

Table of Contents

Table of Contents	1
Режим конфигурации	2
Режим конфигурации (описание)	3

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

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: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображен под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show</pre> <pre>adapter: port0 interface-name : port0 node-name : utmcore@dineanoulwer zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp</pre> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end два раза: <pre>Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#</pre> Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду top: <pre>Admin@nodename# top Level: network interface Admin@nodename#</pre>

Наименование	Описание
<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»
<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: <pre>Admin@nodename# show network interface adapter port0</pre> 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: <pre>Admin@nodename# show network interface adapter (node-name another_nodename interface port0)</pre> Важно! Круглые скобки должны быть отделены пробелами с обеих сторон
<configuration_info>	Указание параметра с аргументом. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать IP-лист в библиотеке с названием New list: <pre>Admin@nodename# create libraries ip-list name "New list"</pre> 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]: <pre>Admin@nodename# set libraries ip-list "New list" ips [10.10.0.2 10.10.0.3]</pre> 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: <pre>Admin@nodename# execute cache ldap-clear</pre>
check-geoip	Проверка географической принадлежности IP-адреса по текущей базе GeoIP: <pre>Admin@nodename# execute check-geoip ip <ip-address></pre>

Параметр	Описание
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): <pre>Admin@nodename# execute clear-cli-history</pre> <pre>Admin@nodename# execute clear-cli-history modes [<configure diagnostic>]</pre>
configure-cluster	Генерация секретного кода, необходимого для добавления нового узла в кластер конфигурации: <pre>Admin@nodename# execute configure-cluster generate-secret-key <parameter></pre> Где: - secret — ключ для генерации секретного кода в формате [0-9a-zA-Z]+#[0-9a-zA-Z]+ (например, example#key); - expiration-time — срок действия кода в секундах; - request-limit — срок действия запроса на генерацию кода. Важно! Для использования данной команды необходимо наличие лицензии на модуль Cluster
date	Просмотр текущих даты и времени на узле: <pre>Admin@nodename# execute date</pre>
dig	Проверка записи DNS домена: <pre>Admin@nodename# execute dig host <hostname> <parameters></pre> <pre>Admin@nodename# execute dig host <IP-address> <parameters></pre> - 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: <pre>Admin@nodename# execute factory-reset</pre> Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
firewall	Применение всех правил межсетевого экрана заново с обрывом текущих сессий: <pre>Admin@nodename# execute firewall force-changes</pre>
license	Команда регистрации продукта: <pre>Admin@nodename# execute license activate <pin-code></pre> В качестве <pin-code> укажите код активации продукта
logs	Команда разовой отправки журналов по имеющемуся правилу экспорта журналов: <pre>Admin@nodename# execute logs send-once <export-log-name></pre>

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»

Параметр	Описание
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](#)».

