request":"GET / ws HTTP/ 1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-

Тип поля	Название поля	Описание	Пример значения
			websocket-version: 13\r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com\r\n\r\n","response":"HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8ssleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-server\r\n\r\n","websocket_profile_name":"test","websocket_profile_guid":"9e939b74-5620-46de-ad4b-7df4a90bd3fb"}
	proto	Используемый протокол 4-го уровня	TCP или SSL
	app	Используемый протокол прикладного уровня и его версия	HTTP/1.1
	src	IPv4-адрес источника трафика	10.10.10.10

Тип поля	Название поля	Описание	Пример значения
	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 HTTP-запроса	GET
	request	URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com
	requestContext	URL-адрес 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	40

Тип поля	Название поля	Описание	Пример значения
		назначение — источник	
	cs1Label	Поле используется для указания срабатывания правила reverse-прокси	Rule
	cs1	Название правила reverse-прокси, срабатывание которого вызвало событие	Test rule
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Management
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Management
	cs5Label	Поле используется для указания страны назначения	Destination Country
	cs5	Название страны назначения	RU (отображается двухбуквенный код страны)

Тип поля	Название поля	Описание	Пример значения
	flexString1Label	Поле используется для указания типа контента	Media type
	flexString1	Тип контента	application/json
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник	1
	cn3Label	Поле используется для указания кода HTTP-ответа	Response
	cn3	Код HTTP-ответа	101

Формат журнала WebSocket **CEF Compact**

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	NGFW
	Device Version	Версия продукта	7
	Source	Тип журнала	websocket
	Origin	Источник события	log
	Severity	Уровень опасности	Не используется. Поле передается с пустыми данными
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1759728622455
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
	act	Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
	reason	Информация о причине возникновения события	{"request":"GET / ws HTTP/1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-

Тип поля	Название поля	Описание	Пример значения
			websocket-version: 13\r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com\r\n\r\n","response":"HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8ssleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-server\r\n\r\n","websocket_profile_name":"test","websocket_profile_guid":"9e939b74-5620-46de-ad4b-7df4a90bd3fb"}
	proto	Используемый протокол 4-го уровня	TCP или SSL
	app	Используемый протокол прикладного уровня и его версия	HTTP/1.1
	src	IPv4-адрес источника трафика	10.10.10.10

Тип поля	Название поля	Описание	Пример значения
	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 HTTP-запроса	GET
	request	URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com
	requestContext	URL-адрес 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	40

Тип поля	Название поля	Описание	Пример значения
		назначение — источник	
	cs1Label	Поле используется для указания срабатывания правила reverse-прокси	Rule
	cs1	Название правила reverse-прокси, срабатывание которого вызвало событие	Test rule
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Management
	cs3Label	Поле используется для указания страны источника	Source Country
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3

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	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие	firewall
	Threat Level	Уровень угрозы приложения	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками	accept

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня	TCP или UDP
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	smac	MAC-адрес источника	00:50:56:80:28:08
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	dmac	MAC-адрес назначения	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40

Тип поля	Название поля	Описание	Пример значения
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT)	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT)	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Allow trusted to untrusted
	cs2Label	Поле используется для указания зоны источника	Source Zone
	cs2	Название зоны источника	Trusted
	cs3Label	Поле используется для указания страны источника	Source Country

Тип поля	Название поля	Описание	Пример значения
	cs3	Название страны источника	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Untrusted
	cs5Label	Поле используется для указания страны назначения	Destination Country
	cs5	Название страны назначения	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник	Packets received

Тип поля	Название поля	Описание	Пример значения
	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	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие	firewall
	Threat Level	Уровень угрозы приложения	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство,	wafcore@ersthetatica

Тип поля	Название поля	Описание	Пример значения
		генерирующее это событие	
	act	Действие, принятое устройством в соответствии с настроенными политиками	accept
	proto	Используемый протокол 4-го уровня	TCP или UDP
	src	IPv4-адрес источника трафика	10.10.10.10
	spt	Порт источника	Может принимать значения от 0 до 65535
	smac	MAC-адрес источника	00:50:56:80:28:08
	dst	IPv4-адрес назначения трафика	194.226.127.130
	dpt	Порт назначения	Может принимать значения от 0 до 65535
	dmac	MAC-адрес назначения	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные	40

Тип поля	Название поля	Описание	Пример значения
		передаются в направлении назначение — источник	
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT)	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT)	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT)	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника	SrcZone
	cs2	Название зоны источника	Trusted

Тип поля	Название поля	Описание	Пример значения
	cs3Label	Поле используется для индикации зоны назначения	DstZone
	cs3	Название зоны назначения	Untrusted

Формат журнала атак

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	UserGate
	Device Product	Тип продукта	WAF
	Device Version	Версия продукта	7
	Source	Название журнала	waf
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); принимает значение 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,	wafcore@ersthetatica

Тип поля	Название поля	Описание	Пример значения
		генерирующее это событие	
	act	Действие, принятое устройством в соответствии с настроенными политиками	deny
	proto	Используемый протокол 4-го уровня	TCP.
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	Unknown
	src	IPv4-адрес 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	http://www.secure.com

Тип поля	Название поля	Описание	Пример значения
		указанием используемого протокола	
	requestContext	URL источника запроса (реферер HTTP)	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник	40
	cs1Label	Поле используется для указания срабатывания правила	Rule
	cs1	Название правила, срабатывание которого вызвало событие	Default Allow
	cs2Label	Поле используется для указания идентификатора правила	Rule Id

Тип поля	Название поля	Описание	Пример значения
	cs2	Идентификатор правила	200016017
	cs3Label	Поле используется для указания зоны источника	Source Zone
	cs3	Название зоны источника	Trusted
	cs4Label	Поле используется для указания страны источника	Source Country
	cs4	Название страны источника	RU (отображается двухбуквенный код страны)
	cs5Label	Поле используется для указания зоны назначения	Destination Zone
	cs5	Название зоны назначения	Untrusted
	cs6Label	Поле используется для указания страны назначения	Destination Country
	cs6	Название страны назначения	RU (отображается двухбуквенный код страны)
	cs7Label	Поле используется для указания профиля ответа	Response Profile
	cs7	Название профиля ответа	Unknown

Тип поля	Название поля	Описание	Пример значения
	cs8Label	Поле используется для указания названия исключения	Exception Name
	cs8	Название исключения	exampleException Name
	cs9Label	Поле используется для указания идентификатора исключения	Exception Id
	cs9	Идентификатор исключения	522d6f5b-af87-4473-91e3-780d8874056d
	cs10Label	Поле используется для указания названия пакета экспертизы	Package Name
	cs10	Название пакета экспертизы	Owasp top 10
	cs11Label	Поле используется для указания версии пакета экспертизы	Package Version
	cs11	Версия пакета экспертизы	395
	cs12Label	Поле используется для указания идентификатора WAF-профиля	WAF Profile Id
	cs12	Идентификатор WAF-профиля	234f96b4-c011-4b6d-96ae-260b2a82895c
	cs13Label	Поле используется для указания	Real Ip

Тип поля	Название поля	Описание	Пример значения
		реального IP-адреса источника	
	cs13	Реальный IP-адрес источника	172.25.0.1
	cs14Label	Поле используется для указания названия страны реального IP-адреса источника	Real Country
	cs14	Название страны реального IP-адреса источника	RU (отображается двухбуквенный код стран)
	flexString1Label	Поле используется для указания типа контента	Media type
	flexString1	Тип контента	text/html
	flexString2Label	Поле используется для указания категории запрашиваемого URL-адреса	URL Categories
	flexString2	Категория URL	Computers & Technology
	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 переданных пакетов в направлении назначение — источник	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник	1
	cn3Label	Поле используется для указания исходного ответа сервера	Response
	cn3	Код ответа HTTP	302
	cn4Label	Поле используется для указания уровня угрозы	Threat Level
	cn4	Уровень угрозы	1
	cn5Label	Поле используется для указания времени обновления пакета	Package Update Time
	cn5	Время обновления пакета экспертизы в	1773237844774955

Тип поля	Название поля	Описание	Пример значения
		миллисекундах с 1 января 1970 года	

Формат журнала атак **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	WAF
	Device Version	Версия продукта	7
	Source	Тип журнала	waf
	Name	Тип источника	log
	Threat Level	Уровень угрозы категории URL	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); принимает значение 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	wafcore@ersthetatica
	act	Действие, принятое устройством в	deny

Тип поля	Название поля	Описание	Пример значения
		соответствии с настроенными политиками	
	proto	Используемый протокол 4-го уровня	TCP.
	app	Протокол прикладного уровня и его версия	HTTP/1.1
	suser	Имя пользователя	Unknown
	src	IPv4-адрес 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		https://www.google.com/

Тип поля	Название поля	Описание	Пример значения
		URL источника запроса (реферер HTTP)	
	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 указания идентификатора правила	Rule Id
	cs2	Идентификатор правила	200016017

Тип поля	Название поля	Описание	Пример значения
	cs3Label	Поле используется для указания зоны источника	Source Zone
	cs3	Название зоны источника	Trusted
	cs4Label	Поле используется для указания зоны назначения	Destination Zone
	cs4	Название зоны назначения	Untrusted
	cs5Label	Поле используется для указания профиля ответа	Response Profile
	cs5	Название профиля ответа	Unknown
	cn1Label	Поле используется для указания исходного ответа сервера	Response
	cn1	Код ответа HTTP	302
	cn2Label	Поле используется для указания уровня угрозы	Threat Level
	cn2	Уровень угрозы	1
	flexString1Label	Поле используется для указания категории запрашиваемого URL-адреса	URLCats
	flexString1	Категория URL	Computers & Technology

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	wafcore@ersthetatica
ip_address	IPv4-адрес источника события	192.168.174.134
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

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	

Название поля	Описание	Пример значения
		a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
reasons	Причина, по которой было создано событие, например причина блокировки сайта.	"url_cats":[{"id": 39,"name":"Social Networking","threat_level":3}]
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

Название поля			Описание	Пример значения
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
request_id			Идентификатор запроса	12e4d951-a4a6-4338-a5bb-81a7f4130d93
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

Название поля			Описание	Пример значения
	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
real_ip	**country**		Название страны реального IP-адреса источника	RU (отображается двухбуквенный код страны)
	ip		Реальный IP-адрес источника	172.25.0.1
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика	Untrusted
	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			Имя пользователя	null

Описание журнала WebSocket (версия 7.4.1 и выше)

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	00000006-0a00-010c-c404-ac196d411f90
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@havntohanmin
reasons	Информация о причине возникновения события	{"request":"GET /ws HTTP/1.1\r\nConnection: upgrade\r\nUpgrade: websocket\r\nContent-Length: 0\r\nsec-websocket-version: 13\ r\nsec-websocket-key: +V9uPwL0ZfDTjmwMvnVUZA==\r\nHost: w.com\r\n\r\n","response":"HTTP/1.1 101 Switching Protocols\r\naccess-control-allow-origin: *\r\nX-Request-ID: d8814097-a68c-4120-8912-23a11b8e88da\r\nConnection: Upgrade\r\nDate: Mon, 06 Oct 2025 05:35:52 GMT\r\nsec-websocket-accept: mn0nG2s62J2pY5E8ssleD2gnGRQ=\r\nServer: Cowboy\r\nUpgrade: websocket\r\nx-test-srv: pft-server\r\n\r\n","websocket_profile_name":"test","websocket_profile_guid":"9e939b74-5620-46de-ad4b-7df4a90bd3fb"}
proto	Используемый протокол 4-го уровня	TCP или SSL
host	Имя хоста	w.com

Название поля		Описание	Пример значения
action		Действие, предпринятое модулем анализа websocket-трафика на устройстве	pass или deny
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
request_method		Метод HTTP-запроса	GET
url		URL-адрес запрашиваемого ресурса с указанием используемого протокола	http://www.w.com
media_type		Тип контента	application/json
status_code		Код HTTP-ответа	101
http_referer		URL-адрес 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
request_id		Идентификатор запроса	
application	**id**	Идентификатор приложения	Не используется. Поле передается с пустыми данными
	name	Название приложения	Не используется.

Название поля			Описание	Пример значения
				Поле передается с пустыми данными
	threat_level		Уровень угрозы приложения	Не используется. Поле передается с пустыми данными
	app_protocol		Протокол прикладного уровня	HTTP/1.1
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика	Management
	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	Может отсутствовать
real_ip	**country**		Название страны реального IP-адреса источника	RU (отображается двухбуквенный код страны)
	ip		Реальный IP-адрес источника	172.25.0.1
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика	**Management**
	country		Название страны назначения	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика	104.19.197.151

Название поля		Описание	Пример значения
	port	Порт назначения	Может принимать значения от 0 до 65535
	mac	MAC-адрес назначения	Может отсутствовать
rule	**guid**	Уникальный идентификатор правила reverse-прокси, срабатывание которого создало событие	59e38e06-533a-4771-9664-031c3e8b2e1f
	type	Тип правила	Не используется. Поле передается с пустыми данными
	name	Название правила reverse-прокси, срабатывание которого вызвало событие	test rule

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	wafcore@ersthetatica
proto	Используемый протокол 4-го уровня	TCP или UDP
action	Действие, принятое устройством в соответствии с настроенными политиками	accept
bytes_sent	Количество байтов, переданных в направлении источник — назначение	100

Название поля			Описание	Пример значения
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
	port		Порт источника	Может принимать значения от 0 до 65535

Название поля			Описание	Пример значения
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

Описание журнала атак

Название поля	Описание	Пример значения
timestamp		2022-05-12T08:11:46.15869Z

Название поля	Описание	Пример значения
	Время получения события в формате yyyy-mm-ddThh:mm:ssZ	
session	Идентификатор сессии	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	wafcore@ersthetatica
proto	Используемый протокол 4-го уровня	TCP
host	Имя хоста	www.google.com
action	Действие, принятое устройством в соответствии с настроенными политиками	block
rule_id	Идентификатор правила	200016017
waf_profile_name	Название WAF-профиля	wafProfileName
waf_profile_id	Идентификатор WAF-профиля	522d6f5b-af87-4473-91e3-780d8874056d
waf_layer_name	Название WAF-слоя	Detection Evasion
response_profile_name	Название профиля ответа	Unknown
threat_level	Уровень угрозы атаки	Может принимать значения: • 0 — нулевой; • 1 — низкий; • 2 — средний; • 3 — высокий
package_name	Название пакета экспертизы	Owasp top 10
package_version	Версия пакета экспертизы	340
package_update_time		1773237844774955

Название поля	Описание	Пример значения
	Время обновления пакета экспертизы: миллисекунды с 1 января 1970 года	
exception_name	Название исключения	name
exception_id	Идентификатор исключения	b4ce2bfa-b090-4318-a4b2-676c5ff62051
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/
useragent	Useragent пользовательского браузера	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
request_id	Идентификатор запроса	931d66e1-7d3a-4870-9791-b05b5eb6c01a

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"
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
real_ip	**country**		Название страны реального IP-адреса источника	RU (отображается двухбуквенный код страны)
	ip		Реальный IP-адрес источника	172.25.0.1
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика	Untrusted
	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

Название поля		Описание	Пример значения
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		Имя пользователя	null
url_categories	**id**	Идентификатор категории, к которой относится URL	39
		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

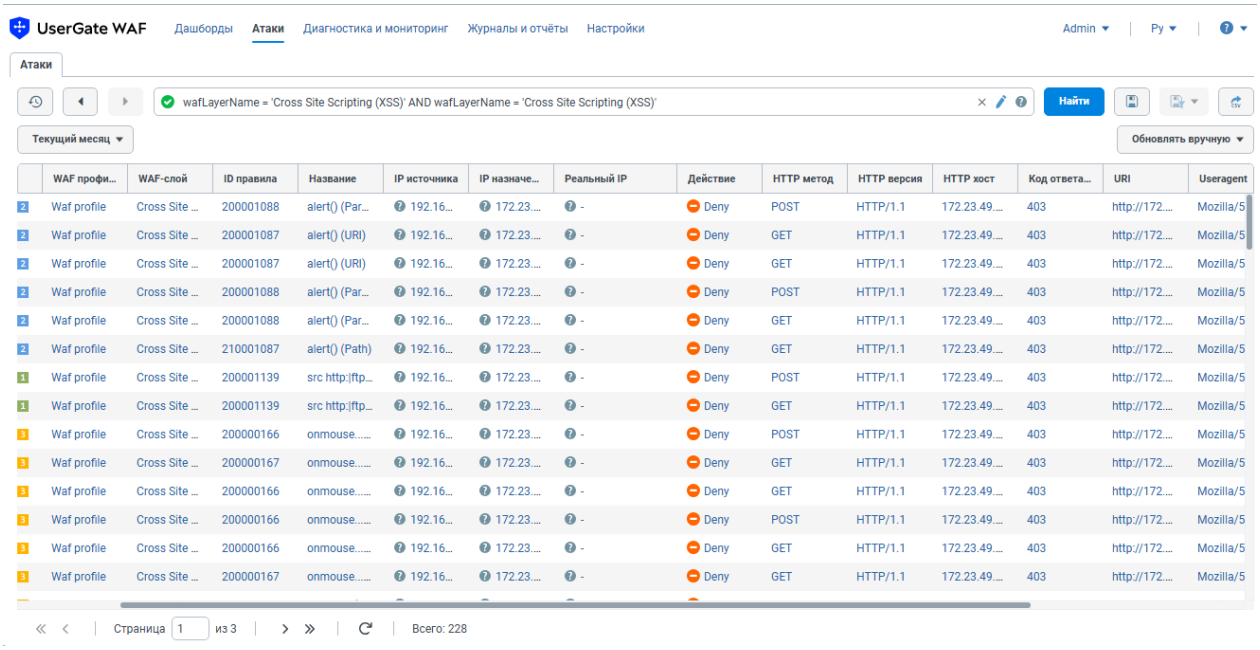
АТАКИ

Просмотр обнаруженных атак

UserGate WAF с настроенными WAF-правилами анализирует HTTP- и HTTPS-трафик на прикладном уровне, чтобы защитить веб-приложения от атак. Под атаками понимаются несанкционированные воздействия на информационную инфраструктуру организации, способные нарушить ее работу или создать угрозу безопасности обрабатываемой в ней информации. Продукт обнаруживает атаки и другие угрозы безопасности с помощью правил в WAF-профилях.

Страница атак

При срабатывании WAF-правила UserGate WAF записывает информацию об обнаружении атаки или другого события ИБ. Эти сведения доступны для просмотра и анализа в разделе **Атаки**.



В таблице атак вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);
- настраивать обновление данных;
- отображать данные за выбранный период времени.

Вы также можете фильтровать данные в таблице с помощью специальных запросов на языке фильтрации продукта. Для ввода запросов используется строка фильтрации. По нажатию на значение параметра срабатывания в строку фильтрации добавляется запрос с этим параметром (например, `name = "(PSM) alert"`). Действие доступно только для тех параметров, значения которых в таблице отображаются в виде ссылок.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**.

> **Примечание**
>
> **Вы можете отправлять сведения об атаках на серверы SSH (SFTP), FTP и Syslog. Подробнее — в разделе «Экспорт журналов».**

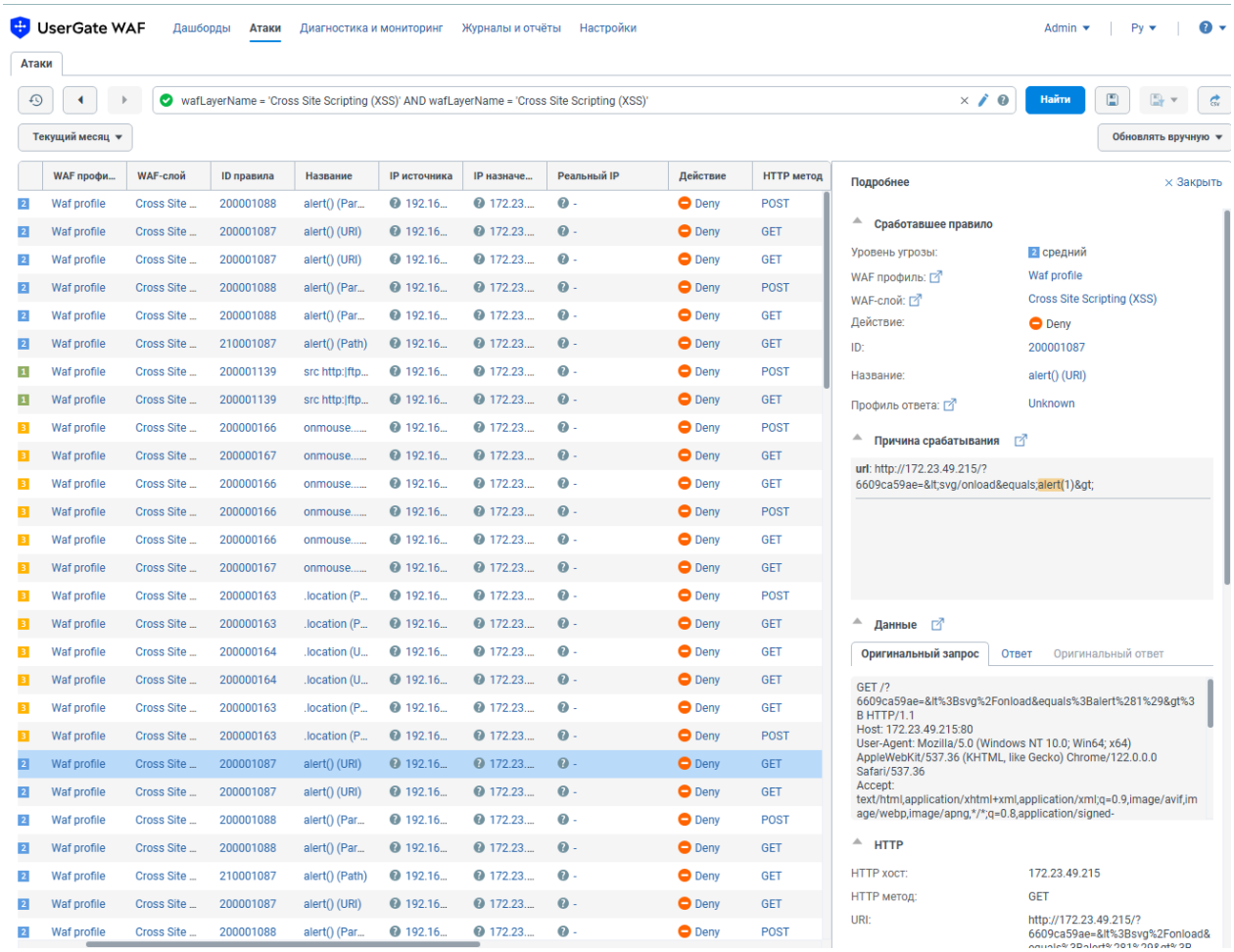
Для каждого срабатывания в списке отображается следующая информация.

Параметр	Описание
Время	Время срабатывания WAF-правила
Уровень угрозы	Уровень опасности угрозы согласно срабатыванию WAF-правила
WAF-профиль	Профиль, к которому относится сработавшее WAF-правило.
WAF-слой	Слой, к которому относится сработавшее WAF-правило.
ID правила	Идентификатор сработавшего WAF-правила
Название	Название сработавшего WAF-правила
IP источника	IP-адрес источника HTTP-запроса
IP назначения	IP-адрес назначения HTTP-запроса
Реальный IP	Реальный IP-адрес источника HTTP-запроса
Действие	Действие, выполненное в результате срабатывания WAF-правила
HTTP метод	Метод HTTP-запроса
HTTP версия	Версия HTTP-протокола
HTTP хост	Адрес узла, которому направлен HTTP-запрос
Код ответа HTTP	Код HTTP-ответа
URI	URI в HTTP-запросе

Параметр	Описание
Useragent	Информация о клиенте в HTTP-запросе
Референр	Ссылка на предыдущую страницу в HTTP-запросе
Профиль ответа	Название профиля ответа, который возвращается клиенту, если его HTTP-запрос был заблокирован WAF-правилом
Идентификатор запроса	Уникальный идентификатор HTTP-запроса

Карточка атаки

По нажатию на строку срабатывания открывается карточка с подробной информацией о сработавшем WAF-правиле: источнике и назначении запроса, пакете экспертизы, в состав которого входит сработавшее WAF-правило, и другими сведениями.



В карточке атаки представлена информация, позволяющая анализировать причину срабатывания WAF-правила и облегчающая поиск ложных срабатываний. В секции **Причина срабатывания** отображаются подсвеченные

значения или фрагменты запроса, на которых сработало WAF-правило. В ряде случаев подсветка не применяется. Например, если WAF-правило сработало при обращении к определенной библиотеке, в секции указывается общая причина блокировки.

В секции **Данные** содержатся сведения о запросе и/или ответе, на которых сработало WAF-правило. На вкладке **Оригинальный запрос** отображается запрос к защищаемому веб-ресурсу, поступивший в UserGate WAF. Вкладка **Оригинальный ответ** содержит заголовки и оригинальное тело ответа от защищаемого веб-ресурса и становится доступной, если WAF-правило сработало на этом ответе. Если WAF-правило с блокирующим действием сработало на запросе, эта вкладка не будет доступна. Если в UserGate WAF ответ был модифицирован (например, из него была удалена чувствительная информация), на вкладке **Ответ** отобразится измененный вариант, а на вкладке **Оригинальный ответ** — ответ до его модификации в UserGate WAF.

ДАШБОРДЫ

Работа с дашбордами и виджетами

В UserGate WAF можно отслеживать текущее состояние устройства, объемы трафика, проходящего через него, работу систем фильтрации, статус лицензии и различные статистические данные, связанные с сетевой безопасностью. Эти данные представлены в виджетах на странице **Дашборды**.

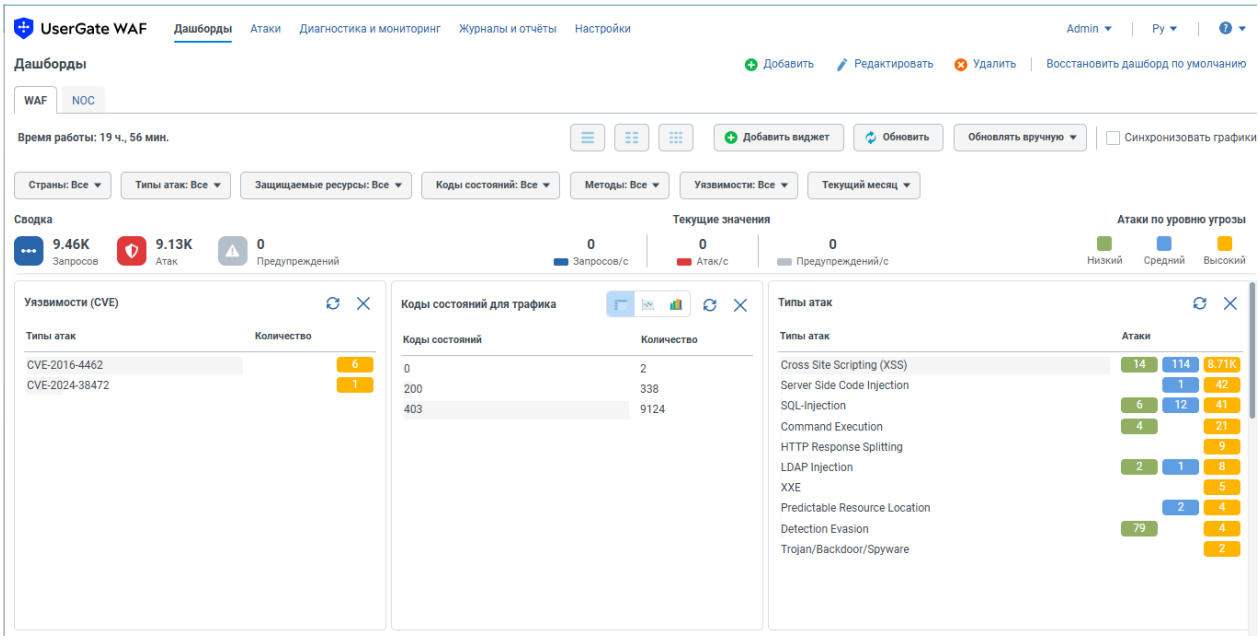
> **Примечание**
>
> **Просмотр и изменение дашбордов доступны, если в профиле доступа вашей учетной записи настроены соответствующие разрешения.**

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. В UserGate WAF есть два типа дашбордов:

- Дашборд **NOC** предназначен для размещения виджетов из коллекции **Центр управления сетью**, которые могут содержать информацию о

загрузке сетевых интерфейсов, статусе лицензии, обновлениях и другие данные, связанные с текущим состоянием устройства.

- На дашборде **WAF** вы можете размещать виджеты из коллекции **WAF** с данными, связанными с сетевой безопасностью. Фильтры, расположенные в верхней части этого дашборда, позволяют настроить отображение данных для всех виджетов, которые добавлены на этот дашборд. Например, настроив фильтры, вы можете просмотреть данные за последний месяц по выбранному типа атак. Сортировка записей на виджетах с индикацией уровня угроз выполняется по следующему принципу: сначала оценивается, угрозы каких уровней выявлены за выбранный период времени, затем выполняется сортировка по количеству угроз, начиная с максимально высокого уровня. Например, если за выбранный период времени были выявлены угрозы среднего и низкого уровня, первая запись в рейтинге будет отображать максимальное число угроз среднего уровня, даже если их будет меньше угроз низкого уровня.



В блоке **Сводка** представлены данные о запросах, атаках и предупреждениях, зафиксированных за выбранный период времени. В блоке **Текущие значения** отображается среднее количество запросов, атак и предупреждений за секунду.

Из некоторых виджетов из коллекции **WAF** по нажатию на нужную строку вы можете перейти на страницу **Атаки**, чтобы просмотреть подробную информацию, отфильтрованную по выбранному значению. Например, если в виджете **Типы атак** вы нажмете **SQL-Injection**, откроется страница **Атаки**, на которой будут отображены все записи, касающиеся этого типа атаки, за выбранный период.

Примечание

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.

Примечание

В виджете количества запросов из коллекции «WAF» учитываются все HTTP-запросы (RPS), которые дошли до UserGate WAF.

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения (Описание)

UserGate WAF позволяет производить настройки устройства с помощью интерфейса командной строки, или CLI (Command Line Interface). С помощью CLI администратор может выполнить ряд диагностических команд, таких, как ping, nslookup, traceroute, произвести сетевые настройки устройства, настройки политик безопасности, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании WAF), через последовательный порт или с помощью SSH по сети.

Внимание

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

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к WAF.	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB
Шаг 2. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin)

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к WAF.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к WAF
Шаг 2. Запустить терминал.	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1
Шаг 3. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin)

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны.	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200

Наименование	Описание
Шаг 2. Запустить SSH-терминал.	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес WAF, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: ssh *Admin@IPWAF* -p *2200*
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге

После успешной авторизации в CLI появится строка, ожидающая ввода команды (режим диагностики и мониторинга). Для просмотра текущих возможных значений или автодополнения необходимо использовать **Tab** или **?**. Доступны:

- **traceroute** — трассировка соединения до определённого хоста.
- **shutdown** — выключение WAF.
- **show** — просмотр сетевых настроек, мониторинг трафика, LLDP.
- **clear** — обновление информации OSPF и BGP.
- **check-geoip** — проверка принадлежности IP-адреса по текущей базе GeoIP.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка WAF.
- **date** — просмотр текущих даты и времени на сервере.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **configure** — переход в режим конфигурации.
- **dig** — проверка записи DNS-домена.

Данные команды доступны в режиме конфигурации; подробнее — в разделах «Команды execute» и «Команды диагностики и мониторинга».

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса WAF.

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

CLI поддерживает ввод команды в несколько строк (многострочный ввод). Для перехода на новую строку необходимо добавить "\" в конце строки. Начиная со второй строки ввод "\" необязателен; чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@nodename# set users user example \
... name username1
... enabled on
... groups [ "Default Group" ]
...
Admin@nodename#
```

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВИЧНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла (Описание)

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации CLI — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и

виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу radmin-emergency.

Доступные команды в режиме диагностики

Команды диагностики позволяют просмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Мониторинг трафика.
- Информацию о маршрутах.
- Отображение системной информации.
- Диагностику работы протоколов динамической маршрутизации.

Подробнее о синтаксисе и примерах использования команд диагностики — в разделе «Команды диагностики и мониторинга».

Доступные команды в режиме конфигурации

Для перехода в режим конфигурации используется команда:

```
Admin@WAF> configure
```

После перехода в режим конфигурации приглашение командной строки будет выглядеть следующим образом:

```
Admin@WAF#
```

В режиме конфигурации доступны команды *execute* (команды, которые не относятся к настройке конфигурации устройства — ping, date, traceroute и т.п.), команды настройки сети (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов), а также команды включения/отключения удалённого доступа к серверу radmin-emergency.

Подробнее о синтаксисе и примерах использования команд *execute* — в разделе «Режим конфигурации».

Подробнее о синтаксисе и примерах использования команд настройки сети — в следующих разделах:

- Команды настройки зон.
- Команды настройки интерфейсов.
- Команды настройки шлюзов.
- Команды настройки виртуальных маршрутизаторов.

Подробнее о синтаксисе и примерах использования команд включения/отключения удалённого доступа к серверу radmin-emergency читайте в разделе Настройка управления устройством.

Подробнее о первоначальной инициализации устройства с помощью CLI читайте в разделе Первоначальная инициализация.

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация (Описание)

Первоначальная инициализацию UserGate WAF с использованием интерфейса командной строки можно произвести несколькими способами.

Установка как главного узла.

Для настройки UserGate WAF в качестве главного узла используется команда:

```
Admin@nodename# execute install master
```

Необходимо указать параметры:

Параметр	Описание
`login`	Задать логин администратора
`password`	Задать пароль учётной записи администратора.

Параметр	Описание
	Указание пароля также доступно при нажатии **Enter** после указания логина администратора; необходимо дважды ввести пароль учётной записи

КОМАНДЫ ДИАГНОСТИКИ И МОНИТОРИНГА

Команды диагностики и мониторинга (Описание)

Команды диагностики позволяют просмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.
- Отображение системной информации.
- Диагностику работы протоколов маршрутизации.

Базовые команды управления

Для просмотра текущих даты и времени на узле используется команда:

```
Admin@nodename> date
```

Для перезагрузки узла используется команда:

```
Admin@nodename> reboot
```

Для выключения узла используется команда:

```
Admin@nodename> shutdown
```

Для перехода в режим конфигурации узла используется команда:

```
Admin@nodename> configure
```

Для выхода из интерфейса CLI используется команда:

```
Admin@nodename> exit
```

Команды проверки доступности сетевых ресурсов

Для проверки доступности определенного хоста утилитой ping используется команда:

```
Admin@nodename> ping <parameters>
```

С командой могут использоваться следующие параметры:

Параметр	Описание
host	IP-адрес или доменное имя хоста.
count	Количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C).
interface	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping.
interval	Интервал времени, через который будет производиться отправка пакетов; указывается в секундах.
mtu	Размер mtu отправляемых пакетов.
numeric	Не резолвить имена.
ttl	Время жизни пакета.

Параметр	Описание
timestamp	Отображение временных меток.
virtual-router	Имя виртуального маршрутизатора.

Для трассировки соединения до определённого хоста используется команда:

```
Admin@nodename> traceroute <parameters>
```

С командой могут использоваться следующие параметры:

Параметр	Описание
host	IP-адрес или доменное имя хоста, для которого производится трассировка.
interface	Интерфейс, с которого будут отправляться пакеты.
min-interval	Минимальный интервал между пакетами.
not-map-ip	Не искать hostname для IP-адреса при отображении.
port	Указать порт вместо порта по умолчанию (1 — 65535).
use-icmp-echo	Использовать ICMP echo.

Для проверки доступности стороннего HTTP/HTTPS-сервера используется команда:

```
Admin@nodename> netcheck <parameters>
```

С командой могут использоваться следующие параметры:

Параметр	Описание
address	Доменное имя хоста для проверки доступности по TCP или URL для HTTP.
type	Проверка доступности по: • **http**. • **tcp** (если порт не указан, то используется порт 80).

Параметр	Описание
check-cert	Проверка SSL-сертификата.
dns-ip	IP-адрес сервера DNS.
dns-tcp	Использование TCP вместо UDP для DNS-запроса.
data	Запрос содержимого сайта. По умолчанию запрашиваются только заголовки.
timeout	Максимальный таймаут ожидания ответа от веб-сервера.
user-agent	Параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.

Для проверки записи DNS домена используется команда:

```
Admin@nodename> dig <parameters>
```

С командой могут использоваться следующие параметры:

Параметр	Описание
host	Доменное имя хоста или IP-адрес для реверсивного поиска.
dns	Указание IP-адреса DNS-сервера.
reverse-lookup	Получение имени хоста по IP-адресу.
tcp	Использование протокола TCP вместо UDP.

Для проверки принадлежности IP-адреса по текущей базе GeoIP используется команда:

```
Admin@nodename> check-geoip ip <IP-address>
```

Статистика и информация об интерфейсах

Для отображения информации об интерфейсах используется следующая команда:

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

Для отображения статистики определенного интерфейса и информации о нём используется следующая команда:

```
Admin@nodename> show network interface <interface-name>
```

Также доступно отображение только информации или только статистики интерфейса:

```
Admin@nodename> show network interface <interface-name> type info
Admin@nodename> show network interface <interface-name> type statistics
```

Для отображения списка упорядоченных имён сетевых интерфейсов и соответствующих им физических адресов предназначена команда:

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

Упорядочивание интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используется следующая команда:

```
Admin@nodename> clear network interfac-mapping
```

После перезагрузки устройства UserGate список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенное устройство UserGate.

ARP-записи

Для просмотра информации о записях ARP:

```
Admin@nodename> show network arp
```

При просмотре записей доступно использование фильтров. Параметры фильтрации:

Параметр	Описание
node-name	Название узла кластера, ARP-записи которого необходимо отобразить. Далее необходимо указать интерфейс или IP-адрес хоста: `Admin@nodename> show network arp node-name <node-name> interface <iface-name>` `Admin@nodename> show network arp node-name <node-name> host <ip>`
interface	Название интерфейса WAF.
host	IP-адрес устройства.
mac	MAC-адрес устройства.

```
Admin@nodename> show network arp host <IP-address>
Admin@nodename> show network arp interface <interface-name>
Admin@nodename> show network arp mac <MAC-address>
```

Просмотр записей ARP также доступен в режиме конфигурации; команды идентичны командам в режиме диагностики и мониторинга.

> **Примечание**
>
> **В режиме диагностики и мониторинга действия производятся с системными записями; в режиме конфигурации – со статическими записями ARP.**

Добавление статических ARP-записей доступно в режиме конфигурации с использованием следующей команды:

```
Admin@nodename# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

Параметры команды:

Параметр	Описание
node-name	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP и MAC-адреса устройства.
interface	Название интерфейса WAF.
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 и мониторинга;
- **delete**: удаление статических записей в режиме конфигурации.

Далее будет представлен формат команд удаления на примере команд режима диагностики и мониторинга.

Для удаления системной записи:

```
Admin@nodename> clear network arp interface <iface-name> host <ip>
```

Чтобы удалить запись на другом узле кластера:

```
Admin@nodename> clear network arp interface <iface-name> node-name <node-name> host <ip>
```

Следующая команда позволяет удалить все системные записи на заданном интерфейсе (можно указать несколько интерфейсов):

```
 Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> … ]
```

Для удаления всех системных записей интерфейса другого узла:

```
 Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> … ] node-name <node-name>
```

Отслеживание пакетов

Чтобы произвести отслеживание пакетов, используется следующая команда:

```
Admin@nodename> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия портов источника и назначения UserGate, номера TCP/UDP портов источника и назначения. Команда также доступна в режиме конфигурации.

Чтобы выйти из режима отслеживания пакетов - **Ctrl+C**.

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации на уровне **network**. Для создания правила используется следующая команда:

```
Admin@nodename# create network trace-rules
```

Далее указываются следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила отслеживания пакетов: • **on**. • **off**.
name	Название правила. Если название правила не было задано, то оно задаётся автоматически в формате: trace_rule_N (где N — порядковый номер создаваемого правила отслеживания пакетов).
zones-in	Список зон источников трафика.
source-ip-lists	

Параметр	Описание
	Список групп IP-адресов источника пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов».
source-ip-addresses	Список IP-адресов источника пакета.
dest-ip-lists	Список групп IP-адресов назначения пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов».
dest-ip-addresses	Список IP-адресов назначения пакета.
services	Тип сервиса.

Пример команды создания правила:

```
Admin@nodename# create network trace-rules enabled on name "Test trace"
source-ip-addresses [ 192.168.0.100 ]
```

Для редактирования правила:

```
Admin@nodename# set network trace-rules <trace-rule-name>

Admin@nodename# set network trace-rules "Test trace" services
[ "[SYSTEM] Any ICMP" ]
```

Для изменения доступны параметры, представленные в таблице выше.

Чтобы просмотреть существующие правила отслеживания пакетов:

```
Admin@nodename# show network trace-rules
```

Для удаления правила отслеживания пакетов используется следующая команда:

```
Admin@nodename# delete network trace-rules <trace-rule-name>
```

Также доступно удаление значений отдельных параметров правил. Для удаления доступны:

- **zones-in**.
- **source-ip-lists**.
- **source-ip-addresses**.
- **dest-ip-lists**.
- **dest-ip-addresses**.
- **services**.

Мониторинг трафика

Следующая команда используется для мониторинга трафика:

```
Admin@nodename> show traffic
```

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Доступна фильтрация по: • **source-ip** — IP-адрес источника. • **source-port** — порт источника. • **dest-ip** — IP-адрес назначения. • **dest-port** — порт назначения. • **vlan-tag** — тег VLAN. • **interface-name** — название интерфейса. • **node-name** — название узла. • **protocol** — протокол.
connections	Отображение информации о соединениях (протокол и его номер; время жизни записи; IP-адреса источника и назначения, порты источника и назначения; IP-адреса источника и назначения, порты источника и назначения, которые ожидаются в ответе; статус сессии (UNREPLIED или ASSURED); количество переданных и принятых пакетов и байтов; зона источника; является ли эта сессия сессией известного WAF пользователя и т.п.).

Параметр	Описание
	Фильтрация доступна по: • **protocol** — протокол. • **source-ip** — IP-адрес источника. • **dest-ip** — IP-адрес назначения. • **node-name** — название узла. • **expect** — отображение неустановленных соединений: ◦ **on**. ◦ **off**.
capture	Отображение захвата пакетов. Доступна фильтрация по следующим параметрам: • **destination** — IP-адрес назначения • **destination-port** — порт назначения. • **ipv4-protocol** — номер протокола IPv4 (0-255). • **interfaces** — название интерфейса. • **protocol** — выбор протокола. • **rule** — выбор имеющегося правила для захвата пакетов. • **source** — IP-адрес источника. • **source-port** — порт источника.

Пример команды мониторинга трафика:

```
Admin@nodename> show traffic connections node-name utmcore@dineanoulwer
dest-ip 192.168.0.100 expect on
```

LLDP

Просмотр информации, полученной по LLDP (Link Layer Discovery Protocol), доступен с использованием команд:

```
Admin@nodename> show lldp
Admin@nodename> show lldp neighbors
Admin@nodename> show lldp statistics
```

Параметры команды:

Параметр	Описание
neighbors	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • **Chassis ID** — идентификатор шасси. • **SysName** — имя системы. • **SysDescr** — описание системы, содержит информацию об оборудовании и операционной системе устройства. • **Management** — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • **Capability** — функции устройства (например, маршрутизатор, коммутатор и т.п.). • **Port ID** — идентификатор порта с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • **PortDescr** — описание порта. • **TTL** — время жизни передаваемых пакетов LLDP.
statistics	Статистика интерфейсов, в настройках которых был указан профиль LLDP: • **Interface** — название интерфейса. • **Transmitted** — общее количество кадров LLDP, переданных через интерфейс. • **Received** — общее количество кадров LLDP, полученных на интерфейсе. • **Discarded** — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • **Unrecognized** — количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе. • **Ageout** — в каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется. • **Inserted** — количество добавлений записей с информацией о соседях LLDP. • **Deleted** — количество удалений записей о соседях LLDP.

> **Примечание**
> **Для просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на WAF (профили LLDP настроены в библиотеке элементов и активированы в настройках интерфейсов).**

Маршруты

Данный раздел необходим для проведения диагностики и мониторинга маршрутной информации на WAF.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

```
Admin@nodename> show network route
```

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить.
node-name	Выбор узла кластера.
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам WAF. 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	

Параметр	Описание
	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> | **all**).

Отображение системной информации

Для просмотра версии ПО системы используется команда:

```
Admin@nodename> show system version
```

Для отображения информации о количестве активных TCP/UDP/ICMP сессий на системе используется команда:

```
Admin@nodename> show system sessions
```

Для отображения информации о количестве активных сессий по отдельным протоколам или временным интервалам используется команда:

```
Admin@nodename> show system sessions counters [ parameters ]
```

Очистить статистику:

```
Admin@nodename> clear system sessions
```

Диагностика работы протоколов маршрутизации

С помощью команд этого раздела можно просматривать события debug-логов протоколов динамической маршрутизации. Включение в debug-лог событий конкретного протокола производится командой debug в режиме конфигурации. Подробнее — в разделе «Режим конфигурации».

Для просмотра записей debug-лога используется команда:

```
Admin@nodename> show log routing
```

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации интерфейса командной строки используется команда:

```
Admin@nodename> configure
```

В режиме конфигурации приглашение командной строки выглядит 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 конфигурации, который соответствует разделам веб-консоли UserGate WAF;

`<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: • `create` — создание новых объектов.

Наименование	Описание
	• `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. • `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». • `export` — экспорт сертификатов. Подробнее — в разделе «Команды export». • `import` — импорт конфигурации. Подробнее — в разделе «Команды import». • `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: `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:

Наименование	Описание
	`` 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# end Level: network interface Admin@nodename# end Level: network Admin@nodename# ``` Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду `top`: ``` Admin@nodename# top Level: network interface Admin@nodename# ```
`<level>`	Уровни в командной строке повторяют веб-интерфейс UserGate WAF: • `settings` — соответствует разделу веб-интерфейса «UserGate»;

Наименование	Описание
	• `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»; • `waf` — соответствует разделу веб-интерфейса «WAF»; • `global-portal` — соответствует разделу веб-интерфейса «Глобальный портал»; • `libraries` — соответствует разделу веб-интерфейса «Библиотеки»; • `logs` — 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` Будет отображена информация об интерфейсе port0 текущего узла WAF. 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 )`

Наименование	Описание
	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 IP-лист в библиотеке с названием New list: `Admin@nodename# create libraries ip-list name "New list"` Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо в список «New list» добавить IP-адреса: 10.10.0.2 и 10.10.0.3. Параметру `ips` необходимо задать аргумент `[ 10.10.0.2 10.10.0.3]`: `Admin@nodename# set libraries ip-list "New list" ips [ 10.10.0.2 10.10.0.3 ]` **Важно!** **Квадратные скобки должны быть отделены пробелами с обеих сторон**

Команды execute

Команды имеет следующую структуру:

```
Admin@nodename# execute <command-name>
```

Список команд раздела `execute`.

Параметр	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> ]`

Параметр	Описание
`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; • `request-limit` — срок действия запроса на генерацию кода. **Важно!** **Для использования данной команды необходимо наличие лицензии на модуль Cluster**
`date`	Просмотр текущих 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>` • `host` — доменное имя узла или IP-адрес для реверсивного поиска; • `reverse-lookup` — получение имени узла по IP-адресу; • `dns` — указание IP-адреса DNS-сервера; • `tcp` — использование протокола TCP вместо UDP
`factory-reset`	Возврат устройства в первоначальное состояние:

Параметр	Описание
	`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 заново с обрывом текущих сессий: `Admin@nodename# execute firewall force-changes`
`license`	Команда регистрации продукта: `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>`
`netcheck`	Проверка доступности стороннего HTTP и HTTPS-сервера. Можно задать следующие параметры: • `address` — доменное имя узла для проверки доступности по TCP или URL — для HTTP; • `dns-ip` — IP-адрес сервера DNS; • `dns-tcp` — использование TCP вместо UDP для DNS-запроса; • `check-cert` — проверка SSL-сертификата; • `type` — проверка доступности по: ◦ `http`; ◦ `tcp` (если порт не указан, то используется порт 80). • `data` — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; • `timeout` — максимальный тайм-аут ожидания ответа от веб-сервера;

Параметр	Описание
	• `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 узла. Можно задать следующие параметры: • `host` — IP-адрес или доменное имя узла. • `count` — количество отправляемых echo-запросов. Если параметр не задан, то 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. `Admin@nodename# execute ping host <hostname> count <number>`
`reboot`	Перезагрузка устройства: `Admin@nodename# execute reboot`

Параметр	Описание
`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. `Admin@nodename# execute traceroute host <hostname>`

Параметр	Описание
`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», «Политики сети», «Глобальный портал».

В разделах «Политики сети» (`network-policy`), «Глобальный портал» (`global-portal`) вы можете импортировать правила, написанные на UPL. При использовании импорта, все существующие правила будут заменены на указанные.

В разделе «Настройки» (`settings`) вы можете импортировать сертификаты. Подробнее — в разделе «Настройка сертификатов».

В разделе «Политики сети» (`network-policy`) вы можете импортировать правила межсетевого экрана и балансировки нагрузки. Подробнее — в разделах «Настройка правил межсетевого экрана» и «Настройка балансировки нагрузки».

В разделе «Глобальный портал» (`global-portal`) вы можете импортировать правила публикации. Подробнее о создании правил — в разделе «Настройка правил публикации».

Команды export

Команда для экспорта сертификатов.

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-
chain on
```

Вы можете экспортировать сертификаты, всю цепочку сертификатов и CSR:

Подробнее об управлении сертификатами — в разделе «Настройка сертификатов».

НАСТРОЙКА УСТРОЙСТВА

Базовые настройки

Настройка параметров работы CLI

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@nodename# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида: `Admin@nodename#`) на удобное вам.

Например, чтобы поменять вид системного приглашения на `NodeAABBCC`, выполните следующую команду:

```
Admin@nodename# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

```
Admin@nodename# set settings cli custom-prompt default
```

Пример использования команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@nodename#
```

Чтобы задать уровень детализации диагностики используется следующая команда:

```
Admin@nodename# 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@nodename# show settings cli
```

Настройка базовых параметров устройства

Настройка базовых параметров UserGate WAF выполняется 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. • `web-ssl-profile` — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». • `api-session-lifetime` — время ожидания сеанса администратора в секундах • `http-connection-timeout` — время ожидания установления HTTP-соединения в секундах. Значение по умолчанию — 20 секунд. (Доступно в версии ПО 7.5.0 и выше). • `http-loading-timeout` — время, выделенное на загрузку HTTP-контента в секундах. Значение по умолчанию — 60 секунд. (Доступно в версии ПО 7.5.0 и выше)

Раздел	Описание
server-time	Параметры установки точного времени: • `ntp-enabled` — включение или 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 модулей устройства: • `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. Указывается в секундах. ◦ `transmit-hold` — значение мультипликатора удержания. Может принимать значения от 1 до 100. Произведение значений `transmit delay` и `transmit hold` определяет время жизни (TTL) пакетов LLDP
cache	Параметры кэширования прокси-сервера: • `caching-mode` — включение или отключение режима кэширования. • `exclusions` — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду:

Раздел	Описание
	``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
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. Для задания расписания обновления программного обеспечения: ```Admin@nodename# set settings general updates-schedule software schedule <schedule/disabled>``` Расписание скачивания обновлений библиотек может быть единым:

Раздел	Описание
	`Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>` Также расписание может быть настроено отдельно для каждого элемента: `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 резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями. Команда для просмотра расписания обновлений: `Admin@nodename# show settings general updates-schedule`

Настройка управления устройством

Настройка диагностики

В этом блоке вы можете управлять параметрами диагностики устройства, необходимыми службе технической поддержки для решения возможных проблем.

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, 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 в работе NGFW;
- `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.

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
```

Настройка Radmin-emergency

Если произошли неполадки с ядром UserGate WAF, 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 WAF. 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@<WAF_IP> -p 2200
```

Команда включения и отключения удаленного доступа к серверу для технической поддержки в режиме emergency:

```
Admin@emergency@WAF# 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.

Настройка операций с сервером

В этом разделе вы можете установить канал получения обновлений для устройства (стабильные 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

Управление резервным копированием происходит на уровне `setting device-mgmt`.

Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

```
Admin@nodename# create settings device-mgmt settings-backup
<parameters>
```

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. 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

Параметр	Описание
	резервное копирование должно выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями

Изменение существующего правила резервного копирования устройства UserGate производится с помощью следующей команды:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения, аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Команда для отображения правила резервного копирования:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве параметра `<filter>` можно использовать не только названия правила, но и другие заданные в правиле параметры (см. список параметров в таблице выше).

Экспорт настроек

Управление экспортом настроек происходит на уровне `settings device-mgmt`.

Правила экспорта настроек создаются с помощью команды :

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Параметры экспорта настроек.

Параметр	Описание
enabled	Включение или отключение правила экспорта настроек устройства
name	Название правила экспорта
description	Описание правила экспорта
type	Тип удаленного сервера для экспорта настроек: • `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 настройки
schedule	Расписание экспорта настроек. 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

Изменение существующего правила экспорта настроек устройства выполняется с помощью следующей команды:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Команда для отображения правила экспорта настроек:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве параметра `<filter>` можно использовать не только название правила, но и другие заданные в правиле параметры (см. список параметров в таблице выше).

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используйте следующую команду:

```
Admin@nodename# set settings change-control config <off | log | block>
```

Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate WAF.

- `log` — активация режима отслеживания изменений конфигурации. При обнаружении изменений UserGate WAF 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 WAF 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 продукта в соответствии с требованиями организации, после чего защищает настройки от изменений (режим `log` или `block`). Любое изменение настроек 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 WAF.

- `log` — активация режима отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate WAF 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 WAF 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 настройки режима ускоренной обработки трафика используется команда:

```
Admin@nodename# show settings fastpath
```

Настройка управления доступом к веб-консоли UserGate WAF

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

```
Admin@nodename# set settings administrators general
```

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора
unblock	Разблокировать администратора
strong-password	Использовать сложный пароль: • **on**. • **off**
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд)
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов)
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов)
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов)
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов)
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов)
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов)

Пример редактирования параметров учетных записей:

```
Admin@nodename# set settings administrators general block-time 400
```

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

```
Admin@nodename# show settings administrators general

strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

```
Admin@nodename# create settings administrators administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **password**: пароль администратора

Параметр	Описание
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее — 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 — 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 — 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 — в разделе «Настройка профилей аутентификации»

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type>
<admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-
type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user
testd.local\user1

login            : testd.local\user1
enabled          : on
type             : ldap_user
locked           : off
admin-profile    : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-
type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user
testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора
description	Описание профиля администратора

Параметр	Описание
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: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: `Admin@nodename# create settings administrators profiles ... webui-permissions <permission> all` или `Admin@nodename# create settings administrators profiles ... webui-permissions <permission> [ object ... ]`
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.

Параметр	Описание
	Возможно назначение прав сразу на все или на отдельные объекты: `Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all` или `Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [ object ... ]`

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

```
Admin@nodename# show settings administrators admin-sessions ( node
<node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

```
Admin@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Пример выполнения команд:

```
Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
```

```
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer

admin-login           : Admin
source                : web
session_start_date    : 2023-08-10T11:33:10Z
ip                    : 10.0.2.2
node                  : utmcore@dineanoulwer

Admin@nodename# execute termination admin-sessions 10.0.2.2/web

Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

```
 Admin@nodename# execute termination admin-sessions ( node <node-name>
ip <session-ip> source <cli | web | ssh> admin-login <administrator-
login> )
```

Настройка сертификатов

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, которое будет отображено в списке
description	Описание сертификата
certificate-data	Сертификат в формате PEM
certificate-chain	Цепочка сертификатов в формате PEM
private-key	Приватный ключ в формате PEM
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение)
user	Локальный пользователь, которому будет назначен пользовательский сертификат
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • **user**: имя пользователя в формате domain\user. • **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. • **ssl-cert**: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • **saml**: сертификат, который будет использован в SAML-клиенте. • **none**

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата
description	Описание сертификата
country	Страна, в которой выписывается сертификат
state	Область/штат, в котором выписывается сертификат
locality	Город, в котором выписывается сертификат
organization	Название организации, для которой выписывается сертификат
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров
email	Электронная почта компании

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата
description	Описание сертификата

Параметр	Описание
role	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **ssl-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **ssl-root**: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • **ssl-cert**: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • **captive-portal**: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • **web-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • **saml**: сертификат, который будет использован в SAML-клиенте. • **none**
user	Локальный пользователь, которому будет назначен пользовательский сертификат
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • **user**: имя пользователя в формате domain\user. • **connector**: выбор LDAP-сервера
certificate-data	Сертификат в формате PEM
certificate-chain	Цепочка сертификатов в формате PEM

Для удаления сертификата:

```
Admin@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Чтобы удалить сертификат из кэша используется команда:

```
Admin@nodename# delete settings certificates-cache <common-name>
```

Настройка профилей клиентских сертификатов

Раздел **Профили клиентских сертификатов** находится на уровне **settings certificate-profiles**.

Для создания профиля клиентского сертификата предназначена команда:

```
Admin@nodename# create settings certificate-profiles <parameters>
```

Далее могут использоваться следующие параметры:

Параметр	Описание
name	Название профиля клиентского сертификата
description	Описание профиля
username-field	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • **common** — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат.

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 истечению которого WAF перестает ожидать ответа от службы списков отзыва сертификатов

Для просмотра ранее созданных профилей клиентских сертификатов используются команды:

```
Admin@nodename# show settings certificate-profiles
Admin@nodename# show settings certificate-profiles <certificate-
profile-name>
```

Для редактирования ранее созданного профиля используется команда:

```
Admin@nodename# set settings certificate-profiles <certificate-profile-name> <parameters>
```

Параметры, доступные для редактирования профиля, аналогичны параметрам создания профиля, рассмотренным ранее.

Для удаления ранее созданного профиля используется команда:

```
Admin@nodename# delete settings certificate-profiles <certificate-profile-name>
```

Настройка кластеров

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда обновления существующего узла кластера:

```
Admin@nodename# set settings device-mgmt configuration-cluster <node-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера
description	Обновить описание узла кластера
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера

Команды для удаления и отображения настроек узла кластера:

```
Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
```

```
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-
name>
```

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

```
Admin@nodename# execute configurate-cluster generate-secret-key
```

НАСТРОЙКИ РАЗДЕЛА ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Настройка серверов аутентификации

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

```
Admin@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
cache-ttl	Время жизни записей LDAP-кэша. (Опция доступна начиная с релиза UGOS 7.1.3).
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, *ou=Office,dc=example,dc=com*. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

```
 Admin@nodename# set users auth-server ldap <ldap-server-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

```
Admin@nodename# show users auth-server ldap <ldap-server-name>
```

Примеры команд создания и редактирования LDAP-коннектора:

```
Admin@nodename# create users auth-server ldap name "New LDAP connector"
ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains
[ testd.local ] search-roots [ dc=testd,dc=local ] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
Admin@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
description      : New LDAP connector description
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
```

Для удаления LDAP-коннектора используется команда:

```
 Admin@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
Admin@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
 Admin@nodename# set users auth-server radius <radius-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS
server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"

name           : New RADIUS server
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server"
description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"

name           : New RADIUS server
description    : New RADIUS server description
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
```

Для удаления сервера:

```
 Admin@nodename# delete users auth-server radius <radius-server-name>
<parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses**.

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name
"New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                 : New TACACS+ server
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
Admin@nodename# set users auth-server tacacs "New TACACS+ server"
description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                 : New TACACS+ server
description          : New TACACS+ server description
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка сервера NTLM

Настройка сервера NTLM производится на уровне **users auth-server ntlm**.

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

```
Admin@nodename# create users auth-server ntlm <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
domain	IP-адрес или доменное имя сервера NLM.

Команда для обновления информации о NTLM-сервере:

```
 Admin@nodename# set users auth-server ntlm <ntlm-server-name>
<parameter>
```

Команда для отображения информации о сервере NTLM:

```
Admin@nodename# show users auth-server ntlm <ntlm-server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Примеры команд для создания и редактирования сервера NTLM:

```
Admin@nodename# create users auth-server ntlm name "New NTLM server"
domain 10.10.0.12 enabled on
Admin@nodename# show users auth-server ntlm "New NTLM server"

name            : New NTLM server
enabled         : on
domain          : 10.10.0.12

Admin@nodename# set users auth-server ntlm "New NTLM server"
description "New NTLM server description"
Admin@nodename# show users auth-server ntlm "New NTLM server"

name            : New NTLM server
description     : New NTLM server description
```

```
enabled         : on
domain          : 10.10.0.12
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers ntlm <ntlm-server-name>
```

Настройка сервера SAML IDP

Настройка сервера SAML IDP производится на уровне **users auth-server saml-idp**.

Для создания сервера аутентификации SAML IDP используется следующая команда:

```
Admin@nodename# create users auth-server saml-idp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
metadata-url	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML.
certificate	Сертификат, который будет использован в SAML-клиенте.
sso-url	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
sso-binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-url	

Параметр	Описание
	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Команда для обновления информации о сервере SAML IDP:

```
 Admin@nodename# set users auth-server saml-idp <saml-idp-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Команда для отображения информации о сервере SAML IDP:

```
Admin@nodename# show users auth-server saml-idp <saml-idp-server-name>
```

Примеры команд для создания и редактирования сервера SAML IDP:

```
Admin@nodename# create users auth-server saml-idp name "New SAML IDP
server" slo-url http://logout.example.org sso-url http://
login.example.o
rg enabled on
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"

name            : New SAML IDP server
enabled         : on
certificate     : Unused
sso-url         : http://login.example.org
sso-binding     : post
slo-url         : http://logout.example.org
slo-binding     : post
Admin@nodename# set users auth-server saml-idp "New SAML IDP server"
description "New SAML IDP server description"
```

```
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"

name            : New SAML IDP server
description     : New SAML IDP server description
enabled         : on
certificate     : Unused
sso-url         : http://login.example.org
sso-binding     : post
slo-url         : http://logout.example.org
slo-binding     : post
```

Для удаления сервера:

```
 Admin@nodename# delete users auth-servers saml-idp <saml-idp-server-name>
```

Настройка профилей аутентификации

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
Admin@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени

Параметр	Описание
	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. • **ntlm**: аутентификация с использованием NTLM-сервера. • **saml-idp**: аутентификация с использованием сервера SAML IDP.

Команда для редактирования настроек профилей аутентификации:

```
Admin@nodename# set users auth-profile <auth-profile-name> <parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
Admin@nodename# create users auth-profile name "New LDAP auth profile"
auth-methods ldap [ "New LDAP connector" ]
Admin@nodename# show users auth-profile "New LDAP auth profile"
```

```
name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
Admin@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
description         : New LDAP auth profile description
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
Admin@nodename# delete users auth-profile <auth-profile-name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-metod>
```

НАСТРОЙКИ СЕТИ

Зоны

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

```
Admin@nodename# create network zone
```

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **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.

Параметр	Описание
	• **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **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.

Параметр	Описание
	• **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). • **"Admin Console"**: доступ к веб-консоли управления (TCP 8001). • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **"REVERSE PROXY"**: сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • **"Log Analyzer"**: сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713). • **"SNMP Proxy"**: сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • **NTP**: доступ к сервису точного времени, запущенному на сервере UserGate.
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**.

Параметр	Описание
	При **antispoof-negate on** адреса источников, указанные в значении **ip-spoofing-networks**, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • **on**. • **off**.
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled
on
```

Команда удаления зоны или её параметров:

```
Admin@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Следующая команда отобразит настройки зоны:

```
Admin@nodename# show network zone <zone-name>
```

Интерфейсы

Список упорядоченных имён сетевых интерфейсов и соответствующие им физические адреса доступен для отображения при выполнении команды (команда доступна и в режиме диагностики и мониторинга и в режиме конфигурации):

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

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

Упорядочивание интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующие команды в режиме диагностики и мониторинга и в режиме конфигурации соответственно:

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

Admin@nodename# delete network interface-mapping
```

После перезагрузки сервера UserGate список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate.

Далее будет рассмотрена настройка интерфейсов, которая производится на уровне **network interface**.

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

```
Admin@nodename# set network interface adapter <adapter_name>
```

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.
description	Описание сетевого интерфейса.

Параметр	Описание
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0.

Параметр	Описание
	Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow».
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе «Настройка профилей LLDP».
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
rx-ring	Размер буфера RX ring интерфейса типа adapter.
tx-ring	Размер буфера TX ring интерфейса типа adapter.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip | none>). • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

```
Admin@nodename# delete network interface adapter <adapter-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

```
Admin@nodename# show network interface adapter
```

Для отображения информации об адаптере:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

```
Admin@nodename# create network interface vlan
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	

Параметр	Описание
	Тип интерфейса: • **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения.

Параметр	Описание
	Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow».
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

```
Admin@nodename# show network interface vlan
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

```
Admin@nodename# create network interface bond
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.

Параметр	Описание
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow».
bonding	

Параметр	Описание
	Дополнительные параметры бонд-интерфейса: • **aggr-mode** — режим работы бонда: ◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ **active-backup**: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). ◦ **xor**: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). ◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ **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

Параметр	Описание
	текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). ◦ **load**: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. • **mii-monitoring**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • **down-delay**: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. • **up-delay**: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. • **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

Параметр	Описание
	бонд-интерфейсе меняется во время обработки отказа. ◦ **follow**: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. • **xmit-hash**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ **l2**: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. ◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. ◦ **l3-4**: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы. • **interface**: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	

Параметр	Описание
	Тип создаваемого интерфейса: • **l3** — Layer 3 интерфейс. • **mirror** — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего бонд-интерфейса:

```
Admin@nodename# set network interface bond <bond-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Настройка bridge-интерфейса

Настройка моста производится на уровне **network interface bridge**.

Чтобы добавить новый bridge-интерфейс:

```
Admin@nodename# create network interface bridge
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).

Параметр	Описание
description	Описание bridge-интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow».
bridging	Дополнительные параметры моста: • **iface-type**: режим работы интерфейса: ◦ **l2**: Layer 2 (создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном

Параметр	Описание
	режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security; контентная фильтрация в этом режиме работает). ◦ **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **interface**: интерфейсы, которые будут использованы для создания моста. • **stp**: включение/отключение использование STP (Spanning Tree Protocol) для защиты от петель: ◦ **on.** ◦ **off**. • **forward-delay**: задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP (указывается в секундах). • **max-age**: время, по истечении которого STP-соединение считается потерянным (указывается в секундах). • **bypass-pair**: пара интерфейсов, которая будет использована для построения байпас моста. Требуется поддержка оборудования ПАК UserGate.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Параметр	Описание
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего bridge-интерфейса:

```
Admin@nodename# set network interface bridge <bridge-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления bridge-интерфейса или его параметров:

```
Admin@nodename# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех bridge-интерфейсах:

```
Admin@nodename# show network interface bridge
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bridge <bridge-name>
```

Настройка loopback-интерфейса

Создание и настройка loopback-интерфейса производится на уровне **network interface loopback**.

Для создания интерфейса используется команда:

```
Admin@nodename# create network interface loopback
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.
interface-name	Название интерфейса.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]**, маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **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».

Параметр	Описание
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow — в разделе «Настройка профилей NetFlow».
node-name	Узел кластера, на котором будет создан интерфейс.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	

Параметр	Описание
	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip | none>). • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего интерфейса:

```
Admin@nodename# set network interface loopback <interface-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания loopback-интерфейса, кроме **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления loopback-интерфейса или его параметров:

```
Admin@nodename# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех loopback-интерфейсах:

```
Admin@nodename# show network interface loopback
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface loopback <interface-name>
```

Шлюзы

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

```
Admin@nodename# create network gateway
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • **on**. • **off**.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет.
virtual-router	Выбор виртуального маршрутизатора, для которого настраивается шлюз.
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • **on**. • **off**.

Параметр	Описание
default	Использование данного шлюза в качестве шлюза по умолчанию: • **on**. • **off**.

Обновление параметров шлюза:

```
Admin@nodename# set network gateway <gateway-name>
```

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

```
Admin@nodename# delete network gateway <gateway-name>
```

Чтобы отобразить информацию о всех шлюзах:

```
Admin@nodename# show network gateway
```

или об определённом шлюзе:

```
Admin@nodename# show network gateway <gateway-name>
```

Настройка виртуальных маршрутизаторов

В данном разделе описана настройка маршрутизации с использованием интерфейса командной строки (настройка рассмотрена в соответствующих разделах). Настройка производится на уровне **network virtual-router**.

Далее представлены команды, использующиеся для общей настройки виртуальных маршрутизаторов.

Команда для добавления нового виртуального маршрутизатора:

```
Admin@nodename# create network virtual-router <parameters>
```

Далее указываются параметры:

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора.
description	Описание виртуального маршрутизатора
node-name	Выбор узла UserGate, на котором будет создан виртуальный маршрутизатор (при наличии кластера).
interfaces	Интерфейсы, которые будут использованы в данном виртуальном маршрутизаторе. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, добавлены быть не могут; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные, бондинг, и другие.

Команда для отображения информации о виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name>
```

Пример создания виртуального маршрутизатора:

```
Admin@nodename# create network virtual-router name test_router
description "Test virtual router" interfaces [ port2 ]
Admin@nodename# show network virtual-router test_router

name                : test_router
description         : Test virtual router
node-name           : node_1
interfaces          : port2
...
```

Команда для редактирования параметров виртуального маршрутизатора:

```
Admin@nodename# set network virtual-router <virtual-router-name>
```

Параметры, доступные для обновления, аналогичны параметрам команды **create**, кроме:

- **name**.
- **node-name**.

Пример редактирования параметров виртуального маршрутизатора:

```
Admin@nodename# set network virtual-router test_router interfaces
[ port3 ]
Admin@nodename# show network virtual-router test_router

name                : test_router
description         : Test virtual router
node-name           : node_1
interfaces          : port2; port3
...
```

Чтобы удалить виртуальный маршрутизатор используется команда:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
```

Настройка статических маршрутов

Для добавления нового статического маршрута используется команда:

```
Admin@nodename# set network virtual-router <virtual-router-name> routes
new
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • **on**.

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 сервера UserGate.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем приоритетней маршрут

Пример добавления статического маршрута:

```
Admin@nodename# set network virtual-router test_router routes new name
"Test static route" description "Test static route description"
destination-ip 192.168.200.0/24 gateway 192.168.100.100 interface port3
type unicast metric 1 enabled on
Admin@nodename#
Admin@nodename# show network virtual-router test_router

name                : test_router
```

```
description         : Test virtual router
node-name           : node_1
interfaces          : port2; port3
routes              :
    Test static route
        name              : Test static route
        enabled           : on
        description       : Test static route description
        destination-ip    : 192.168.200.0/24
        gateway           : 192.168.100.100
        interface         : port3
        metric            : 1
...
```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@nodename# set network virtual-router <virtual-router-name> routes
<static-route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Пример редактирования статического маршрута:

```
Admin@nodename# set network virtual-router test_router routes "Test
static route" metric 10
Admin@nodename# show network virtual-router test_router

name                : test_router
description         : Test virtual router
node-name           : node_1
interfaces          : port2; port3
routes              :
    Test static route
        name              : Test static route
        enabled           : on
        description       : Test static route description
        destination-ip    : 192.168.200.0/24
```

```
        gateway           : 192.168.100.100
        interface         : port3
        metric            : 10
...
```

Используйте следующую команду для удаления статического маршрута:

```
Admin@nodename# delete network virtual-router <virtual-router-name>
routes <static-route-name>
```

Пример удаления статического маршрута:

```
Admin@nodename# delete network virtual-router test_router routes "Test
static route"
Admin@nodename# show network virtual-router test_router

name                : test_router
description         : Test virtual router
node-name           : node_1
interfaces          : port2; port3
routes              : []
...
```

Для отображения статических маршрутов:

```
 Admin@nodename# show network virtual-router <virtual-router-name>
routes
```

НАСТРОЙКИ РАЗДЕЛА ПОЛИТИКИ СЕТИ

Настройка правил межсетевого экрана

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд — в разделе «UserGate Policy Language».

```
Admin@nodename# create network-policy firewall
```

Параметры правил межсетевого экрана:

Параметр	Описание
PASS **DENY**	Действие правила межсетевого экрана: • **PASS** — разрешить трафик. • **DENY** — запретить трафик.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила межсетевого экрана. Например: **name("Rule example")**.
desc	Описание правила. Например: **desc("Firewall rule example configured in CLI")**.
reject_with	Настройка доступна для правил с действием **Запретить**: • **reject_with(no)**. • **reject_with("host_unreach")** — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • **reject_with("tcp_rst")** — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** При выборе действия **Посылать TCP reset** необходимо указание сервиса, использующего протокол TCP (подробнее о добавлении и настройке сервисов читайте в разделе ов). • **reject_with("tcp_reset-both")** — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.

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(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.
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

Параметр	Описание
	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. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
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 ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
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 \
```

```
...service = HTTP \
...rule_log(session) \
...name("Test firewall rule") \
...enabled(true)
...
Admin@nodename# show network-policy firewall 1
% ---------------- 1 ----------------
PASS \
    src.zone = Trusted \
    dst.zone = Untrusted \
    service = HTTP \
    rule_log(session) \
    enabled(true) \
    id("1505d309-621b-4f88-a2e4-98667c477535") \
    name("Test firewall rule")
```

НАСТРОЙКА ПУБЛИКАЦИИ ВЕБ-СЕРВИСОВ

Настройка серверов публикации

Настройка серверов публикации производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера публикации используется следующая команда:

```
Admin@nodename# create global-portal reverse-proxy-servers <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера публикации
description	Описание сервера публикации

Параметр	Описание
address	Адрес или домен сервера публикации
port	TCP-порт сервера публикации
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 WAF, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UserGate WAF или можно настроить статические маршруты через UserGate WAF для «белых» IP-адресов источников.**

Команда для редактирования параметров сервера публикации:

```
Admin@nodename# set global-portal reverse-proxy-servers <server-name>
<parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для отображения информации о сервере публикации:

```
Admin@nodename# show global-portal reverse-proxy-servers <server-name>
```

Структура команды для удаления сервера публикации:

```
Admin@nodename# delete global-portal reverse-proxy-servers <server-
name>
```

Настройка правил публикации

Правила публикации в интерфейсе командной строки настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Структура команды для создания правила публикации:

```
Admin@nodename# create global-portal reverse-proxy-rules <position>
upl-rule <parameters>
```

Параметры настройки правил публикации:

Параметр	Описание
OK	Действие для создания правила публикации с помощью UPL
enabled	Включение/отключение правила публикации: • `enabled(yes)` или `enabled(true)` — включение; • `enabled(no)` или `enabled(false)` — отключение
name	Название правила публикации. Например, `name("Reverse proxy rule example")`
desc	Описание правила публикации. Например, `desc("Reverse proxy rule example set via CLI")`
profile	Сервер публикации, куда UserGate WAF будет пересылать запросы. Для указания сервера: `profile("Reverse proxy server example")`
url.port	Порт, на котором UserGate WAF будет слушать входящие запросы.

Параметр	Описание
	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")`
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 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`).

Параметр	Описание
	Коды названий стран доступны по ссылке: ISO 3166-1. **Важно!** **Существует ограничение на количество GeoIP, которое может быть указано: не более 15**
user	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (подробнее о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора»). Пример 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 UserGate WAF, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: `dst.ip = lib.network()`; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — 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; необходимо указать код страны (например, `dst.geoip = RU`). Коды названий стран доступны по ссылке ISO 3166-1.

Параметр	Описание
	Важно! **Существует ограничение на количество GeoIP, которое может быть указано: не более 15**
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено правило публикации. Для указания Useragent пользовательских браузеров: `request.header.User-Agent = lib.useragent()`; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка Useragent браузеров»
rewrite_path	Подмена домена и/или пути в URL-запросе пользователя. Например, для преобразования запросов, приходящих на http://www.example.com/path1 в http://www.example.loc/path2 нужно указать: `rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2")`
waf_profile	Включение защиты веб-сервисов в правиле публикации. Необходимо указать заранее созданный WAF-профиль. Например, `waf_profile("Example WAF profile")`. Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройки безопасности WAF в CLI»
websocket_profile	Включение обработки websocket-соединений (доступно в версии ПО 7.4.1 и выше). Необходимо указать заранее созданный websocket-профиль. Например, `websocket_profile("Example websocket profile")` Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройка WebSocket-профилей в CLI»

Для редактирования правила публикации используется команда:

```
Admin@nodename# set global-portal reverse-proxy-rules <position> upl-
rule <parameters>
```

Для просмотра параметров правила публикации используется команда:

```
Admin@nodename# show global-portal reverse-proxy-rules <position>
```

Пример создания правила публикации:

```
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") \
...waf_profile("Example WAF profile") \
...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") \
    waf_profile("Example WAF profile") \
    enabled(true) \
    id("7dc7041a-6538-400b-8f1e-9b18287218ac") \
    name("Test reverse proxy rule")
```

Для удаления правила публикации используется команда:

```
Admin@nodename# delete global-portal reverse-proxy-rules <position>
```

Настройка балансировки нагрузки

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing** с использованием языка описания политик 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 балансировки нагрузки на серверы публикации

Настройка правил балансировки производится на уровне **network-policy load-balancing reverse-proxy**.

Для создания правила балансировки:

```
Admin@nodename# create network-policy load-balancing reverse-
proxy <position> upl-rule
```

Параметры правил балансировки:

Параметр	Описание
PASS **OK**	Действие для создания правила балансировки с помощью UPL.
enabled	Включение/отключение правила балансировки: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила балансировки. Например: **name("RP balancer")**.
desc	Описание правила балансировки. Например: **desc("Test reverse-proxy balancing rule")**.

Параметр	Описание
profile	Указание профилей серверов публикации, на которые будет распределяться нагрузка. Подробнее о создании и настройке серверов публикации с использованием CLI — в разделе «Настройка серверов публикации». Например, **profile("Reverse proxy server1", "Reverse proxy server2")**.

Команда для редактирования параметров правила балансировки:

```
 Admin@nodename# set network-policy load-balancing reverse-
proxy <position> upl-rule
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании правила балансировки.

Команды для отображения информации о всех правилах балансировки:

```
Admin@nodename# show network-policy load-balancing reverse-proxy
```

Для отображения информации об определённом правиле балансировки:

```
Admin@nodename# show network-policy load-balancing reverse-proxy
<position>
```

Пример создания правила балансировки с использованием UPL:

```
Admin@nodename# create network-policy load-balancing reverse-proxy 1
upl-rule OK \
...profile("Reverse proxy server1", "Reverse proxy server2") \
...desc("Test reverse proxy balancing rule") \
...name(test_reversep1) \
...enabled(true)
...
Admin@nodename# show network-policy load-balancing reverse-proxy

% ----------------- 1 -----------------
OK \
```

```
    profile("Reverse proxy server1", "Reverse proxy server2") \
    desc("Test reverse proxy balancing rule") \
    enabled(true) \
    id("1ed892bb-26ee-4ab1-8a55-2f412ce8b55a") \
    name(test_reversep1)
```

Для удаления существующего правила балансировки используется следующая команда:

```
 Admin@nodename# delete network-policy load-balancing reverse-
proxy <position>
```

НАСТРОЙКИ БИБЛИОТЕК

Настройка библиотек (Описание)

Настройка IP-адресов

Группы IP-адресов создаются и настраиваются на уровне `libraries ip-list`.

Для создания группы IP-адресов используется команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название группы адресов
`description`	Описание группы
`threat-lvl`	Уровень угрозы: • `very-low` — очень низкий уровень угрозы. • `low` — низкий уровень угрозы. • `medium` — средний уровень угрозы.

Параметр	Описание
	• `high` — высокий уровень угрозы. • `very-high` — высокий уровень угрозы
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается параметром `shedule` в 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»
`lists`	Выбор существующих групп для добавления в создаваемую группу
`ips`	IP-адреса или диапазон IP-адресов, которые необходимо включить в группу. Указывается в формате: `<ip>`, `<ip/mask>` или `<ip_range_start-ip_range_end>`

Для редактирования группы (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы) используется команда:

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые IP-адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ]
```

Следующие команды используются для удаления всей группы IP-адресов или IP-адресов, содержащихся в ней:

```
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 группах:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определенной группе, необходимо указать название интересующей группы IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого группы IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка useragent браузеров

Списки user agent браузеров создаются и настраивается на уровне `libraries useragents`.

Для добавления нового списка use ragent браузеров используется команда:

```
Admin@nodename# create libraries useragents <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название списка user agent
`description`	Описание списка

Параметр	Описание
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается параметром `shedule` в 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»
`patterns`	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php

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.

Команда для добавления новых 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
```

Чтобы отобразить информацию об определенном списке, необходимо указать название списка user agent браузеров. Команда для просмотра содержания списка user agent браузеров:

```
 Admin@nodename# show libraries useragents <useragent-list-name>
patterns
```

Настройка списков URL

Списки URL настраиваются на уровне `libraries url-list`.

Для добавления нового списка URL используется команда:

```
Admin@nodename# create libraries url-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название списка URL
`description`	Описание списка URL
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается

Параметр	Описание
	параметром `shedule` 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»
`urls`	URL, которые необходимо добавить в список
`case-sensitivity`	Чувствительность к регистру в написании адреса URL: • `sensitive` — чувствительно к регистру букв в адресе. • `insensitive` — нечувствительно к регистру букв в адресе. • `domain` — список адресов доменов

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 удаление всего списка URL или отдельных адресов URL:

```
Admin@nodename# delete libraries url-list <url-list-name>
Admin@nodename# delete libraries url-list <url-list-name> urls
[ <url> ... ]
```

Команды для просмотра информации о всех списках URL, об определённом 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 группы используется команда:

```
Admin@nodename# create libraries time-sets <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название группы
`description`	Описание группы
`time-set`	• `interval-name` — название интервала повторения. • `type` — тип интервала повторения: ◦ `daily` — ежедневно: ■ `time-from` — время начала (указывается в формате HH:MM). ■ `time-to` — время окончания (указывается в формате HH:MM). ■ `all-day on` — весь день. ◦ `weekly` — каждую неделю: ■ `time-from` — время начала (указывается в формате HH:MM). ■ `time-to` — время окончания (указывается в формате HH:MM). ■ `all-day on` — весь день. ■ `days [ Mon | Tue | Wed | Thu | Fri | Sat | Sun ]` — дни недели. ◦ `monthly` — каждый месяц: ■ `time-from` — время начала (указывается в формате HH:MM). ■ `time-to` — время окончания (указывается в формате HH:MM).

Параметр	Описание
	■ `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>` — активация/деактивация параметра для 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>` — активация/деактивация параметра для 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 по текущим значениям 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>
```

Команда для удаления элемента календаря:

```
 Admin@nodename# delete libraries time-sets <time-sets-name> <time-set-
type> ( <time-set-filter> )
```

Команда для для отображения информации о всех календарях:

```
 Admin@nodename# show libraries time-sets
```

Команда для отображения информации об определённом 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 шаблонов страниц

Шаблоны страниц настраиваются на уровне `libraries response-pages` (доступно с версии 7.5.0).

Для добавления нового шаблона страницы используется команда:

```
Admin@nodename# create libraries response-pages <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название шаблона страницы
`description`	Описание шаблона страницы
`type`	Выбор типа шаблона страницы: • `blockpage` — шаблон страницы блокировки. ◦ `original-template` — выбор языка шаблона: ■ `blockpage-en` — шаблон страницы на английском. ■ `blockpage-ru` — шаблон страницы на русском. • `network-error-page` — шаблон страницы сетевых ошибок. ◦ `original-template` — выбор языка шаблона: ■ `network-error-page-en` — шаблон страницы на английском. ■ `network-error-page-ru` — шаблон страницы на русском
`use-by-default`	Назначение шаблона страницы шаблоном по умолчанию

Команда для изменения параметров шаблона страницы:

```
Admin@nodename# set libraries response-pages <response-page-name>
<parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команда для удаления шаблона страницы:

```
Admin@nodename# delete libraries response-pages <response-page-name>
```

> **Примечание**
> **Шаблон страницы, назначенный шаблоном по умолчанию, удалить нельзя.**

Команда для отображения информации об определенном шаблоне страницы:

```
Admin@nodename# show libraries response-pages <response-page-name>
```

Настройка почтовых адресов

Группы почтовых адресов настраиваются на уровне `libraries email-list`.

Для добавления новой группы почтовых адресов используется команда:

```
Admin@nodename# create libraries email-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название группы почтовых адресов
`description`	Описание группы почтовых адресов
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`).

Параметр	Описание
	Периодичность обновления списка указывается параметром `shedule` 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»
`emails`	Почтовые адреса, которые необходимо добавить в данную группу

Команда для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Команды для удаления группы или почтовых адресов из нее:

```
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 группах, об определенных группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка телефонных номеров

Группы телефонных номеров настраиваются на уровне `libraries phone-list`.

Для создания группы телефонных номеров используется команда:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название группы телефонных номеров
`description`	Описание группы телефонных номеров
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается параметром `shedule` в 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»
`phones`	Номера телефонов, которые необходимо добавить в данную группу

Команда для редактирования информации о группе телефонных номеров:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команды для удаления всей группы или номеров телефонов из нее:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones
[ <phone> ... ]
```

Команда для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

Команда для просмотра информации об определенных группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Команда для просмотра номеров, содержащихся в группе:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка списка Websocket-расширений

Списки Websocket-расширений настраиваются на уровне `libraries ws-extensions-list` (доступно с версии 7.4.1).

Для создания списка расширений используется команда:

```
Admin@nodename# create libraries ws-extensions-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название списка Websocket-расширений

Параметр	Описание
`description`	Описание списка
`extensions`	Расширения, которые необходимо включить в список
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается параметром `shedule` в 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. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»

Команда для редактирования списка расширений:

```
Admin@nodename# set libraries ws-extensions-list <ws-extensions-list
name> <parameter>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Команды, с использованием которых доступно удаление всего списка расширений или отдельных расширений:

```
Admin@nodename# delete libraries ws-extensions-list <ws-extensions-list
name>
Admin@nodename# delete libraries ws-extensions-list <ws-extensions-list
name> extensions [ <extension> ... ]
```

Команды для просмотра информации о всех списках расширений, об определенном списке или о расширениях, входящих в определенный список:

```
Admin@nodename# show libraries ws-extensions-list
Admin@nodename# show libraries ws-extensions-list <ws-extensions-list
name>
Admin@nodename# show libraries ws-extensions-list <ws-extensions-list
name> extensions
```

Настройка списка Websocket-субпротоколов

Списки Websocket-субпротоколов настраиваются на уровне `libraries ws-protocols-list` (доступно с версии 7.4.1).

Для создания списка Websocket-субпротоколов используется команда:

```
Admin@nodename# create libraries ws-protocols-list <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название списка Websocket-субпротоколов
`description`	Описание списка
`protocols`	Websocket-субпротоколы, которые необходимо включить в список
`type`	Тип списка: • `local` — локальный. • `updatable` — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (`url`). Периодичность обновления списка указывается параметром `shedule` в 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.

Параметр	Описание
	◦ Дефис (-) — для указания диапазона значений. ◦ Запятая (,) — в качестве разделителя значений. ◦ Косая черта (/) — для указания шага между значениями. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа»

Команда для редактирования списка Websocket-субпротоколов:

```
Admin@nodename# set libraries ws-protocols-list <parameter>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Команды для удаления всего списка Websocket-субпротоколов или отдельных Websocket-субпротоколов:

```
Admin@nodename# delete libraries ws-protocols-list <ws-protocols-list
name>
Admin@nodename# delete libraries ws-protocols-list <ws-protocols-list
name> protocols [ <protocol> ... ]
```

Команды для просмотра информации о всех списках Websocket-субпротоколов, об определенном списке или о Websocket-субпротоколах, входящих в определенный список:

```
Admin@nodename# show libraries ws-protocols-list
Admin@nodename# show libraries ws-protocols-list <ws-protocols-list
name>
Admin@nodename# show libraries ws-protocols-list <ws-protocols-list
name> protocols
```

Настройка профилей оповещений

Профили оповещений SMTP (по эл. почте) 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>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название профиля
`description`	Описание профиля
`host`	IP-адрес или FQDN SMTP-сервера, который будет использоваться для отсылки почтовых сообщений
`port`	Порт TCP, используемый SMTP-сервером. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера
`connection-security`	Способ безопасной отправки писем по эл. почте: • `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 добавления нового профиля оповещения SMPP (по SMS) используется команда:

```
 Admin@nodename# create libraries notification-profiles smpp
<parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название профиля
`description`	Описание профиля
`host`	IP-адрес или FQDN SMPP-сервера, который будет использоваться для отсылки SMS
`port`	Порт TCP, который используется для подключения к SMPP-серверу. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550
`ssl`	Включение/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 в начале всех номеров заменить «+7» на «8», используется команда `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).

Параметр	Описание
	• 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). • `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>
```

Также для профилей оповещений SMPP доступно удаление правил трансляции номеров:

```
 Admin@nodename# delete libraries notification-profiles smpp <profile-
name> phone-translation-rules [ phone1¦phone2 ]
```

Команда для отображения информации о всех имеющихся профилях оповещений:

```
 Admin@nodename# show libraries notification-profiles
```

Команда для отображения информации о всех профилях одного типа:

```
 Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

Команда для отображения информации об определённом профиле оповещения:

```
 Admin@nodename# show libraries notification-profiles <smtp | smpp>
<profile-name>
```

Настройка профилей NetFlow

Профили NetFlow настраиваются на уровне `libraries netflow-profiles`.

Для создания профиля NetFlow используется команда:

```
Admin@nodename# create libraries netflow-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название профиля NetFlow
`description`	Описание профиля
`ip`	IP-адрес NetFlow коллектора, на который сенсор будет отправлять статистику
`port`	UDP-порт, на котором NetFlow-коллектор будет принимать статистику
`protocol`	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): • `5` — NetFlow версии 5. • `9` — NetFlow версии 9. • `10` — NetFlow версии 10
`active-timeout`	Тайм-аут отправки статистики на коллектор до завершения потока (например, при передаче большого файла через сеть); указывается в секундах. Значение по умолчанию — 1800 секунд; максимальное значение — 3600 секунд
`inactive-timeout`	Тайм-аут завершения неактивного потока; указывается в секундах. Значение по умолчанию — 15 секунд; максимальное значение — 3600 секунд
`max-flows`	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. По достижении указанного количества все последующие потоки не будут учитываться (ограничение необходимо для защиты от DoS-атак). Значение по умолчанию — 2 000 000; для снятия ограничения необходимо установить значение 0
`nat-events`	Включение/отключение отправки информации о NAT-преобразованиях в статистику NetFlow: • `on`; • `off`
`refresh-rate`	Количество пакетов, после получения которого шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9 и 10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов

Параметр	Описание
`timeout-rate`	Тайм-аут отправки старого шаблона на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд

Команда для редактирования существующего профиля NetFlow:

```
Admin@nodename# set libraries netflow-profiles <profile-name>
```

Параметры, значения которых можно изменить, представлены в таблице выше.

Команда для удаления профиля NetFlow:

```
Admin@nodename# delete libraries netflow-profiles <profile-name>
```

Команды для отображения информации о всех профилях NetFlow или об отдельном профиле:

```
Admin@nodename# show libraries netflow-profiles
Admin@nodename# show libraries netflow-profiles <profile-name>
```

Настройка LLDP-профилей

LLDP-профили (Link Layer Discovery Protocol) создаются и настраиваются на уровне `libraries lldp-profiles`.

Для создания LLDP-профиля используется команда:

```
Admin@nodename# create libraries lldp-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название LLDP-профиля

Параметр	Описание
`description`	Описание LLDP-профиля
`port-status`	Режимы: • `rx` — только приём данных LLDP: UserGate не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей • `tx` — только передача данных LLDP: UserGate будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей • `rx-tx` — прием и передача данных LLDP: UserGate будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей

Команда для редактирования информации о LLDP-профиле:

```
Admin@nodename# set libraries lldp-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании LLDP-профиля.

Команда для удаления LLDP-профиля:

```
Admin@nodename# delete libraries lldp-profiles <profile-name>
```

Команды для отображения информации о всех LLDP-профилях или обо одном LLDP-профиле:

```
Admin@nodename# show libraries lldp-profiles
Admin@nodename# show libraries lldp-profiles <profile-name>
```

Настройка SSL-профилей

SSL-профили создаются и настраиваются на уровне `libraries ssl-profiles`.

Для создания SSL-профиля используется команда:

```
Admin@nodename# create libraries ssl-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
`name`	Название SSL-профиля
`description`	Описание SSL-профиля.
`min-tls-version`	Самая низкая версия TLS, которая может быть использована в данном SSL-профиле: • `tls1`; • `tls1.1`; • `tls1.2`
`max-tls-version`	Самая высокая версия TLS, которая может быть использована в данном SSL-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 SSL-профиле:

```
Admin@nodename# set libraries ssl-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании SSL-профиля.

Команды для удаления SSL-профиля полностью или отдельных алгоритмов шифрования и цифровой подписи, заданных в нем:

```
Admin@nodename# delete libraries ssl-profiles <profile-name>
Admin@nodename# delete libraries ssl-profiles <profile-name> ssl-
ciphers [ cipher ... ]
```

Команда для отображения информации о SSL-профилях:

```
Admin@nodename# show libraries ssl-profiles
Admin@nodename# show libraries ssl-profiles <profile-name>
```

НАСТРОЙКИ РАЗДЕЛА ЖУРНАЛЫ И ОТЧЕТЫ

Настройка экспорта журналов

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM.

Для создания нового правила экспорта журналов используется команда:

```
Admin@nodename# create logs logs-export <parameters>
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение правила: • **on**. • **off**.
name	Название правила.
description	Описание правила.
server-type	Тип сервера: • **ssh**; • **ftp**; • **syslog**. При выборе типа сервера доступны следующие дополнительные настройки: • **port** — Порт сервера, на который следует отправлять данные. • **login** — Имя учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • **password** — Пароль учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). • **path** — Каталог на сервере для копирования файлов журналов (не применяется к методу отправки syslog). • **passive** — Пассивный режим ftp. • **transport** — Только для типа серверов syslog. TCP или UDP. • **protocol** — Только для типа серверов syslog. RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. • **severity** — Только для типа серверов syslog. Критичность. Возможны следующие значения: **alert**, **critical**, **error**, **warning**, **notice**, **info**. • **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).

Параметр	Описание
	• **app-name** — Только для типа серверов syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
target	IP-адрес или доменное имя сервера.
logs	Журналы для экспорта: • **events** — Журнал событий. • **webaccess** — Журнал веб-доступа. • **traffic** — Журнал трафика. • **waf** — Журнал срабатываний правил WAF. Для каждого журнала можно выбрать синтаксис выгрузки: • **cef**; • **cef-compact**; • **json**; • **cee-json**; • **off**.
schedule	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. rontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.

Для редактирования ранее созданных правил используется команда:

```
Admin@nodename# set logs logs-export <log-export-rule-name>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил экспорта.

Для просмотра параметров созданных ранее правил экспорта используется команда:

```
Admin@nodename# show logs logs-export
Admin@nodename# show logs logs-export <log-export-rule-name>
```

Для удаления созданных ранее правил экспорта используется команда:

```
Admin@nodename# delete logs logs-export <log-export-rule-name>
```

Для настройки параметров разового экспорта журналов используется команда:

```
Admin@nodename# execute logs send-once <log-export-rule-name>
<parameters>
```

Параметр	Описание
fresh	Экспортировать свежие логи.
range	Указать диапазон экспорта: • **start-export-range** — начало диапазона в формате: 2022-12-31T23:59:59 • **end-export-range** — конец диапазона в формате: 2022-12-31T23:59:59

НАСТРОЙКА БЕЗОПАСНОСТИ

Настройка параметров безопасности WAF

Настройка персональных слоев

Персональные WAF-слои настраиваются на уровне `waf custom-layers` с использованием языка описания политик UPL. Подробнее о структуре команд — в разделе «UserGate Policy Language».

Для создания персонального слоя используется команда:

```
Admin@nodename# create waf custom-layers name <custom_layer_name>
description <description> upl-rule
```

Команда для изменения параметров персонального слоя:

```
 Admin@nodename# set waf custom-layers <custom_layer_name> upl-rule
```

Команда для отображения информации о всех персональных слоях:

```
Admin@nodename# show waf custom-layers
```

Команда для отображения информации об определенном персональном слое:

```
Admin@nodename# show waf custom-layers <custom_layer_name>
```

Пример создания тестового персонального слоя с использованием UPL:

```
Admin@nodename# create waf custom-layers name "Layer 2" upl-rule DENY
src.ip = lib.network("Bad ips", "Test ips")
DENY dst.ip = lib.network("Bad ips")
PASS request.header.User-Agent = lib.useragent(Browsers)
DENY time = lib.time(Weekends)
Admin@nodename#
Admin@nodename# show waf custom-layers "Layer 2"

name        : Layer 2
upl-rule    : DENY src.ip = lib.network("Bad ips", "Test ips")
```

```
DENY dst.ip = lib.network("Bad ips")
PASS request.header.User-Agent = lib.useragent(Browsers)
DENY time = lib.time(Weekends)

Admin@nodename#
```

Команда для удаления существующего персонального слоя:

```
Admin@nodename# delete waf custom-layers <custom_layer_name>
```

Настройка WAF-профилей

WAF-профили настраиваются на уровне `waf profiles`.

Для создания WAF-профиля используется команда:

```
Admin@nodename# create waf profiles name <profile_name> description
<description> enable-layers [ layer_1 layer_2 layer_n ]
```

Команда для изменения параметров WAF-профиля:

```
 Admin@nodename# set waf profiles <profile_name> name <new_name>
description <new_description> enable-layers [ list of layers to
enable ] system <change_system_layer>
```

Команда для изменения профиля ответа в WAF-профиле:

```
Admin@nodename# set waf profiles  system  overridden-rules rules-names
[ "#RefRef DoS tool (1)" "#RefRef DoS tool (2)" ] response-profile
<tab>
```

По умолчанию выбрано значение `Do not use`. Другие значения станут доступны после того, как будут созданы профили ответов.

Команда для отображения информации о всех WAF-профилях:

```
Admin@nodename# show waf profiles
```

Команда для изменения размера анализируемого тела запроса/ответа:

```
set waf profiles ProfileName max-body-inspection-size 200000
```

Команда для отображения информации об определенном WAF-профиле:

```
Admin@nodename# show waf profiles <profile_name>
```

Пример создания WAF-профиля:

```
Admin@nodename# create waf profiles name "Test profile 1" description
"Test profile #1" enable-layers [ "Layer 4 (custom)" "HTTP
Constraint" ]
Admin@nodename#
Admin@nodename# show waf profiles "Test profile 1"

name             : Test profile 1
description      : Test profile #1
enable-layers    : Layer 4 (custom); HTTP Constraint

Admin@nodename#
```

Команда для удаления существующего WAF-профиля:

```
Admin@nodename# delete waf profiles <profile_name>
```

Настройка параметров системных WAF-правил

Параметры системных WAF-правил настраиваются на уровне `waf system-rules`.

У системных WAF-правил могут быть изменены следующие параметры:

- состояние (`enabled`) — `on/off`;
- журналирование (`enable-logging`) — `on/off`;
- действие (`action`) — `pass, deny, force-pass, force-deny`;

- профиль ответа (`response-profile`) — `do not use`, `<response-profile name>`.

Пример команды настройки системного WAF-правила:

```
Admin@nodename# set waf system-rules rules ["#RefRef DoS tool (1)"]
enabled on enable-logging on action deny response-profile "<response-
profile name>"
```

В квадратных скобках указывается название одного или нескольких системных WAF-правил, к которым применяются изменения параметров. Названия WAF-правил указываются в кавычках и разделяются пробелами.

Пример команды изменения параметров нескольких системных WAF-правил:

```
Admin@oulineeladin# set waf system-rules rules ["#RefRef DoS tool (1)"
"#RefRef DoS tool (2)"] enabled off
```

Команда для отображения информации о всех системных WAF-правилах:

```
Admin@nodename# show waf system-rules
```

Пример отображения информации об определенном системном WAF-правиле:

```
Admin@oulineeladin# show waf system-rules "#RefRef DoS tool (1)"

name              : #RefRef DoS tool (1)
enabled           : on
action            : deny
description       : This event is trigerred when a malicious/suspicious
user-agent is detected in the request.
reference         : https://www.owasp.org/index.php/Denial_of_Service
threat-level      : medium
technology        : All systems
layer             : Denial of Service
enable-logging    : on
last-update       : 2016-03-17T00:00Z
response-profile  : Do not use
```

Просмотр системных WAF-слоев

Команда для отображения информации об имеющихся системных WAF-слоях:

```
Admin@nodename# show waf system-layers
```

Команда для отображения информации о конкретном системном WAF-слое:

```
Admin@minhanhicont# show waf system-layers <system_layer_name>
```

Настройка профиля ответа

Настройка профиля ответа выполняется на уровне `response-profiles`.

Для создания профиля ответа используется следующая команда:

```
Admin@nodename# create security-policy response-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название профиля ответа
response-type	Выбор политики, определяющей, какой ответ будет возвращен клиенту при срабатывании блокирующего WAF-правила: • `redirect` — перенаправление запроса на страницу указанного ресурса. Доступны следующие параметры: ◦ `custom-redirect` — ссылка на ресурс для перенаправления запроса. ◦ `response-code` — трехзначный код состояния HTTP (должен начинаться с цифры 3). ◦ `response-text` — текст ответа. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду. • `tcp-rst` — сообщение о разрыве соединения.

Параметр	Описание
	• `response-page` — страница блокировки с указанием кода состояния HTTP. Доступны следующие параметры: ◦ `template` — указание шаблона страницы. ◦ `response-code` — трехзначный код состояния HTTP (должен начинаться с цифры 1, 2, 4 или 5). ◦ `response-text` — текст ответа. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду
description	Описание профиля ответа

Команда для редактирования параметров профиля ответа:

```
Admin@nodename# set security-policy response-profiles <response-
profile_name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команда для удаления профиля ответа:

```
Admin@nodename# delete security-policy response-profiles <response-
profile_name>
```

Команда для отображения информации о всех профилях ответа:

```
Admin@nodename# show security-policy response-profiles
```

Команда для отображения информации об определенном профиле ответа:

```
Admin@nodename# show security-policy response-profiles <response-
profile_name>
```

Настройка WebSocket-профилей

Настройка WebSocket-профилей происходит на уровне **websocket-profiles**.

Для создания WebSocket-профилей используется следующая команда:

```
Admin@nodename# create security-policy websocket-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название WebSocket-профиля
description	Описание WebSocket-профиля
block	Включение/отключение блокирования любого WebSocket-трафика, который приходит в UserGate WAF: • **On**; • **Off**
check-request	Проверка целостности handshake-запроса: • **On**; • **Off**
log	Включение/отключение журналирования событий: • **On**; • **Off**
check-origin	Проверка наличия в запросе заголовка `Origin`: • **On**; • **Off**
origin	Добавление списка URL источников, с которыми разрешается устанавливать WebSocket-соединение. Подробнее о создании списков URL в разделе — «Настройка списков URL»
origin-negate	Добавление списка URL нежелательных источников. WebSocket-соединения с ними будут игнорироваться

Параметр	Описание
check-extension	Включение/отключение проверки расширений в заголовке `Sec-WebSocket-Extensions`: • **On**; • **Off**
extension	Добавление списка разрешенных расширений. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные расширения
extension-negate	Инвертация проверки по списку, указанному в параметре **extension**: • **On**; • **Off**. WebSocket-соединения по запросам, в заголовках которых указаны расширения из списка, будут игнорироваться
check-protocol	Включение/отключение проверки субпротоколов в заголовке `Sec-WebSocket-Protocols`: • **On**; • **Off**
protocol	Добавление списка разрешенных субпротоколов. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные субпротоколы
protocol-negate	Инвертация проверки по списку, указанному в параметре **protocol**: • **On**; • **Off**. WebSocket-соединения по запросам, в заголовках которых указаны субпротоколы из списка, будут игнорироваться

Команда для редактирования параметров WebSocket-профиля:

```
Admin@nodename# set security-policy websocket-profiles <websocket-profile_name> <parameter>
```

Команда для отображения информации о всех WebSocket-профилях:

```
Admin@nodename# show security-policy websocket-profiles
```

Команда для отображения информации об определенном WebSocket-профиле:

```
Admin@nodename# show security-policy websocket-profiles <profile_name>
```

Команда для удаления существующего WebSocket-профиля используется следующая команда:

```
Admin@nodename# delete security-policy websocket-
profiles <profile_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.

> **Важно!**
> **Условие не должно в качестве триггера содержать другое условие. В противном случае, если правило с условием-триггером будет добавлено в профиль WAF, другие правила в этом профиле срабатывать не будут.**

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

> **Примечание**
> **При настройке правил сначала указывается действие, потом условия и затем свойства.**

UPL используется для создания WAF-правил в персональных слоях. Также с помощью UPL в интерфейсе CLI создаются правила политик сети для следующих разделов:

- Межсетевой экрана (уровень: **network-policy firewall**).
- Правила публикации (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 \
...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 ::= firewall | reverseproxy | 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*), "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.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 =
">"
```

http.request.body.re2, http.response.body.re2

Проверка тела HTTP-запроса или HTTP-ответа с использованием регулярных выражений.

Синтаксис:

request.body.re2 = string

response.body.re2 = string

Пример:

```
http.request.body.re2 = "example|test"
```

request.header.<h_name> и response.header.<h_name>

Проверка HTTP-заголовка запроса/ответа. *h_name* может принимать одно из поддерживаемых значений. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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. Подробнее о поддерживаемых HTTP-заголовках — в разделе «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_names 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 | substring.nocase | 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 | substring.nocase | 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 % Проверить длину/количество query-параметров <name>

qparam.<name>[.base64][.(nocase | substring | substring.nocase | regex | re2)] = string % проверить имя <name> на вхождение подстроки/регулярные выражения

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

qparam.values.length = numeric % проверить длину всех значений

qparam.names.length = numeric % проверить длину всех имен

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"
```

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*.

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 | useragent | network | time>(list_names)

list_names ::= name list_names

name ::= word | string

url — список URL;
useragent — список юзерагентов;
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
```

```
PASS request.header.User-Agent = lib.useragent("Browsers")
DENY time = lib.time(Weekends)
```

Определения

В файлах политик определения (def) служат для объединения наборов условий или действий. Каждое определение должно иметь уникальное пользовательское имя, по которому к нему можно обратиться из правил.

def condition

Наборы условий. Все условия в одной строке проверяются по логическому *И*. Перевод строки означает логическое *ИЛИ*. Символ экранирования — обратный слэш ("****") в конце строки позволяет перенести условие по *И* на следующую строку.

Синтаксис:

def condition label_name

conditions

end

conditions ::= condition '\'? [conditions]

condition ::= name '=' value

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

def var

Определение переменных. Служит для подсчета некоторых событий за определенный интервал времени. Для изменения значения предназначены действия *inc* и *dec*.

Синтаксис:

def var label_name

init ::= integer

window ::= time

key ::= condition_name | condition_list

end

label_name ::= atom

atom ::= [a-z][0-9a-zA-Z_]+

condition_list ::= '(' condition_name , condition_list ')'

init — это начальное значение переменной, к которому она вернется по истечении времени *window*;

key — поле или список полей, по которым группируются значения переменной (необязательный параметр).

Свойства

Свойства (properties) — это некие атрибуты правила, например, *name* или *enabled*. Они используются для предоставления дополнительной информации в процессе обработки правил. Синтаксис свойств точно такой же, как у действий.

Синтаксис:

property = prop_name | prop_name '(' list_params ')'

prop_name ::= name | desc | id | rule_log | enabled

list_params ::= value ',' list_params

name и desc

Атрибуты *имя* и *описание* для правила.

Синтаксис:

Name ::= name '(' string|word ')'

Description ::= desc '(' string ')'

Пример:

```
DENY hour = 9..18 category = News name("Запретить News")
desc("Запретить категорию News в рабочее время")
```

enabled

Атрибут, который включает или выключает работу правила.

Синтаксис:

Enable ::= enabled '(' boolean ')'

boolean ::= yes | no | true | false % (по умолчанию false)

rule_log

Устанавливает атрибут журналирования правила.
Значение *session* действительно только для правил межсетевого экрана, защиты от dos-атак и пропускной способности.

Синтаксис:

Logging ::= rule_log '(' boolean | session ')'

LoggingFwRule ::= rule_log '(' boolean , interval, burst')'

boolean ::= yes | no | true | false % (по умолчанию no)

interval ::= "integer/[s,m,h,d]"

burst ::= integer

interval — среднее число пакетов, попадающих под условие *limit* в единицу времени (1/s, 1/m, 1/h, 1/d) , default = 3/h;
burst — максимальное число пакетов, попадающих в под условие *limit* за один раз (default = 5).

profile

Устанавливает профиль правила.

Синтаксис:

Profile ::= profile '(' string | word | list ')'

certificate

Сертификат, используемый для поддержки HTTPS-соединения. Действительно только для правил reverse-прокси.

Синтаксис:

CertAuthEnabled ::= cert_auth_enabled '(' boolean ')'

Certificate ::= certificate '(' certificate_name ')'

certificate_name ::= string | word

gateway

Шлюз. Имя одного из существующих шлюзов. Действительно только для правил NAT и маршрутизации, и для условий сценария "Проверка состояния".

Синтаксис:

Gateway ::= gateway '(' string | word ')'

Свойства правил межсетевого экрана

reject_with

Устанавливает способ, с помощью которого будет блокироваться трафик. Действительно только для правил межсетевого экрана.

Синтаксис:

Reject ::= reject_with '(' "tcp-reset-both" | "tcp-rst" | "host-unreach" ')'

fragmented

Проверка на фрагментированность пакетов. Действительно только для правил межсетевого экрана.

Синтаксис:

Fragmented ::= fragmented '(' boolean ')'

boolean ::= yes | no | true | false

yes — проверяются только фрагментированные пакеты;
no — проверяются только нефрагментированные пакеты;
—, если свойство *fragmented* не указано, то будут проверяться все пакеты.

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 ')'

Свойства правил публикации

is_https

Включение поддержки HTTPS. Действительно только для правил публикации.

Синтаксис:

IsHttps ::= is_https '(' boolean ')'

boolean ::= yes | no | true | false

rewrite_path

Подмена путей. Действительно только для правил публикации.

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).

waf_profile

WAF-профиль. Действительно только для правил публикации.

Синтаксис:

WafProfile ::= waf_profile '(' string | word | list ')'

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 ::= 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 | action_label

action_label ::= 'action'.<action_label_name>

action_label_name ::= atom

list_params ::= value ',' list_params

log_message

Записать сообщения в журнал.

Пример:

```
DENY category = lib.category(Productivity) log_message("Deny porno")
```

append

Добавить заголовок к HTTP-запросу/ответу. Подробнее о поддерживаемых заголовках — в разделе «Список поддерживаемых HTTP-заголовков».

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

append([request | response,] <headername>, value)

headername — см. в разделе «Список поддерживаемых HTTP-заголовков».
value ::= string | numeric | condition_name.

set

Переписать значение конкретному HTTP-заголовку. Подробнее о поддерживаемых заголовках — в разделе «Список поддерживаемых HTTP-заголовков».
Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

set([request | response,] <headername>, value)

headername — см. в разделе «Список поддерживаемых HTTP-заголовков».
value ::= string | numeric | condition_name.

delete

Удалить HTT- заголовок. Подробнее о поддерживаемых заголовках — в разделе «Список поддерживаемых HTTP-заголовков».

Первый параметр может быть опущен, если заголовок относится к одной группе *request* или *response*.

Синтаксис:

delete([request | response,] <headername>)

headername — см. в разделе «Список поддерживаемых HTTP-заголовков».

replace

Модифицировать значение HTTP-заголовка. Подробнее о поддерживаемых заголовках — в разделе «Список поддерживаемых HTTP-заголовков».

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 разделе «Список поддерживаемых HTTP-заголовков».

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. Подробнее о поддерживаемых заголовках — в разделе «Список поддерживаемых HTTP-заголовков».
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 разделе «Список поддерживаемых HTTP-заголовков».

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")
```

Типы правил

Экспертные правила временной блокировки IP-адреса

Префиксы

Имя	Описание
DENY	Блокировка IP-адреса

Условия

http.response.code

Свойства

name, enabled

Пример

В примере для конкретного источника (условие `scr.ip`) настроен подсчет количества кодов ответа 404. Если количество таких ответов за последние 30 секунд превысит 10, IP-адрес этого источника будет заблокирован на одну минуту.

```
def var counter_404
    init = 0
    window = 00:00:30
    key = src.ip
end
def var block
    init = 0
    window = 00:01:00
    key = src.ip
end

DENY var.block = 1.. log_message("Black list") enabled(true)
name("Black list")
http.response.code = 404 inc(var.counter_404, 1) log_message("Incriment
```

```
counter")  enabled(true) name("Incriment counter")
DENY var.counter_404 = 10.. inc(var.block, 1) log_message("Enable
block") enabled(true) name("Enable block")
```

Сетевые правила, настраиваемые с помощью CLI

Правила межсетевого экрана

Префиксы

Имя	Описание
PASS	Разрешение трафика.
DENY	Блокировка трафика.

Условия

src.zone, src.geoip, src.ip.

dst.zone, dst.geoip, dst.ip.

time, url.

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")
% ----------------- 2 -----------------
```

```
PASS \
    scenario = "Example torrent detection scenario" \
    src.zone = Trusted \
    dst.zone = Untrusted \
    rule_log(yes, "3/h", 5) \
    enabled(true) \
    name("Allow trusted to untrusted")
```

Правила публикации

Префиксы

Имя	Описание
OK	Всегда OK.

Условия

src.zone, src.geoip, src.ip, src.mac.

dst.zone, dst.geoip, dst.ip.

request.header.User-Agent, url.port.

Свойства

name, desc, enabled, rule_log, profile, certificate, is_https, ssl_profile,

waf_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") \
```

```
    waf_profile("Example WAF profile") \
    enabled(true) \
    name("Example reverse proxy rule")
```

Правила балансировки

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	✅	✅	✅

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
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	Request/ Response			
ETag	Response	✓	✓	
Expect	Request	✓		
Expires	Request/ Response		✓	✓
From	Request	✓	✓	

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
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	✓	✓	
Retry-After	Response	✓	✓	
Server	Response	✓	✓	
Set-Cookie	Response	✓	✓	✓
TE	Request	✓		
Trailer	Request/ Response		✓	

HTTP Header	Request/ Response	SET/REPLACE/ ENCRYPT	APPEND	DELETE
Transfer-Encoding	Request/ Response		✓	
Upgrade	Request/ Response		✓	
User-Agent	Request	✓	✓	
Vary	Response	✓	✓	✓
Via	Request/ Response	✓	✓	✓
Warning	Request/ Response	✓	✓	✓
WWW-Authenticate	Response			

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Раздел технической поддержки

Раздел технической поддержки на сайте компании содержит дополнительную информацию по настройке устройства. Здесь же вы можете оставить заявку на решение возникшей проблемы с оборудованием.

Аварийные ситуации

Сбои в работе устройства могут возникнуть при некорректной установке обновлений программного обеспечения.

Для профилактики аварийных ситуаций:

1. Перед установкой обновления сделайте резервную копию устройства. Подробнее — в разделе «Управление резервным копированием».

2. Во время установки обновления создайте точку восстановления системы. Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении устройства:

1. Восстановите предыдущую стабильную версию ПО. Подробнее — в разделе «Обновление ПО».

2. Обратитесь в службу технической поддержки в зависимости от уровня вашего сервисного контракта:

- Premium-поддержка: позвоните по выделенному телефону для экстренной помощи.
- Brilliant-поддержка: свяжитесь с вашим выделенным техническим специалистом.
- Базовая поддержка: обратитесь за квалифицированной помощью на странице поддержки.

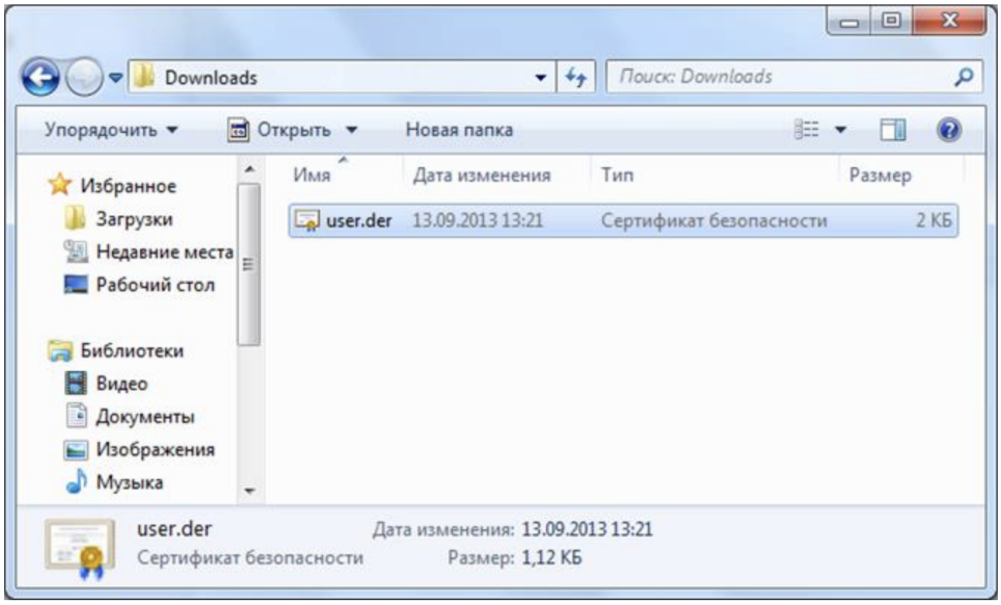
ПРИЛОЖЕНИЯ

Установка сертификата локального удостоверяющего центра

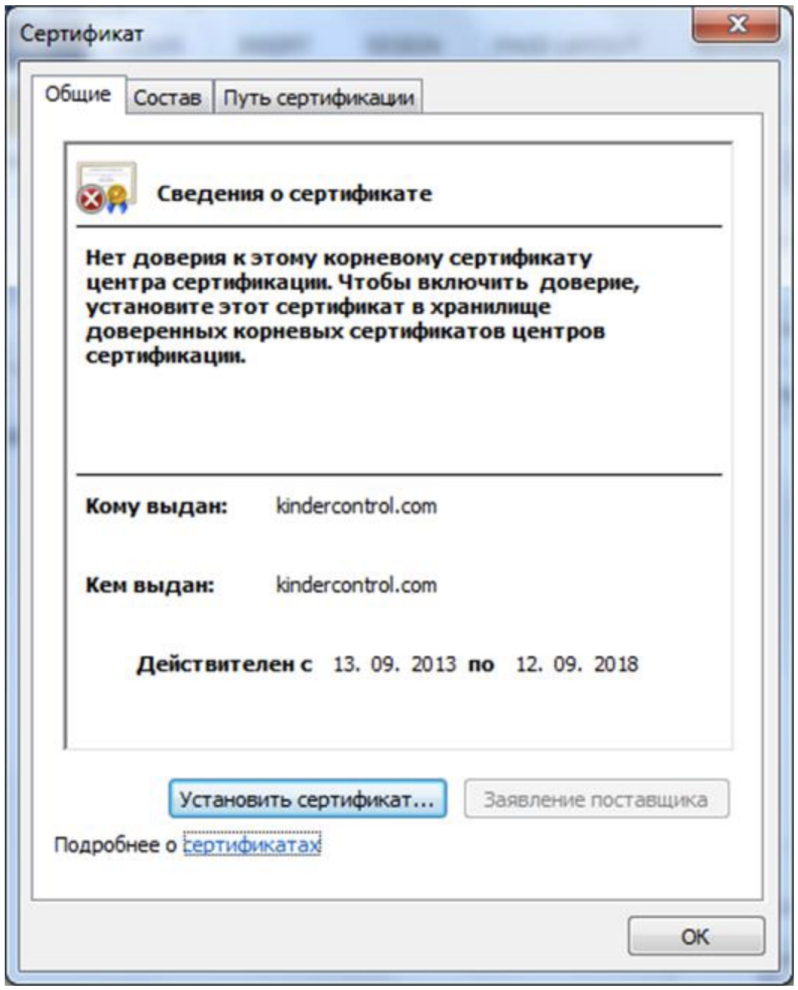
Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

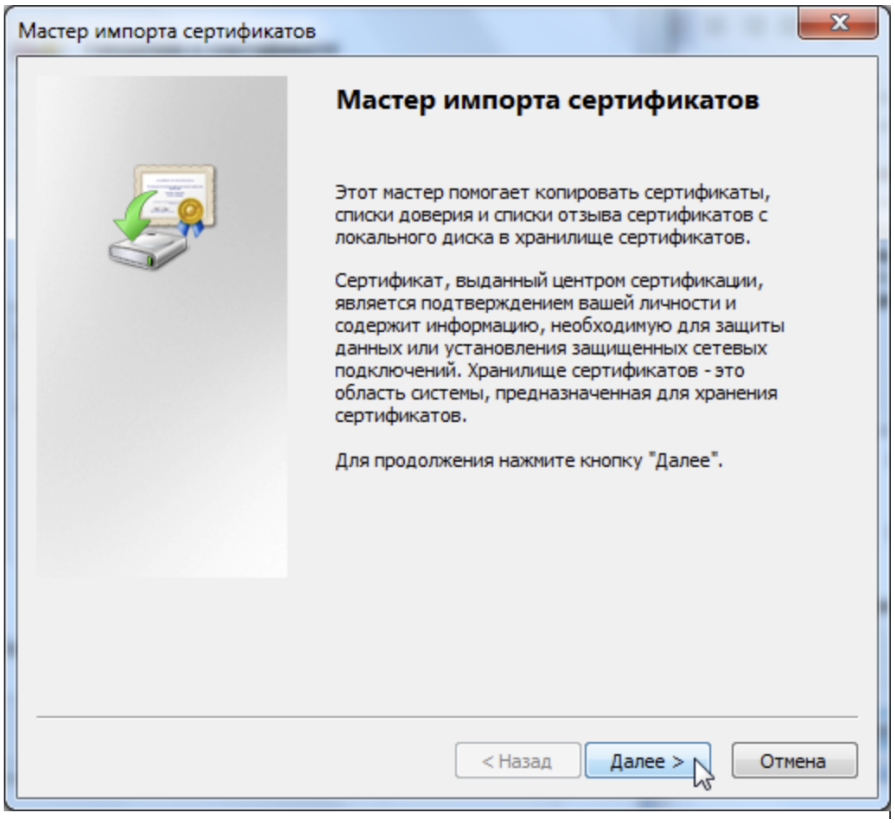
Откройте папку, куда вы скачали pem-сертификат, переименуйте его в `user.der` и дважды нажмите на него:



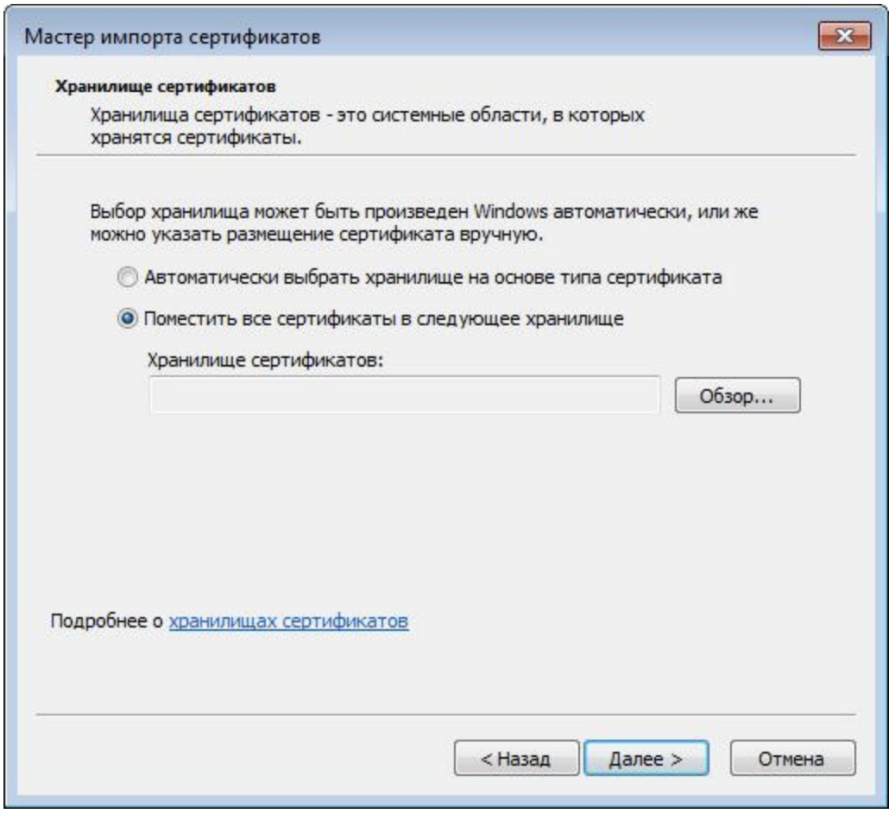
Откроется информация о сертификате. Нажмите **Установить сертификат**:



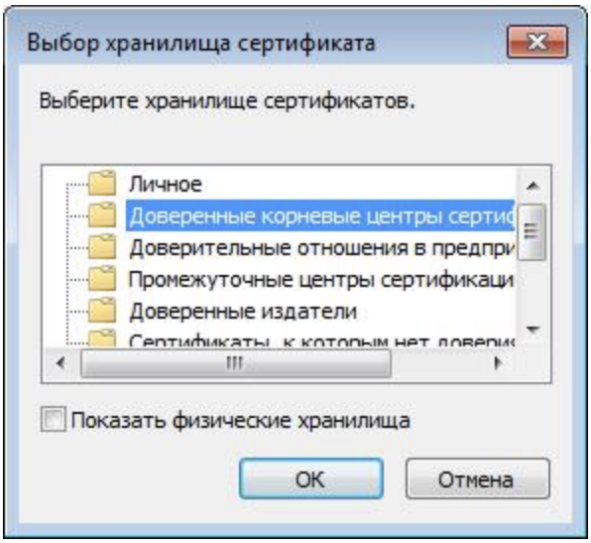
Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:



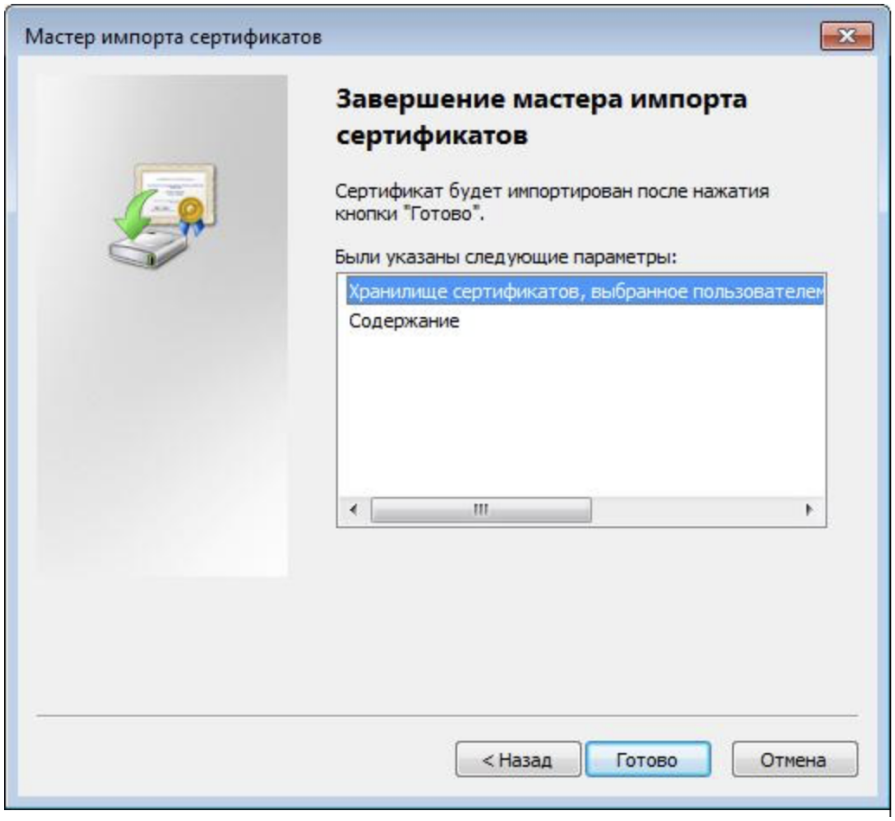
Выберите хранилище сертификата и нажмите **Обзор**:



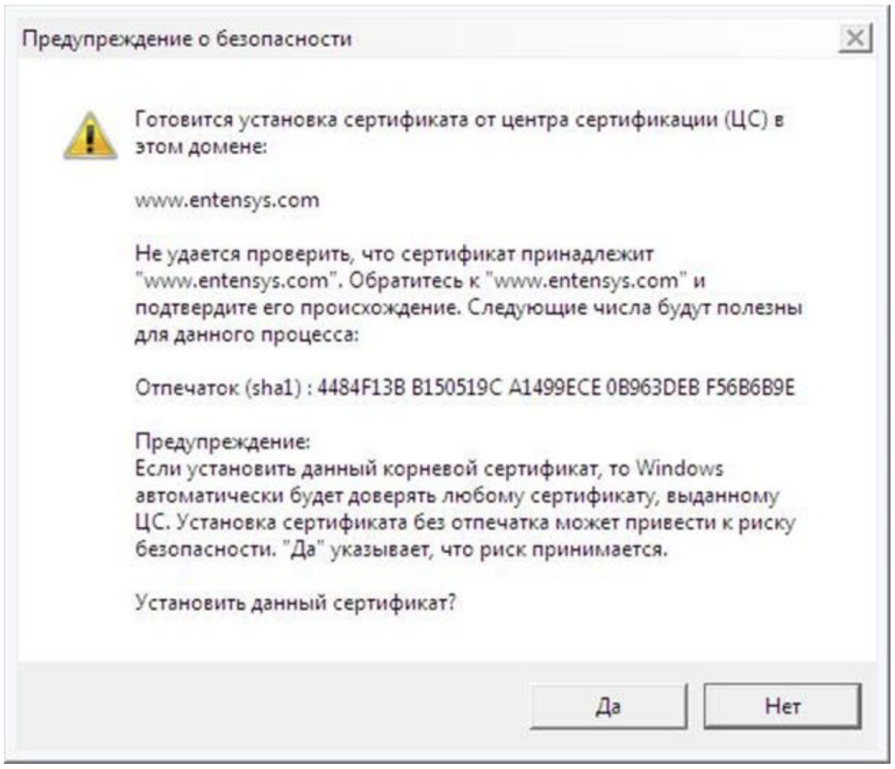
Выберите **Доверенные корневые центры сертификации** и нажмите **ОК**:



Нажмите **Готово**:



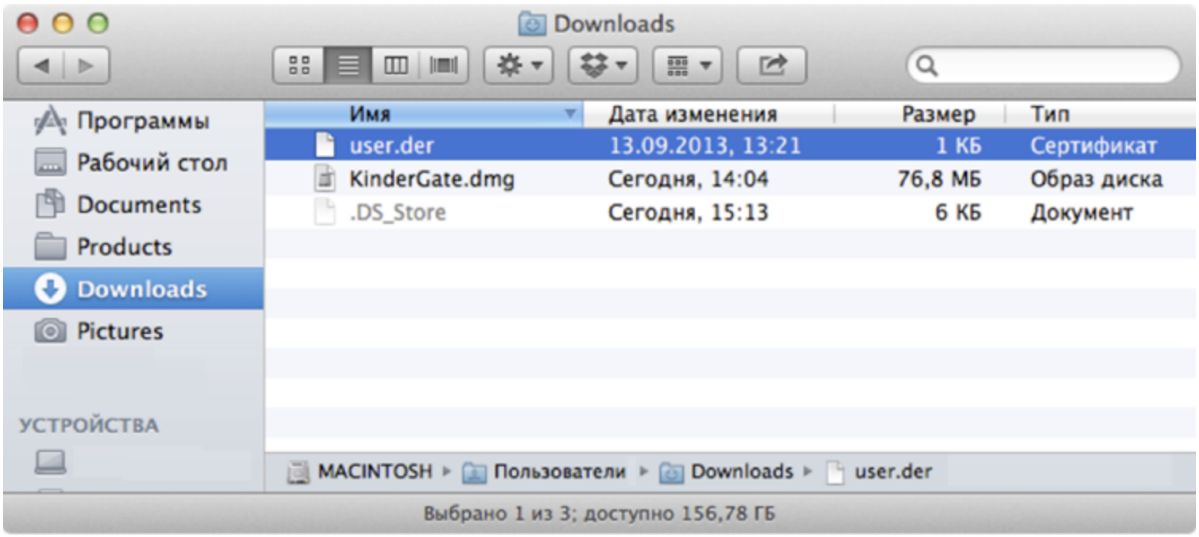
Когда появится предупреждение системы безопасности, нажмите **Да**:



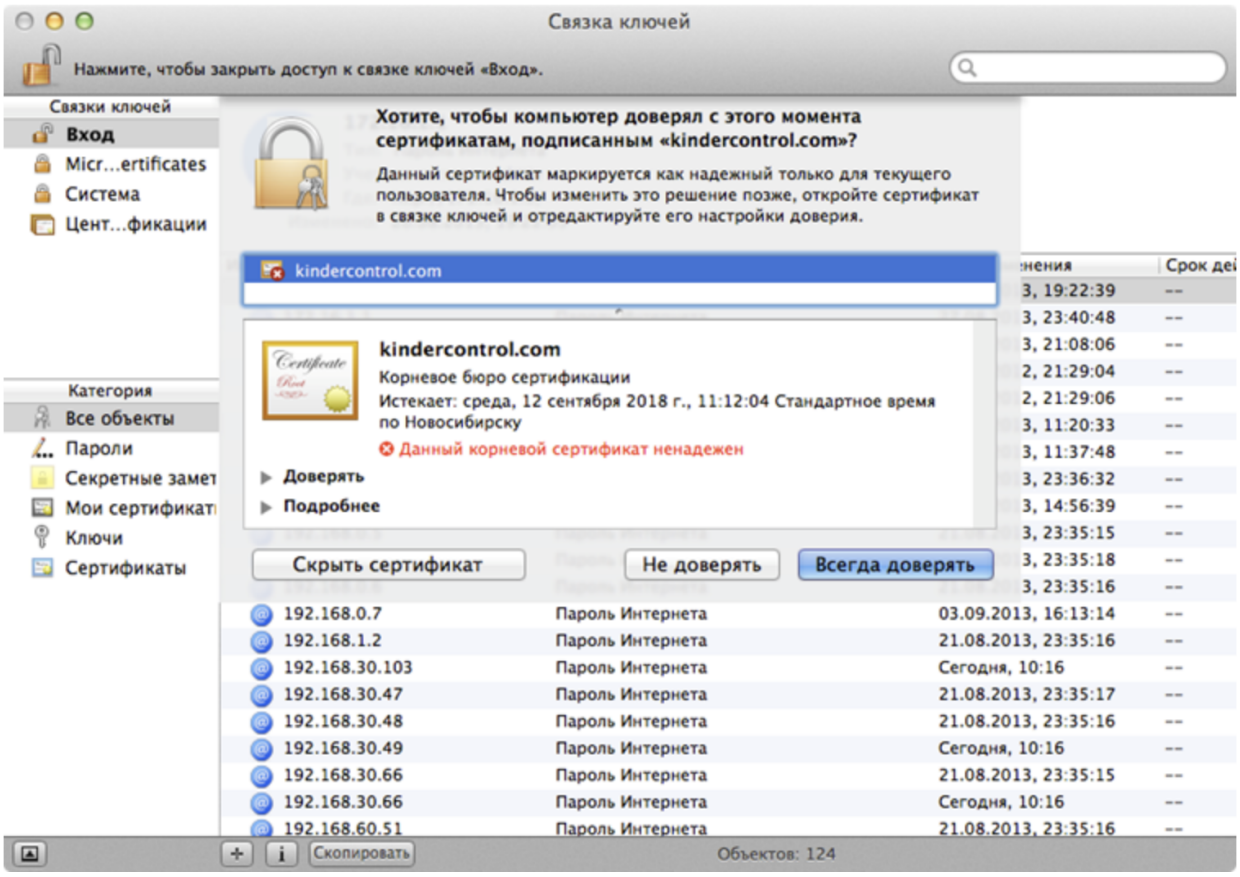
Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в ОС MacOSX

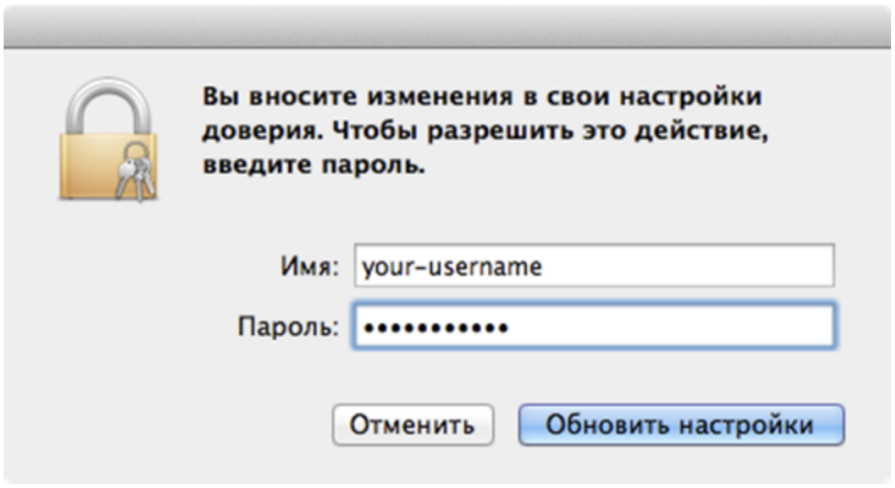
Перейдите в папку, куда вы скачали pem-сертификат и дважды нажмите на него:



Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:



Введите свой пароль для подтверждения данной операции:

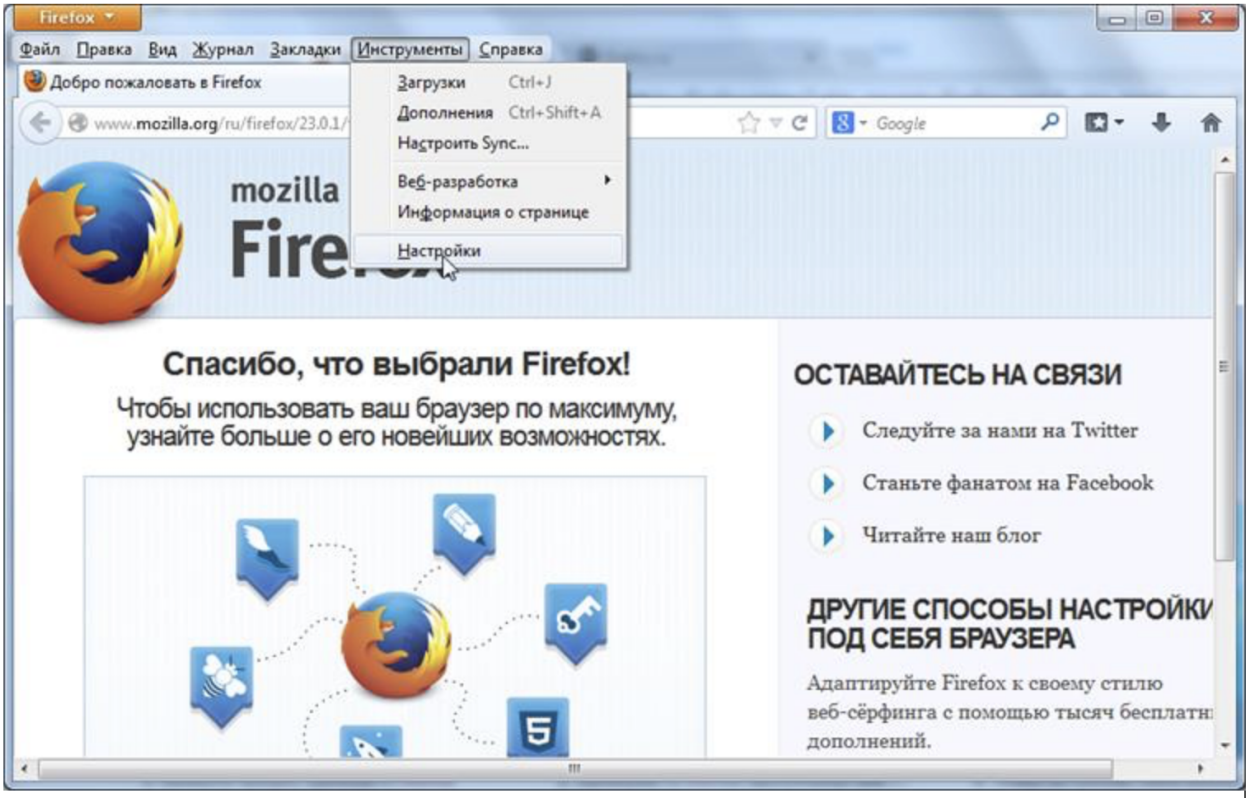


Сертификат установлен.

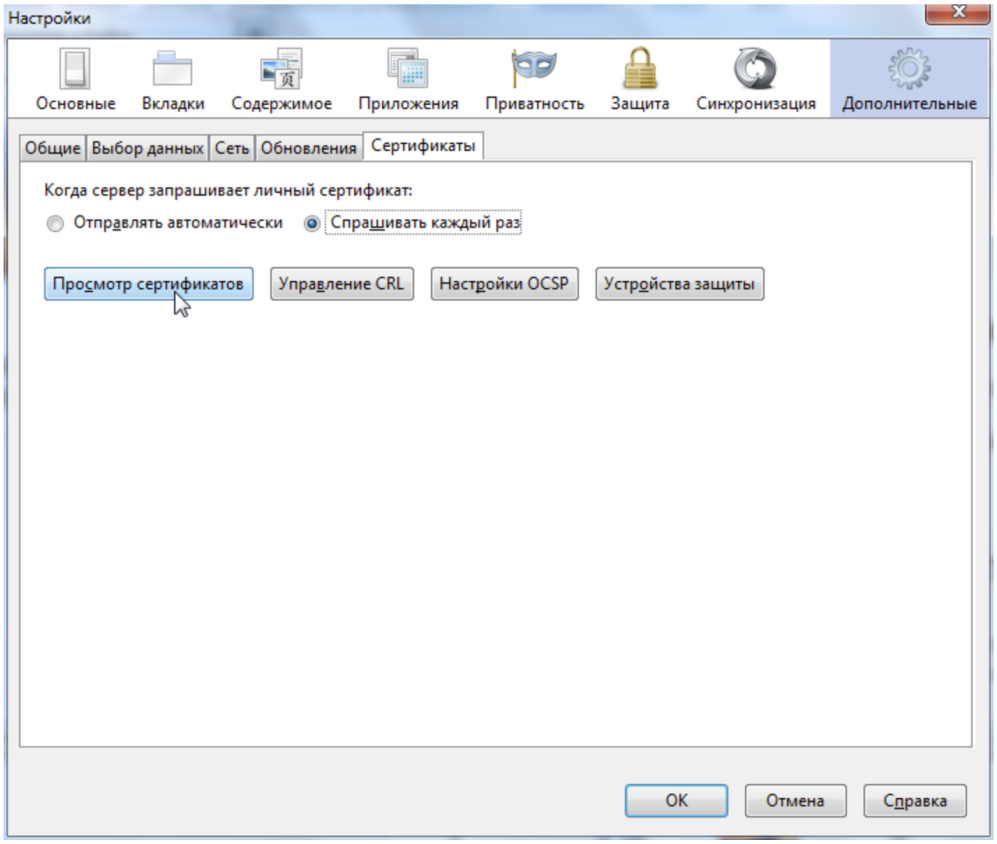
Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется одинаково для всех операционных систем. Рассмотрим установку на примере ОС Windows.

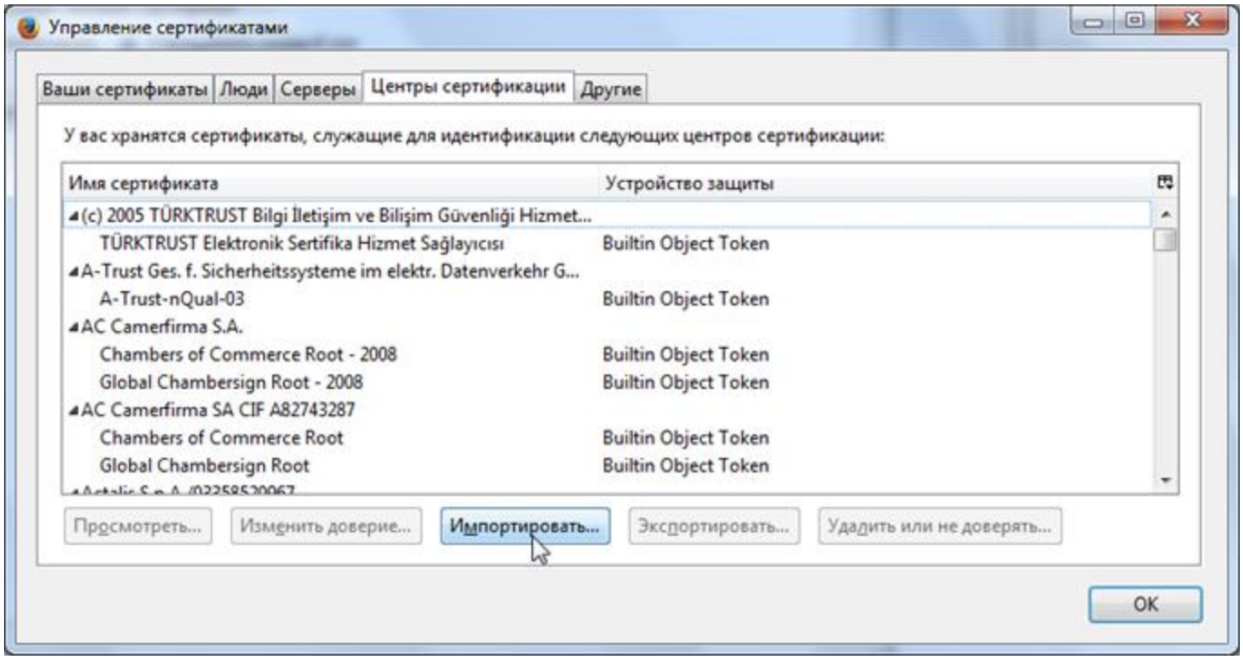
Откройте настройки браузера Firefox (**Инструменты → Настройки**):

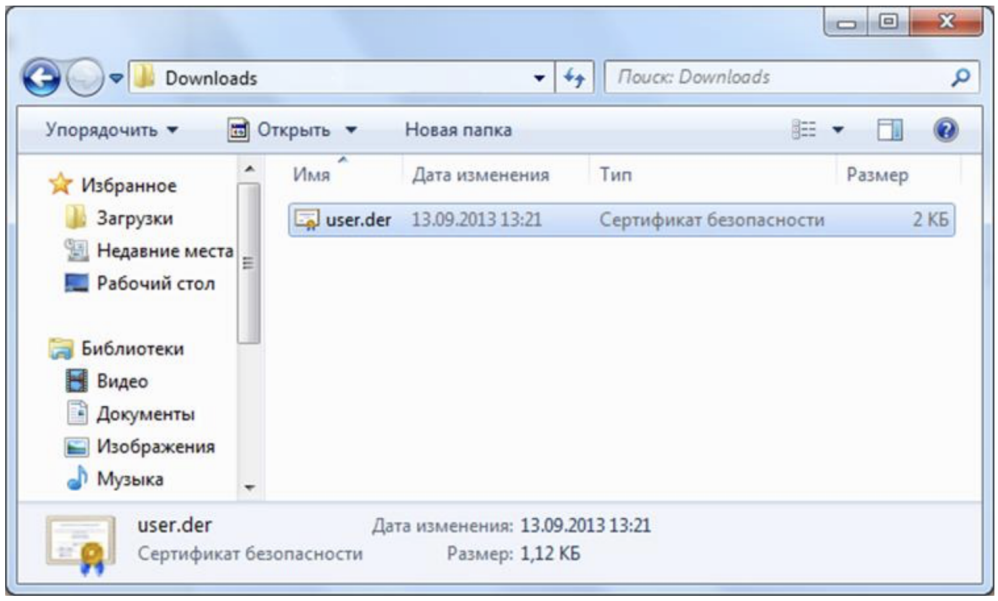


Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите **Просмотр сертификатов**:

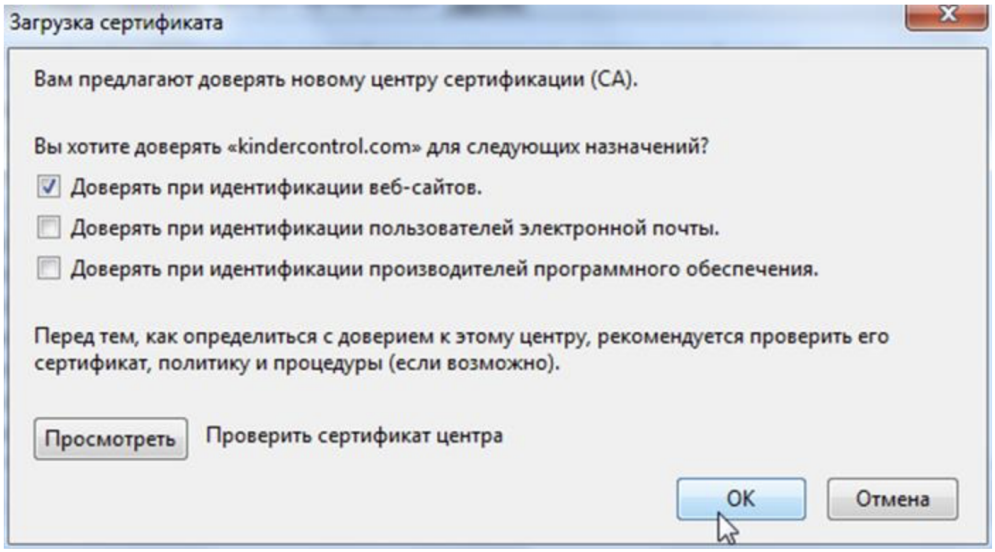


Нажмите **Импортировать** и укажите путь к скачанному pem-сертификату:





Установите флажок **Доверять при идентификации веб-сайтов** и нажмите **OK**:



Установка сертификата завершена.