

Table of Contents

Table of Contents	1
Режим конфигурации	2
Режим конфигурации	3

Режим конфигурации

Product: DCFW
Version: 8.x

Для перехода в режим конфигурации используется команда:

Admin@nodename> configure

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

Admin@nodename#

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

- * — обязательное поле в командах create и ряде других команд;
- + — необязательное/вариативное поле;
- > — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin@nodename# set network virtual-router default
* name          Name
+ description    Description
+ interfaces     List of network interfaces attached to this virtual router
> bgp            BGP router
> multicast-router Multicast router
> ospf           OSPF router
> rip            RIP router
> routes         List of static network routes
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

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

где:

- <action> — действие, которое необходимо выполнить.
- <level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса DCFW.
- <filter> — идентификатор объекта, к которому происходит обращение.
- <configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • execute — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • set — редактирование всех объектов, а также включение различных параметров, например, radmin. • end — переход на один уровень выше. • show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • top — возврат на самый верхний уровень конфигурации. • exit — выход из режима конфигурации. • export — экспорт конфигурации. • import — импорт конфигурации. • create — создание новых объектов. • delete — удаление объекта или параметра из списка параметров. • debug — включение журналирования событий протоколов динамической маршрутизации. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображён над командной строкой: <pre>Admin@nodename# edit network interface [network interface] Admin@nodename#</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 2 раза: <pre>[network interface] Admin@nodename# end [network] Admin@nodename# end Admin@nodename#</pre> Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду top: <pre>[network interface] Admin@nodename# top Admin@nodename#</pre>

Наименование	Описание
<level>	Уровни в командной строке повторяют веб-интерфейс UserGate DCFW: • security-policy — соответствует разделу веб-интерфейса Политики безопасности. • network — соответствует разделу веб-интерфейса Сеть. • settings — соответствует разделу веб-интерфейса UserGate. • global-portal — соответствует разделу веб-интерфейса Глобальный портал. • network-policy — соответствует разделу веб-интерфейса Политики сети. • vpn — соответствует разделу веб-интерфейса VPN. • users — соответствует разделу веб-интерфейса Пользователи и устройства. • libraries — соответствует разделу веб-интерфейса Библиотеки. • monitoring — соответствует разделу веб-интерфейса Диагностика и мониторинг. • waf — соответствует разделу веб-интерфейса WAF.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info> (рассмотрено далее в разделе). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках. Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду: <pre>Admin@nodename# show network interface adapter port0</pre> то будет отображена информация об интерфейсе port0 текущего узла UserGate. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла: <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>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать группу с именем VPN users: <pre>Admin@nodename# create users group "VPN users"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо в группу VPN users добавить пользователей user1 и user2. Параметру users необходимо задать аргумент [user1 user2]: <pre>Admin@nodename# set users group "VPN users" users [user1 user2]</pre> Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

```
Admin@nodename# execute <command-name>
```

Доступны следующие команды:

Параметр	Описание
update	Обновление: • software-updates — обновление программного обеспечения. • libraries-updates — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.

Параметр	Описание
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • 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 hostname <hostname>
license	Команда регистрации продукта имеет следующую структуру: Admin@nodename# execute license activate <pin-code> Укажите код активации продукта вместо <pin-code>.
logs	• send-once — команда разовой отправки журналов по правилу.
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Настройка сессий администраторов.
cache	Очистка кэша LDAP-записей: • ldap-clear.
check-geoip	Проверка принадлежности IP-адреса по текущей базе GeoIP.
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • 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). • numeric — не резолвить имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — размер mtu отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. Admin@nodename# execute ping hostname <hostname> count <number>
reboot	Перезагрузка сервера UserGate.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение сервера UserGate.

Параметр	Описание
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • dns-ip — IP-адрес сервера DNS. • dns-tcp — использование TCP вместо UDP для DNS-запроса. • check-cert — проверка SSL-сертификата • type — проверка доступности по: ◦ http. ◦ tcp (если порт не указан, то используется порт 80). • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • timeout — максимальный таймаут ожидания ответа от веб-сервера. • user-agent — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name>
dig	Проверка записи DNS домена. • host — доменное имя хоста или IP-адрес для реверсивного поиска. • reverse-lookup — получение хоста по IP-адресу. • dns — указание IP-адреса DNS-сервера. • tcp — использование протокола TCP вместо UDP. Admin@nodename# execute dig hostname <host-domain-name> Admin@nodename# execute dig hostname <IP-address> reverse-lookup on
configure-cluster	Генерирование секретного кода, необходимого для добавления нового узла в кластер конфигурации: Admin@nodename# execute configure-cluster generate-secret-key <parameter> • 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, иначе будет отображена ошибка.
mc-force-disconnect	Команда аварийного отключения узла от MC, с которым он был интегрирован. В зависимости от выбранного аргумента импортированные из MC объекты сохраняются локально или удаляются: • keep — отключение от MC с сохранением всех импортированных из MC объектов (библиотеки, правила итд.). Импортированные из MC объекты конвертируются в локальные. • delete — отключение от MC с удалением всех импортированных из MC объектов (библиотеки, правила итд.). Импортированные объекты, которые в настоящий момент используются, конвертируются в локальные. Admin@nodename# execute mc-force-disconnect keep Admin@nodename# execute mc-force-disconnect delete
firewall	Операции с межсетевым экраном: • force-changes — применение всех правил межсетевого экрана заново с обрывом текущих сессий.
restore-mac	Восстановление mac-адреса интерфейса.

Часть представленных выше команд, кроме команд обновления, регистрации продукта, управления сессиями администраторов и очистки кэша, также доступны в режиме [диагностики и мониторинга](#). Для их выполнения используется команда:

Admin@nodename> <command-name>

Команды import

Импорт доступен в разделах **Настройки**, **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN**, **WAF**.

В разделе настроек UserGate доступен импорт сертификатов. Подробнее читайте в разделе [Настройка сертификатов](#).

В разделах **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN**, **WAF** доступен импорт правил, написанных на UPL. При использовании импорта, все существующие правила будут заменены на указанные; можно указать сразу несколько правил.

В разделе **Пользователи** доступен импорт правил Captive-портала. Подробнее о добавлении правил читайте в соответствующем разделе [Настройка Captive-портала](#).

В разделе **Сеть** доступен импорт правил DNS. Подробнее читайте в разделе [Настройка правил DNS](#).

В разделе **Политики сети** доступен импорт правил межсетевого экрана, NAT и маршрутизации, пропускной способности, балансировки нагрузки. Подробнее читайте в соответствующих разделах [Настройка правил межсетевого экрана](#), [Настройка правил NAT и маршрутизации](#), [Настройка правил пропускной способности](#), [Настройка балансировки нагрузки](#).

В разделе **VPN** доступен импорт серверных и клиентских правил, о добавлении которых написано в разделах [Настройка серверных правил](#) и [Настройка клиентских правил](#).

Команды export

Доступен экспорт сертификатов и элементов библиотек.

Подробнее об экспорте сертификатов смотрите в разделе [Настройка сертификатов](#).

Для экспорта доступны следующие элементы библиотек: IP-адреса, Useragent браузеров, списки URL, категории URL, изменённые категории URL, типы контента, морфология, почтовые адреса и номера телефонов. Для экспорта элемента библиотеки используется команда:

```
Admin@nodename# export libraries <library-name> <list-name>
```

где:

<library-name> — название библиотеки элементов (IP-адреса, Списки URL и т.д.).

<list-name> — название элемента библиотеки.

Команда debug

Команда debug позволяет включать журналирование событий протоколов маршрутизации. События записываются в debug-лог. Их просмотр также возможен в режиме мониторинга в консоли CLI (подробнее — в разделе [Диагностика и мониторинг](#)).

Для включения журналирования конкретного протокола маршрутизации используется команда:

```
Admin@nodename# debug <protocol> <parameters>
```

Поддерживаются следующие протоколы:

Параметр	Описание
rip	Протокол RIP.
bgp	Протокол BGP.
igmp	Протокол IGMP
pim	Протокол PIM.
ospf	Протокол OSPF.
bfd	Протокол BFD.
msdp	Протокол MSDP.
mroute	Таблица мультикаст-маршрутизации mroute.
ssmppingd	Инструмент тестирования мультикаст-вещания ssmppingd.

