

Table of Contents

Table of Contents	1
Команды диагностики и мониторинга	2
Команды диагностики и мониторинга (Описание)	3
Трассировка пакетов	17

Команды диагностики и мониторинга (Описание)

Product: DCFW
Version: 8.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.
- Мониторинг состояния кластера.
- Мониторинг заблокированных COB IP-адресов.
- Отображение системной информации.
- Диагностику работы протоколов динамической маршрутизации.
- Информацию об авторизованных пользователях.

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.

Параметр	Описание
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.
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 DCFW.
host	IP-адрес устройства.
mac	MAC-адрес устройства.

Параметр	Описание

```
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
node-name	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP и MAC-адреса устройства.
interface	Название интерфейса DCFW.
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

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 читайте 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 читайте в разделе Настройка IP-адресов .
dest-ip-addresses	Список IP-адресов назначения пакета.
services	Тип сервиса. Подробнее читайте в разделе Настройка сервисов .

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 DCFW 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
----------	----------

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 DCFW (профили LLDP [настроены в библиотеке элементов](#) и активированы в [настройках интерфейсов](#)).

Маршруты

Данный раздел необходим для проведения диагностики и мониторинга маршрутной информации на DCFW.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

Admin@nodename> show network route

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить.
node-name	Выбор узла кластера.
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам DCFW. Данные маршруты помечены символом С в списке маршрутов.
kernel	Отображение маршрутов, добавленных администратором; маршруты помечены символом К 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 О в списке маршрутов.
bgp	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации BGP; маршруты помечены символом В в списке маршрутов.

Параметр	Описание
rip	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации RIP; маршруты помечены символом R в списке маршрутов.
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all).

Мониторинг OSPF

Диагностика и мониторинг OSPF производится с использованием команд, представленных ниже. Отображение информации OSPF:

```
Admin@nodename> show network ospf
...
Admin@nodename> show network ospf <parameter>
```

Параметр	Описание
node-name	Выбор узла кластера.
virtual-router	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF: (<vrf-name> all).
route	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF.
database	Отображена информация: • Router Link States: пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны; используются для передачи информации соседним маршрутизаторам, находящихся в той же зоне, о собственных интерфейсах и своих соседях. • Network Link States: пакеты LSA Type 2 (Network LSA) генерируются выделенным маршрутизатором (Designated Router, DR) для описания всех маршрутизаторов, подключённых к его сегменту напрямую. • Summary Link States: пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • ASBR-Summary Link States: пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора (Autonomous System Border Router, ASBR) в других областях.
neighbor	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора). • Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором - Designated Router, DR. Если приоритеты маршрутизаторов равны, то будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например, Full/DR, Full/BDR, Full/Drother. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Доступно указание дополнительных параметров: • interface-name — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • all — отображение таблицы со всеми соседями. • detail — отображение подробной информации о соседях.

Параметр	Описание
interface	Отображение информации об интерфейсах OSPF. Дополнительно: interface-name — отображение информации об указанном интерфейсе. traffic — статистика переданных и принятых пакетов OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment).
border-routers	Отображение информации о пограничных маршрутизаторах.

Команда для перезапуска процесса OSPF:

Admin@nodename> clear network ospf <parameter>

Параметр	Описание
interface-name	Название интерфейса.
node-name	Выбор узла кластера.
virtual-router	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<vrf-name> all).
interface	Интерфейс, на котором необходимо перезапустить процесс OSPF (<interface-name>).
neighbor	Выбор соседей в отношении которых будет перезапущен процесс

Мониторинг BGP

В данном разделе представлены команды диагностики и мониторинга BGP.

Для отображения таблиц BGP маршрутизатора:

Admin@nodename> show network bgp
...
Admin@nodename> show network bgp <parameter>

Параметр	Описание
node-name	Выбор узла кластера.
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all).
ip	IP-адрес, маршрут до которого необходимо отобразить.
statistics	Отображение статистики BGP.
neighbors	Отображение информации о BGP-соседах (доступно отображение информации об определённом соседе; необходимо указание IP-адреса соседа). Дополнительные параметры, доступные при указании соседа: received-routes — принятые маршруты до применения к ним входящей политики (Routemap и фильтры). advertised-routes — маршруты, которые анонсируются указанному соседу.
summary	Просмотр краткой информации о соседях.

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии):

Admin@nodename> clear network bgp

Далее доступно указание параметров:

Параметр	Описание
ip	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации.
node-name	Выбор узла кластера.
virtual-router	Название виртуального маршрутизатора, которому принадлежит BGP-сосед.

В случае, если на соседних устройствах поддерживается метод Route Refresh, то можно избежать полной реинициализации сессии с соседом, отправив специальное сообщение типа ROUTE REFRESH. Отправка данного сообщения позволяет обновить информацию без прерывания в маршрутизации.

Для обновления информации без обрыва сессии с соседом используется команда:

```
Admin@nodename> clear network bgp ip <neighbor-ip> soft in | out
Admin@nodename> clear network bgp virtual-router <vrf-name> ip <neighbor-ip> soft in | out
```

Мониторинг RIP

В данном разделе представлены команды диагностики и мониторинга RIP.

Для отображения информации RIP из таблицы маршрутизатора по умолчанию (адрес сети, полученный по RIP; адрес Next Hop; метрика маршрута; тэг маршрута, предназначенный для разделения внутренних и внешних маршрутов; интервал времени, по истечении которого маршрут будет признан недействительным, если информация о нём не была получена):

```
Admin@nodename> show network rip
...
Admin@nodename> show network rip <parameter>
```

Доступно использование следующих параметров:

Параметр	Описание
node-name	Выбор узла кластера.
status	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т.п.
virtual-router	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить: <vrf-name> all.

Мониторинг мультикаст-трафика

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию:

```
Admin@nodename> show network mroute
...
Admin@nodename> show network mroute <parameter>
```

Доступно использование следующих параметров:

Параметр	Описание
node-name	Выбор узла кластера.
count	Отображение статистики о группе и источнике.
virtual-router	Выбор виртуального маршрутизатора: <vrf-name> all.
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации.
fill	Таблица маршрутизации мультикаст-трафика. Доступно указание параметра: ip — отображение записи для определённого IP-адреса; далее необходимо указать IP-адрес.

Параметр	Описание
ip	Отображение записи для определённого IP-адреса; необходимо указать IP-адрес.

Мониторинг IGMP

Мониторинг работы протокола IGMP (Internet Group Management Protocol) доступен с использованием следующей команды (указание параметров является обязательным). Для отображения информации для маршрутизатора по умолчанию:

```
Admin@nodename> show network igmp <parameters>
```

Далее необходимо указать параметры:

Параметр	Описание
node-name	Выбор узла кластера.
virtual-router	Выбор виртуального маршрутизатора.
statistics	Статистика по сообщениям: - IGMP Membership Query — сообщение сервера клиенту, в котором сервер просит обновить подписку на получаемые клиентом группы иначе, сервер перестанет вещать группу/группы в данный сегмент сети. - IGMP Leave — сообщение клиента серверу; клиент сообщает, что желает убрать мультикаст-группу из списка получаемых. - IGMP Membership Report — сообщение клиента серверу; клиент желает получать трафик этой группы.
join	Отображение информации о группах IGMP.
sources	Отображение информации об источниках мультикаст-трафика.
groups	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: - Общее количество групп. - Интерфейс, через который группа доступна. - Адрес группы. - Режим INCLUDE или EXCLUDE. - Таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report. - Время, в течение которого группа известна.
interface	Отображение информации об интерфейсе, связанной с мультикаст-маршрутизацией: - Название интерфейса, его статус и адрес. - Версия IGMP. - Опрашиватель и его адрес (Querier). - Таймер, который обнуляется каждый раз, как приходит сообщение Query с меньшим IP-адресом. Доступно указание: interface-name — название интерфейса. detail — подробная информация об интерфейсе.

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды (указание параметров является обязательным). Для отображения информации для маршрутизатора по умолчанию:

Admin@ndename> show network pim <parameter>

Далее необходимо указать параметры:

Параметр	Описание
node-name	Выбор узла кластера, для которого необходимо отобразить информацию.
virtual-router	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию.
vxlan-groups	Информация о группах VXLAN, использующихся в мультитевещании.
statistics	Статистика протокола.
join	Отображение информации о группах PIM протокола.
neighbor	Информация о соседях: • Интерфейс, через который была получена информация о соседе. • Адрес соседа. • Время, с последнего начала работы PIM. • Время, в течении которого сосед доступен. • Приоритет DR.
next-hop	Записи о адресах next-hop.
state	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List).
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешённые ASM группы с данного RP.
interface	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т.п. Также доступно указание параметров: • interface-name — название интерфейса. • traffic — статистика отправленных/полученных сообщений. • detail — подробная информация об интерфейсе.
group-type	Список разрешённых групповых адресов для SSM (Source Specific Multicast).
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса.

Мониторинг состояния кластера

Команды мониторинга состояния кластера могут быть запущены на любом из узлов, входящих в кластер. Они позволяют получить информацию о текущем состоянии кластера, его узлов, режиме работы кластера и истории переключения состояний кластера.

Для мониторинга состояния кластера используется следующая команда:

```
Admin@nodename> show ha-cluster state
```

Для мониторинга состояния узлов кластера используется команда:

```
Admin@nodename> show ha-cluster tablestat
```

Для отображения информации об истории переключения состояния кластера используется команда:

```
Admin@nodename> show ha-cluster failover
```

Мониторинг заблокированных COB IP-адресов

Для просмотра таблицы с заблокированными системой COB IP-адресами используется команда:

Admin@nodename> show blocked-ip

Для разблокирования отдельных IP-адресов используется команда:

Admin@nodename> clear blocked-ip ips [ip-address ip-address ...]

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 динамической 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 читайте в разделе [Режим конфигурации](#)).

Для просмотра записей debug-лога используется команда:

Admin@nodename> show log routing <parameters>

Далее необходимо указать один из параметров:

Параметр	Описание
all	Все протоколы.
rip	Протокол RIP.
bgp	Протокол BGP.
igmp	Протокол IGMP
pim	Протокол PIM.
ospf	Протокол OSPF.
bfd	Протокол BFD.
msdp	Протокол MSDP.
mroute	Таблица мультикаст-маршрутизации mroute.
ssmpingd	Инструмент тестирования мультикаст-вещания ssm pingd.

Для вывода событий debug-лога в консоль в реальном времени используется команда:

Admin@nodename> show log tail on routing <parameters>

Далее необходимо указать один из параметров из таблицы команды просмотра записей debug-лога, размещенной выше.

Для отключения вывода событий debug-лога в консоль в реальном времени по отдельным протоколам используется команда:

Admin@nodename> show log tail off routing <parameters>

Параметры команды аналогичны параметрам, указанным ранее.

Просмотр информации об авторизованных пользователях

Для просмотра информации обо всех авторизованных пользователях используется следующая команда интерфейса командной строки:

```
Admin@nodename> show user-auth
```

Для просмотра деталей аутентификационной сессии определенного пользователя используется команда:

```
Admin@nodename> show user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (login), так и его IP-адрес (ip-address).

Для удаления сессии определенного пользователя используется команда:

```
Admin@nodename> clear user-auth <parameter>
```

В качестве параметра может использоваться как имя пользователя (login), так и его IP-адрес (ip-address).

Трассировка пакетов

Product: DCFW
Version: 8.x

С помощью механизма трассировки можно анализировать прохождение сетевых пакетов через IP-стек и фильтрующие правила межсетевого экрана.

Настраивать режимы трассировки и просматривать ее результаты можно в режиме диагностики и мониторинга CLI на уровне `packet-tracing`.

Для настройки параметров трассировки используется команда:

```
Admin@nodename> setup packet-tracing <n> <parameters>
```

<n> — порядковый номер задачи трассировки (0-9).

Параметры трассировки пакетов определены в таблице.

Параметр	Описание
bidir	Режим отслеживания пакетов: • off — отслеживаются пакеты с заданными параметрами. • on — отслеживаются пакеты с заданными значениями параметров и с инверсией значений источника и назначения для параметров IP-адреса и порта без учета входного интерфейса (ответные пакеты соединения)
count	Трассировка заданного количества пакетов (1-16)
device	Имя сетевого интерфейса (portX, tunnelX и т. д.), на котором включается отслеживание входящих пакетов с заданными параметрами
dport	Порт назначения трафика (1-65 535)
dst	IP-адрес назначения трафика. Форматы значений: • <ip> — например, 192.168.0.1; • <ip/mask> — например, 192.168.0.1/24
fin	Фильтрация TCP-пакетов с FIN-флагом (корректное завершение соединения): • on — включено; • off — отключено
mark	Фильтрация пакетов по меткам: • <xx> — метка в виде десятичного числа (10); • <0xx> — метка в виде восьмеричного числа (04); • <0xXX> — метка в виде шестнадцатеричного числа (0xAA); • <mark/mask> — метка и битовая маска в виде шестнадцатеричных чисел (0xAA/0xBB)
proto	Фильтрация пакетов по типу протокола: • udp; • tcp; • icmp; • <num> — номер протокола
rst	Фильтрация TCP-пакетов с RST-флагом (обрыв соединения): • on — включено; • off — отключено

Параметр	Описание
syn	Фильтрация TCP-пакетов с SYN-флагом (инициация установки соединения): - on — включено; - off — отключено
sport	Порт источника трафика (1-65 535)
src	IP-адрес источника трафика. Форматы значений: <ip> — например, 192.168.0.1; <ip/mask> — например, 192.168.0.1/24
tout	Общий тайм-аут включения режима трассировки в минутах (1-60). При отсутствии параметра в команде трассировки используется значение по умолчанию — 5 минут
tout1	Тайм-аут включения режима трассировки в минутах (1-60). При активации параметра tout2 параметр tout1 задает время ожидания первого пакета
tout2	Время ожидания последующих пакетов после получения первого в минутах (1-60)
vlan	Идентификатор VLAN. Форматы значений: <num> — для указания конкретного идентификатора VLAN (например, 10); <num/0xN> — для указания диапазона идентификаторов VLAN с помощью битовой маски (например, 10/0x5)

Для просмотра результатов трассировки используется команда:

```
Admin@nodename> show packet-tracing <n> <full|short>
```

<n> — порядковый номер задачи трассировки (0-9).

<full|short> — выбор режима отображения отфильтрованных пакетов (полный или сокращенный).

Полный режим вывода демонстрирует весь путь пакета через стек протоколов, включая временные метки и промежуточные решения. В сокращенном режиме отображается итоговый результат, ключевые точки обработки пакета, а при блокировке — соответствующий фрагмент журнала.

В выводе результатов трассировки указываются только сработавшие правила межсетевого экрана.

Пример прохождения пакета через разрешающее правило межсетевого экрана:

```
Admin@nodename> show packet-tracing 0 short
```

```
Tracing task: 1 packet(s)
SRC=ANY DST=10.255.4.6 VLAN=ANY InDev:ANY
Mark:ANY Proto:ANY SrcPort:ANY DstPort:ANY
INPUT direction with 5min timeout
```

```
processing time 186.771us FINAL Result -> SUCCESS
```

```
Direction path: Forwarding
```

```
DEV=port3 ifindex=10 ZONE=4
IPv4 SRC=10.255.3.6 DST=10.255.4.6
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=22977 DF
PROTO=TCP
SPT=58698 DPT=80 SYN
```

```
conntrack state: CT_NEW ctid:0000000060be4ad8 dir:ORIGINAL
TCP connection state: SYN_SENT
jiff:64982901 timeout:+1250 no guid
cssid: 165488077E38F85C
SNAT: off
DNAT: off
```

```
rtable: type=UNICAST (1) GW:0.0.0.0 OUTDEV=port4 outZONE=4
```

```
FireWall: VFW Stage3 Rule=8 Verdict=ACCEPT_CP1
```

Neighbour Type:01 Flags:00
OUTDEV=port4 ifindex=3 ZONE=4 mtu=1500

Пример отбрасывания пакета правилом межсетевого экрана:

Admin@nodename> show packet-tracing 0 short

Tracing task: 1 packet(s)
SRC=ANY DST=10.255.4.6 VLAN=ANY InDev:ANY
Mark:ANY Proto:ANY SrcPort:ANY DstPort:ANY
INPUT direction with 5min timeout

processing time 145.262us FINAL Result -> ERROR(-1)

Direction path: UNKNOWN

DEV=port3 ifindex=10 ZONE=4
IPv4 SRC=10.255.3.6 DST=10.255.4.6
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=59745 DF
PROTO=TCP
SPT=58810 DPT=80 SYN

conntrack state: CT_NEW ctid:00000000ed7dc4d dir:ORIGINAL
TCP connection state: SYN_SENT
jiff:65332391 timeout:1250 no guid
cssid: 1337BC6AB9570671
SNAT: off
DNAT: off

FireWall: VFW Stage2 Rule=8 Verdict=DROP_CP1

Point of failure:

[261625.445465] t14p01c00 RECEIVE stage start 130.845us -> ERROR(-1)
[261625.445465] t14p01c00 ...
[261625.445470] t14p01c00 | NF IPV4 PRE_ROUTING INDEV=port3 from entry 0 of 10 125.426us -> ERROR(-1)
[261625.445470] t14p01c00 ...
[261625.445585] t14p01c00 || hook#9 pri=+2147483647 vfw_ipv4_prert_last [utm_vfw] 4.559us -> DROP
(err=0)
[261625.445589] t14p01c00 || | VFW Stage2 Rule=8 Verdict=DROP_CP1

Пример отбрасывания пакета модулем IDPS:

Packet #3 processing time 83.727us FINAL Result -> ERROR(-1)

Direction path: Forwarding

DEV=port3 ifindex=10 ZONE=4
IPv4 SRC=10.255.3.6 DST=10.255.4.6
LEN=123 TOS=0x00 PREC=0x00 TTL=64 ID=41034 DF
PROTO=TCP
SPT=58814 DPT=80 ACK PSH

conntrack state: CT_ESTABLISHED ctid:00000000e1574f38 dir:ORIGINAL
TCP connection state: ESTABLISHED
jiff:123262 timeout:4623262 guid:44035455-46AD-4A70-9615-CDD72BFF15C7
cssid: 79B4F1075D450351
SNAT: off
DNAT: off

rtable: type=UNICAST (1) GW:0.0.0.0 OUTDEV=port4 outZONE=4

Last seen header

IPv4 SRC=10.255.3.6 DST=10.255.4.6
LEN=123 TOS=0x00 PREC=0x00 TTL=63 ID=41034 DF
PROTO=TCP
SPT=58814 DPT=80 ACK PSH

Point of failure:

[793.270366] t02p03c00 OUTPUT stage start 49.793us -> ERROR(-1)
[793.270366] t02p03c00 ...
[793.270366] t02p03c00 | NF IPV4 POST_ROUTING OUTDEV=port4 from entry 0 of 9 48.812us -> ERROR(-1)
[793.270366] t02p03c00 ...
[793.270372] t02p03c00 || hook#6 pri=+2147483627 utm_ipsv3_hook [utm_ipsv3] 42.189us -> DROP (err=0)

Пример отбрасывания пакета по причине отсутствия маршрута до адреса назначения:

Tracing task: 1 packet(s)
SRC=ANY DST=10.255.5.6 VLAN=ANY InDev:ANY
Mark:ANY Proto:ANY SrcPort:ANY DstPort:ANY
INPUT direction with 5min timeout

processing time 218.180us FINAL Result -> ERROR(-101)

Direction path: UNREACHABLE

DEV=port3 ifindex=10 ZONE=4
IPv4 SRC=10.255.3.6 DST=10.255.5.6
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=62293 DF
PROTO=TCP
SPT=56688 DPT=80 SYN

conntrack state: CT_NEW ctid:000000004878a2bc dir:ORIGINAL
TCP connection state: SYN_SENT
jiff:453314 timeout:1250 no guid
cssid: 5475B8894DAF1161
SNAT: off
DNAT: off

rtable: type=UNREACHABLE (7) GW:0.0.0.0 OUTDEV=lo outZONE=0
destination ERROR code 101

Point of failure:

[2113.457413] t03p01c00 ROUTING stage start 8.716us -> ERROR(-101)
[2113.457413] t03p01c00 ...
[2113.457413] t03p01c00 | call ip_route_input 7.644us -> ERROR(-101) routing unsuccessful

Для отключения задачи трассировки пакетов используется команда:

Admin@nodename> clear packet-tracing <n>

<n> — порядковый номер задачи трассировки (0-9).

