Table of Contents

Table of Contents 1
Интерфейс командной строки 2
Общие положения 3
Общие положения (Описание) 4
Команды, доступные до первичной инициализации узла 5
Команды, доступные до первичной инициализации узла (Описание) 6
Первоначальная инициализация 7
Первоначальная инициализация (Описание) 8
Команды диагностики и мониторинга 9
Команды диагностики и мониторинга (Описание) 10
Режим конфигурации 15
Режим конфигурации (описание) 16
Настройка устройства 19
Базовые настройки 20
Настройка управления доступом к веб-консоли UserGate WAF 24
Настройка сертификатов 27
Настройка профилей клиентских сертификатов 29
Настройка кластеров 30
Настройки раздела Пользователи и устройства 31
Настройка серверов аутентификации 32
Настройка профилей аутентификации 35
Настройки сети 36
Зоны 37
Интерфейсы 39
Шлюзы 46
Настройка виртуальных маршрутизаторов 47
Настройки раздела Политики сети 49
Настройка правил межсетевого экрана 50
Настройка публикации веб-сервисов 52
Настройка серверов публикации 53
Настройка правил публикации 54
Настройка балансировки нагрузки 56
Настройки библиотек 57
Настройка библиотек (Описание) 58
Настройки раздела журналы и отчеты 67
Настройка экспорта журналов 68
Настройка безопасности 70
Настройка параметров безопасности WAF 71
Настройка JSON-профиля в CLI 73
Настройка XML-профиля в CLI 74
Настройка WebSocket-профиля в CLI 75
Настройка профиля ответа 76

Общие положения

Общие положения (Описание)

Product: WAF
Version: 7.7.x

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
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)

Product: WAF
Version: 7.7.x

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)

Product: WAF
Version: 7.7.x

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

Команды диагностики и мониторинга (Описание)

Product: WAF
Version: 7.7.x

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.
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.

Параметр	Описание
type	Проверка доступности по: • **http**. • **tcp** (если порт не указан, то используется порт 80).
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.

ПримечаниеВ 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

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	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

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.).
	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

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	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 (описание)

Product: WAF
Version: 7.7.x

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. • 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: 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» ; • 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»

Наименование	Описание
<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) **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>]
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: 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>

Параметр	Описание

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;
	• 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
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>
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».

Product: WAF
Version: 7.7.x

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)

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: 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

Раздел	Описание
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: 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 UserGate WAF;
- 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

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 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

Product: WAF
Version: 7.7.x

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

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

Параметр	Описание
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" 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
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 ...]

Параметр	Описание
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all или Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [object ...]

Для редактирования профиля используется команда:

Admin@nodename# set settings administrators profiles <profile-name> <parameter>

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

Admin@nodename# show settings administrators profiles

Для отображения информации об определённом профиле:

Admin@nodename# show settings administrators profiles <profile-name>

Чтобы удалить профиль администратора:

Admin@nodename# delete settings administrators profiles <profile-name>

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

Admin@nodename# show settings administrators admin-sessions

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

Admin@nodename# show settings administrators admin-sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

Admin@nodename# execute termination admin-sessions <IP-address/connection type>

Пример выполнения команд:

Admin@nodename# show settings administrators admin-sessions

```
admin-login          : Admin
source               : ssh
session_start_date   : 2023-08-10T11:33:47Z
ip                   : 127.0.0.1
node                 : utmcore@dineanoulwer

admin-login          : Admin
source               : web
session_start_date   : 2023-08-10T11:33:10Z
ip                   : 10.0.2.2
node                 : utmcore@dineanoulwer
```

Admin@nodename# execute termination admin-sessions 10.0.2.2/web

Admin@nodename# show settings administrators admin-sessions

```
admin-login          : Admin
source               : ssh
session_start_date   : 2023-08-10T11:33:47Z
ip                   : 127.0.0.1
node                 : utmcore@dineanoulwer
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

Admin@nodename# execute termination admin-sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Настройка сертификатов

Product: WAF
Version: 7.7.x

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. • **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
role	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • **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

Параметр	Описание
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

Product: WAF
Version: 7.7.x

Раздел **Профили клиентских сертификатов** находится на уровне **settings certificate-profiles**.

Для создания профиля клиентского сертификата предназначена команда:

Admin@nodename# create settings certificate-profiles <parameters>

Далее могут использоваться следующие параметры:

Параметр	Описание
name	Название профиля клиентского сертификата
description	Описание профиля
username-field	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: • **common** — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. • **email** — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name) . • **principal** — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. 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>

Documentation:
Product: WAF
Version: 7.7.x
Technology: Clustering and HA

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

Product: WAF
Version: 7.7.x

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.

Параметр	Описание
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	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

Product: WAF
Version: 7.7.x
Technology: Identification and Authentication

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 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>

Зоны

Product: WAF
Version: 7.7.x

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.
	• **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.
	• **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**. 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.

Параметр	Описание
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>

Product: WAF
Version: 7.7.x

Список упорядоченных имён сетевых интерфейсов и соответствующие им физические адреса доступен для отображения при выполнении команды (команда доступна и в режиме диагностики и мониторинга и в режиме конфигурации):

Admin@nodename> show network interface-mapping

Admin@nodename# show network interface-mapping

Упорядочивание интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующие команды в режиме диагностики и мониторинга и в режиме конфигурации соответственно:

Admin@nodename> clear network interface-mapping

Admin@nodename# delete network interface-mapping

После перезагрузки сервера UserGate список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate.

Далее будет рассмотрена настройка интерфейсов, которая производится на уровне **network interface**.

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

Admin@nodename# set network interface adapter <adapter_name>

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	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».
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.

Параметр	Описание

dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать:
	• **enabled**: включение/отключения релея:
	  ◦ **on**.
	  ◦ **off**.
	• **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip | none>).
	• **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

Admin@nodename# delete network interface adapter <adapter-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

Admin@nodename# show network interface adapter

Для отображения информации об адаптере:

Admin@nodename# show network interface adapter <adapter-name>

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

Admin@nodename# create network interface vlan

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
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».
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.

Параметр	Описание
mtu	Указание размера MTU.
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**.
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».

Параметр	Описание

bonding	Дополнительные параметры бонд-интерфейса:
	• **aggr-mode** — режим работы бонда:
	  ◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости).
	  ◦ **active-backup**: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости).
	  ◦ **xor**: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости).
	  ◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости).
	  ◦ **802.3ad**: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику).
	  ◦ **transmit**: режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты).
	  ◦ **load**: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
	• **mii-monitoring**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов.
	• **down-delay**: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon.
	• **up-delay**: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon.
	• **lacp-rate**: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:
	  ◦ **slow**: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.
	  ◦ **fast**: запрос партнера на передачу LACPDU-пакетов каждую секунду.
	• **failover-mac**: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения:
	  ◦ **disabled**: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.
	  ◦ **active**: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа.
	  ◦ **follow**: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.
	• **xmit-hash**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:
	  ◦ **l2**: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad.
	  ◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.
	  ◦ **l3-4**: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
	• **interface**: интерфейсы, которые будут объединены в бонд.

iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	Тип создаваемого интерфейса: • **l3** — Layer 3 интерфейс. • **mirror** — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
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

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

Admin@nodename# show network interface bond

или об определённом интерфейсе:

Admin@nodename# show network interface bond <bond-name>

Настройка bridge-интерфейса

Настройка моста производится на уровне **network interface bridge**.

Чтобы добавить новый bridge-интерфейс:

Admin@nodename# create network interface bridge

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).
description	Описание bridge-интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
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 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.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.

Параметр	Описание

dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать:
	• **enabled**: включение/отключения релея:
	  ◦ **on**.
	  ◦ **off**.
	• **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея.
	• **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

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».
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.

Параметр	Описание
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 (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

Product: WAF
Version: 7.7.x

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**.
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

Product: WAF
Version: 7.7.x
Technology: Routing

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**. • **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

Product: WAF
Version: 7.7.x
Technology: Firewall

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
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 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 серверов публикации

Product: WAF
Version: 7.7.x

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
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

Product: WAF
Version: 7.7.x

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. 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). 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. **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»

Параметр	Описание
allowed_web_services	Путь к одному или нескольким веб-сервисам, запросы к которым будет обрабатывать правило. 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.
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 »
json_profile_id	Включение обработки HTTP-запросов с данными в формате JSON. Необходимо указать заранее созданный JSIN-профиль. Например, json_profile_id("Example_json_profile")
xml_profile_id	Включение обработки HTTP-запросов с данными в формате XML. Необходимо указать заранее созданный XML-профиль. Например, xml_profile_id("Example_XML_profile")
websocket_profile	Включение обработки websocket-соединений. 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

Product: WAF
Version: 7.7.x
Technology: Firewall

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")**.
profile	Указание 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>

Product: WAF
Version: 7.7.x

Настройка JSON-схем

JSON-схемы создаются и настраиваются на уровне libraries json-schemas.

Для создания JSON-схемы используется команда:

Admin@nodename# create libraries json-schemas <parameter>

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название JSON-схемы
description	Описание JSON-схемы
schema	Содержимое JSON-схемы
version	Версия спецификации JSON-схемы

Пример команды для создания JSON-схемы:

Admin@nodename# create libraries json-schemas name test description description schema "{\"$schema\":\"http://json-schema.org/draft-04/schema#\",\"type\":\"object\",\"properties\":{\"name\":{\"type\":\"string\"},\"age\":{\"type\":\"integer\",\"minimum\":18},\"email\":{\"type\":\"string\",\"format\":\"email\"}},\"required\":[\"name\",\"age\",\"email\"]}"

Настройка XML-схем

XML-схемы создаются и настраиваются на уровне libraries json-schemas.

Для создания XML-схемы используется команда:

Admin@nodename# create libraries xml-schemas <parameter>

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название XML-схемы
description	Описание XML-схемы
schema	Содержимое XML-схемы
version	Версия спецификации

Пример команды для создания XML-схемы:

Admin@nodename# create waf xml-schemas name test description description schema "<?xml version=\"1.0\"?><xs:schema xmlns:xs=\"http://www.w3.org/2001/XMLSchema\"><xs:element name=\"note\"><xs:complexType><xs:sequence><xs:element name=\"to\" type=\"xs:string\"/><xs:element name=\"from\" type=\"xs:string\"/><xs:element name=\"heading\" type=\"xs:string\"/><xs:element name=\"body\" type=\"xs:string\"/></xs:sequence></xs:complexType></xs:element></xs:schema>"

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. • 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

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 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). ▪ 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>

ПримечаниеШаблон 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). 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

Параметр	Описание
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
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

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»

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]

Параметр	Описание
source-ton	Тип номера (type of number) для источника сообщения: • 0 — unknown (неизвестный). • 1 — international (международный). • 2 — national (государственный). • 3 — network specific (сетевой специальный). • 4 — subscriber number (номер абонента). • 5 — alphanumeric (алфавитно-цифровой). • 6 — abbreviated (сокращенный)
dest-ton	Тип номера (type of number) для адресата: • 0 — unknown (неизвестный). • 1 — international (международный). • 2 — national (государственный). • 3 — network specific (сетевой Специальный). • 4 — subscriber number (номер абонента). • 5 — alphanumeric (алфавитно-цифровой). • 6 — abbreviated (сокращенный)
source-npi	Индикатор схемы присвоения номеров (numbering plan indicator) для источника: • 0 — unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — data numbering plan (X.121). • 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

Параметр	Описание
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
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
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

Параметр	Описание
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

Product: WAF
Version: 7.7.x

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). • **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.

Параметр	Описание
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 параметров безопасности WAF

Product: WAF
Version: 7.7.x
Technology: 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 JSON-профиля в CLI

Documentation:
Product: WAF
Version: 7.7.x

Настройка JSON-профилей происходит в режиме конфигурации на уровне json-profiles.

Для создания JSON-профиля используется следующая команда:

Admin@nodename# create security-policy json-profiles <parameter>

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название JSON-профиля
description	Описание JSON-профиля
log	Включение/отключение журналирования: • On; • Off
content-types	Указание одного или нескольких значений заголовка Content-type
action	Выбор действия JSON-профиля: • deny; • pass
response-profile	Добавление профиля ответа. Необходимо указать название заранее созданного профиля ответа
json-schemas	Выбор проверки на соответствие любой или всем JSON-схемам: • any; • all
json-schemas	Добавление JSON-схем. Необходимо указать одно или несколько названий заранее созданных JSON-схем
check-limits	Включение/отключение проверки лимитов: • On; • Off
max-body-size	Лимит на размер тела формата JSON в байтах. Максимальное значение — 10240000. Значение по умолчанию — 0
max-depth	Лимит на глубину вложенности элементов. Максимальное значение — 256. Значение по умолчанию — 0
max-array-elements	Лимит на количество элементов «ключ: значение» в объекте. Максимальное значение — 4096. Значение по умолчанию — 0
max-object-members	Лимит на количество элементов (значений) в массиве. Максимальное значение — 4096. Значение по умолчанию — 0
max-string-length	Лимит на количество символов в значении типа «строка». Максимальное значение — 4096. Значение по умолчанию — 0
max-key-length	Лимит на количество символов в имени ключа. Максимальное значение: 1024. Значение по умолчанию — 0

Пример команды создания JSON-профиля:

Admin@nodename# create security-policy json-profiles name json_test action deny check-limits on max-body-size 5000

Команда для редактирования параметров JSON-профиля:

Admin@nodename# set security-policy json-profiles <json-profile_name> <parameter>

Команда для отображения информации о всех JSON-профилях:

Admin@nodename# show security-policy json-profiles

Команда для отображения информации об определенном JSON-профиле:

Admin@nodename# show security-policy json-profiles <profile_name>

Команда для удаления существующего JSON-профиля используется следующая команда:

Admin@nodename# delete security-policy json-profiles <profile_name>

Настройка XML-профиля в CLI

Documentation:
Product: WAF
Version: 7.7.x

Настройка XML-профилей происходит в режиме конфигурации на уровне xml-profiles.

Для создания XML-профиля используется следующая команда:

Admin@nodename# create security-policy xml-profiles <parameter>

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название XML-профиля
description	Описание XML-профиля
log	Включение/отключение журналирования: • On; • Off
content-types	Указание одного или нескольких значений заголовка Content-type
action	Выбор действия XML-профиля: • deny; • pass
response-profile	Добавление профиля ответа. Необходимо указать название заранее созданного профиля ответа
xml-schemas	Выбор проверки на соответствие любой или всем XML-схемам: • any; • all
xml-schemas	Добавление XML-схем. Необходимо указать одно или несколько названий заранее созданных XML-схем
check-limits	Включение/отключение проверки лимитов: • On; • Off
max-body-size	Лимит на размер тела формата XML в байтах. Максимальное значение — 10240000. Значение по умолчанию — 0
max-depth	Лимит на глубину вложенности элементов. Максимальное значение — 256. Значение по умолчанию — 0
max-elements	Лимит на количество элементов «ключ: значение» в объекте. Максимальное значение — 4096. Значение по умолчанию — 0
max-attributes	Лимит на количество атрибутов. Максимальное значение: 4096 — Значение по умолчанию — 0
max-tag-len	Лимит на количество символов в имени ключа. Максимальное значение — 1024. Значение по умолчанию — 0
max-attr-name-len	Лимит на длину имени атрибута. Максимальное значение — 1024. Значение по умолчанию — 0
max-attr-value-len	Лимит на длину текстового значения. Максимальное значение — 4096. Значение по умолчанию — 0
max-data-len	Лимит на длину значения атрибута. Максимальное значение — 10485760. Значение по умолчанию — 0

Пример команды создания XML-профиля:

Admin@nodename# create security-policy xml-profiles name xml_test action deny check-limits on max-body-size 5000

Команда для редактирования параметров XML-профиля:

Admin@nodename# set security-policy xml-profiles <xml-profile_name> <parameter>

Команда для отображения информации о всех XML-профилях:

Admin@nodename# show security-policy xml-profiles

Команда для отображения информации об определенном XML-профиле:

Admin@nodename# show security-policy xml-profiles <profile_name>

Команда для удаления существующего XML-профиля используется следующая команда:

Admin@nodename# delete security-policy xml-profiles <profile_name>

Настройка WebSocket-профиля в CLI

Product: WAF
Version: 7.7.x
Technology: WAF

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
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>

Настройка профиля ответа

Product: WAF
Version: 7.7.x
Technology: WAF

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.
	• 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>