

Table of Contents

Table of Contents	1
Настройки сети	2
Зоны	3
Интерфейсы	5
Шлюзы	12
Настройка виртуальных маршрутизаторов	13

Product: WAF
Version: 7.x

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): <ul style="list-style-type: none">• enabled: включение/отключение защиты.<ul style="list-style-type: none">◦ on.◦ off.• aggregate:<ul style="list-style-type: none">◦ 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: <ul style="list-style-type: none">• enabled: включение/отключение защиты.<ul style="list-style-type: none">◦ on.◦ off.• aggregate:<ul style="list-style-type: none">◦ 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: <ul style="list-style-type: none">• enabled: включение/отключение защиты.<ul style="list-style-type: none">◦ on.◦ off.• aggregate:<ul style="list-style-type: none">◦ 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.
enabled-services	Параметры контроля доступа зоны: <ul style="list-style-type: none">• "Any ICMP": разрешение использования команды ping адреса UserGate.• SNMP: доступ к UserGate по протоколу SNMP (UDP 161).• "Admin Console": доступ к веб-консоли управления (TCP 8001).• "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.• "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси.• "Log Analyzer": сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный сервер UserGate в качестве Log analyzer (TCP 2023 и 9713).• "SNMP Proxy": сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры).• NTP: доступ к сервису точного времени, запущенному на сервере UserGate.
service-addresses	Указание разрешённых IP-адресов для сервисов: <ul style="list-style-type: none">• service: выбор сервисов (список соответствует enabled-services).• allowed-addresses: разрешённые IP-адреса:<ul style="list-style-type: none">◦ geoip — код GeoIP.◦ ip-list — заранее созданный в библиотеке элементов список IP-адресов.
antispoof-enabled	Включение/отключение защиты от IP-спуфинга: <ul style="list-style-type: none">• on.• off.
antispoof-negate	Возможные значения: <ul style="list-style-type: none">• on.• off. <p>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.</p>

Параметр	Описание
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: <ul style="list-style-type: none">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): <ul style="list-style-type: none">excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: <ul style="list-style-type: none">excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: <ul style="list-style-type: none">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>

Product: WAF
Version: 7.x

Список упорядоченных имён сетевых интерфейсов и соответствующие им физические адреса доступен для отображения при выполнении команды (команда доступна и в режиме диагностики и мониторинга и в режиме конфигурации):

Admin@nodename> show network interface-mapping

Admin@nodename# show network interface-mapping

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

Для удаления списка используйте следующие команды в режиме диагностики и мониторинга и в режиме конфигурации соответственно:

Admin@nodename> clear network interface-mapping

Admin@nodename# delete network interface-mapping

После перезагрузки сервера UserGate список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate.

Далее будет рассмотрена настройка интерфейсов, которая производится на уровне **network interface**.

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

Admin@nodename# set network interface adapter <adapter_name>

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: <ul style="list-style-type: none">on.off.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: <ul style="list-style-type: none">l3: интерфейс, работающий в режиме Layer 3 (можно 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 Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: <ul style="list-style-type: none">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: <ul style="list-style-type: none">bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate 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] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей читайте в разделе Настройка профилей LLDP .
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
rx-ring	Размер буфера RX ring интерфейса типа adapter.
tx-ring	Размер буфера TX ring интерфейса типа adapter.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: <ul style="list-style-type: none">enabled: включение/отключения релея:<ul style="list-style-type: none">on.off.utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip поле>).server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

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

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

Admin@nodename# show network interface adapter

Для отображения информации об адаптере:

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

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

Admin@nodename# create network interface vlan

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: <ul style="list-style-type: none">on.off.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: <ul style="list-style-type: none">I3: Layer 3 (можно 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 Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: <ul style="list-style-type: none">dhcp: получение динамического IP-адреса по DHCP.manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: <ul style="list-style-type: none">bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate 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] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.

Параметр	Описание
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: <ul style="list-style-type: none">enabled: включение/отключения релея:<ul style="list-style-type: none">on.off.utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея.server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

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

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **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:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

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

или об определённом интерфейсе:

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

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

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

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: <ul style="list-style-type: none">on.off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: <ul style="list-style-type: none">bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate 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] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .

Параметр	Описание
bonding	<p>Дополнительные параметры бонд-интерфейса:</p> <ul style="list-style-type: none">aggr-mode — режим работы бонда:<ul style="list-style-type: none">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, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости).xor: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»-]. Получается, 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: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для 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. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику).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, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты).load: режим Adaptive load balancing. Включает в себя предыдущую политику плюс 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 наружу, 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 (miimon). Значение параметра должно быть кратным значениям miimon.up-delay: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon.lacp-rate: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:<ul style="list-style-type: none">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:<ul style="list-style-type: none">disabled: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.active: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа.follow: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.xmit-hash: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:<ul style="list-style-type: none">I2: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста 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 хэша. Алгоритм совместим с IEEE 802.3ad.I3-4: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. 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 дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.interface: интерфейсы, которые будут объединены в бонд.
iface-mode	<p>Режим назначения IP-адреса:</p> <ul style="list-style-type: none">dhcp: получение динамического IP-адреса по DHCP.manual: без адреса. <p>Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.</p>
iface-type	<p>Тип создаваемого интерфейса:</p> <ul style="list-style-type: none">I3 — Layer 3 интерфейс.mirror — интерфейс зеркалирования трафика.
ip-addresses	<p>Назначение интерфейсу IP-адреса.</p> <p>Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде.</p> <p>Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.</p>
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	<p>Настройка работы DHCP-релея на интерфейсе. Необходимо указать:</p> <ul style="list-style-type: none">enabled: включение/отключения релея:<ul style="list-style-type: none">on.off.utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея.server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего бонд-интерфейса:

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

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

Команда удаления бонд-интерфейса или его параметров:

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

Параметры, доступные для удаления:

Параметр	Описание

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

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

или об определённом интерфейсе:

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

Настройка bridge-интерфейса

Настройка моста производится на уровне **network interface bridge**.

Чтобы добавить новый bridge-интерфейс:

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

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: <ul style="list-style-type: none">on.off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).
description	Описание bridge-интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.
link-info	Настройка параметров сетевого интерфейса: <ul style="list-style-type: none">bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate 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] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
bridging	Дополнительные параметры моста: <ul style="list-style-type: none">iface-type: режим работы интерфейса:<ul style="list-style-type: none">I2: Layer 2 (создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security; контентная фильтрация в этом режиме работает).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/отключение использование STP (Spanning Tree Protocol) для защиты от петель:<ul style="list-style-type: none">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: <ul style="list-style-type: none">dhcp: получение динамического IP-адреса по DHCP.manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: <ul style="list-style-type: none">enabled: включение/отключения релея:<ul style="list-style-type: none">on.off.utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея.server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего bridge-интерфейса:

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

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

Команда удаления bridge-интерфейса или его параметров:

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

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех bridge-интерфейсах:

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

или об определённом интерфейсе:

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

Настройка loopback-интерфейса

Создание и настройка loopback-интерфейса производится на уровне **network interface loopback**.

Для создания интерфейса используется команда:

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

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса: <ul style="list-style-type: none">on.off.
interface-name	Название интерфейса.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>], маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
iface-mode	Режим назначения IP-адреса: <ul style="list-style-type: none">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 читайте в разделе Настройка профилей LLDP .
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров интерфейса: <ul style="list-style-type: none">bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate 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] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
node-name	Узел кластера, на котором будет создан интерфейс.
mac	MAC-адрес интерфейса.

Параметр	Описание
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: <ul style="list-style-type: none">• enabled: включение/отключения релея:<ul style="list-style-type: none">◦ on.◦ off.• utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея (принимает значения <ip поле>).• server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего интерфейса:

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

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

Команда удаления loopback-интерфейса или его параметров:

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

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех loopback-интерфейсах:

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

или об определённом интерфейсе:

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

Product: WAF
Version: 7.x

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: <ul style="list-style-type: none">on.off.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет.
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: <ul style="list-style-type: none">on.off.
default	Использование данного шлюза в качестве шлюза по умолчанию: <ul style="list-style-type: none">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>

Настройка виртуальных маршрутизаторов

Product: WAF
Version: 7.x
Technology: Routing

В данном разделе описана настройка 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, бондинг, 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: <ul style="list-style-type: none">• on.• off.
name	Имя маршрута.
description	Описание маршрута.
type	Тип маршрута: <ul style="list-style-type: none">• 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

```

