

Table of Contents

Table of Contents	1
Настройки сети	2
Зоны	3
Интерфейсы	6
Шлюзы	15
DHCP	16
DNS-настройки	17
Настройка виртуальных маршрутизаторов	19
Настройка WCCP	29

Documentation: 
Version: 7.x
Product: NGFW

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.

Параметр	Описание
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • response-pages: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • rpc: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • ha: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • VRRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "Admin Console": доступ к веб-консоли управления (TCP 8001). • DNS: доступ к сервису DNS-прокси (TCP 53, UDP 53). • "HTTP Proxy": доступ к сервису HTTP(S)-прокси (TCP 8090). • "Authorization agent": доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • "SMTP Proxy": сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "POP3 Proxy": сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • "PROXY PORTAL": сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • L7 DNS: детектирование трафика DNS на уровне приложений. • L7 NTP: детектирование трафика NTP на уровне приложений. • "SAML SERVER": выбор SAML-сервера в списке сервисов зоны и общих настройках UserGate. • "Log Analyzer": сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713). • "Dynamic routing OSPF": сервис динамической маршрутизации OSPF. • "Dynamic routing BGP": сервис динамической маршрутизации BGP. • "SNMP Proxy": сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • "SSH Proxy": сервис, использующийся для инициирования трафика SSH. • Multicast: сервис мультикастинга. • NTP: доступ к сервису точного времени, запущенному на сервере UserGate. • "Dynamic routing RIP": сервис динамической маршрутизации RIP. • UserID agent: сервис для осуществления прозрачной аутентификации. В качестве источника данных аутентификации используются журналы ActiveDirectory и Syslog. • BFD: сервис Bidirectional Forwarding Detection для быстрого обнаружения сетевых ошибок. • "HTTPS RPC": доступ к API поверх HTTPS (TCP 4443). Доступен в версии 7.3.3 и выше.
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.
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>

Version: 7.x
Product: NGFW
Documentation: 

В интерфейсе командной строки можно отобразить список упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов. Команда просмотра доступна как в режиме диагностики и мониторинга, так и в режиме конфигурации.

Admin@nodename> show network interface-mapping

Admin@nodename# show network interface-mapping

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

Для удаления списка используйте следующую команду (в режиме диагностики и мониторинга и в режиме конфигурации соответственно):

Admin@nodename> clear network interface-mapping

Admin@nodename# delete network interface-mapping

После добавления сетевых портов в настроенный UserGate NGFW его необходимо перезагрузить — список обновится и станет доступным для отображения.

На уровне network interface доступна настройка параметров различных типов интерфейсов UserGate NGFW.

Настройка физических сетевых интерфейсов

Физические сетевые интерфейсы (адаптеры) настраиваются на уровне network interface adapter.

Для отображения информации обо всех сетевых адаптерах используйте команду:

Admin@nodename# show network interface adapter

Для отображения информации об определенном сетевом адаптере:

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

Для изменения параметров сетевого адаптера используйте команду вида:

Admin@nodename# set network interface adapter <adapter-name> <parameters>

В команде необходимо указать параметры сетевого адаптера.

Параметр	Описание
enabled	Включение или отключение сетевого интерфейса: - on; - off
description	Описание сетевого интерфейса
alias	Псевдоним («алиас») интерфейса
iface-type	Тип интерфейса: - i3 — интерфейс, работающий в режиме Layer 3. Вы можете назначить IP-адрес для интерфейса и использовать его в правилах межсетевого экрана, контентной фильтрации и других. Это стандартный режим работы интерфейса. - mirror — интерфейс, работающий в режиме зеркалирования. 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_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW 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] - key — название параметра. Название может состоять из строчных букв латинского алфавита (a-z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info 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 IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40
rx-ring	Размер буфера RX ring интерфейса типа adapter
tx-ring	Размер буфера TX ring интерфейса типа adapter

Параметр	Описание
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение или отключение ретранслятора (on/off). - utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP -адрес/none). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов
user-speed	Выбор скорости интерфейса. Параметр доступен только для ПАК UserGate FG в версии 7.5.0 и выше. Для портов 10-17 вы можете переключить скорость работы интерфейса с 10 Гбит/с на 25 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например: Admin@nodename# set network interface adapter port10 user-speed 25000 Для портов 18-19 вы можете переключить скорость работы интерфейса со 100 Гбит/с на 40 Гбит/с и обратно. В команде значение скорости указывается в Мбит/с, например: Admin@nodename# set network interface adapter port18 user-speed 100000 Примечание При просмотре параметров интерфейса с помощью команды show network interface adapter <adapter-name> параметр speed отображает фактическую скорость интерфейса, полученную из системы; параметр user-speed — указанную администратором скорость или значение auto для портов 0-9.

Для удаления значений параметров сетевого адаптера используйте команду:
Admin@nodename# delete network interface adapter <adapter-name> <parameters>

- Параметры, доступные для удаления:
- ip-address — заданный IP-адрес;
 - dhcp-relay server-address — IP-адрес DHCP-сервера.

Настройка VLAN-интерфейса

VLAN-интерфейсы создаются и настраиваются на уровне network interface vlan.
Для добавления нового VLAN-интерфейса используйте команду вида:

Admin@nodename# create network interface vlan <parameters>
В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение VLAN-интерфейса: - on; - off
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
iface-type	Тип интерфейса: - l3 — Layer 3. Вы можете 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 зеркалирования. 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	Tag VLAN. Допускается создание до 4094 интерфейсов
node-name	Имя узла кластера, на котором создается 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_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW 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] - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info 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 IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса

Параметр	Описание
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение или отключение ретранслятора (on/off). - utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP -адрес/none). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего VLAN-интерфейса используйте команду:

```
Admin@nodename# set network interface vlan <vlan-name> <parameters>
```

Параметры, доступные для изменения, аналогичны параметрам создания VLAN-интерфейса, кроме параметров 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:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Для отображения информации обо всех VLAN-интерфейсах используйте команду:

```
Admin@nodename# show network interface vlan
```

Для отображения информации об определенном интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Bond-интерфейсы создаются и настраиваются на уровне network interface bond.

Для создания bond-интерфейса используйте команду вида:

```
Admin@nodename# create network interface bond <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: - on; - off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет bond1
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Узел кластера, на котором будет создан bond-интерфейс
zone	Зона, которой будет принадлежать bond-интерфейс
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_vlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info 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 bond-интерфейса: - aggr-mode — режим работы bond-интерфейса: - 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, если станет недоступным текущий активный интерфейс. При использовании этого режима MAC-адрес bond-интерфейса виден вовне только через один сетевой порт. Такая политика применяется для обеспечения отказоустойчивости. - xor — режим XOR. Передача распределяется между сетевыми картами с применением формулы: «<MAC-адрес источника> XOR <MAC-адрес назначения>» по модулю «число интерфейсов». 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 — передача на все сетевые интерфейсы. Эта политика применяется для обеспечения 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. Интерфейс, через который будет отправляться пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать политику xmit_hash. - 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, другая сетевая карта получает MAC-адрес вышедшей из строя карты. - load — режим adaptive load balancing. Включает в себя предыдущую политику, а также 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 вовне, 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 (miiimon). Значение параметра должно быть кратным значениям miiimon. - up-delay — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miiimon). Значение параметра должно быть кратным значениям miiimon. - 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 bond-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на bond-интерфейсе меняется во время обработки отказа. - follow — MAC-адрес на bond-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. Пока второй и последующий интерфейсы находятся в резервном режиме, этот MAC-адрес на них не устанавливается. MAC-адрес присваивается во время обработки отказа. Когда резервный интерфейс становится активным, он принимает новый MAC-адрес (тот же, что присвоен bond-интерфейсу), а старому активному интерфейсу присваивается MAC-адрес, который принадлежал текущему активному интерфейсу. - xmit-hash — определение хеш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: - I2 — использует только MAC-адреса для генерации хеш-суммы. При использовании этого алгоритма трафик для конкретного сетевого узла будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. - I2-3 — использует как MAC-адреса, так и IP-адреса для генерации хеш-суммы. Алгоритм совместим с IEEE 802.3ad. - I3-4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хеш-суммы. 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 пойти до получателя не в том порядке, в котором были отправлены, так как отправляются через разные интерфейсы. - interface — интерфейсы, которые будут объединены в bond-интерфейс
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 интерфейса: - I3 — Layer 3. Вы можете 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 зеркалирования. Может получать трафик со SPAN-порта сетевого оборудования для его анализа
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение или отключение ретранслятора (on/off). - utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP -адрес/none). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bond-интерфейса используйте команду:

```
Admin@nodename# set network interface bond <bond-name> <parameters>
```

Параметры, доступные для изменения, аналогичны параметрам создания bond-интерфейса, кроме interface-name, node-name (изменение значений этих параметров недоступно).

Команда удаления bond-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.
- bonding interface — интерфейсы, объединенные в bond-интерфейс.

Для отображения информации обо всех bond-интерфейсах используйте команду:

```
Admin@nodename# show network interface bond
```

Для отображения информации об определенном интерфейсе:

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

Настройка bridge-интерфейса

Bridge-интерфейсы создаются и настраиваются на уровне network interface bridge.

Для добавления нового bridge-интерфейса используйте команду:

```
Admin@nodename# create network interface bridge <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: - on; - off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет bridge 1
description	Описание bridge-интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Имя узла кластера, на котором создается интерфейс
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_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW 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] - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info 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 bridge-интерфейса: - iface-type — режим работы интерфейса: - I2 — Layer 2, создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В этом режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security и правила контентной фильтрации. - I3 — 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 или отключение использование Spanning Tree Protocol (STP) 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 IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40
tso	Включение или выключение механизма TCP Segmentation Offload (TSO) — технологии сетевой оптимизации, которая позволяет разгрузить центральный процессор путем переноса задачи по сегментации TCP-пакетов на сетевое оборудование
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение или отключение ретранслятора (on/off). - utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP -адрес/none). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bridge-интерфейса используйте команду:

```
Admin@nodename# set network interface bridge <bridge-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме interface-name, node-name (изменение значений этих параметров недоступно).

Для удаления bridge-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface bridge <bridge-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Для отображения информации обо всех bridge-интерфейсах используйте команду:

```
Admin@nodename# show network interface bridge
```

Для отображения информации об определенном bridge-интерфейсе используйте команду:

```
Admin@nodename# show network interface bridge <bridge-name>
```

Настройка PPPoE-интерфейса

PPPoE-интерфейсы создаются и настраиваются на уровне network interface PPPoE.

Для создания PPPoE-интерфейса используйте команду вида:

```
Admin@nodename# create network interface pppoe <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: • on; • off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет ppp1
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
node-name	Имя узла кластера, на котором создается интерфейс
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 — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_vlan UserGate NGFW 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] • key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). • value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
config	Дополнительные параметры PPPoE-интерфейса: • interface — интерфейс, на котором будет создаваться PPPoE-интерфейс. • login — имя пользователя для соединения PPPoE. • password — пароль пользователя для соединения PPPoE. • persist-connection — автоматическое переподключение при обрыве связи. • auth-type — тип авторизации: ◦ CHAP; ◦ PAP. • holdoff — интервал времени в секундах после разрыва соединения перед повторным запуском. • default-route — PPPoE-интерфейс, который будет использоваться как маршрут по умолчанию. • echo-interval — интервал проверки соединения. • echo-failure — количество неуспешных проверок соединения, по достижении которого UserGate NGFW будет считать, что соединение отсутствует, и разорвет его. • providers-dns — использование DNS-серверов, выданных провайдером. • connection-attempts — количество неуспешных попыток подключения, по достижении которого попытки автосоединения будут прекращены. • service-name — имя сервиса, которое необходимо указать в случае его предоставления провайдером
mtu	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40

Для изменения параметров существующего PPPoE-интерфейса используйте команду:

```
Admin@nodename# set network interface pppoe <pppoe-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме interface-name (изменение значения этого параметра недоступно).

Для удаления PPPoE-интерфейса используйте команду:

```
Admin@nodename# delete network interface pppoe <pppoe-name>
```

Для отображения информации обо всех PPPoE-интерфейсах используйте команду:

```
Admin@nodename# show network interface pppoe
```

Для отображения информации об определенном PPPoE-интерфейсе используйте команду:

```
Admin@nodename# show network interface pppoe <pppoe-name>
```

Настройка VPN-интерфейса

VPN-интерфейсы создаются и настраиваются на уровне network interface vpn.

Для создания VPN-интерфейса используйте команду вида:

```
Admin@nodename# create network interface vpn <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: - on; - off
interface-name	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет tunnel1
description	Описание VPN-интерфейса
alias	Псевдоним («алиас») интерфейса
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_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW 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] - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow-коллектор. Подробнее о настройке профилей NetFlow — в разделе « Настройка профилей NetFlow »
iface-mode	Режим назначения IP-адреса: - dhcp — получение динамического IP-адреса по DHCP. - manual — без адреса. Если предполагается, что интерфейс будет принимать VPN-подключения (site-to-site VPN или remote access VPN), необходимо использовать статический IP-адрес. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. Для использования интерфейса в роли клиента необходимо выбрать динамический режим
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mtu	Размер MTU для выбранного интерфейса
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40

Для изменения параметров существующего VPN-интерфейса используйте команду:

```
Admin@nodename# set network interface vpn <vpn-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме interface-name (изменение значения этого параметра недоступно).

Для удаления VPN-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface vpn <vpn-name>
```

Параметр, доступный для удаления: ip-addresses.

Для отображения информации обо всех VPN-интерфейсах используйте команду:

```
Admin@nodename# show network interface vpn
```

Для отображения информации об определенном VPN-интерфейсе используйте команду:

```
Admin@nodename# show network interface vpn <vpn-name>
```

Настройка туннельного интерфейса

Туннельные интерфейсы создаются и настраиваются на уровне network interface tunnel.

Для создания туннельного интерфейса используйте команду вида:

```
Admin@nodename# create network interface tunnel <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: - on; - off
interface-number	Номер, который будет отображен в имени интерфейса. Например, если указать 1, названием созданного интерфейса будет gre1
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса

Параметр	Описание
node-name	Узел кластера, на котором будет создан туннельный интерфейс
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 — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_vlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info недоступно.
mtu	Размер MTU для выбранного интерфейса
mss	Размер MSS (доступно в версии 7.3.0 и выше). Корректные значения: 0; - для VXLAN — число в диапазоне от 4 до числа, получаемого по формуле MTU - 40; - для IPIP — число в диапазоне от 4 до числа, получаемого по формуле MTU - 60; - для GRE — число в диапазоне от 4 до числа, получаемого по формуле MTU - 64
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
local-ip	Локальный адрес интерфейса point-to-point
remote-ip	Удаленный адрес интерфейса point-to-point
mode	Режим работы туннельного интерфейса: - gre — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер IP-протокола — 47. - iPIP — протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP-пакета в другой — это добавление внешнего заголовка, в котором IP-адресом источника является адрес точки входа в туннель, а IP-адресом назначения — адрес точки выхода из туннеля. - vxlan — протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789
vxlan-id	Идентификатор VXLAN. Только для типа туннельного интерфейса VXLAN

Для изменения параметров существующего туннельного интерфейса используйте команду:

```
Admin@nodename# set network interface tunnel <tunnel-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме interface-number, node-name (изменение значений этих параметров недоступно).

Для удаления туннельного интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface tunnel <tunnel-name> <parameters>
```

Параметры, доступные для удаления: ip-addresses.

Для отображения информации обо всех туннельных интерфейсах используйте команду:

```
Admin@nodename# show network interface tunnel
```

Для отображения информации об определенном туннельном интерфейсе:

```
Admin@nodename# show network interface tunnel <tunnel-name>
```

Настройка loopback-интерфейса

Loopback-интерфейсы создаются и настраиваются на уровне network interface loopback.

Для создания интерфейса используется команда вида:

```
Admin@nodename# create network interface loopback <parameters>
```

В команде укажите параметры интерфейса.

Параметр	Описание
enabled	Включение или отключение интерфейса: - on; - off
interface-name	Название интерфейса
description	Описание интерфейса
alias	Псевдоним («алиас») интерфейса
ip-addresses	Назначение IP-адреса для интерфейса. Адрес задается в виде [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел). Маска подсети задается в десятичном виде Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.

Параметр	Описание
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 сетевого интерфейса: - bc_forwarding — управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_pvlan — механизмы Proxy ARP. При указании параметра proxy_arp UserGate NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; при указании параметра proxy_arp_pvlan UserGate NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@nodename# create network interface <iface-type> ... link-info [key/value]</pre> - key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). - value — значение параметра. Параметры могут принимать только целочисленные значения. Например, чтобы включить применение механизма Proxy ARP, используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления соответствующих параметров Важно! Удаление заданных параметров link-info 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
mtu	Размер MTU
mss	Размер MSS (доступно в версии 7.3.0 и выше): 0 или число в диапазоне от 4 до числа, получаемого по формуле MTU - 40
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение или отключение ретранслятора (on/off). - utm-address — IP-адрес интерфейса UserGate NGFW, на который добавляется функция ретранслятора (принимает значения IP -адрес/none). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего loopback-интерфейса используйте команду вида:

```
Admin@nodename# set network interface loopback <interface-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам создания loopback-интерфейса, кроме node-name, interface (изменение значений этих параметров недоступно).

Для удаления loopback-интерфейса или его параметров используйте команду:

```
Admin@nodename# delete network interface loopback <interface-name>
```

Параметры, доступные для удаления:

- ip-address — заданный IP-адрес;
- dhcp-relay server-address — IP-адрес DHCP-сервера.

Для отображения информации обо всех loopback-интерфейсах используйте команду:

```
Admin@nodename# show network interface loopback
```

Для отображения информации об определенном loopback-интерфейсе используйте команду:

```
Admin@nodename# show network interface loopback <interface-name>
```

Version: 7.x
Product: NGFW
Documentation: 

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: - Выбор конкретного порта (port0, port1, port2 итд.); auto — после выбора этого параметра порт определится автоматически. Данная опция доступна для узлов, прошедших инициализацию. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0.
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>
```

Version: 7.x
Product: NGFW
Documentation: 

Раздел находится на уровне **network dhcp**.

Для создания подсети DHCP, используется команда:

```
Admin@nodename# create network dhcp
```

Далее необходимо указание параметров:

Параметр	Описание
enabled	Включение/отключение использования данного диапазона IP-адресов: - on. - off.
name	Название подсети.
description	Описание подсети.
interface	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
ip-range	Диапазон IP-адресов, выдаваемый клиентам DHCP. Диапазон задаётся в формате: <IP_start-IP_end>.
mask	Маска подсети, выдаваемая клиентам DHCP.
expiration-time	Время в секундах, на которое выдаются IP-адреса.
domain	Название домена, выдаваемое клиентам DHCP.
gateway	IP-адрес шлюза, выдаваемый клиентам DHCP.
dns-servers	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
reserved-hosts	MAC-адреса и сопоставленные с ними IP-адреса: - mac: MAC-адрес. - ip: IP-адрес, сопоставленный MAC-адресу. - hostname: имя хоста.
ignored-mac	Список MAC-адресов, игнорируемых DHCP-сервером.
pxe-boot-ip	Адрес сервера PXE.
pxe-boot-filename	Название файла для загрузки с PXE-сервера.
options	Номер опции и ее значение: - code: номер опции DHCP. - values: значение опции.

Обновление существующей DHCP-подсети:

```
Admin@nodename# set network dhcp <dhcp-name>
```

Параметры, информацию о которых можно обновить, аналогичны параметрам, доступным при создании.

Для удаления подсети:

```
Admin@nodename# delete network dhcp <dhcp-name>
```

Также доступно удаление отдельных параметров подсети DHCP:

- dns-servers.
- ignored-mac.
- reserved-hosts (необходимо указать все три значения: **mac**, **ip**, **hostname**).
- options (необходимо указать оба значения: **code**, **values**).

Чтобы отобразить информацию о всех созданных подсетях:

```
Admin@nodename# show network dhcp
```

или об определённой подсети DHCP:

```
Admin@nodename# show network dhcp <dhcp-name>
```

Version: 7.x
Product: NGFW
Documentation: 

Раздел находится на уровне **network dns**.

Настройка системных DNS-серверов

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.
Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:
Admin@nodename# set network dns system-dns-servers ip [<ip> <ip> ...]

Для удаления всего списка адресов серверов DNS:
Admin@nodename# delete network dns system-dns-servers
Для удаления определённых серверов:
Admin@nodename# delete network dns system-dns-servers ip [<ip> <ip> ...]
Для отображения списка системных DNS-серверов используется команда:
Admin@nodename# show network dns system-dns-servers

Настройка DNS-прокси

DNS-прокси настраивается на уровне **network dns proxy-settings**.
Для редактирования настроек DNS-прокси используется следующая команда:
Admin@nodename# set network dns proxy-settings
Далее необходимо указать параметры, значения которых необходимо изменить:

Параметр	Описание
filtering	Фильтрация DNS-запросов: - on. - off.
caching	Кэширование ответов DNS: - on. - off.
limit	Ограничение количества DNS-запросов в секунду для каждого пользователя (значение по умолчанию: 100).
max-ttl	Максимально возможное время жизни для записей DNS.
recursive	Осуществление рекурсивных DNS-запросов: - on. - off.
dns-timeout	Время до следующей попытки отправления запроса на DNS-сервера (указывается в миллисекундах).
a-aaaa-unknown	Ответы только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS: - on. - off.
retries	Количество попыток DNS-запроса.
factory-defaults	Сброс до заводских настроек значения выбранного параметра (параметры представлены в данной таблице) или всех параметров (all).

Пример команды редактирования параметров DNS-proxy:
Admin@nodename# set network dns proxy-settings limit 10 dns-timeout 10
Чтобы просмотреть настройки DNS-прокси:
Admin@nodename# show network dns proxy-settings

Настройка правил DNS

Внимание! NGFW не может работать в роли DNS сервера. Предусмотрена только роль DNS проку. При указании в правилах DNS адреса самого NGFW, возможно образование DNS петли, со всеми вытекающими последствиями.

Правила DNS настраиваются на уровне **network dns rules** с использованием UPL. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Параметры правил DNS:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение использования правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила. Например: name("DNS rule example").
desc	Описание правила DNS-прокси. Например: desc("DNS rule example set via CLI").

Параметр	Описание
url.domain	Список доменов, на которые необходимо перенаправлять. Допускается использование звёздочки (*) для указания шаблона доменов. Чтобы указать список доменов: url.domain = "**.example.com" .
dns_server	Список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены. Для указания сервера: dns_server(1.2.3.4) .

Пример создания правила DNS с использованием UPL:

```
Admin@nodename# create network dns rules 1 upl-rule OK \
...url.domain = "**.example.com" \
...dns_server(1.2.3.4) \
...name("DNS rule example") \
...desc("DNS rule example description over CLI") \
...enabled(true) \
...
Admin@nodename#
Admin@nodename# show network dns rules

% ----- 1 -----
OK \
  url.domain = "**.example.com" \
  dns_server(1.2.3.4) \
  desc("DNS rule example description over CLI") \
  enabled(true) \
  id("0f83e1bb-0aa5-4f42-8eeb-9c4ffa30c04a") \
  name("DNS rule example")
```

Настройка статических записей DNS-прокси

Раздел находится на уровне **network dns static-records**.

Для добавления статической DNS-записи предназначена команда:

```
Admin@nodename# create network dns static-records
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статической записи: - on. - off.
name	Название записи.
description	Описание DNS-записи.
domain	FQDN (Fully Qualified Name) статической записи, например, www.example.com .
ips	Список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN.

Команда

```
Admin@nodename# show network dns static-records
```

отобразит информацию о всех существующих статических DNS-записях. Для отображения информации об определённой записи:

```
Admin@nodename# show network dns static-records <static-record-name>
```

Пример создания статической записи DNS:

```
Admin@nodename# create network dns static-records name "Test DNS static record" description "Test DNS static record description" enabled on domain example.com ips [ 10.10.0.100 ]
Admin@nodename#
Admin@nodename# show network dns static-records
```

```
Test DNS static record
name      : Test DNS static record
description : Test DNS static record description
domain    : example.com
ips       : 10.10.0.100
enabled   : on
```

Для редактирования информации о статических записях DNS:

```
Admin@nodename# set network dns static-records <static-record-name>
```

Список параметров, доступных для изменения, аналогичен списку команды **create**.

Пример редактирования ранее созданной статической записи DNS:

```
Admin@nodename# set network dns static-records "Test DNS static record" ips [ 10.10.0.101 ]
Admin@nodename# show network dns static-records "Test DNS static record"
```

```
name      : Test DNS static record
description : Test DNS static record description
domain    : example.com
ips       : 10.10.0.100; 10.10.0.101
enabled   : on
```

Для удаления статической записи:

```
Admin@nodename# delete network dns static-records <static-record-name>
```

Также возможно удаление из статической записи только значений параметра **ips**.

Пример удаления значения параметра **ips** в ранее созданной записи и удаления всей статической записи DNS.

```
Admin@nodename# delete network dns static-records "Test DNS static record" ips [ 10.10.0.101 ]
Admin@nodename# show network dns static-records "Test DNS static record"
```

```
name      : Test DNS static record
description : Test DNS static record description
domain    : example.com
ips       : 10.10.0.100
enabled   : on
```

```
Admin@nodename# delete network dns static-records "Test DNS static record"
Admin@nodename# show network dns static-records
```

```
Admin@nodename#
```

Настройка виртуальных маршрутизаторов

Technology: Routing
Version: 7.x
Product: NGFW
Documentation: 

В данном разделе описана настройка статических маршрутов, протоколов динамической маршрутизации OSPF, BGP, RIP и мультикаст-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 (VLAN), бондинг, VPN 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
```

Настройка OSPF

Для настройки OSPF с использованием CLI используйте следующую команду:

```
Admin@nodename# set network virtual-router <virtual-router-name> ospf
```

Далее необходимо указать параметры OSPF-маршрутизатора:

Параметр	Описание
enabled	Включение/отключение OSPF-маршрутизатора: - on. - off.
router-id	IP-адрес маршрутизатора. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору). При выключении OSPF (enabled off) значение router-id может быть удалено (none).
metric	Метрика распространяемых маршрутов.
default-originate	Оповещение других маршрутизаторов о том, что у данного роутера настроен маршрут по умолчанию: - on. - off.

Параметр	Описание
interfaces	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор. Для добавления интерфейса или изменения параметров добавленного ранее интерфейса используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> ospf interfaces new Admin@nodename# set network virtual-router <virtual-router-name> ospf interfaces <interface-name></pre> Далее указываются следующие параметры: enabled <on off>: включение/отключение использования интерфейса. interface: название интерфейса, входящего в данный виртуальный маршрутизатор. description: описание интерфейса. bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. cost: стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1. priority: целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1. network-type: выбор типа сети для оптимизации процесса установления соседства. Доступны: none — не установлен. bc — broadcast. ptm — point to multipoint. ptp — point to point. passive-mode <on off>: включение/отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается слать пакеты обновления протокола маршрутизации. hello-interval: время, через которое маршрутизатор посылает hello-пакеты; указывается в секундах. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд. dead-interval: время, по истечению которого маршрутизатор считается неработающим; указывается в секундах. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд. retransmit-interval: временный интервал перед повторной отсылкой пакета LSA; указывается в секундах. Значение по умолчанию 5 секунд. transmit-delay: примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state); задаётся в секундах. Значение по умолчанию 1 секунда. authentication: тип аутентификации. Доступны: enabled <on off> — включение/отключение требования аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов. auth-type — выбор типа аутентификации: plain (передача ключа в открытом виде для аутентификации роутеров) или digest (использование MD5-хеша для ключа для аутентификации OSPF-пакетов). md5 — идентификатор ключа. key — ключ. Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.
areas	Настройка области OSPF. Для добавления новой области или изменения параметров созданной ранее области используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> ospf areas new Admin@nodename# set network virtual-router <virtual-router-name> ospf areas <area-name></pre> Далее указываются следующие параметры: enabled <on off>: включение/отключение использования данной области. name: название области. description: описание области. cost: стоимость LSA, анонсируемых в stub-области. area-id: идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Идентификатор области должен совпадать для установления соседства OSPF. auth-type: тип аутентификации. Доступны следующие значения: none — не требовать аутентификацию OSPF-пакетов. plain — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. digest — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне зоны. area-type: тип области OSPF. Доступны следующие типы: normal — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. nssa — Not-So-Stubby Area определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR). stub — тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. no-summary: разрешение/запрет инъекции суммированных маршрутов в тупиковые типы областей: on. off. interfaces: выбор интерфейсов OSPF, на которых будет доступна данная зона. virtual-links: Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений. Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону.
redistribute	Распространение OSPF маршрутов: connected — распространение маршрутов в непосредственно подключённые к UserGate сети. kernel — распространение маршрутов, которые были добавлены администратором.

Для отображения конфигурации OSPF в виртуальном маршрутизаторе используется команда:

```
Admin@nodename# show network virtual-router <virtual-router-name> ospf
```

Пример конфигурирования OSPF в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router ospf router-id 192.168.100.3 areas new area-id 1 area-type normal name "New OSPF area" enabled on interfaces []
```

```
...
```

```
Admin@nodename# show network virtual-router test_router
```

```
name      : test_router
description : Test virtual router
```

```
node-name      : node_1
interfaces     : port2; port3
routes        : []
ospf           :
  router-id    : 192.168.100.3
  enabled      : off
  default-originate : off
  metric       : None
  areas        :
    New OSPF area
      name      : New OSPF area
      enabled    : on
      cost       : 1
      area-id    : 1
      area-type  : normal
      no-summary : off

  interfaces    : []
...

```

Для удаления настроек OSPF используется команда:

```
Admin@nodename# delete network virtual-router <virtual-router-name> ospf <parameter>
```

Параметры, доступные для удаления:

- **interface.**
- **area.**

Настройка BGP

Настройка протокола динамической маршрутизации BGP (Border Gateway Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> bgp
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение или отключение OSPF-маршрутизатора: • on. • off
router-id	IP-адрес маршрутизатора. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору. При выключении BGP (enabled off) значение router-id может быть удалено (none)
asn	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
multiple-path	Включение или отключение балансировки трафика на маршруты с одинаковой стоимостью: • on. • off.
redistribute	Распространение BGP маршрутов: • connected — распространение маршрутов в непосредственно подключённые к UserGate сети. • kernel — распространение маршрутов, которые были добавлены администратором. • ospf — распространение маршрутов, полученных по протоколу OSPF.
networks	Список сетей, относящихся к данной автономной системе. Необходимо указать в формате <ip/mask>.
routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами. Для создания routemap или изменения параметров созданного ранее routemap используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp routemaps new Admin@nodename# set set network virtual-router <virtual-router-name> bgp routemaps <routemap-name></pre> Параметры routemap: • name — название routemap. • description — описание routemap. • action — действие: • allow — разрешить прохождение данных, попадающих под условия routemap. • block — запретить прохождение данных, попадающих под условия routemap. • next-hop — установка для отфильтрованных маршрутов значения next hop в указанный IP-адрес. • weight — установка для отфильтрованных маршрутов веса в указанное значение. • metric — установка для отфильтрованных маршрутов метрики в указанное значение. • position — порядковый номер routemap в общем списке. • preference — установка для отфильтрованных маршрутов предпочтения в указанное значение. • as-prepend — установка значения AS-prepend — список автономных систем, добавляемых для данного маршрута. • community — установка значения для BGP community для отфильтрованных маршрутов. • append-community — Добавлять community. • ip-match — необходимо добавить все необходимые IP-адреса при выборе сравнения по IP-адресу. • as-path-match — необходимо добавить все необходимые номера автономных сетей при выборе сравнения по AS-пути. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (_), который интерпретируется как: • Пробел. • Запятая. • Начало строки. • Конец строки. • AS set delimiter { and }. • AS confederation delimiter (and). • community-match — необходимо добавить строки всех необходимых BGP community при выборе сравнения по Community.

Параметр	Описание
filters	Фильтр позволяет фильтровать маршруты при перераспределении. Для создания фильтра или изменения параметров созданного ранее фильтра используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp filters new Admin@nodename# set network virtual-router <virtual-router-name> bgp filters <filter-name></pre> Параметры: • name — название фильтра. • description — описание фильтра. • action — действие: ◦ allow — разрешить прохождение данных, попадающих под условия routemap. ◦ block — запретить прохождение данных, попадающих под условия routemap. • ip-filter — необходимо добавить все необходимые IP-адреса при выборе фильтрации по IP-адресу. Адреса могут быть указаны в следующих форматах: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0/8:11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. • as-path-filter — необходимо добавить все необходимые номера автономных сетей при выборе фильтрации по AS пути. • position — порядковый номер фильтра в общем списке.

Параметр	Описание
neighbors	BGP-соседи. Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды: <pre>Admin@nodename# set network virtual-router <virtual-router-name> bgp neighbors new Admin@nodename# set network virtual-router <virtual-router-name> bgp neighbors <host-ip></pre> Параметры: enabled — включение/отключение использования соседа: on. off. description — описание BGP-соседа. host — IP-адрес соседа. remote-asn — номер автономной системы, к которой относится сосед. weight — вес маршрутов, получаемых от данного соседа. ttl — максимальное количество хопов, разрешенное до этого соседа. allows-in — параметр (allow autonomous system in), который разрешает маршрутизатору принимать BGP-маршруты, даже если в пути (AS-Path) этих маршрутов присутствует номер его собственной автономной системы (AS). on. off. allows-in-number — максимально допустимое количество вхождений своей AC в пути. Возможны значения от 0 до 10 (0 — origin) bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. next-hop-self — замена значения next-hop-self на собственный IP-адрес, если сосед является BGP: on. off. ebgp-multihop — до этого BGP-соседа не прямое соединение (более одного хопа): on. off. route-reflector-client — определение, является ли BGP-сосед клиентом Route reflector: on. off. soft-reconfiguration — использование soft reconfiguration (без разрыва соединений) для обновления конфигурации: on. off. default-originate — анонс соседу маршрут по умолчанию: on. off. send-community — пересылать community BGP-соседам: on. off. enable-auth — включение/отключение аутентификации для соседа: on. off. password — пароль для аутентификации соседа. filter-in — ограничение информации о маршрутах, получаемых от соседей. filter-out — ограничение информации о маршрутах, анонсируемых соседям. route-map-in — ограничение маршрутизирующей информации, которую BGP получает от соседей. route-map-out — ограничение маршрутизирующей информации, которую BGP отдаёт соседям. graceful-restart-disable — отключение механизма плавного восстановления BGP-соединения для конкретного соседа, даже если в параметрах BGP виртуального маршрутизатора эта функция включена (доступно в версии 7.5.1 и выше). Добавление альтернативного номера AC виртуального маршрутизатора для анонсирования выбранному внешнему BGP-соседу. Альтернативный номер AC будет добавляться в начало пути анонсируемого маршрута перед реальным номером AC. Функция доступна в версии 7.5.1 и выше. Параметры функции: local-as-enabled — разрешить использование альтернативного номера AC. local-as-number — указать альтернативный номер AC. local-as-no-prepend — не добавлять альтернативный номер локальной AC. Альтернативный номер AC настроен на локальном маршрутизаторе, но он не будет добавляться в начало AS Path при формировании анонсируемых этому соседу маршрутов. local-as-replace-as — заменить на альтернативный номер локальной AC; альтернативный номер AC заменит реальный номер AC при формировании анонсируемых этому соседу маршрутов Удаление номеров частных AC из атрибута AS-Path перед тем, как анонсировать маршрут внешнему BGP-соседу. Функция доступна в версии 7.5.1 и выше. Параметры функции: remove-private-as — из списка автономных систем в атрибуте AS-Path удаляются только последовательные номера частных AC, находящиеся в конце AS-Path, непосредственно перед локальным AC. Если в пути встречается публичный номер AC, удаление прекращается. remove-private-as-all — удалять частные номера AC из смешанных AS-Path. Если в анонсируемом маршруте путь состоит одновременно из частных и публичных номеров AC, при включении опции из атрибута AS-Path будут удалены все номера частных AC. remove-private-as-replace — заменять частные номера AC номером локальной AC. При включении опции номера частных AC в атрибуте AS-Path будут заменены на номер локальной AC виртуального маршрутизатора

Параметр	Описание
graceful-restart	Механизм graceful restart (GR) позволяет перезапустить процесс BGP на маршрутизаторе без мгновенного прерывания маршрутизации. Если режим GR согласован с соседними устройствами, массового удаления маршрутов и потери трафика во время перезапуска не происходит. Настройка параметров GR доступна в версии 7.5.1 и выше. Согласование режима GR выполняется непосредственно в момент установления BGP-сессии между соседними устройствами. Параметры настройки GR: enabled — включение и отключение работы механизма BGP Graceful Restart на виртуальном маршрутизаторе. При активации параметра механизм применяется ко всем BGP-соседям по умолчанию. Механизм можно отключить для любого BGP-соседа в параметрах соответствующего соседа. Значения параметра: on; off. stalepath-time — время, в течение которого перезапускающийся маршрутизатор будет продолжать физически пересылать пакеты, используя старую информацию о маршрутах в таблице пересылки (forwarding information base, FIB), пока BGP-процесс еще не восстановился. Возможные значения: 0-4095 сек. rib-stale-time — время, в течение которого принимающий узел будет хранить маршруты, помеченные как устаревшие (stale), в своей таблице маршрутизации (routing information base, RIB). Возможные значения: 0-3600 сек. restart-time — время, в течение которого принимающий узел ожидает восстановления BGP-сессии от перезапускающегося соседа. Возможные значения: 0-4095 сек. select-defer-time — время, в течение которого перезапускающийся узел откладывает выполнение процедуры выбора лучшего маршрута (best path selection), ожидая восстановления информации от всех соседей. Параметр позволяет уменьшить количество перерасчетов маршрутов. Возможные значения: 0-3600 сек notification — параметр определяет, применять ли механизм GR после аварийного завершения BGP-сессии и получения сообщения Notification. Позволяет сохранить маршрутизацию даже после возникновения определенных типов ошибок, если обе стороны поддерживают такую функцию. Значения параметра: on; off. preserve-fw-state — при включенном параметре перезапускающийся узел информирует соседей о возможности продолжать пересылку трафика, используя существующую таблицу FIB, пока BGP-процесс перезапускается. Значения параметра: on; off

Команда для отображения конфигурации BGP в виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name> bgp
```

Пример команды конфигурирования BGP в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router bgp router-id 192.168.95.224 asn 1 networks [ 192.168.100.0/24 ] redistribute [ connected kernel ]
Admin@nodename# show network virtual-router test_router
```

```
name      : test_router
description : Test virtual router
node-name  : node_1
interfaces : port2; port3
...
bgp       :
  enabled  : off
  asn      : 1
  router-id : 192.168.95.224
  redistribute : connected; kernel
  multiple-path : off
  networks  : 192.168.100.0/24
  routemaps : []
  neighbors : []
  filters   : []
...
```

Команда для удаления параметров BGP-маршрутизатора:

```
Admin@nodename# delete network virtual-router <virtual-router-name> bgp <parameter>
```

Для удаления доступны следующие параметры:

- Адреса сетей, относящихся к данной автономной системе: **networks**.
- Условия применения routemap: **routemaps <routemap-name> ip-match | community-match | as-path-match**.
- Условия применения фильтра: **filters <filter-name> ip-filter | as-path-filter**.
- Фильтры BGP-соседей и routemaps: **neighbors <host-ip> filter-in | filter-out | routemap-in | routemap-out**.
- опции распространения BGP маршрутов: **redistribute [connected | kernel]**.

Настройка RIP

Настройка протокола маршрутизации RIP (Routing Information Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> rip
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: on. off.
version	Версия протокола RIP: 1. 2. Как правило, используется 2-я версия протокола.
metric	Метрика RIP. По умолчанию метрика равна 1; максимальное значение — 15. Значение 16 считается бесконечным.
distance	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
originate	Отправлять себя в качестве маршрута по умолчанию.
networks-cidr	Указание сети в виде CIDR. Указывается в формате <ip/mask>.
networks-interface	Указание сетевого интерфейса, с которого будут отправлять обновления маршрутной информации; указываются интерфейсы, принадлежащие виртуальному маршрутизатору.

Параметр	Описание
redistribute	Распространение маршрутов: • connected — распространение другим роутерам RIP маршрутов в непосредственно подключённые к UserGate сети: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • static — распространение другим маршрутизаторам статических маршрутов: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • kernel — распространение другим роутерам RIP маршрутов, которые были добавлены администратором: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • ospf — распространение другим RIP-роутерам маршрутов, полученных по OSPF: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • bgp — распространение другим RIP-роутерам маршрутов, полученных по BGP: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off.
interfaces	Настройка интерфейсов, на которых поддерживается протокол RIP; интерфейсы должны быть добавлены в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: <pre>Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces new Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces <interface-name></pre> Параметры: • interface — выбор интерфейса. • send-version — версия протокола RIP, которую маршрутизатор будет отправлять. Доступны: ◦ 0. ◦ 1. ◦ 2. ◦ 3. • receive-version — версия протокола RIP, которую маршрутизатор будет принимать. Доступны: ◦ 0. ◦ 1. ◦ 2. ◦ 3. • password — строка для авторизации, которая будет посылаться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль. • split-horizone — метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который прибыло обновление. ◦ on. ◦ off. • poisoned-reverse — метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отправляет его соседу, от которого его получил. ◦ on. ◦ off. • passive-mode — режим работы интерфейса, при котором он принимает обновления RIP, но не отправляет их. ◦ on. ◦ off.

Команда для отображения конфигурации RIP в виртуальном маршрутизаторе:

```
Admin@nodename# show network virtual-router <virtual-router-name> rip
```

Пример команды конфигурирования RIP в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router rip version 2 originate on
Admin@nodename# show network virtual-router test_router
```

```
name      : test_router
description : Test virtual router
node-name  : node_1
interfaces : port2; port3
...
rip       :
  enabled  : off
  distance : 120
  metric   : 1
  originate : on
  interfaces : []
  redistribute : {}
  version   : 2
```

```
Admin@nodename# set network virtual-router test_router rip interfaces new interface port2
Admin@nodename# show network virtual-router test_router
```

```
name      : test_router
description : Test virtual router
node-name  : node_1
interfaces : port2; port3
...
rip       :
  enabled  : off
  distance : 120
  metric   : 1
  originate : on
  interfaces :
    port2
      interface : port2
      passive-mode : off
      poisoned-reverse : off
      receive-version : 0
      send-version : 0
      split-horizone : off
  redistribute : {}
```

```
version      : 2
...
```

Команда для удаления параметров RIP-маршрутизатора:

```
Admin@nodename# delete network virtual-router <virtual-router-name> rip <parameter>
```

Для удаления доступны следующие параметры:

- Интерфейсы RIP: **interfaces**.
- Сети RIP: **networks-cidr**.
- Сетевого интерфейса, с которого будут отправлять обновления маршрутной информации: **networks-interface**.

Настройка мультикаст-маршрутизации

Настройка мультикаст-маршрутизации в виртуальном маршрутизаторе производится с использованием следующей команды:

```
Admin@nodename# set network virtual-router <virtual-router-name> multicast-router
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: on. off.
ecmp	Разрешение распределения трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP): on. off. Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если данная опция отключена, то весь трафик на определенный хост назначения будет пересылаться только через один из роутеров (next hop).
ecmp-rebalance	Использование ECMP rebalance: on — если один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). off — если один из интерфейсов, через который отсылался трафик, отключился, то перераспределяются только те потоки, которые передавались через отключенный интерфейс.
join-prune	Интервал отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.
register-suppress	Интервал, после которого маршрутизатор отправляет сообщение register suppress.
keep-alive	Интервал, через который маршрутизатор будет посылать сообщения keeralive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.
interfaces	Интерфейс, который будет использоваться для работы мультикаста; для указания доступны только интерфейсы, добавленные в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: Admin@nodename# set network virtual-router <virtual-router-name> multicast-router interfaces new Admin@nodename# set network virtual-router <virtual-router-name> multicast-router interfaces <interface-name> Далее необходимо указать параметры: interface — выбор интерфейса для работы мультикаст. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор. hello-timeout — интервал отправки PIM HELLO сообщений в секундах. PIM Hello сообщения отправляются периодически со всех интерфейсов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг. dr-priority — приоритет при выборе Designated router (DR), с помощью которого администратор может управлять процессом выбора DR для локальной сети. bfd: добавить профиль bfd (Bidirectional Forwarding Detection). Профили bfd создаются в библиотеке элементов, подробнее читайте в разделе Настройка библиотек. enable-igmp — приём сообщений IGMP report и IGMP query на данном интерфейсе. use-igmpv2 — использование версии IGMP v2, по умолчанию используется IGMP v3.
rendevouz-points	При настройке Rendezvous points можно указать следующие параметры: enabled — включение/отключение данного RP: on. off. name — название RP. ip — Unicast IP-адрес RP. asm-allowed-groups — список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Если ничего не задано, то ограничений нет.
ssm-allowed-groups	Настройка мультикаст роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть указаны любые сети из диапазона 232.0.0.0/8; если ничего не задано, то ограничений нет.
spt-exclusions	Настройка мультикаст роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

Для отображения конфигурации мультикастинга в виртуальном маршрутизаторе используйте следующую команду:

```
Admin@nodename# show network virtual-router <virtual-router-name> multicast-router
```

Пример команды конфигурирования мультикаст-маршрутизации в виртуальном маршрутизаторе:

```
Admin@nodename# set network virtual-router test_router multicast-router interfaces new interface port2 use-igmpv2 on
Admin@nodename# show network virtual-router test_router
```

```
name          : test_router
description    : Test virtual router
node-name     : node_1
interfaces    : port2; port3
...
multicast-router :
  enabled       : off
  ecmp-rebalance : off
  ecmp          : off
  join-prune    : 60
  keep-alive    : 31
  register-suppress : 5
  interfaces    :
    port2
      interface  : port2
      enabled    : off
```

```
enable-igmp      : off
use-igmpv2       : on
bfd              : Not set
```

```
rendevouz-points : []
```

...

Команда для удаления параметров мультикаст-маршрутизатора:

```
Admin@nodename# delete network virtual-router <virtual-router-name> multicast-router
```

Для удаления доступны следующие параметры:

- Интерфейсы, использующиеся для работы мультикаста: **interfaces**.
- Rendezvous points: **rendevouz-points <rp-name>**, а также список разрешенных групповых адресов для any source multicast с данного RP: **rendevouz-points <rp-name> asm-allowed groups**.
- Список разрешенных групповых адресов для source specific multicast: **ssm-allowed-groups**.
- Список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree: **spt-exclusions**.

Настройка WCCP

Version: 7.x
Product: NGFW
Documentation: 

Настройка WCCP (Web Cache Communication Protocol) производится на уровне **network wccp**. Для создания сервисной группы WCCP используется следующая команда:

Admin@nodename# create network wccp <parameter>

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение сервисной группы: - on. - off.
name	Название сервисной группы WCCP.
description	Описание сервисной группы.
password	Пароль, необходимый для аутентификации UserGate в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
fwd-type	Способ перенаправления трафика с серверов WCCP на UserGate: - I2 — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес UserGate. - gre — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
ret-type	Способ перенаправления трафика с UserGate на серверы WCCP: - I2 — используя перенаправление L2. В этом случае UserGate (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер). - gre — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
service-group	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
priority	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
ports	Порты для перенаправления (порты назначения трафика). При необходимости указываются несколько портов в формате: ports-to-redirect + [80 442] . Важно! UserGate может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate с другими портами, будет отправляться в интернет без фильтрации.
ports-source	Перенаправление трафика на основании значений портов источника: - on. - off.
protocol	Выбор протокола: - tcp — Transmission Control Protocol (TCP). - udp — User Datagram Protocol (UDP).
routers-lists	Список IP-адресов серверов WCCP. Подробнее о создании списков IP-адресов с помощью CLI читайте в разделе Настройка IP-адресов .
routers-ips	IP-адреса серверов WCCP.
assignment-type	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. - hash — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета: - source-ip — вычисление хэша по IP-адресу источника. - source-port — вычисление хэша по порту источника. - dest-ip — вычисление хэша по IP-адресу назначения. - dest-port — вычисление хэша по порту назначения. - alt-source-ip — вычисление альтернативного хэша по IP-адресу источника. - alt-source-port — вычисление альтернативного хэша по порту источника. - alt-dest-ip — вычисление альтернативного хэша по IP-адресу назначения. - alt-dest-port — вычисление альтернативного хэша по порту назначения. - mask — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP. - source-ip — схема маскирования по IP-адресу источника. - source-port — схема маскирования по порту источника. - dest-ip — схема маскирования по IP-адресу назначения. - dest-port — схема маскирования по порту назначения. - mask-value — значение маски схемы маскирования. Для схемы маскирования по порту — 16 бит; по IP-адресу — 32 бита; указываются в шестнадцатеричном формате.

Для задания значений сервисной группы WCCP или обновления информации о ней:

Admin@nodename# set network wccp <service-group-name> <parameter>

Далее указываются параметры, значения которых необходимо обновить; параметры представлены в таблице выше.

Для просмотра информации о сервисной группе WCCP:

Admin@nodename# show network wccp <service-group-name>

Примеры команд создания и редактирования WCCP:

```
Admin@nodename# create network wccp name "Test service group" protocol tcp service-group 1 routers-ips [ 192.168.100.120 ] fwd-type l2 ret-type l2 ports [ 80 ] priority 1 password 12345
Admin@nodename# show network wccp "Test service group"
```

```
name          : Test service group
enabled       : off
fwd-type      : l2
ret-type      : l2
service-group : 1
priority      : 1
protocol      : tcp
ports        : 80
assignment-type : hash
source-ip     : off
source-port   : off
dest-ip       : off
dest-port     : off
alt-source-ip : off
alt-source-port : off
alt-dest-ip   : off
alt-dest-port : off
routers-ips   : 192.168.100.120
Admin@nodename# set network wccp "Test service group" description "Test service group description" service-group 100
Admin@nodename# show network wccp "Test service group"
```

```
name          : Test service group
description    : Test service group description
enabled       : off
fwd-type      : l2
ret-type      : l2
service-group : 100
priority      : 1
protocol      : tcp
ports        : 80
assignment-type : hash
source-ip     : off
source-port   : off
dest-ip       : off
dest-port     : off
alt-source-ip : off
alt-source-port : off
alt-dest-ip   : off
alt-dest-port : off
routers-ips   : 192.168.100.120
```

Удаление сервисной группы полностью или некоторых её параметров:

```
Admin@nodename# delete network wccp <service-group-name>
```

Параметры, доступные для удаления:

- **routers-lists.**
- **routers-ips.**
- **ports.**

