

Table of Contents

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

Команды диагностики и мониторинга (Описание)

Product: WAF
Version: 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.

Параметр	Описание
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 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
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).

Параметр	Описание
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 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

Параметр	Описание
neighbors	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • Chassis ID — идентификатор шасси. • SysName — имя системы. • SysDescr — описание системы, содержит информацию об оборудовании и операционной системе устройства. • Management — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • Capability — функции устройства (например, маршрутизатор, коммутатор и т.п.). • Port ID — идентификатор порта с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • PortDescr — описание порта. • TTL — время жизни передаваемых пакетов LLDP.
statistics	Статистика интерфейсов, в настройках которых был указан профиль LLDP: • Interface — название интерфейса. • Transmitted — общее количество кадров LLDP, переданных через интерфейс. • Received — общее количество кадров LLDP, полученных на интерфейсе. • Discarded — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • Unrecognized — количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе. • Ageout — в каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется. • Inserted — количество добавлений записей с информацией о соседях LLDP. • Deleted — количество удалений записей о соседях LLDP.

Примечание Для просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на WAF (профили LLDP [настроены в библиотеке элементов](#) и активированы в [настройках интерфейсов](#)).

Маршруты

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

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

Admin@nodename> show network route

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить.
node-name	Выбор узла кластера.
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам WAF. Данные маршруты помечены символом 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).

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

Для просмотра записей debug-лога используется команда:

```
Admin@nodename> show log routing
```

