

Table of Contents

Table of Contents	1
Интерфейс командной строки	3
Общие положения	4
Общие положения (Описание)	5
Команды, доступные до первоначальной инициализации узла	8
Команды, доступные до первичной инициализации узла (Описание)	9
Первоначальная инициализация	24
Первоначальная инициализация NGFW	25
Мастер первоначальной настройки узла	26
Команды диагностики и мониторинга	27
Команды диагностики и мониторинга (Описание)	28
Режим конфигурации	37
Режим конфигурации (описание)	38
Настройка устройства	42
Настройка устройства (Описание)	43
Настройка кластеров	49
Настройка кластеров (версия 7.5.0 и выше)	51
Настройка управления доступом к консоли UserGate NGFW	54
Настройка сертификатов	57
Настройка параметров устройства	59
Настройка прокси-сервера	60
Настройка работы с вышестоящими прокси-серверами	61
Настройка параметров мониторинга устройства	64
Настройка профилей клиентских сертификатов	66
Настройка параметров управления телеметрией	67
Экспорт и импорт конфигурации в текстовом формате	68
Настройки сети	69
Зоны	70
Интерфейсы	73
Шлюзы	82
DHCP	83
DNS-настройки	84
Настройка виртуальных маршрутизаторов	86
Настройка WCCP	96
Настройка раздела Пользователи и устройства	98
Настройка групп пользователей	99
Настройки пользователей	100
Настройка серверов аутентификации	101
Настройка профилей аутентификации	104
Настройка Captive-профилей	105
Captive-портал	107
Настройка терминальных серверов	109
Настройка профилей MFA (мультифакторной аутентификации)	110
Просмотр информации об авторизованных пользователях	112
Настройка применения политик к пользователям	113
Настройка UserID-агента	114
Настройка раздела Политики сети	116
Настройка правил межсетевого экрана	117
Настройка правил NAT и маршрутизации	119
Настройка балансировки нагрузки	127

Настройка правил управления пропускной способностью	130
Настройка раздела Политики безопасности	132
Настройка фильтрации контента	133
Настройка веб-безопасности	135
Настройка правил инспектирования туннелей	137
Настройка инспектирования SSL	138
Настройка инспектирования SSH	140
Настройка COB	142
Настройка защиты почтового трафика	143
Настройка правил ICAP	145
Настройка ICAP-серверов	147
Настройка профилей DoS	148
Настройка правил защиты DoS	149
Настройка глобального портала	151
Настройка веб-портала	152
Настройка правил reverse-прокси	153
Настройка серверов reverse-прокси	155
Настройка VPN в CLI	156
Настройка серверных правил	157
Настройка клиентских правил	158
Настройка сетей VPN	159
Настройка профилей безопасности VPN	160
Настройка VPN в CLI (в версии 7.5.0 и выше)	164
Настройка серверных правил VPN	165
Настройка клиентских правил VPN	169
Управление VPN-сессиями в CLI	172
Настройка библиотек	173
Настройка библиотек (Описание)	174
Настройка раздела журналы и отчеты	197
Настройка экспорта журналов	198
Настройка отчетов	200

Общие положения (Описание)

Documentation: 
Product: NGFW
Version: 7.x

UserGate NGFW поддерживает работу через интерфейс командной строки (CLI).

С помощью CLI вы можете:

- просматривать конфигурацию устройства;
- выполнять диагностику работы устройства;
- настраивать параметры конфигурации устройства;
- перезагружать или выключать устройство.

Подключение к интерфейсу командной строки

К интерфейсу командной строки можно подключиться с помощью стандартных портов для монитора и клавиатуры (при наличии таких портов на устройстве), с помощью терминала через консольный порт или удаленно с помощью протокола SSH.

ПримечаниеЕсли устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — usergate.

Для подключения с помощью монитора и клавиатуры:

1. Подключите монитор к разъему VGA (HDMI), клавиатуру — к разъему USB.
2. Войдите в CLI, используя имя и пароль пользователя с правами администратора (по умолчанию — Admin и usergate).

Для подключения с помощью консольного порта:

1. Подключите компьютер к устройству с помощью кабеля для консольного порта.
2. Запустите программу — эмулятор терминала, например Putty для Windows или minicom для Linux. Установите подключение через последовательный порт, указав параметры подключения: 115200, 8 n 1.
3. Введите логин а пароль для доступа в интерфейс (по умолчанию — Admin и usergate).

Для подключения с помощью протокола SSH:

1. Разрешите доступ для протокола CLI по SSH в параметрах зоны, к которой вы собираетесь подключаться (доступ по порту TCP 2200). Подробнее о настройке зоны в CLI — в разделе « Зоны».
 2. Запустите на компьютере SSH-терминал, например SSH для Linux или Putty для Windows.
 3. Укажите IP-адрес устройства, порт для подключения (по умолчанию — 2200), имя пользователя с правами администратора (по умолчанию — Admin).
- Пример команды подключения для Linux: ssh Admin@<IP-address> -p 2200.
3. Войдите в CLI, используя пароль пользователя, указанного на предыдущем шаге.

В версии 7.4.0 и выше для подключения к CLI по SSH поддерживаются следующие алгоритмы:

- Kex: diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256;
- Public key: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-256, rsa-sha2-512, ssh-rsa;
- Ciphers: aes128-ctr, aes192-ctr, aes256-ctr;
- MAC: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-256.

Режимы работы интерфейса командной строки

CLI имеет два основных режима работы — режим диагностики и режим конфигурации.

Режим диагностики

После авторизации вы попадаете в режим диагностики.

В режиме диагностики доступны команды:

- проверки доступности сетевых ресурсов;
- просмотра статистики и информации об интерфейсах;
- просмотра информации о записях ARP;
- отслеживания пакетов по установленным правилам;
- мониторинга трафика;
- просмотра информации о маршрутах;
- просмотра состояния кластера;
- просмотра заблокированных COB IP-адресов;
- отображения системной информации;
- диагностики работы протоколов динамической маршрутизации;
- просмотра информации об авторизованных пользователях.

Приглашение командной строки в режиме диагностики имеет следующий вид:

Admin@nodename>

Режим конфигурации

Настройка параметров устройства выполняется в режиме конфигурации.

Для переключения в режим конфигурации используется команда configure. В режиме конфигурации символ приглашения в командной строке меняется на #. Вернуться в режим просмотра можно с помощью команды exit.

```
Admin@nodename> configure
Admin@nodename#
Admin@nodename# exit
Admin@nodename>
```

Система до первичной инициализации

Если система находится в состоянии до первичной инициализации, в CLI доступны команды режима диагностики и ограниченный набор команд режима конфигурации, позволяющий выполнить настройку сетевых параметров устройства. Подробнее — в разделе «Команды, доступные до первичной инициализации узла».

Приглашение командной строки такой системы по умолчанию имеет вид:

- в режиме диагностики — <user-name>@<product-type>> (например, Admin@NGFW>);
- в режиме конфигурации — <user-name>@<product-type># (например, Admin@NGFW#).

Аварийное состояние

Если система находится в аварийном состоянии, для восстановления рабочего состояния в нее можно войти в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации устройства. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Приглашение командной строки в режиме emergency по умолчанию имеет вид:

<user-name>@emergency@<product-type># (например, Admin@emergency@NGFW#).

Подробнее о режиме emergency — в разделе « Настройка устройства».

Формат команд

Команды интерфейса командной строки имеют следующий формат:

- <action> <level> <filter> <configuration_info>
- <action> — действие, которое необходимо выполнить (create, set, show, delete).
 - <level> — уровень контекста конфигурации. Соответствует одному из разделов структуры конфигурации в веб-интерфейсе NGFW (network, network-policy, security-policy, users, settings, libraries, logs и т. д.).
 - <filter> — идентификатор объекта, к которому происходит обращение для выполнения действия <action>.
 - <configuration_info> — значения параметров, которые необходимо применить к объекту <filter>.

Поддерживается ввод команды в несколько строк (многострочный ввод). Примером таких команд могут быть команды описания правил, использующих [синтаксис UPL](#). Для перехода на новую строку необходимо добавить символ «\» в конце строки. Начиная со второй строки ввод символа « \» необязателен. Чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@nodename# set users user example \  
... name username1  
... enabled on  
... groups [ "Default Group" ]  
...  
Admin@nodename#
```

В версии 7.5.0 и выше поддерживается последовательное исполнение нескольких команд, вставленных из буфера обмена. Исключением являются многострочные команды, например команды, написанные с помощью синтаксиса UPL. Импортировать многострочные команды можно с помощью [команды import](#).

Фильтрация вывода команд

В версии 7.5.0 и выше в интерфейсе командной строки поддерживается функция фильтрации вывода команд. С помощью функции фильтрации вы можете управлять отображением результатов выполнения команд в соответствии с заданными критериями.

Фильтрация может применяться к различным типам команд просмотра, включая:

- команды отображения состояния устройства;
- команды просмотра конфигурации;
- команды просмотра системных журналов;
- команды с динамическим выводом данных (такие, как show traffic capture и show network trace).

Формат команд с фильтрацией вывода:

- <cli-command> | grep <pattern> -f <include|exclude> -BA <Num>:<Num>
- <cli-command> — команда CLI, вывод которой нужно отфильтровать.
 - <pattern> — искомое выражение. Поддерживается формат выражений RegExp.
 - -f <include|exclude> — включение или исключение искомого выражения из вывода команды.
 - -BA <Num>:<Num> — отображение строк, соседних с совпадением («количество отображаемых строк до совпадения» :<количество отображаемых строк после совпадения>).

Пример фильтрации вывода команд просмотра состояния интерфейсов:

```
Admin@nodename> show network interface  
  
+-----+-----+-----+-----+  
| Name | IP | Link status | Mode | Zone |  
+-----+-----+-----+-----+  
| tunnel1 | 172.30.250.1/24 | DOWN | | VPN for remote access |  
| tunnel2 | 172.30.255.1/24 | DOWN | | VPN for Site-to-Site |  
| tunnel3 | | DOWN | | VPN for Site-to-Site |  
| port0 | 172.26.147.146/16 | 10000 | main | MGMT |  
| port1 | 10.150.185.119/16 | 10000 | main | [MC] LAN |  
| port2 | 10.153.219.236/16 | 10000 | main | [MC] WAN |  
+-----+-----+-----+-----+  
Admin@nodename> show network interface | grep VPN  
| tunnel1 | 172.30.250.1/24 | DOWN | | VPN for remote access |  
| tunnel2 | 172.30.255.1/24 | DOWN | | VPN for Site-to-Site |  
| tunnel3 | | DOWN | | VPN for Site-to-Site |  
Admin@nodename> show network interface | grep VPN -f exclude  
+-----+-----+-----+-----+  
| Name | IP | Link status | Mode | Zone |  
+-----+-----+-----+-----+  
| port0 | 172.26.147.146/16 | 10000 | main | MGMT |  
| port1 | 10.150.185.119/16 | 10000 | main | [MC] LAN |  
| port2 | 10.153.219.236/16 | 10000 | main | [MC] WAN |  
+-----+-----+-----+-----+
```

Пример фильтрации вывода команд поиска правил межсетевого экрана:

```
Admin@nodename# show network-policy firewall | grep "name\(\\\"VPN\"  
name(\"VPN for remote access to Trusted and Untrusted\")  
name(\"VPN for Site-to-Site to Trusted and Untrusted\")  
Admin@nodename# show network-policy firewall | grep "name\(\\\"VPN\" -BA 4:  
src.zone = \"VPN for remote access\" \  
dst.zone = (Untrusted, Trusted) \  
desc(\"Example firewall rule which allows traffic from VPN for remote access zone to Trusted and Untrusted zones. This is an example rule which can be changed or deleted if necessary.\") \  
enabled(false) \  
name(\"VPN for remote access to Trusted and Untrusted\")  
-----  
src.zone = \"VPN for Site-to-Site\" \  
dst.zone = (Untrusted, Trusted) \  
desc(\"Example firewall rule which allows traffic from VPN for Site-to-Site zone to Trusted and Untrusted zones. This is an example rule which can be changed or deleted if necessary.\") \  
enabled(false) \  
name(\"VPN for Site-to-Site to Trusted and Untrusted\")  
-----
```

Пример фильтрации вывода команды просмотра событий журнала:

```
Admin@nodename> show logs log core static | grep ldap  
2025-08-05 11:58:32.861039<0.2336.0> [critical] database:wait_tables/1:253 'ldap_server' loaded in 0.0ms  
2025-08-05 11:58:33.392739<0.3953.0> [critical] database:wait_tables/1:253 'ldap_server' loaded in 0.0ms  
2025-08-05 11:58:33.569880<0.4287.0> [critical] nagent:start_app/1:340 ldap_sync starting ...  
2025-08-05 11:58:33.571394<0.4287.0> [critical] nagent:start_app/1:343 [uuid,ldap_sync] started  
2025-08-05 11:59:03.889299<0.4903.0> [critical][ldap] ldap_utm:find_group_by_guid/1:1149 could not find domain sid,  
2025-08-05 11:59:12.366764<0.4903.0> [critical][ldap] ldap_utm:find_group_by_guid/1:1149 could not find domain sid,  
2025-08-05 12:00:10.162520<0.4903.0> [critical][ldap] ldap_utm:find_group_by_guid/1:1149 could not find domain sid,
```

Пример фильтрации вывода команды с динамическим выводом:

```
Admin@nodename> show traffic capture | grep ICMP  
  
92 0.305709456 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping) request id=0x0e30, seq=3/768, ttl=30  
93 0.305739062 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping) reply id=0x0e30, seq=3/768, ttl=64 (request in 92)  
706 1.329727201 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping) request id=0x0e30, seq=4/1024, ttl=30  
707 1.329755455 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping) reply id=0x0e30, seq=4/1024, ttl=64 (request in 706)
```

Горячие клавиши

В интерфейсе командной строки вы можете использовать следующие горячие клавиши:

- Tab — вызов встроенной помощи, автодополнение команды:
 - Если нажать Tab в режиме ожидания ввода, выводится полный список команд, доступных на текущем уровне.
 - Если нажать Tab на этапе ввода команды после пробела, отображается список возможных параметров команды с кратким описанием.
 - Если написать первые несколько букв команды и нажать Tab, команда будет дополнена.
- Ctrl + C — отмена ввода текущей команды.

- ↑, ↓ — прокрутка истории ввода команд.

В выводе встроенной помощи после нажатия клавиши Tab могут использоваться следующие вспомогательные символы:

- * — обязательный параметр в командах `create` и ряде других команд.
- + — опциональный параметр.
- > — вложенные параметры. После введения такого параметра появляется новый список параметров, которые можно указать.

Например:

```
Admin@nodename# set network virtual-router default
+ interfaces      List of network interfaces attached to this virtual router
> routes          List of static network routes
```

Команды, доступные до первоначальной инициализации узла

Команды, доступные до первичной инициализации узла (Описание)

Documentation: 
Product: NGFW
Version: 7.x

Если устройство еще не прошло первоначальную инициализацию, в CLI доступен минимальный набор команд для настройки сетевых параметров устройства и запуска инициализации.

ПримечаниеВ случае сбоя в работе ядра CLI также может перейти в состояние до первичной инициализации.

Команды режима диагностики

В режиме диагностики доступны команды, позволяющие просмотреть:

- доступность сетевых ресурсов;
- статистику и информацию об интерфейсах;
- информацию о записях ARP;
- информацию о маршрутах;
- системную информацию.

Также в режиме диагностики можно выполнять мониторинг сетевого трафика и диагностику работы протоколов динамической маршрутизации.

Базовые команды управления устройством

Для просмотра текущих даты и времени на узле используется команда:

Admin@NGFW> date

Для перезагрузки узла используется команда:

Admin@NGFW> reboot

Для выключения узла используется команда:

Admin@NGFW> shutdown

Для перехода в режим конфигурации узла используется команда:

Admin@NGFW> configure

Для выхода из интерфейса CLI используется команда:

Admin@NGFW> exit

Команды проверки доступности сетевых ресурсов

Команда	Описание
dig	Проверка записи DNS домена: <pre>Admin@NGFW> dig host <hostname> <parameters> Admin@NGFW> dig host <IP-address> <parameters></pre> В команде можно использовать следующие параметры: • reverse-lookup — получение имени устройства по IP-адресу; • dns — указание IP-адреса DNS-сервера; • tcp — использование протокола TCP вместо UDP
netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: • address — IP-адрес и порт, доменное имя узла — для проверки доступности по TCP; URL — для HTTP; • dns-ip — IP-адрес сервера DNS; • dns-tcp — использование TCP вместо UDP для DNS-запроса; • check-cert — проверка SSL-сертификата; • type — проверка доступности по: ◦ http; ◦ tcp (если порт не указан, то используется порт 80); • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; • timeout — максимальный тайм-аут ожидания ответа от веб-сервера; • user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. <pre>Admin@NGFW> netcheck type tcp address <host-domain-name> data on Admin@NGFW> netcheck address <host-domain-name></pre>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: • host — IP-адрес или доменное имя узла. • count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). • numeric — не определять имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — максимальный размер блока данных отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. <pre>Admin@NGFW> ping host <hostname> count <number></pre>
traceroute	Трассировка соединения до определенного узла. Параметры команды: • host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; • interface <iface-name> — интерфейс, с которого будут отправляться пакеты; • not-map-ip — не искать hostname для IP-адреса при отображении; • use-icmp-echo — использовать ICMP echo; • port — указать порт вместо порта по умолчанию (1 — 65535); • min-interval — минимальный интервал между пакетами. <pre>Admin@NGFW> raceroute host <hostname></pre>

Статистика и информация об интерфейсах

Для отображения информации об интерфейсах используется команда:

```
Admin@NGFW> show network interface
```

Для отображения статистики определенного интерфейса и информации о нем используется следующая команда:

```
Admin@NGFW> show network interface <interface-name>
```

Также доступно отображение только информации или только статистики интерфейса:

```
Admin@NGFW> show network interface <interface-name> type info
Admin@NGFW> show network interface <interface-name> type statistics
```

Для отображения списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов предназначена команда:

```
Admin@NGFW> show network interface-mapping
```

ПримечаниеПод физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. Изменения MAC-адресов интерфейсов в настройках NGFW данной командой не отображаются. Измененные настройками NGFW MAC-адреса можно посмотреть командой: show network interface <interface-name>.

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

Для удаления списка используется команда:

```
Admin@NGFW> clear network interface-mapping
```

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенное устройство.

ARP-записи

Для просмотра информации о записях ARP:

```
Admin@NGFW> show network arp
```

Для просмотра ARP-записей вы можете использовать фильтры.

Параметр	Описание
interface	Название интерфейса NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

```
Admin@NGFW> show network arp host <IP-address>
Admin@NGFW> show network arp interface <interface-name>
Admin@NGFW> show network arp mac <MAC-address>
```

ПримечаниеВ режиме диагностики действия производятся с системными записями; в режиме конфигурации - со статическими ARP-записями.

Для удаления системной ARP-записи используется команда:

```
Admin@NGFW> clear network arp interface <iface-name> host <ip>
```

Для удаления всех системных записей на заданном интерфейсе (можно указать несколько интерфейсов) используется команда:

```
Admin@NGFW> clear network arp interfaces [ <iface-name1> <iface-name2> ... ]
```

Отслеживание пакетов

Для включения функции отслеживания пакетов используется команда:

```
Admin@NGFW> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия входящих и исходящих интерфейсов, номера TCP/UDP портов источника и назначения.

Для выхода из режима отслеживания пакетов нажмите комбинацию клавиш Ctrl + C.

Мониторинг трафика

Для мониторинга трафика используется команда:

```
Admin@NGFW> show traffic <parameters>
```

Параметры мониторинга трафика.

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Параметры фильтрации: - source-ip — IP-адрес источника; - source-port — порт источника; - dest-ip — IP-адрес назначения; - dest-port — порт назначения; - vlan-tag — тег VLAN; - interface-name — название интерфейса; - node-name — название узла; - protocol — протокол
connections	Отображение информации о соединениях: протокол и его номер; время жизни записи; IP-адреса источника и назначения, порты источника и назначения; IP-адреса источника и назначения, порты источника и назначения, которые ожидаются в ответе; статус сессии (UNREPLIED или ASSURED); количество переданных и принятых пакетов и байтов; зона источника; является ли эта сессия сессией известного NGFW пользователя и т. п.. Возможна фильтрация по параметрам: - protocol — протокол; - source-ip — IP-адрес источника; - dest-ip — IP-адрес назначения; - node-name — название узла; - expect — отображение неустановленных соединений (on/off)

Пример команды мониторинга трафика:

```
Admin@NGFW> show traffic connections dest-ip 192.168.0.100 expect on
```

Просмотр информации LLDP

Для просмотра информации, полученной по LLDP (Link Layer Discovery Protocol) используется команда:

```
Admin@NGFW> show lldp <parameters>
```

Параметры фильтрации.

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

Маршруты

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

Admin@NGFW> show network route <parameters>

Параметры просмотра маршрутов.

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам NGFW. Данные маршруты помечены символом «С» в списке маршрутов
kernel	Отображение маршрутов, добавленных администратором; маршруты помечены символом «К» в списке маршрутов
summary	Количество активных подключений и записей FIB (Forwarding Information Base)
ospf	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации OSPF. Данные маршруты помечены символом «О» в списке маршрутов
bgp	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации BGP; маршруты помечены символом «В» в списке маршрутов
rip	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации RIP; маршруты помечены символом «R» в списке маршрутов
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all)

Мониторинг OSPF

Диагностика и мониторинг OSPF выполняется с помощью команд, представленных ниже. Отображение информации OSPF:

Admin@NGFW> show network ospf

...

Admin@NGFW> show network ospf <parameter>

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

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

Команда для перезапуска процесса OSPF:

Admin@NGFW> clear network ospf <parameter>

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

Мониторинг BGP

Для отображения таблиц BGP-маршрутизатора:

Admin@NGFW> show network bgp

...

Admin@NGFW> show network bgp <parameter>

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

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

Admin@nodename> clear network bgp <parameter>

Параметры команды.

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

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

Для обновления информации без обрыва сессии с соседом используется команда:

Admin@NGFW> clear network bgp ip <neighbor-ip> soft in | out

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

Мониторинг RIP

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

Admin@NGFW> show network rip

...

Admin@NGFW> show network rip <parameter>

Параметры команды.

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

Мониторинг мультикаст-трафика

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

Admin@NGFW> show network mroute

...

Admin@NGFW> show network mroute <parameter>

Параметры команды.

Параметр	Описание
count	Отображение статистики о группе и источнике

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

Мониторинг IGMP

Мониторинг работы протокола IGMP (Internet Group Management Protocol) доступен с использованием следующей команды (указание параметров является обязательным):

Admin@NGFW> show network igmp <parameters>

Параметры команды.

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

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды:

Admin@NGFW> show network pim <parameter>

Параметры команды.

Параметр	Описание
virtual-router	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию
vxlan-groups	Информация о группах VXLAN, использующихся в мультивещании
statistics	Статистика протокола
join	Отображение информации о группах PIM протокола
neighbor	Информация о соседях: - Интерфейс, через который была получена информация о соседе. - Адрес соседа. - Время, с последнего начала работы PIM. - Время, в течении которого сосед доступен. - Приоритет DR
next-hop	Записи о адресах next-hop
state	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List)
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP

Параметр	Описание
interface	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т.п. Также доступно указание параметров: - interface-name — название интерфейса. - traffic — статистика отправленных/полученных сообщений. - detail — подробная информация об интерфейсе
group-type	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Отображение системной информации

Для просмотра версии ПО системы используется команда:

```
Admin@NGFW> show system version
```

Для отображения информации о количестве активных TCP/UDP/ICMP сессий на системе используется команда:

```
Admin@NGFW> show system sessions
```

Для отображения информации о количестве активных сессий по отдельным протоколам или временным интервалам используется команда:

```
Admin@NGFW> show system sessions counters [ parameters ]
```

Очистить статистику:

```
Admin@NGFW> clear system sessions
```

Диагностика работы протоколов динамической маршрутизации

С помощью команд этого раздела можно просматривать события debug-логов протоколов динамической маршрутизации. Включение в debug-лог событий конкретного протокола выполняется командой debug в режиме конфигурации.

Для просмотра записей debug-лога используется команда:

```
Admin@NGFW> show logs log routing <parameters>
```

Далее необходимо указать один из параметров:

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

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

Просмотр системных журналов устройства

Для просмотра событий системных журналов устройства используется команда:

```
Admin@NGFW> show logs log core <static | dynamic>
```

Параметры команды (static или dynamic) определяют режим отображения сообщений журналов в консоли.

Команды режима конфигурации

В режиме конфигурации доступны команды `execute` (команды, которые не относятся к настройке конфигурации устройства — ping, date, traceroute и т.п.), базовые [команды настройки устройства](#) и [команды настройки сети](#) (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, статических ARP-записей).

Команды execute

Команды имеют следующую структуру:

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

Список команд раздела `execute`.

Команда	Описание
date	Просмотр текущих значений даты и времени на узле: Admin@NGFW# execute date
dig	Проверка записи DNS домена: Admin@NGFW# execute dig host <hostname> <parameters> Admin@NGFW# execute dig host <IP-address> <parameters> В команде можно использовать следующие параметры: - reverse-lookup — получение имени устройства по IP-адресу; - dns — указание IP-адреса DNS-сервера; - tcp — использование протокола TCP вместо UDP

Команда	Описание
factory-reset	Возврат устройства в первоначальное состояние (доступно в версии 7.5.0 и выше): <pre>Admin@NGFW# execute factory-reset</pre> Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
install	Первоначальная настройка устройства. <pre>Admin@NGFW# execute install <parameter></pre> - master — настройка устройства в качестве главного узла. Задайте логин и пароль администратора. - slave — настройка устройства в качестве дополнительного узла кластера. Укажите следующие параметры: - interface — интерфейса для подключения к кластеру; - master-ip — IP-адрес главного узла; - master-secret — секретный код, необходимый для подключения узла в кластер; - slave-ip — IP-адрес резервного узла, который будет назначен на интерфейс, используемый для подключения к кластеру. Можно указать в виде IP-адреса (например, 192.168.0.1) или в виде IP-адреса и маски подсети (например, 192.168.0.1/24). Доступно в версии 7.4.0 и выше. - gateway-address — IP-адрес шлюза. Шлюз необходимо указать, если узлы кластера находятся в разных подсетях. - mc — настройка устройства через UserGate Management Center. Укажите следующие параметры: - device-code — уникальный код устройства, используемый для подключения узла к UGMC; - mc-ip — IP-адрес UGMC; - login — задать логин администратора NGFW; - password — задать пароль учетной записи администратора NGFW
netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: - address — доменное имя узла для проверки доступности по TCP или URL — для HTTP; - dns-ip — IP-адрес сервера DNS; - dns-tcp — использование TCP вместо UDP для DNS-запроса; - check-cert — проверка SSL-сертификата; - type — проверка доступности по: - http; - tcp (если порт не указан, то используется порт 80); - data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; - timeout — максимальный тайм-аут ожидания ответа от веб-сервера; - user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. <pre>Admin@NGFW# execute netcheck type tcp address <host-domain-name> data on</pre> <pre>Admin@NGFW# execute netcheck address <host-domain-name></pre>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: - host — IP-адрес или доменное имя узла. - count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). - numeric — не определять имена. - timestamp — отображение временных меток. - interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. - ttl — время жизни пакета. - interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. - mtu — максимальный размер блока данных отправляемых пакетов. - virtual-router — имя виртуального маршрутизатора. <pre>Admin@NGFW# execute ping host <hostname> count <number></pre>
reboot	Перезагрузка устройства: <pre>Admin@NGFW# execute reboot</pre>
restore-mac	Восстановление mac-адреса интерфейса: <pre>Admin@NGFW# execute restore-mac interface <interface-name></pre>
shutdown	Выключение устройства: <pre>Admin@NGFW# execute shutdown</pre>
traceroute	Трассировка соединения до определенного узла. Параметры команды: - host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; - interface <iface-name> — интерфейс, с которого будут отправляться пакеты; - not-map-ip — не искать hostname для IP-адреса при отображении; - use-icmp-echo — использовать ICMP echo; - port — указать порт вместо порта по умолчанию (1 — 65535); - min-interval — минимальный интервал между пакетами. <pre>Admin@NGFW# execute traceroute host <hostname></pre>

Команды настройки устройства

На уровне settings cli настраиваются следующие параметры работы интерфейса командной строки:

- вид системного приглашения (prompt) консоли CLI;
- уровень детализации диагностики.

Для настройки системного приглашения консоли CLI используется команда:

```
Admin@NGFW# set settings cli custom-prompt <new-custom-prompt>
```

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида: Admin@nodename#) на удобное вам.

Например, чтобы поменять вид системного приглашения на NodeAABBCC, выполните следующую команду:

```
Admin@NGFW# set settings cli custom-prompt NodeAABBCC
```

```
NodeAABBCC#  
  
Вернуть системное приглашение в первоначальное состояние можно с помощью команды:  
  
Admin@NGFW# set settings cli custom-prompt default  
  
Пример использования команды:  
  
NodeAABBCC#  
NodeAABBCC# set settings cli custom-prompt default  
Admin@NGFW#
```

Чтобы задать уровень детализации диагностики используется следующая команда:
Admin@NGFW# set settings cli log-level <off | error | debug | warning | info>

- Вы можете установить следующие уровни детализации:
- off — отключить журналирование;
 - error — только ошибки;
 - warning — ошибки и предупреждения;
 - info — ошибки, предупреждения и дополнительная информация;
 - debug — максимальная детализация.

Посмотреть текущие значения параметров работы интерфейса командной строки можно с помощью команды:
Admin@NGFW# show settings cli

Для включения или отключения режима ускоренной обработки трафика используется команда:
Admin@NGFW# set settings fastpath enabled <on/off>

Для просмотра настройки режима ускоренной обработки трафика используется команда:
Admin@NGFW# show settings fastpath

Команды настройки сетевых параметров устройства

Настройки сетевых параметров выполняются на уровне network.

Настройка зон

Для создания зоны используется команда:
Admin@NGFW# create network zone <parameter>

Параметры настройки зон.

Параметр	Описание
name	Название зоны
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • enabled — включение/отключение защиты. • aggregate — суммирование пакетов: ◦ 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 указанный порог, происходит запись события в системный журнал. • drop-threshold — порог отбрасывания пакетов. Если количество запросов превышает указанное значение, UserGate отбрасывает пакеты и записывает это событие в системный журнал. • excluded-ips — список IP-адресов, которые необходимо исключить из защиты
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • enabled — включение/отключение защиты. • aggregate — суммирование пакетов: ◦ 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. • aggregate — суммирование пакетов: ◦ 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 ACY ТП-трафика. Необходим только при контроле ACY 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 распределенной системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределенной 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
service-addresses	Указание разрешенных IP-адресов для сервисов: - service — выбор сервисов (список соответствует enabled-services); - allowed-addresses — разрешенные адреса: - allowed-ips — указать разрешенные IP-адреса; - geoip — указать код GeoIP; - ip-list — указать заранее созданный в библиотеке элементов список IP-адресов
antispoof-enabled	Включение/отключение защиты от IP-спуфинга
antispoof-negate	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
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга

```
Для изменения параметров зоны используется команда:
Admin@nodename# set network zone <zone-name> <parameters>

Пример изменения параметров зоны:
Admin@NGFW# set network zone Test_zone dos-protection-syn enabled on

Для удаления зоны или ее параметров используется команда:
Admin@nodename# delete network zone <zone-name>

Для просмотра параметров зон используется команда:
Admin@NGFW# show network zone
```

Настройка интерфейсов

Вы можете настроить следующие типы интерфейсов:

- [bond](#);
- [bridge](#);
- [loopback](#);
- [pppoe](#);
- [tunnel](#);
- [vlan](#);
- [adapter](#).

```
Для создания bond-интерфейса используется команда:
Admin@NGFW# create network interface bond <parameters>
```

Параметры bond-интерфейса.

Параметр	Описание

Параметр	Описание
enabled	Включение/отключение интерфейса
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1)
zone	Зона, которой будет принадлежать бонд-интерфейс
bonding	Дополнительные параметры бонд-интерфейса: - mode — режим работы бонда: - 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: - 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 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: - 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 прийти до получателя не в том порядке, так как отправляются через разные интерфейсы. - interface — интерфейсы, которые будут объединены в бонд
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 следующем 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	Указание размер MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение/отключения ретранслятора. - ultm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего бонд-интерфейса используется команда:

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

Для удаления бонд-интерфейса или его параметров используется команда:

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

Параметры, доступные для удаления.

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

Чтобы просмотреть информацию о всех бонд-интерфейсах, используйте команду:

Admin@NGFW# show network interface bond

или об определенном интерфейсе:

Admin@NGFW# show network interface bond <bond-name>

Для создания bridge-интерфейса используется команда:

Admin@nodename# create network interface bridge

Параметры bridge-интерфейса.

Параметр	Описание
enabled	Включение/отключение моста
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет bridge1)
zone	Зона, которой будет принадлежать мост
bridging	Дополнительные параметры моста: - 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 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. - 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. Необходима 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 интерфейсу IP-адреса. Адрес задается 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 задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
mac	MAC-адрес интерфейса
mtu	Указание размера MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение/отключения ретранслятора. - utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего bridge-интерфейса используется команда:

Admin@NGFW# set network interface bridge <bridge-name>

Для удаления bridge-интерфейса или его параметров используется команда:

Admin@NGFW# 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

Для просмотра информации о всех bridge-интерфейсах используется команда:

Admin@NGFW# show network interface bridge

или об определенном интерфейсе:

Admin@NGFW# show network interface bridge <bridge-name>

Для создания loopback-интерфейса используется команда:

Admin@NGFW# create network interface loopback <parameters>

Параметры loopback-интерфейса.

Параметр	Описание
enabled	Включение/отключение интерфейса
interface-name	Название интерфейса
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задается в следующем виде: [<ip_address/mask>], маска подсети задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
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

Параметр	Описание
zone	Зона, которой будет принадлежать интерфейс
mac	MAC-адрес интерфейса
mtu	Указание размера MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение/отключения ретранслятора. - utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения < ip none>). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего интерфейса используется команда:

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

Для удаления loopback-интерфейса или его параметров используется команда:

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

Параметры, доступные для удаления.

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

Для просмотра информации о всех loopback-интерфейсах используется команда:

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

Об определенном интерфейсе:

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

Для создания интерфейса PPPoE используется команда:

```
Admin@NGFW# create network interface pppoe
```

Параметры PPPoE-интерфейса.

Параметр	Описание
enabled	Включение/отключение интерфейса PPPoE
interface-name	Необходимо ввести номер, который будет отображен в имени интерфейса (например, 1, тогда название созданного интерфейса будет ppp1)
zone	Зона, которой будет принадлежать интерфейс
config	Дополнительные параметры PPPoE интерфейса: - interface — интерфейс, на котором будет создаваться интерфейс PPPoE; - 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 — интерфейс PPPoE в качестве маршрута по умолчанию; - echo-interval — интервал проверки соединения; - echo-failure — количество неуспешных проверок соединения, после которого NGFW считает, что соединение отсутствует и разрывает его; - providers-dns — использование DNS-серверов, выданных провайдером; - connection-attempts — количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены; - service-name — имя сервиса необходимо прописывать в случае предоставления провайдером
mtu	Указание размера MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet

Для изменения существующего интерфейса PPPoE используется команда:

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

Для удаления интерфейса PPPoE используется команда:

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

Для просмотра информации о всех интерфейсах PPPoE используется команда:

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

Об определенном интерфейсе:

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

Для создания туннелей используется команда:

```
Admin@NGFW# create network interface tunnel
```

Параметры туннеля.

Параметр	Описание
enabled	Включение/отключение туннеля
interface-number	Необходимо ввести номер, который будет отображен в названии туннеля (например, 1, тогда название созданного интерфейса будет gre1)

Параметр	Описание
zone	Зона, которой будет принадлежать интерфейс
mtu	Размер MTU для выбранного интерфейса
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. Адрес задается 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 задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
tunnel-config	Дополнительные параметры настройки туннеля: - local-ip — локальный адрес Point-to-Point интерфейса; - remote-ip — удаленный адрес Point-to-Point интерфейса; - iface-mode — режим работы туннеля: - gre — GRE (протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47). - ipip — IPIP (протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP-пакета в другой IP-пакет, это добавление внешнего заголовка с Source IP — точкой входа в туннель, и Destination — точкой выхода из туннеля). - vxlan — VXLAN (протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789). - vxlan-id — Идентификатор VXLAN. Только для типа туннеля VXLAN

Для изменения параметров существующего туннеля используется команда:

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

Для удаления интерфейса туннель или его параметров используется команда:

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

Для просмотра информации о всех туннелях используется команда:

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

Об определенном интерфейсе:

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

Для создания нового VLAN-интерфейса используется команда:

```
Admin@NGFW# create network interface vlan <parameters>
```

Параметры VLAN-интерфейса.

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса
iface-type	Тип интерфейса: - 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: - 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
interface	Физический интерфейс, на котором создается VLAN
zone	Зона, которой будет принадлежать интерфейс
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задается 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 задается в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон
mac	MAC-адрес интерфейса
mtu	Указание размера MTU
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение/отключения ретранслятора. - utm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора. - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для изменения параметров существующего VLAN-интерфейса используется команда:

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

Для удаления VLAN-интерфейса или его параметров используется команда:

```
Admin@NGFW# 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

Для просмотра информации о всех VLAN-интерфейсах используется команда :

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

Об определенном интерфейсе:

Admin@NGFW# show network interface vlan <vlan-name>

Настройка сетевых адаптеров

Сетевые адаптеры создать нельзя, но вы можете настраивать параметры сетевых адаптеров устройства с помощью следующей команды:

Admin@NGFW# set network interface adapter <adapter-name>

Параметры сетевых адаптеров.

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса
iface-type	Тип интерфейса: - i3 — 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: - 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
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
rx-ring	Размер буфера RX ring интерфейса типа adapter
tx-ring	Размер буфера TX ring интерфейса типа adapter
dhcp-relay	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо указать: - enabled — включение/отключения ретранслятора. - ultm-address — IP-адрес интерфейса устройства, на который добавляется функция ретранслятора (принимает значения <ip none>). - server-address — адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов

Для удаления параметров адаптеров используется команда:

Admin@NGFW# delete network interface adapter <adapter-name> <parameters>

Параметры, доступные для удаления.

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

Для просмотра параметров сетевых адаптеров используется команда:

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

Настройка шлюзов

Для создания шлюза используется команда:

Admin@NGFW# create network gateway <parameters>

Параметры шлюза.

Параметр	Описание
enabled	Включение/отключение шлюза
interface	Интерфейс, используемый для выхода в Интернет: - port — выбор конкретного порта (port0, port1, port2 и т. д.); - auto — после выбора этого параметра порт определится автоматически. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0
virtual-router	Виртуальный маршрутизатор, для которого настраивается шлюз
ip	IP-адрес шлюза
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз)
balancing	Включение режима балансировки — весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами
default	Использование данного шлюза в качестве шлюза по умолчанию

Для изменения параметров шлюза используется команда:

Admin@NGFW# set network gateway <gateway-name>

Для удаления шлюза используется команда:

Admin@NGFW# delete network gateway <gateway-name>

Для просмотра информации о всех шлюзах используется команда:

Admin@NGFW# show network gateway

Об определенном шлюзе:

```
Admin@NGFW# show network gateway <gateway-name>
```

Настройка виртуальных маршрутизаторов

Для создания виртуального маршрутизатора используется команда:

```
Admin@NGFW# create network virtual-router <parameters>
```

Параметры виртуального маршрутизатора.

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора
interfaces	Интерфейсы, которые будут использованы в 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
routes	Добавление статических маршрутов. - destination-ip — IP-адрес подсети назначения. Указывается в формате <ip/mask>. - 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. - enabled — включение/отключение использования статического маршрута. - gateway — IP-адрес шлюза, через который будет доступна указанная подсеть. Этот IP-адрес должен быть доступен с устройства. - metric — метрика маршрута. Маршрут с меньшей метрикой более приоритетен

Для изменения параметров виртуального маршрутизатора используется команда:

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

Для удаления виртуального маршрутизатора или его параметров используется команда:

```
Admin@NGFW# delete network virtual-router <virtual-router-name> <parameters>
```

Для просмотра информации о всех виртуальных маршрутизаторах используется команда:

```
Admin@NGFW# show network virtual-router
```

Об определенном виртуальном маршрутизаторе:

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

Статические ARP-записи

Для добавления статических ARP-записей используется команда:

```
Admin@NGFW# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

Параметры статических ARP-записей.

Параметр	Описание
interface	Название интерфейса NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

Для удаления статических ARP-записей используется команда:

```
Admin@NGFW# delete network arp host <host-ip-address> interfaces [ port1 port2 ]
```

Журналирование событий протоколов маршрутизации

Команда debug позволяет включить журналирование событий протоколов маршрутизации в режиме отладки. События записываются в debug-журнал. Их просмотр также возможен в режиме диагностики консоли CLI.

Для включения журналирования конкретного протокола маршрутизации используется команда:

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

Поддерживаются следующие протоколы:

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

Первоначальная инициализация NGFW

Documentation: 
Product: NGFW
Version: 7.x

При первоначальной инициализации UserGate NGFW в интерфейсе командной строки доступны три режима конфигурации:

- Автономный (главный) узел.
- Дополнительный узел кластера.
- Управление через UserGate Management Center.

Автономный узел

Для настройки UserGate NGFW в качестве автономного узла используется команда:

Admin@nodename# execute install master login <login-name> password <password>

Необходимо задать логин и пароль администратора устройства.

Дополнительный узел кластера

Для настройки UserGate NGFW в качестве дополнительного узла кластера используется команда:

Admin@nodename# execute install slave <parameters>

Укажите дополнительные параметры настройки.

Параметр	Описание
interface	Интерфейс для подключения к кластеру
slave-ip	IP-адрес резервного узла, который будет назначен на интерфейс, использующийся для подключения к кластеру. Возможные опции: - ip — IP-адрес (например, 192.168.0.1); - ip/mask — IP-адрес и маска подсети (например, 192.168.0.1/24). Доступно в версии 7.4.0 и выше
gateway-address	IP-адрес шлюза. Шлюз необходимо указывать, если узлы кластера находятся в разных подсетях
master-ip	IP-адрес мастер-сервера
master-secret	Секретный код, использующийся для подключения узла в кластер
login	Логин администратора UserGate NGFW. Начиная с версии 7.3.0 логин указывать не нужно
password	Пароль учетной записи администратора. Начиная с версии 7.3.0 пароль указывать не нужно

Управление через UserGate Management Center

Для настройки UserGate NGFW с помощью UGMC используется команда:

Admin@nodename# execute install mc <parameters>

Укажите дополнительные параметры настройки.

Параметр	Описание
login	Логин администратора NGFW
password	Пароль учетной записи администратора
mc-ip	IP-адрес сервера UGMC
device-code	Уникальный код устройства, использующийся для подключения узла к UGMC

Мастер первоначальной настройки узла

Product: NGFW
Version: 7.x

Мастер первоначальной настройки (доступен в версии 7.5.0 и выше) позволяет в диалоговом режиме запустить установку UserGate NGFW в качестве автономного (главного) узла, задать логин и пароль учетной записи корневого администратора, выбрать язык веб-интерфейса и установить IP-адрес интерфейса port0 для подключения к веб-консоли управления.

Чтобы запустить мастер первоначальной настройки:

- 1. Подключитесь к консоли устройства с помощью монитора и клавиатуры (при наличии соответствующих портов на устройстве) или с помощью эмулятора терминала через консольный порт.
- 2. Войдите в интерфейс командной строки, указав логин и пароль администратора, используемые по умолчанию.

UGOS login: Admin
Password: usergate
Admin@NGFW>

- 3. Перейдите в режим конфигурации интерфейса командной строки.

Admin@NGFW> configure
Admin@NGFW#

- 4. Запустите мастер первоначальной настройки узла с помощью команды:

Admin@NGFW# execute install master login <admin-login> password <admin-password> language <en | ru>

В команде запуска первоначальной настройки узла вы можете назначить новый логин и пароль корневого администратора и установить язык по умолчанию для веб-консоли устройства.

После запуска мастер первоначальной настройки предложит прочитать и принять условия лицензионного соглашения. Если условия лицензионного соглашения приняты, будет запущен процесс установки устройства в качестве автономного узла NGFW. В процессе установки устройство запустит процедуру получения IP-адреса интерфейса port0 по протоколу DHCP.

Admin@NGFW# execute install master login Admin password usergate language ru
Вы должны принять условия лицензионного соглашения, чтобы продолжить. Прочитать условия соглашения сейчас? [Y/n] y

USERGATE

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ

....

....

Продолжая, вы принимаете условия лицензионного соглашения. Хотите продолжить? [Y/n] y
Установка началась. Пожалуйста, подождите
IP-адрес для Port0 192.168.56.252. Используйте этот IP-адрес для доступа к веб-консоли через браузер.
Пожалуйста, сохраните этот IP-адрес, так как это окно будет перезагружено. Хотите продолжить? [Y/n] y

Installation completed successfully

Если IP-адрес не получен (например, в сегменте сети отсутствует DHCP-сервер), будет предложено ввести IP-адрес с маской подсети вручную в формате ip-address/mask (например, 192.168.0.1/24).

После успешного завершения первичной установки вы можете продолжить настройку устройства в интерфейсе командной строки или подключиться к веб-консоли управления для продолжения настройки устройства.

Команды диагностики и мониторинга (Описание)

Product: NGFW
Version: 7.x

С помощью команд режима диагностики CLI вы можете просматривать информацию о системе, выполнять базовые команды управления системой, получать информацию о доступности сетевого окружения, выполнять мониторинг трафика по заданным параметрам.

Базовые команды управления

Для перезагрузки узла:

Admin@nodename> reboot

Для выключения узла:

Admin@nodename> shutdown

Для перехода в режим конфигурации CLI:

Admin@nodename> configure

Для выхода из интерфейса CLI:

Admin@nodename> exit

Команды просмотра системной информации

Для просмотра версии ПО системы:

Admin@nodename> show system version

Для просмотра количества активных сессий TCP/UDP/ICMP:

Admin@nodename> show system sessions

Для просмотра количества активных сессий по отдельным протоколам или временным интервалам:

Admin@nodename> show system sessions counters [parameters]

Для очистки статистики:

Admin@nodename> clear system sessions

Для просмотра текущих даты и времени на узле:

Admin@nodename> date

Команды мониторинга состояния системы

Команды мониторинга позволяют отображать состояние компонентов системы в виде временных диаграмм (доступны в версии 7.5.0 и выше).

С помощью команды show monitoring <parameters> вы можете получить информацию о состоянии процессора, дисковой подсистемы, интерфейсов, оперативной памяти, RAID-массива, просматривать статистику по рабочей температуре устройства и по DNS- и HTTP-запросам. Например:

При использовании команды без аргументов будет последовательно выведено состояние всех системных объектов мониторинга:

Admin@nodename> show monitoring

С помощью аргументов команды вы можете выводить информацию о каждом объекте мониторинга по отдельности.

Для мониторинга загрузки процессора:

Admin@nodename> show monitoring cpu

Для мониторинга состояния файловой системы:

Admin@nodename> show monitoring disk-info

Для мониторинга состояния RAID-массива:

Admin@nodename> show monitoring raid

Для мониторинга загрузки дисковой подсистемы операциями ввода/вывода:

Admin@nodename> show monitoring disk-io

Для мониторинга загрузки swap-раздела:

Admin@nodename> show monitoring swap

Для мониторинга загрузки интерфейсов:

Admin@nodename> show monitoring interface <port-name>

Для мониторинга загрузки оперативной памяти:

Admin@nodename> show monitoring memory

Для мониторинга рабочей температуры устройства:

Admin@nodename> show monitoring temperature

Для мониторинга состояния источников питания:

Admin@nodename> show monitoring power-supply

Для мониторинга статистики DNS-запросов:

Admin@nodename> show monitoring dns-requests

Для мониторинга статистики HTTP-запросов:

Admin@nodename> show monitoring http-requests

Команды просмотра информации об интерфейсах

Для просмотра информации обо всех имеющихся в системе интерфейсах используйте команду:

Admin@nodename> show network interface

Вы можете просмотреть статистику и подробную информацию об определенном интерфейсе. Для этого необходимо указать в команде его название:

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

Также вы можете вывести отдельно информацию об интерфейсе либо статистику интерфейса:

```
Admin@nodename> show network interface <interface-name> type info
Admin@nodename> show network interface <interface-name> type statistics
```

Для просмотра списка упорядоченных имен сетевых интерфейсов и соответствующих им физических адресов используйте команду:

```
Admin@nodename> show network interface-mapping
```

ПримечаниеПод физическими адресами подразумеваются реальные аппаратные адреса сетевых карт ПАК или адреса интерфейсов, назначаемые системой виртуализации. При использовании этой команды не отображаются изменения MAC-адресов в параметрах UserGate NGFW. Измененные MAC-адреса можно посмотреть с помощью команды show network interface <interface-name>.

Сортировка интерфейсов выполняется по номеру порта PCI-шины.

Для удаления списка используйте команду:

```
Admin@nodename> clear network interface-mapping
```

После перезагрузки устройства список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов на настроенном устройстве UserGate.

Команды проверки доступности сетевых ресурсов

Для проверки доступности узла с помощью утилиты ping используйте команду:

```
Admin@nodename> ping <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
host	IP-адрес или доменное имя узла
count	Количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет продолжаться, пока соединение не будет прервано пользователем. Чтобы прервать отправку запросов, используйте комбинацию клавиш Ctrl + C
interface	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для отправки echo-запросов
interval	Интервал времени, определяющий частоту отправки пакетов. Указывается в секундах
mtu	Размер MTU отправляемых пакетов
numeric	Не определять имя узла
ttl	Время жизни пакета
timestamp	Отображение временных меток
virtual-router	Имя виртуального маршрутизатора

Для трассировки соединения до определенного узла используйте команду:

```
Admin@nodename> traceroute <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
host	IP-адрес или доменное имя узла, для которого выполняется трассировка
interface	Интерфейс, с которого будут отправляться пакеты
min-interval	Минимальный интервал между отправкой пакетов
not-map-ip	Не искать имя узла для IP-адреса при отображении
port	Указать порт вместо порта по умолчанию (1-65535)
use-icmp-echo	Использовать ICMP-echo

Для проверки доступности удаленного HTTP/HTTPS-сервера используйте команду:

```
Admin@nodename> netcheck <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
address	Адрес или имя узла для проверки доступности: - доменное имя узла для проверки доступности по TCP; - URL для проверки доступности по HTTP; - IP-адрес с портом для проверки по TCP (в этом случае в параметре type необходимо указать tcp)
type	Протокол для проверки доступности узла: - http; - tcp (если порт не указан, используется порт 80)
check-cert	Проверка SSL-сертификата
dns-ip	IP-адрес DNS-сервера
dns-tcp	Использование TCP вместо UDP для DNS-запроса
data	Запрос содержимого сайта. По умолчанию запрашиваются только заголовки
timeout	Максимальный тайм-аут ожидания ответа от веб-сервера
user-agent	Параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только через определенные браузеры. Значение параметра указывается в двойных кавычках

Для проверки записи DNS-домена используйте команду:

```
Admin@nodename> dig <parameters>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
host	Доменное имя узла или IP-адрес для реверсивного поиска
dns	Указание IP-адреса DNS-сервера
reverse-lookup	Получение имени узла по IP-адресу
tcp	Использование протокола TCP вместо UDP

Для проверки принадлежности IP-адреса по текущей базе GeoIP используйте команду:

```
Admin@nodename> check-geoip ip <IP-address>
```

Команды управления ARP-записями

Для просмотра информации о динамических ARP-записях используйте команду:

```
Admin@nodename> show network arp
```

При просмотре записей вы можете использовать дополнительные фильтры.

Параметр	Описание
node-name	Название узла кластера, ARP-записи которого необходимо отобразить. Далее необходимо указать интерфейс или IP-адрес узла: Admin@nodename> show network arp node-name <node-name> interface <iface-name> Admin@nodename> show network arp node-name <node-name> host <ip>
interface	Название интерфейса UserGate NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

```
Admin@nodename> show network arp host <IP-address>
Admin@nodename> show network arp interface <interface-name>
Admin@nodename> show network arp mac <MAC-address>
```

ARP-записи также можно просматривать в режиме конфигурации CLI. Команды просмотра в режиме конфигурации идентичны командам режима диагностики.

ПримечаниеВ режиме диагностики действия выполняются с системными (динамическими) ARP-записями; в режиме конфигурации — со статическими.

Вы можете добавлять статические ARP-записи в режиме конфигурации с помощью команды:

```
Admin@nodename# set network arp host <IP-address> interface <interface-name> mac <MAC-address>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP- и MAC-адреса устройства
interface	Название интерфейса UserGate NGFW
host	IP-адрес устройства
mac	MAC-адрес устройства

Команды удаления системных и статических ARP-записей имеют аналогичную структуру, отличается действие, которое необходимо выполнить:

- clear — удаление системных записей в режиме диагностики;
- delete — удаление статических записей в режиме конфигурации.

Для удаления системной ARP-записи используйте команду:

```
Admin@nodename> clear network arp interface <iface-name> host <ip>
```

Чтобы удалить запись на другом узле кластера:

```
Admin@nodename> clear network arp interface <iface-name> node-name <node-name> host <ip>
```

Чтобы удалить все системные записи на заданном интерфейсе:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> ... ]
```

Для удаления всех системных записей интерфейса другого узла:

```
Admin@nodename> clear network arp interfaces [ <iface-name1> <iface-name2> ... ] node-name <node-name>
```

Команды отслеживания пакетов

В режиме диагностики CLI вы можете отслеживать сетевые пакеты с помощью команды:

```
Admin@nodename> show network trace
```

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации CLI на уровне network. Подробнее — в разделе «[Настройка устройства](#)».

В выводе команды отслеживания пакетов будет отображаться следующая информация:

- IP-адреса источника и назначения;
- сетевой протокол;
- названия портов источника и назначения;
- номера TCP/UDP-портов источника и назначения.

Команда отслеживания пакетов также доступна в режиме конфигурации.

Для выхода из режима отслеживания пакетов используйте комбинацию клавиш Ctrl + C.

Команды мониторинга трафика

Для мониторинга трафика используйте команду:

```
Admin@nodename> show traffic
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
flows	Отображение информации о входящем и исходящем потоках. Вы можете установить фильтрацию по параметрам: - source-ip — IP-адрес источника; - source-port — порт источника; - dest-ip — IP-адрес назначения; - dest-port — порт назначения; - vlan-tag — ter VLAN; - interface-name — название интерфейса; - node-name — название узла; - protocol —протокол
connections	Отображение информации о соединениях. Вы можете установить фильтрацию по параметрам: - protocol — протокол; - source-ip — IP-адрес источника; - dest-ip — IP-адрес назначения; - node-name — название узла; - expect — отображение неустановленных соединений
capture	Отображение захвата пакетов. Вы можете установить фильтрацию по параметрам: - count — количество захватываемых пакетов. Значение по умолчанию — 1000. Для захвата без ограничения количества пакетов явно укажите: count unlimited . Опция доступна в версии ПО 7.3.0 и выше. - destination — IP-адрес назначения. - destination-port — порт назначения. - ipv4-protocol — номер протокола IPv4 (0-255). - interfaces — название интерфейса. - protocol — выбор протокола. - rule — выбор имеющегося правила для захвата пакетов. - source — IP-адрес источника. - source-port — порт источника

Пример команды мониторинга трафика:

Admin@nodename> show traffic connections node-name utmcore@dineanoulwer dest-ip 192.168.0.100 expect on

Команды просмотра LLDP

Вы можете просматривать информацию о сетевом окружении, полученную по LLDP (Link Layer Discovery Protocol) с помощью команды:

Admin@nodename> show lldp <parameters>

В команде могут быть указаны дополнительные параметры.

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

ПримечаниеДля просмотра информации, полученной по LLDP, сервис LLDP должен быть активирован на UserGate NGFW: профили LLDP должны быть настроены [в библиотеке элементов](#) и активированы [в настройках интерфейсов](#).

Мониторинг работы протоколов маршрутизации

С помощью команд этого раздела вы можете выполнять мониторинг работы протоколов маршрутизации, настроенных на UserGate NGFW.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используйте команду:

Admin@nodename> show network route

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить
node-name	Выбор узла кластера

Параметр	Описание
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate NGFW. Такие маршруты помечены символом « C» в списке маршрутов
kernel	Маршруты, добавленные администратором. Маршруты помечены символом « K» в списке маршрутов
summary	Количество активных подключений и записей FIB (Forwarding Information Base)
ospf	Маршруты, полученные с помощью протокола динамической маршрутизации OSPF. Такие маршруты помечены символом « O» в списке маршрутов
bgp	Маршруты, полученные с помощью протокола динамической маршрутизации BGP. Такие маршруты помечены символом « B» в списке маршрутов
rip	Маршруты, полученные с помощью протокола динамической маршрутизации RIP. Маршруты помечены символом «R» в списке маршрутов
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all)

Мониторинг OSPF

С помощью команд этого раздела вы можете выполнять диагностику протокола OSPF.

Для просмотра информации протокола OSPF используйте команду:

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

В команде могут быть указаны дополнительные параметры.

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

Для перезапуска процесса OSPF используйте команду:

```
Admin@nodename> clear network ospf <parameter>
```

В команде могут быть указаны дополнительные параметры.

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

Мониторинг BGP

С помощью команд этого раздела вы можете выполнять диагностику протокола BGP.

Для просмотра таблиц BGP-маршрутизатора используйте команду:

```
Admin@nodename> show network bgp
```

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

В команде могут быть указаны дополнительные параметры.

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

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

Admin@nodename> clear network bgp

В команде могут быть указаны дополнительные параметры.

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

Если на соседних устройствах поддерживается метод Route Refresh, вы можете избежать полной реинициализации сессии с соседом. Для этого необходимо отправить специальное сообщения **ROUTE REFRESH**, позволяющее обновить информацию без прерывания работы маршрутизации.

Для обновления информации без обрыва сессии с соседом используйте команду:

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

Мониторинг RIP

С помощью команд этого раздела вы можете выполнять диагностику протокола RIP.

Для просмотра информации протокола RIP из таблицы маршрутизатора по умолчанию используйте команду:

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

В команде могут быть указаны дополнительные параметры.

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

Мониторинг мультикаст-трафика

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

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

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера
count	Отображение статистики о группе и источнике
virtual-router	Выбор виртуального маршрутизатора (<vrf-name> all)
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации
fill	Таблица маршрутизации мультикаст-трафика
ip	Отображение записи для определенного IP-адреса

Мониторинг IGMP

Для мониторинга работы протокола IGMP (Internet Group Management Protocol) используйте команду:

Admin@nodename> show network igmp <parameters>

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера

Параметр	Описание
virtual-router	Выбор виртуального маршрутизатора
statistics	Статистика по сообщениям: - IGMP Membership Query — сообщение от сервера к клиенту с директивой обновить подписку на получаемые клиентом группы. Без обновления сервер перестанет вещать группы в данном сегменте сети. - IGMP Leave — сообщение от клиента к серверу с запросом убрать мультикаст-группу из списка получаемых. - IGMP Membership Report — сообщение от клиента к серверу с запросом получать трафик этой группы
join	Отображение информации о группах IGMP
sources	Отображение информации об источниках мультикаст-трафика
groups	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: - общее количество групп; - интерфейс, через который группа доступна; - адрес группы; - режим INCLUDE или EXCLUDE; - таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report; - время, в течение которого группа известна
interface	Отображение информации об интерфейсе, связанном с мультикаст-маршрутизацией: - название интерфейса, его статус и адрес; - версия IGMP; - опрашиватель (IGMP querier) и его адрес; - таймер, который обнуляется каждый раз, когда приходит сообщение Query с меньшим IP-адресом. Дополнительные параметры: - interface-name — название интерфейса; - detail — подробная информация об интерфейсе

Мониторинг PIM

Для мониторинга работы протокола PIM (Protocol-Independent Multicast) используйте команду:

```
Admin@ndename> show network pim <parameter>
```

В команде могут быть указаны дополнительные параметры.

Параметр	Описание
node-name	Выбор узла кластера, для которого необходимо отобразить информацию
virtual-router	Выбор виртуального маршрутизатора, для которого необходимо отобразить информацию
vxlان-groups	Информация о группах VXLAN, использующихся в мультивещании
statistics	Статистика протокола
join	Отображение информации о группах протокола PIM
neighbor	Информация о соседях: - интерфейс, через который была получена информация о соседе; - адрес соседа; - время, прошедшее с последнего начала работы PIM; - время, в течение которого сосед доступен; - приоритет DR
next-hop	Записи об адресах next-hop
state	Информация об известных S, G маршрутах, Incoming Interface (IIF), Outgoing Interface List (OIL)
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешенные ASM группы с данного RP
interface	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т. п. Дополнительные параметры: - interface-name — название интерфейса; - traffic — Статистика отправленных и полученных сообщений; - detail — подробная информация об интерфейсе
group-type	Список разрешенных групповых адресов для SSM (Source Specific Multicast)
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса

Команды мониторинга состояния кластера

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

Для мониторинга состояния кластера используйте команду:

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

Для мониторинга состояния узлов кластера используйте команду:

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

Для просмотра информации об истории переключения состояния кластера используйте команду:

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

Команды управления заблокированными COB IP-адресами

Для просмотра таблицы с заблокированными системой COB IP-адресами используйте команду:

Admin@nodename> show blocked-ip

Для разблокирования отдельных IP-адресов используйте команду:

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

Команды управления VPN-сессиями

Блок команд доступен в версии 7.5.1 и выше.

Для просмотра активных VPN-сессий используется команда:

Admin@nodename> show vpn-sessions

Команда для принудительного завершения активных VPN-сессий:

Admin@nodename> clear vpn-sessions <remote-access | site-to-site> [session1 session2 ...]

В некоторых случаях требуется оперативная блокировка доступа пользователей к VPN-серверу. Команда для добавления локальных пользователей в список заблокированных:

Admin@nodename> block-vpn-user users [user_name1 user_name2 ...]

Команда для добавления доменных пользователей в список заблокированных:

Admin@nodename> block-vpn-user ldap-users connector "Connector name" users [donain\user_name1 domain\user_name2 ...]

Команда для просмотра списка заблокированных пользователей VPN:

Admin@nodename> show blocked-vpn-users

Команда для удаления пользователей из списка заблокированных:

Admin@nodename> clear blocked-vpn-users users [user_name1 user_name2 ...]

Команды просмотра журналов диагностики

С помощью команд этого раздела вы можете просматривать события, содержащиеся в журналах диагностики системы, в статическом и динамическом режиме.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

Admin@nodename> show logs log core static | grep ldap

Подробнее о функции фильтрации вывода — в разделе «[Общие положения](#)».

Просмотр системного журнала диагностики

Для вывода всего системного журнала диагностики в консоль используйте команду:

Admin@nodename> show logs log core static

Для вывода событий системного журнала диагностики в консоль в реальном времени используйте команду:

Admin@nodename> show logs log core dynamic

Для отключения вывода событий журнала используйте комбинацию клавиш Ctrl + C.

Просмотр журналов диагностики протоколов маршрутизации

С помощью команд этого раздела вы можете просматривать события журналов диагностики протоколов маршрутизации. Включение в журналы событий выбранного протокола выполняется командой debug в режиме конфигурации (подробнее — в разделе «[Режим конфигурации](#)»).

Для вывода событий журнала диагностики в консоль используется команда вида:

Admin@nodename> show logs log routing <parameters> <static|dynamic>

В команде необходимо указать протоколы, для которых будут выводиться события диагностики.

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

Для вывода всего журнала диагностики в консоль используйте команду:

Admin@nodename> show logs log routing <parameters> static

Для вывода событий журнала диагностики в консоль в реальном времени используйте команду:

Admin@nodename> show logs log routing <parameters> dynamic

Параметры команд аналогичны параметрам, указанным ранее.

Для отключения вывода событий журнала используйте комбинацию клавиш Ctrl + C.

Просмотр журналов диагностики VPN-сервера

С помощью команд этого раздела вы можете просматривать события журналов диагностики VPN-сервера и VPN-клиента (когда UserGate NGFW выступает в роли узла-инициатора соединения в сценарии Site-to-site VPN).

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

Admin@nodename> show logs log vpn-server static

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

Admin@nodename> show logs log vpn-server dynamic

Для вывода всего журнала диагностики VPN-сервера, работающего в режиме инициатора соединения в сценарии Site-to-site VPN, используйте команду:

Admin@nodename> show logs log vpn-client static

Для вывода событий журнала диагностики VPN-сервера, работающего в режиме инициатора соединения в сценарии Site-to-site VPN, в реальном времени используйте команду:

Admin@nodename> show logs log vpn-client dynamic

Для отключения вывода событий журнала используйте комбинацию клавиш Ctrl + C.

Просмотр информации об авторизованных пользователях

Для просмотра информации обо всех авторизованных пользователях используйте команду:

Admin@nodename> show user-auth

Для просмотра деталей сессии определенного пользователя используйте команду:

Admin@nodename> show user-auth <parameter>

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

Для удаления сессии определенного пользователя используйте команду:

Admin@nodename> clear user-auth <parameter>

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

Documentation: 
Product: NGFW
Version: 7.x

Для перехода в режим конфигурации интерфейса командной строки используется команда:

Admin@nodename> configure

В режиме конфигурации приглашение командной строки будет выглядеть следующим образом:

Admin@nodename#

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

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

Где:

<action> — действие, которое необходимо выполнить;

<level> — уровень контекста конфигурации, который соответствует одному из разделов структуры конфигурации в веб-интерфейсе NGFW;

<filter> — идентификатор объекта, к которому происходит обращение;

<configuration_info> — значение параметров, которые необходимо применить к объекту.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: - execute — выполнение команд, которые не относятся к текущей конфигурации устройства (ping, date, traceroute и т. п.) Команда доступна независимо от уровня конфигурации. Подробнее — в разделе «Команды execute». - create — создание новых объектов. - set — изменение параметров объектов, включение различных параметров. - show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено все, что находится глубже текущего уровня. - delete — удаление объекта или параметра из списка параметров. - edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображен под командной строкой. - end — переход на один уровень конфигурации выше. - top — возврат на самый верхний уровень конфигурации. - export — экспорт сертификатов. Подробнее — в разделе «Команды export». - import — импорт конфигурации. Подробнее — в разделе «Команды import». - debug — включение журналирования событий протоколов динамической маршрутизации в режиме отладки. Подробнее — в разделе «Команды debug». - exit — выход из режима конфигурации. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображен под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show</pre> <pre>adapter: port0 interface-name : port0 node-name : ulmcore@dineanoulwer zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp</pre> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end два раза: <pre>Admin@nodename# Level: network interface Admin@nodename# end Level: network Admin@nodename# end Admin@nodename#</pre> Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду top: <pre>Admin@nodename# Level: network interface Admin@nodename# top Admin@nodename#</pre>
<level>	Уровни контекста конфигурации в командной строке повторяют разделы конфигурации в веб-интерфейсе UserGate NGFW: - settings — соответствует разделу веб-интерфейса «UserGate»; - users — соответствует разделу веб-интерфейса «Пользователи и устройства»; - network — соответствует разделу веб-интерфейса «Сеть»; - network-policy — соответствует разделу веб-интерфейса «Политики сети»; - security-policy — соответствует разделу веб-интерфейса «Политики безопасности»; - vpn — соответствует разделу веб-интерфейса «VPN»; - global-portal — соответствует разделу веб-интерфейса «Глобальный портал»; - libraries — соответствует разделу веб-интерфейса «Библиотеки»; - monitoring — соответствует разделу веб-интерфейса «Диагностика и мониторинг»

Наименование	Описание
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать параметры(<configuration_info>). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках. Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду: <pre>Admin@nodename# show network interface adapter port0</pre> Будет отображена информация об интерфейсе port0 текущего узла NGFW. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла: <pre>Admin@nodename# show network interface adapter (node-name another_nodename interface port0)</pre> Важно! Круглые скобки должны быть отделены пробелами с обеих сторон
<configuration_info>	Указание параметра с аргументом. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать группу с именем VPN users: <pre>Admin@nodename# create users group "VPN users"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра. Параметры записываются в квадратных скобках и разделяются пробелами. Например, необходимо в группу VPN users добавить пользователей user1 и user2. Параметру users необходимо задать аргумент [user1 user2]: <pre>Admin@nodename# set users group "VPN users" users [user1 user2]</pre> Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон

Команды execute

Команды имеют следующую структуру:

Admin@nodename# execute <command-name>

Список команд раздела execute.

Команда	Описание
cache	Очистка кэша LDAP-записей: <pre>Admin@nodename# execute cache ldap-clear</pre>
check-geoip	Проверка географической принадлежности IP-адреса по текущей базе GeoIP: <pre>Admin@nodename# execute check-geoip ip <ip-address></pre>
clear-cli-history	Удаление истории команд интерфейса CLI (доступно в версии 7.5.0 и выше). Можно удалить историю всех введенных команд интерфейса CLI или только команд в одном из режимов работы интерфейса (в режиме конфигурации или в режиме диагностики): <pre>Admin@nodename# execute clear-cli-history Admin@nodename# execute clear-cli-history modes [<configure diagnostic>]</pre>
configure-cluster	Генерация секретного кода, необходимого для добавления нового узла в кластер конфигурации: <pre>Admin@nodename# execute configure-cluster generate-secret-key <parameter></pre> Где: - secret — ключ для генерации секретного кода в формате [0-9a-zA-Z]+#[0-9a-zA-Z]+ (например, example#key); - expiration-time — срок действия кода в секундах; - request-limit — срок действия запроса на генерацию кода. Важно! Для использования этой команды необходимо наличие лицензии на модуль Cluster
date	Просмотр текущих значений даты и времени на узле: <pre>Admin@nodename# execute date</pre>
dig	Проверка записи DNS домена: <pre>Admin@nodename# execute dig host <hostname> <parameters> Admin@nodename# execute dig host <IP-address> <parameters></pre> В команде можно использовать следующие параметры: - reverse-lookup — получение имени устройства по IP-адресу; - dns — указание IP-адреса DNS-сервера; - tcp — использование протокола TCP вместо UDP.
factory-reset	Возврат устройства в первоначальное состояние (доступно в версии 7.5.0 и выше): <pre>Admin@nodename# execute factory-reset</pre> Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды
firewall	Применение всех правил межсетевого экрана с обрывом текущих сессий: <pre>Admin@nodename# execute firewall force-changes</pre>
license	Команда регистрации продукта имеет следующую структуру: <pre>Admin@nodename# execute license activate <pin-code></pre> В качестве <pin-code> укажите код активации продукта
logs	Команда разовой отправки журналов по имеющемуся правилу экспорта журналов: <pre>Admin@nodename# execute logs send-once <export-log-name></pre>
mc-force-disconnect	Команда аварийного отключения узла от MC, с которым он был интегрирован. В зависимости от выбранного аргумента импортированные из MC объекты сохраняются локально или удаляются: - keep — отключение от MC с сохранением всех импортированных из MC объектов (библиотеки, правила и т. д.). Импортированные из MC объекты конвертируются в локальные. - delete — отключение от MC с удалением всех импортированных из MC объектов (библиотеки, правила и т. д.). Импортированные объекты, которые в настоящий момент используются, конвертируются в локальные. <pre>Admin@nodename# execute mc-force-disconnect keep Admin@nodename# execute mc-force-disconnect delete</pre>

Команда	Описание
netcheck	Проверка доступности стороннего HTTP или HTTPS-сервера. Могут быть использованы следующие параметры: - address — доменное имя узла для проверки доступности по TCP или URL — для HTTP; - dns-ip — IP-адрес сервера DNS; - dns-tcp — использование TCP вместо UDP для DNS-запроса; - check-cert — проверка SSL-сертификата; - type — проверка доступности по: - http; - tcp (если порт не указан, то используется порт 80); - data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки; - timeout — максимальный тайм-аут ожидания ответа от веб-сервера; - user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name>
ping	Проверка доступности определенного узла. Можно задать следующие параметры: - host — IP-адрес или доменное имя узла. - count — количество отправляемых echo-запросов. Если параметр не задан, отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C). - numeric — не определять имена. - timestamp — отображение временных меток. - interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах. - ttl — время жизни пакета. - interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. - mtu — максимальный размер блока данных отправляемых пакетов. - virtual-router — имя виртуального маршрутизатора. Admin@nodename# execute ping host <hostname> count <number>
reboot	Перезагрузка устройства: Admin@nodename# execute reboot
restore-mac	Восстановление mac-адреса интерфейса: Admin@nodename# execute restore-mac interface <interface-name>
shutdown	Выключение устройства: Admin@nodename# execute shutdown
termination	Закрытие сессий администраторов или пользователей: Admin@nodename# execute termination <admin-sessions user-sessions> Подробнее — в разделе «Настройка сессий администраторов»
traceroute	Трассировка соединения до определенного узла. Параметры команды: - host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка; - interface <iface-name> — интерфейс, с которого будут отправляться пакеты; - not-map-ip — не искать hostname для IP-адреса при отображении; - use-icmp-echo — использовать ICMP echo; - port — указать порт вместо порта по умолчанию (1 — 65535); - min-interval — минимальный интервал между пакетами. Admin@nodename# execute traceroute host <hostname>
update	Обновление: - software-updates — обновление программного обеспечения. - libraries-updates — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.

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

Admin@nodename> <command-name>

Команды import

Импорт доступен в разделах «Настройки», «Пользователи», «Сеть», «Политики сети», «Политики безопасности», «Глобальный портал», «VPN».

В разделе «Настройки» (settings) можно импортировать сертификаты. Подробнее — в разделе «[Настройка сертификатов](#)».

В разделах «Пользователи» (users), «Сеть» (network), «Политики сети» (network-policy), «Политики безопасности» (security-policy), «Глобальный портал» (global-portal), «VPN» (vpn-server, vpn-client) можно импортировать правила, написанные на UPL. При использовании импорта, все существующие правила будут заменены на указанные.

В разделе «Пользователи» (users) можно импортировать правила captive-портала. Подробнее о правилах — в разделе «[Captive-portal](#)».

В разделе «Сеть» (network) можно импортировать правила DNS. Подробнее — в разделе «[Настройка правил DNS](#)».

В разделе «Политики сети» (network-policy) можно импортировать правила межсетевого экрана, NAT и маршрутизации, пропускной способности, балансировки нагрузки. Подробнее о правилах читайте в соответствующих разделах: «[Настройка правил межсетевого экрана](#)», «[Настройка правил NAT и маршрутизации](#)», «[Настройка правил пропускной способности](#)». «[Настройка балансировки нагрузки](#)».

В разделе «Политики безопасности» (security-policy) можно импортировать правила контентной фильтрации, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, сценариев, защиты почтового трафика, ICAP-правил и правил защиты DoS. О добавлении правил читайте в соответствующих разделах: «[Настройка фильтрации контента](#)», «[Настройка веб-безопасности](#)», «[Настройка правил инспектирования туннелей](#)», «[Настройка инспектирования SSL](#)», «[Настройка инспектирования SSH](#)», «[Настройка сценариев](#)», «[Настройка правил защиты почтового трафика](#)», «[Настройка правил ICAP](#)», «[Настройка правил защиты DoS](#)».

В разделе «Глобальный портал» (global-portal) можно импортировать правила веб-портала и reverse-прокси. Подробнее о создании правил — в разделах: «[Настройка веб-портала](#)» и «[Настройка правил reverse-прокси](#)».

В разделе «VPN» (vpn-server, vpn-client) можно импортировать серверные и клиентские правила, о добавлении которых читайте в разделах: «[Настройка серверных правил](#)» и «[Настройка клиентских правил](#)».

Команды экспорт

Команда для экспорта сертификатов.

Вы можете экспортировать сертификаты, всю цепочку сертификатов и CSR:

Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on

Подробнее об управлении сертификатами — в разделе «[Настройка сертификатов](#)».

Команда debug

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

Для включения журналирования конкретного протокола маршрутизации используется команда:

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

Поддерживаются следующие протоколы:

- rip;
- ospf
- bgp;
- igmp;
- pim;
- bfd;
- msdp;
- mroute — таблица мультикаст-маршрутизации;
- ssm pingd — инструмент тестирования мультикаст-вещания.

Настройка устройства (Описание)

Documentation: ☒
Version: 7.x
Product: NGFW

Настройка параметров работы CLI

Параметры работы интерфейса командной строки UserGate NGFW настраиваются на уровне settings cli.

С помощью команд этого уровня вы можете:

- настроить [вид системного приглашения консоли](#) CLI;
- [уровень детализации журналирования действий](#) в CLI;
- [уровень детализации журналирования операций экспорта и импорта конфигурации](#) CLI.

Чтобы посмотреть текущие значения параметров работы интерфейса командной строки, используйте команду:

Admin@nodename# show settings cli

Пример выполнения команды:

Admin@mynode1# show settings cli

```
log-level      : info
transfer-log-level : warning
prompt        : Admin@mynode1
```

Настройка системного приглашения

Для настройки вида системного приглашения консоли CLI используется команда:

Admin@nodename# set settings cli custom-prompt <new-custom-prompt>

Вы можете поменять системное приглашение в консоли CLI с установленного по умолчанию (вида Admin@nodename#) на удобное вам. Например, чтобы поменять вид системного приглашения на NodeAABBCC, выполните следующую команду:

```
Admin@nodename# set settings cli custom-prompt NodeAABBCC
NodeAABBCC#
```

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

Admin@nodename# set settings cli custom-prompt default

Пример выполнения команды:

```
NodeAABBCC#
NodeAABBCC# set settings cli custom-prompt default
Admin@nodename#
```

Настройка уровня детализации журналирования действий в CLI

Чтобы задать уровень детализации журналирования действий в CLI используется команда:

Admin@nodename# set settings cli log-level

Вы можете установить следующие уровни детализации:

- off — отключить журналирование;
- error — только ошибки;
- warning — ошибки и предупреждения;
- info — ошибки, предупреждения и дополнительная информация;
- debug — максимальная детализация.

Журнал консоли CLI записывается в файл cli.log. Файл доступен для скачивания вместе с остальными системными журналами в веб-консоли в разделе **Настройки → Консоль администратора → Управление устройством → Диагностика**.

ПримечаниеЭта команда задает только уровень детализации журналирования действий в CLI и не влияет на общий уровень детализации диагностических сообщений системы. Чтобы изменить уровень детализации диагностики системы, используйте команду set settings loglevel value [в CLI](#) или настройте соответствующий параметр в разделе веб-консоли: «Настройки» → «Консоль администратора» → «Управление устройством» → «Диагностика».

Пример выполнения команды:

```
Admin@mynode1# set settings cli log-level debug
Admin@mynode1# show settings cli
```

```
log-level      : debug
transfer-log-level : warning
prompt        : Admin@mynode1
```

Настройка уровня детализации журналирования операций экспорта и импорта конфигурации

Чтобы задать уровень детализации журналирования операций экспорта и импорта конфигурации в CLI используется команда:

Admin@nodename# set settings cli transfer-log-level

Вы можете установить следующие уровни детализации:

- off — отключить журналирование;
- error — только ошибки;
- warning — ошибки и предупреждения;
- info — ошибки, предупреждения и дополнительная информация;
- debug — максимальная детализация.

Пример выполнения команды:

```
Admin@mynode1# set settings cli transfer-log-level debug
Admin@mynode1# show settings cli
```

```
log-level      : debug
transfer-log-level : debug
prompt        : Admin@mynode1
```

Настройка базовых параметров устройства

На уровне settings general настраиваются базовые параметры UserGate NGFW.

Структура команд для настройки базовых параметров устройства:

Admin@nodename# set settings general <settings-module> <parameters>

Базовые параметры устройства сгруппированы в разделы.

Раздел	Описание

Раздел	Описание
admin-console	Параметры консоли управления: - timezone — часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т. п. - language — язык интерфейса: - ru — русский; - en — английский. - webaccess — режим аутентификации веб-консоли: - password — аутентификация по имени и паролю; - cert — аутентификация по X.509-сертификату. - uc-profile — выбор профиля пользовательских сертификатов. - web-ssl-profile — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». - response-pages-ssl-profile — выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации captive-портала. Подробнее о профилях SSL — в разделе «Настройка профилей SSL». - api-session-lifetime — время ожидания сеанса администратора в минутах. По истечении этого времени при вводе команды CLI, использующей API-вызовы (команды создания объектов, изменения параметров, просмотра параметров, удаления объектов или параметров), сессия администратора будет завершена сообщением Authentication session expired. Restart CLI
server-time	Параметры установки точного времени: - ntp-enabled — включение и отключение использования NTP-серверов. - primary-ntp-server — адрес основного NTP-сервера. - second-ntp-server — адрес запасного NTP-сервера. - time — установка времени на устройстве. Время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
modules	Настройка работы модулей устройства: - proxy-port — указание нестандартного номера порта, который будет использоваться для подключения к встроенному прокси-серверу. - auth-captive — указание служебного домена, который будет использоваться UserGate NGFW при авторизации пользователей через captive-портал. - logout-captive — указание служебного домена, который будет использоваться пользователями UserGate NGFW для окончания сессии. - cert-captive — указание служебного домена, который будет использоваться UserGate NGFW при авторизации пользователей через captive-портал с помощью сертификатов. - block-page-domain — указание служебного домена, который будет использоваться для отображения страницы блокировки. - ftp-enabled — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. - ftp-domain — указание служебного домена, который будет использоваться для предоставления пользователям сервиса FTP поверх HTTP. - tunnel-inspection-zone — выбор зоны для инспектируемых туннелей: - name — название зоны; - enabled — включение или отключение зоны. - snmp-engine-id — настройка идентификатора SNMP устройства: - length <fixed dynamic> — длина идентификатора. Фиксированная (не более 8 байт), только для типа text или динамическая (не более 27 байт). - type <ip4 ip6 mac text octets> — формат идентификатора SNMP (IPv4, IPv6, MAC-адрес, текст, октеты). - value — значение идентификатора. - terminal-sever-agent — настройка пароля для подключения агентов авторизации терминального сервера. - lldp — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: - transmit-delay — задержка передачи. Указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например после изменения имени узла или адреса управления. Может принимать значения от 1 до 3600. Указывается в секундах. - transmit-hold — значение мультипликатора удержания. Произведение значений transmit-delay и transmit-hold определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100
cache	Параметры кэширования прокси-сервера: - caching-mode — включение или отключение режима кэширования. - exclusions — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду: Admin@nodename# delete settings general cache exclusions [<URL>] - max-cacheable-size — максимальный размер объектов, которые будут кэшироваться (МБ). - ram-size: размер оперативной памяти, отведенный под кэширование (МБ)
log-analyzer	Параметры модуля сбора статистики: use-local-stat-server — использование локальной службы журналирования

Раздел	Описание
proxy-portal	Параметры предоставления доступа к внутренним ресурсам компании с помощью веб-портала: - enabled — включение или отключение использования веб-портала. - hostname — имя узла, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. - port — порт TCP, который будет использоваться сервисом веб-портала. - auth-profile — указание профиля аутентификации, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей аутентификации». - auth-template — выбор шаблона страницы аутентификации. - portal-template — выбор шаблона веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. - enable-ldap — выбор домена AD или LDAP на странице аутентификации: - on — показывать; - off — не показывать. - use-captcha — показывать на странице аутентификации веб-портала код для ввода пользователем: - on — показывать; - off — не показывать. - ssl-profile — выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей SSL». - certificate — выбор сертификата, который будет использоваться для создания HTTPS-соединения. - auth-mode — выбор метода аутентификации: - aaa — аутентификация через логин и пароль локальных пользователей или аутентификация пользователей на AAA-сервере; - pki — аутентификация посредством X.509-сертификатов. - user-cert-profile — выбор профиля пользовательских сертификатов при аутентификации посредством сертификатов
pcap	Настройка захвата пакетов. Команда для настройки: <pre>Admin@nodename# set settings general pcap packet-capture-mode <parameters></pre> Параметры: - no-capture — без захвата; - one-packet — один пакет; - previous — предшествующие пакеты; - previous-and-following — предшествующие и последующие пакеты: - previous-packets — количество предшествующих пакетов (от 4 до 30 пакетов); - following-packets — количество последующих пакетов (от 2 до 15 пакетов)
change-tracker	Настройка учета изменений параметров устройства: - enabled — включение или отключение учета изменений параметров. - event-tracker-types — типы изменений (например, приказ, регламентные работы и т. д.). Для удаления типа изменения используется команда: <pre>Admin@nodename# delete settings general change-tracker event-tracker-types [type1 ...]</pre>
management-center	Настройка агента UserGate Management Center. Команда для настройки: <pre>Admin@nodename# set settings general management-center <parameters></pre> Параметры: - enabled — включение или отключение агента UserGate Management Center; - mc-address — адрес сервера UserGate Management Center; - device-code — уникальный код устройства для подключения устройства к UserGate Management Center
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек. Расписание для обновления программного обеспечения задается командой: <pre>Admin@nodename# set settings general updates-schedule software schedule <schedule disabled></pre> Единое расписание для скачивания обновлений библиотек задается командой: <pre>Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule disabled></pre> Расписание для скачивания обновлений отдельных библиотек задается командой: <pre>Admin@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule disabled></pre> Время задается в cronab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями. Команда для просмотра расписания обновлений: <pre>Admin@nodename# show settings general updates-schedule</pre>
upstream-proxy	Настройка перенаправления HTTP-трафика на вышестоящий прокси-сервер (для версий ПО 7.1.x-7.3.x): - enabled — включение или выключение перенаправления трафика на вышестоящий прокси-сервер (on/off); - mode — тип вышестоящего прокси-сервера (HTTP(S)/SOCKS5); - ip — IP-адрес вышестоящего прокси-сервера; - port — порт вышестоящего прокси-сервера; - auth — аутентификация на вышестоящем прокси-сервере (on/off); - name — логин на вышестоящем прокси-сервере; - password — пароль на вышестоящем прокси-сервере

Раздел	Описание
metrics-collection	Настройка параметров передачи метрик телеметрии. Доступна в версии 7.5.0 и выше. - enabled — включение или выключение отправки метрик телеметрии. По умолчанию отправка метрик телеметрии включена. - masking-sensitive-data — маскирование чувствительных данных в отправляемых метриках. К чувствительным данным относятся IP-адреса, MAC-адреса, URL, адреса эл. почты и т. д. По умолчанию маскирование чувствительных данных отключено.

Настройка управления устройством

Настройка диагностики

В этом разделе вы можете управлять параметрами диагностики устройства, необходимыми службе технической поддержки для решения возможных проблем.

Параметры диагностики задаются на уровне settings loglevel.

С помощью следующей команды вы можете установить необходимый уровень детализации журналирования событий:

Admin@nodename# set settings loglevel value <off | error | warning | info | debug>

- off — ведение журналов диагностики отключено;
- error — журналировать только ошибки;
- warning — журналировать только ошибки и предупреждения;
- info — журналировать только ошибки, предупреждения и дополнительную информацию;
- debug — журналировать все возможные события.

При журналировании на уровнях warning, info и debug может снижаться производительность UserGate NGFW, поэтому рекомендуется устанавливать уровни error или off, если технической поддержкой UserGate не было предложено иное.

Для просмотра состояния уровня детализации диагностики используется команда:

Admin@nodename# show settings loglevel

Для включения или отключения удаленного помощника (radmin) используется команда:

Admin@nodename# set settings radmin enabled <on | off>

Для просмотра состояния удаленного помощника используется команда:

Admin@nodename# show settings radmin

Режим emergency

Если произошел сбой в работе ядра UserGate NGFW, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации UserGate NGFW. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Команда входа в режим emergency CLI выглядит следующим образом:

ssh Admin@emergency@<NGFW_IP> -p 2200

Команда включения и отключения удаленного доступа к серверу для технической поддержки в режиме emergency:

Admin@emergency@NGFW# set radmin-emergency enabled <on | off> <parameters>

В команде указываются следующие сетевые параметры:

- interface — название интерфейса;
- ip-addr — IP-адрес интерфейса;
- gateway-address — IP-адрес шлюза.

В версии 7.5.0 и выше в режиме emergency доступна команда возврата устройства в первоначальное состояние:

Admin@emergency@NGFW# execute factory-reset

Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды.

Настройка получения обновлений

В этом разделе вы можете установить канал получения обновлений для устройства (стабильные версии или бета-версии).

Канал обновлений устанавливается с помощью команды:

Admin@nodename# set settings device-mgmt updates-channel <stable | beta>

Для просмотра наличия обновлений и выбранного канала обновления используется команда:

Admin@nodename# show settings device-mgmt updates-channel

Управление резервным копированием

На уровне settings device-mgmt вы можете создавать правила резервного копирования.

Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

Admin@nodename# create settings device-mgmt settings-backup <parameters>

Параметры правил резервного копирования.

Параметр	Описание
enabled	Включение или отключение правила создания резервной копии устройства
name	Название правила резервного копирования
description	Описание правила резервного копирования
type	Выбор типа удаленного сервера для экспорта файлов: - ssh; - ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи
path	Путь на сервере, куда будут выгружены файлы

Параметр	Описание
schedule	Расписание экспорта файлов резервных копий. Время задается в cronTab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями

Для изменения существующего правила резервного копирования используется команда:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения, аналогичен списку параметров, доступных при создании правила.

Для удаления правила резервного копирования используется команда:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Для просмотра параметров правила резервного копирования используется команда:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в правиле параметры (см. список параметров [в таблице выше](#)).

Экспорт параметров

Создание и настройка правил экспорта параметров устройства происходит на уровне settings device-mgmt settings-export.

Для создания правила экспорта параметров используется команда:

```
Admin@nodename# create settings device-mgmt settings-export ( <parameters> )
```

Параметры правила экспорта.

Параметр	Описание
enabled	Включение или отключение правила экспорта параметров устройства
name	Название правила экспорта
description	Описание правила экспорта
type	Тип удаленного сервера для экспорта параметров: - ssh; - ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи на удаленном сервере
path	Путь на сервере, куда будут выгружены параметры
schedule	Расписание экспорта параметров. Время задается в cronTab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями

Для изменения существующего правила экспорта параметров устройства используется команда:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения, аналогичен [списку параметров](#), доступных при создании правила.

Для удаления правила экспорта параметров используется команда:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Для просмотра параметров правила экспорта используется команда:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Для команд изменения, удаления или отображения правил в качестве идентификатора правила можно использовать не только название, но и другие заданные в существующем правиле параметры (см. список параметров [в таблице выше](#)).

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используйте следующую команду:

```
Admin@nodename# set settings change-control config <off | log | block>
```

Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate NGFW.

- log — активация режима отслеживания изменений конфигурации. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- off — отключение режима отслеживания изменений конфигурации. Необходимо указать пароль, который был задан при активации режима отслеживания конфигурации.
- block — активация режима отслеживания изменений конфигурации. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик.

Перед активацией защиты конфигурации администратор производит настройку устройства в соответствии с требованиями организации, после чего защищает параметры от изменений (режим log или block). Любое изменение параметров через веб-интерфейс, CLI или другими способами будет приводить к журналированию и блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений используется команда:

```
Admin@nodename# show settings change-control config
```

Настройка защиты исполняемых файлов от изменения

Для настройки защиты исполняемого кода устройства от потенциального несанкционированного изменения используется команда:

```
Admin@nodename# set settings change-control code <off | log | block>
```

Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate NGFW.

- log — активация режима отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания.
- off — отключение режима отслеживания несанкционированных изменений исполняемого кода. Необходимо указать пароль, который был задан при активации режима отслеживания исполняемого кода.
- block — активация режима отслеживания несанкционированных изменений исполняемого кода. Необходимо задать пароль, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик. Чтобы отключить созданное правило межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов используется команда:

```
Admin@nodename# show settings change-control code
```

Настройка режима ускоренной обработки сетевого трафика

Для включения или отключения режима ускоренной обработки трафика используется команда:

```
Admin@nodename# set settings fastpath enabled <on/off>
```

Для просмотра параметров режима ускоренной обработки трафика используется команда:

```
Admin@nodename# show settings fastpath
```

Version: 7.x
Product: NGFW
Documentation: 

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда для изменения параметров существующего узла кластера:

Admin@nodename# set settings device-mgmt configuration-cluster <node-name>

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменение имени узла кластера.
description	Изменение описание узла кластера.
ip	Установка IP-адреса интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения параметров узла кластера:

Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>

...

Admin@nodename# show settings device-mgmt configuration-cluster <node-name>

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

Admin@nodename# execute configure-cluster generate-secret-key

Настройка кластера отказоустойчивости

Настройка кластеров отказоустойчивости производится на уровне **settings device-mgmt ha-clusters**.

Для создания кластера отказоустойчивости:

Admin@nodename# create settings device-mgmt ha-clusters

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: - on, - off.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: - active-passive: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных); - active-active: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
session-sync	Настройка синхронизации пользовательских сессий в кластере: - off — отключение синхронизации пользовательских сессий; - on — включение синхронизации пользовательских сессий; - ha-cluster-id: <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP(S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info> Доступные параметры для <virtual-ips-filter>: - new: создать виртуальный IP-адрес для заданного кластера; <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: - ip: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask); - ha-interfaces: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка session-sync активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Пример команды создания кластера:

Admin@nodename# create settings device-mgmt ha-clusters nodes [node_1] name "Test HA cluster" description "Test HA cluster description" mode active-passive enabled on virtual-ips new ha-interfaces [node_1/port3] ip 192.168.1.5/24

Для редактирования настроек кластера:

Admin@nodename# set settings device-mgmt ha-cluster <cluster-name>

Параметры для редактирования:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • on, • off.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • active-passive: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных); • active-active: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
master-node	Назначение мастер-узла кластера отказоустойчивости.
session-sync	Настройка синхронизации сессий в кластере: • off — отключение синхронизации пользовательских сессий; • on — включение синхронизации пользовательских сессий; • ha-cluster-id: ◦ <code><num></code> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP(S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: <pre>Admin@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info></pre> Доступные параметры для <code><virtual-ips-filter></code>: • new: создать виртуальный IP-адрес для заданного кластера; • <code><ip></code>: изменить данные для выбранного виртуального адреса. Доступные параметры для <code><virtual-ip-info></code>: • ip: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask); • ha-interfaces: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка session-sync активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Примеры редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster" nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces [ node_1/port3 node_2/port3 ]
...
Admin@nodename# set settings device-mgmt ha-clusters "Test HA cluster" master-node utmcore@iononsteswer
```

Для удаления кластера:

```
Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- **nodes**,
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>
```

Product: NGFW
Version: 7.x

Настройка кластера конфигурации

Кластер конфигурации настраивается на уровне settings device-mgmt configuration-cluster.

Для изменения параметров существующего узла кластера используется команда:

Admin@nodename# set settings device-mgmt configuration-cluster <node-name>

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменение имени узла кластера
description	Изменение описание узла кластера
ip	Установка IP-адреса интерфейса, входящего в зону, выделенную для кластера

Команды для удаления и отображения параметров узла кластера:

Admin@nodename# delete settings device-mgmt configuration-cluster <node-name>
...
Admin@nodename# show settings device-mgmt configuration-cluster <node-name>

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

Admin@nodename# execute configure-cluster generate-secret-key

Настройка кластера отказоустойчивости

Кластер отказоустойчивости настраивается на уровне settings device-mgmt ha-clusters.

Для создания кластера отказоустойчивости используется команда:

Admin@nodename# create settings device-mgmt ha-clusters

Далее необходимо задать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: - on, - off
name	Название кластера отказоустойчивости
description	Описание кластера отказоустойчивости
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
delivery-mode	Выбор режима отправки служебного трафика: - Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. - Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
virtual-ips	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: - ip — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask); - ha-interfaces — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)
mode	Выбор режима работы кластера: - active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен); - active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
advertise-time	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
master-down-timer	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
preemption-delay	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
use-vmac	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
no-preempt	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
heartbeat	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
ha-cluster-multicast-id	<num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически
sync-session	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
sync-udp-icmp	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии

Параметр	Описание
vrid	Идентификатор виртуального маршрутизатора (VRID)
node-sync	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
unicast-sync-ip	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-sync-port	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-ip	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-port	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
track-interfaces-enabled	Включение/отключение проверки интерфейсов
track-interfaces	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): - change-priority — понизить приоритет узла кластера. - fault — считать узел недоступным

Пример команды создания кластера отказоустойчивости:

```
Admin@nodename# create settings device-mgmt ha-clusters name ExampleCluster nodes [ node_1 node_2 ] mode active-passive delivery- mode multicast heartbeat [ node_1/port0 node_2/port0 ] node-sync [ node_1/port1 node_2/port1 ]
```

Команда для редактирования параметров кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters <cluster-name>
```

Команда для настройки кластера отказоустойчивости в облачной среде Yandex Cloud

```
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster cloud service-provider yandex-cloud yandex-cloud-settings routes new
```

Параметры для редактирования:

Параметр	Описание
heartbeat	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
mode	Выбор режима работы кластера: - active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен). - active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
name	Название кластера отказоустойчивости
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
delivery-mode	Выбор режима отправки служебного трафика: - Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. - Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
enabled	Включение/отключение кластера отказоустойчивости: - on, - off
description	Описание кластера отказоустойчивости
virtual-ips	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: - ip — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask); - ha-interfaces — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)
advertise-time	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
master-down-timer	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
preemption-delay	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
use-vmac	Назначение/отключение виртуального MAC-адреса кластеру узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
no-preempt	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
master-node	Назначение мастер-узла кластера отказоустойчивости
ha-cluster-multicast-id	<num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически

Параметр	Описание
sync-session	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
sync-udp-icmp	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
vrid	Идентификатор виртуального маршрутизатора (VRID)
node-sync	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
unicast-sync-ip	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-sync-port	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-ip	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-port	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
track-interfaces-enabled	Включение/отключение проверки интерфейсов
track-interfaces	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): - change-priority — понизить приоритет узла кластера. - fault — считать узел недоступным
checkers	Настройка диагностики узлов кластера. Проверка доступности шлюзов - gateway-availability — проверка доступности шлюзов: - enabled — включение/включение/отключение проверки доступности шлюзов. Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. - action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). - fall-count — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. - interval-time — регулярная проверка шлюзов через указанный промежуток времени. Можно указывать значения от 0 до 300. - rise-count — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. - resource-availability — проверка доступности ресурсов: - enabled — включение/включение/отключение проверки доступности ресурсов. - action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). - fall-count — количество последовательных неудовлетворительных результатов проверки, после которых узел признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. - interval-time — регулярная проверка ресурсов через указанный промежуток времени. Можно указывать значения от 0 до 300. - rise-count — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. - resources — указание IP-адресов или FQDN тех ресурсов, доступ к которым будет проверяться
cloud	Параметры кластера: - destination-prefix — укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud. - next-hops — IP-адреса интерфейсов узлов кластера. - route-table-id — идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud

Примеры редактирования настроек кластера:

```
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces [ node_1/port3 node_2/port3 ]
...
Admin@nodename# set settings device-mgmt ha-clusters ExampleCluster master-node utmoore@iononsteswer
```

Для удаления кластера:

```
Admin@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- nodes,
- virtual-ips.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin@nodename# show settings device-mgmt ha-cluster <cluster-name>
```

Version: 7.x
Product: NGFW
Documentation: 

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

Admin@nodename# set settings administrators general

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: - on. - off.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

Admin@nodename# set settings administrators general block-time 400

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

Admin@nodename# show settings administrators general

```
strong-password : off
block-time      : 400
min-length      : 7
min-uppercase   : 1
min-lowercase   : 1
min-digits      : 1
spec-characters : 1
char-repetition : 2
num-auth-attempts : 10
```

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

Admin@nodename# create settings administrators administrators

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: - enabled: включение/отключение учётной записи администратора: - on. - off. - login: логин администратора. - description: описание учётной записи администратора. - admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. - password: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): - enabled: включение/отключение учётной записи администратора: - on. - off. - login: логин администратора в формате domainuser. Структура команды при указании данного параметра: - connector: название сконфигурированного ранее LDAP-коннектора. - description: описание учётной записи администратора. - admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.localuser1 enabled on

Параметр	Описание
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): enabled: включение/отключение учётной записи администратора: on. off. login: логин администратора connector: название используемого LDAP-коннектора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): enabled: включение/отключение учётной записи администратора: on. off. login: логин администратора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. auth-profile: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type> <admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user testd.local\user1
```

```
login      : testd.local\user1
enabled    : on
type       : ldap_user
locked     : off
admin-profile : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
api-permissions	Права доступа к API: no-access: нет доступа. read: только чтение. write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... api-permissions <permission> all или Admin@nodename# create settings administrators profiles ... api-permissions <permission> [object ...]
webui-permissions	Права доступа к веб-интерфейсу UserGate: no-access: нет доступа. read: только чтение. write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... webui-permissions <permission> all или Admin@nodename# create settings administrators profiles ... webui-permissions <permission> [object ...]

Параметр	Описание
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • no-access: нет доступа. • read: только чтение. • write: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@nodename# create settings administrators profiles ... cli-permissions <permission> all или Admin@nodename# create settings administrators profiles ... cli-permissions <permission> [object ...]

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

```
Admin@nodename# show settings administrators admin-sessions ( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

```
Admin@nodename# execute termination admin-sessions <IP-address/connection type>
```

Пример выполнения команд:

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : utmcore@dineanoulwer
```

```
admin-login      : Admin
source           : web
session_start_date : 2023-08-10T11:33:10Z
ip               : 10.0.2.2
node             : utmcore@dineanoulwer
```

```
Admin@nodename# execute termination admin-sessions 10.0.2.2/web
```

```
Admin@nodename# show settings administrators admin-sessions
```

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : utmcore@dineanoulwer
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

```
Admin@nodename# execute termination admin-sessions ( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login> )
```

Настройка сертификатов

Version: 7.x
Product: NGFW
Documentation: 

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, которое будет отображено в списке.
description	Описание сертификата.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.
private-key	Приватный ключ в формате PEM.
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение).
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. user: имя пользователя в формате domain\user. connector: выбор LDAP сервера.
role	Тип сертификата: web-cert-chain: цепочка сертификатов веб-консоли. ssl-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. ssl-root: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. user: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. ssl-cert: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. captive-portal: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы fpr-прокси. web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. saml: сертификат, который будет использован в SAML-клиенте. none.

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

```
Admin@nodename# export settings certificates <certificate-name>  
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.

Параметр	Описание
role	Тип сертификата: • web-cert-chain: цепочка сертификатов веб-консоли. • ssl-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • ssl-root: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • user: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • ssl-cert: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • captive-portal: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы fpr-прокси. • web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • saml: сертификат, который будет использован в SAML-клиенте. • none.
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP сервера.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

Admin@nodename# delete settings certificates <certificate-name>

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

Admin@nodename# show settings certificates

Admin@nodename# show settings certificates <certificate-name>

Чтобы удалить сертификат из кэша используется команда:

Admin@nodename# delete settings certificates-cache <common-name>

Настройка параметров устройства

Version: 7.x
Product: NGFW
Documentation: 

Изменение параметров устройства в CLI производится на уровне **settings device**. Для изменения используется следующая команда (где <setting-name> — название параметра):

Admin@nodename# set settings device <setting-name>

Доступно изменение следующих параметров:

Параметр	Описание
l7	Включение или отключение загрузки модуля L7: - on; - off. По умолчанию модуль загружен. Важно! После изменения этого параметра требуется перезагрузка устройства UserGate
sip	Включение или отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: Admin@nodename# set settings device sip enabled - on; - off. По умолчанию модуль выгружен. Для разрешения передачи медиа-трафика напрямую между конечными участниками разговора: Admin@nodename# set settings device sip direct-media - on; - off. Важно! После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (нажать «Принудительно применить» в разделе «Политики сети» → «Межсетевой экран»)
h323	Включение или отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: - on; - off. По умолчанию модуль выгружен
idps	Включение или отключение загрузки модуля IDPS: - on; - off. По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка устройства UserGate
sunrpc	Включение или отключение загрузки модуля SunRPC: - on; - off. По умолчанию модуль выгружен
ftp-alg	Включение или отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: - on; - off. Важно! Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен
auth-type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: - ah — включение подписи; - pass — отключение проверки
fw-drop-invalid	Включение или отключение блокировки пакетов с некорректным набором параметров в полях заголовка: - on; - off. По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной
fw-established	Включение или отключение создания одного общего правила межсетевого экрана для обратных пакетов: - on; - off. По умолчанию настройка выключена
bypass-optimization	Включение или отключение оптимизации инспектирования SSL: - on; - off. При включённом параметре bypass-optimization для снижения нагрузки на прокси-сервер инспекция SSL не будет происходить, если на узле нет запрещающих правил инспектирования SSL. При этом в журнале веб-доступа при включённой опции журналирования будет присутствовать только информация уровней L3/L4. По умолчанию настройка выключена

Для просмотра текущих настроек используйте команду:

Admin@nodename# show settings device

Настройка прокси-сервера

Version: 7.x
Product: NGFW
Documentation: 

Набор команд для просмотра и настройки параметров прокси-сервера доступны на уровне **settings proxy**. Позволяет настроить такие параметры, как добавление заголовков HTTP — `via` и `forwarded`, а также настройки таймаутов на подключение к сайтам и на загрузку контента. Для изменения параметров прокси-сервера используется команда (где `<setting-name>` — название параметра):

Admin@nodename# set settings proxy <setting-name>

Для изменения доступны следующие параметры:

Параметр	Описание
via	Добавление HTTP заголовков Via: • on. • off. По умолчанию отключено.
forwarded	Добавление HTTP заголовков Forwarded: • on. • off. По умолчанию отключено.
xforwarded	Добавление HTTP заголовков X-Forwarded-For: • on. • off. По умолчанию отключено.
connection-timeout	Время ожидания, выделяемое на подключение HTTP. По умолчанию — 20 секунд.
loading-timeout	Время ожидания, выделяемое на загрузку контента HTTP. По умолчанию — 60 секунд.
smode	Режим SYN Proxy: • on. • off. По умолчанию режим включен.
icap-wait-timeout	Время, которое сервер UserGate ждет ответа от ICAP-сервера; указывается в секундах. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила Переслать и игнорировать , UserGate отправит данные пользователю без модификации, если же действие правила Переслать , UserGate не отдаст данные пользователю. Значение по умолчанию — 10 секунд.
proxy_host_rfc	Доступно: • relaxed — использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • strict — соблюдать RFC. Данный режим используется по умолчанию.

Для просмотра текущих настроек используйте команду:

Admin@nodename# show settings proxy

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка работы с вышестоящими прокси-серверами в версии 7.4.0 и выше

В интерфейсе командной строки настройка сценария перенаправления трафика доступна на уровне upstream-proxy.

Настройка состоит из следующих основных шагов:

- 1. Настройка подключения к вышестоящему прокси-серверу.
- 2. Создание профиля подключения.
- 3. Создание правила вышестоящего прокси.

Настройка подключения к вышестоящему прокси-серверу

Создание подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

Admin@nodename# create upstream-proxy servers <parameters>

Параметры для настройки подключения:

Параметр	Описание
enabled	Подключение к вышестоящему прокси-серверу: - on — включено; - off — отключено.
name	Название подключения к вышестоящему прокси-серверу
description	Описание подключения.
mode	Тип вышестоящего прокси-сервера: - https; - socks5.
ip	IP-адрес вышестоящего прокси-сервера.
port	Порт вышестоящего прокси-сервера.
auth	Аутентификация на вышестоящем прокси-сервере: - on — требуется; - off — не требуется.
user	Логин для подключения к вышестоящему прокси-серверу.
password	Пароль для подключения к вышестоящему прокси-серверу.

Редактирование параметров ранее созданного подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

Admin@nodename# set upstream-proxy servers <server-name> <parameters>

В команде редактирования можно использовать те же параметры, которые используются в команде создания подключения.

Посмотреть настройки ранее созданного подключения можно с помощью команды:

Admin@nodename# show upstream-proxy servers <server-name>

Удалить ранее созданное подключение к вышестоящему прокси-серверу можно с помощью команды:

Admin@nodename# delete upstream-proxy servers <server-name>

Создание профиля подключения

Создать профиль подключения к вышестоящему прокси-серверу можно с помощью команды:

Admin@nodename# create upstream-proxy profiles <parameters>

Параметры для настройки профиля:

Параметр	Описание
enabled	Включение/отключение профиля: - on — включен; - off — отключен.
name	Название профиля.
description	Описание профиля.
used-servers	Указание вышестоящих прокси-серверов из списка ранее настроенных в системе.
http-method	Выбор метода HTTP-запроса для проверки состояния подключения с помощью контрольного обращения к указанному URL-ресурсу: GET, HEAD, OPTIONS.
url-host	Указание URL-ресурса для проверки состояния подключения через вышестоящий прокси-сервер.
check-interval	Интервал проверки подключения в секундах.
check-timeout	Время ожидания ответа проверки подключения в секундах.

Редактирование параметров ранее созданного профиля подключения к вышестоящему прокси-серверу можно выполнить с помощью команды:

Admin@nodename# set upstream-proxy profiles <profile-name>

В команде редактирования можно использовать те же параметры, которые используются в команде создания профиля.

Посмотреть настройки ранее созданного профиля можно с помощью команды:

Admin@nodename# show upstream-proxy profiles <profile-name>

Удалить ранее созданный профиль можно с помощью команды:

Admin@nodename# delete upstream-proxy profiles <profile-name>

Создание правила вышестоящего прокси

Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе [UserGate Policy Language](#).

Создать правило подключения к вышестоящему прокси-серверу можно с помощью команды:

Admin@nodename# create upstream-proxy rules <position> upl-rule <parameters>

Редактировать ранее созданные правила можно с помощью команды:

Admin@nodename# set upstream-proxy rules <position> upl-rule <parameters>

Посмотреть ранее созданные правила можно с помощью команды:

Admin@nodename# show upstream-proxy rules <position>

Удалить ранее созданные правила можно с помощью команды:

Admin@nodename# delete upstream-proxy rules <position>

Параметры для настройки правил:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила.
name	Название правила. Например, name("Rule 1").
desc	Описание правила. Например, desc("Rule example set via CLI").
proxy_profile	Профиль подключения к вышестоящему прокси-серверу. Например, proxy_profile(Profile1").
fallback_action	Резервное действие при недоступности вышестоящего прокси-сервера: - прямое подключение — fallback_action(direct); - страница блокировки — fallback_action(blockpage).
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Например, для указания зоны Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.uri(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 .
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе Настройка LDAP-коннектора . Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2").
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Настройка активации лицензии и обновления ПО

Для настройки активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

Admin@nodename# set settings device-mgmt licensing-upstream-proxy <parameters>

В качестве дополнительных параметров указываются:

Параметр	Описание

Параметр	Описание
enabled	Включение/отключение режима активации лицензии и обновления ПО через внешний прокси-сервер: - on — включен; - off — отключен.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: - on — требуется; - off — не требуется.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

Подробнее о функциональности Upstream Proxy, сценариях использования и настройках в веб-консоли администратора — в разделе [Upstream Proxy](#).

Настройка функциональности Upstream Proxy в версиях 7.1.x - 7.3.x

Для перенаправления HTTP-трафика на вышестоящий прокси-сервер используется команда:

```
Admin@nodename# set settings general upstream-proxy <parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/отключение перенаправления трафика на вышестоящий прокси-сервер: - on — включено; - off — отключено.
mode	Тип вышестоящего прокси-сервера: - https; - socks5.
ip	IP-адрес вышестоящего прокси-сервера.
port	Порт вышестоящего прокси-сервера.
auth	Аутентификация на вышестоящем прокси-сервере: - on — требуется; - off — не требуется.
name	Логин на вышестоящем прокси-сервере.
password	Пароль на вышестоящем прокси-сервере.

Для просмотра созданных настроек перенаправления HTTP-трафика на вышестоящий прокси-сервер используется команд а:

```
Admin@nodename# show settings general upstream-proxy
```

Настройка активации лицензии и обновления ПО производится на уровне settings device-mgmt. Для настройки активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# set settings device-mgmt licensing-upstream-proxy <parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/отключение режима активации лицензии и обновления ПО через внешний прокси-сервер: - on — включен; - off — отключен.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: - on — требуется; - off — не требуется.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер используется команда:

```
Admin@nodename# show settings device-mgmt licensing-upstream-proxy
```

Настройка параметров мониторинга устройства

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе [Оповещения](#).

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring snmp-parameter**:

Admin@nodename# edit monitoring snmp-parameter <parameters>

Для редактирования доступны следующие параметры:

Наименование	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.
location	Информация о физическом расположении SNMP-агента.
description	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (length), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text . Engine ID может быть сформирован в формате: ip4 — IPv4. ipv6 — IPv6. mac — MAC-адрес. text — Текст. octets — Октеты.

Подробнее о параметрах SNMP устройства UserGate читайте в разделе [SNMP](#).

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring snmp**:

Admin@nodename# edit monitoring snmp <parameters>

Для редактирования доступны следующие параметры:

Наименование	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
events	Выбор типов параметров, доступных для мониторинга по правилу.

Для работы SNMP-менеджера с UserGate NGFW необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе [Настройки сети](#).

Настройка профилей безопасности SNMP

Для настройки профилей безопасности для аутентификации SNMP-менеджеров используются команды на уровне **monitoring snmp-security-profile**:

Admin@nodename# edit monitoring snmp-security-profile <parameters>

Для редактирования доступны следующие параметры:

Наименование	Описание
name	Название профиля безопасности SNMP
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.

Наименование	Описание
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • none — без аутентификации, без шифрования. • no-encrypt — с аутентификацией, без шифрования. • encrypt — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • sha; • md5; • sha224; • sha256; • sha384; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.

Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

Admin@nodename# edit monitoring alert-rules <parameters>

Для редактирования доступны следующие параметры:

Наименование	Описание
enabled	Включает/отключает данное правило.
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

Настройка захвата пакетов

Захват пакетов позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, Wireshark. Это бывает необходимо при диагностировании сетевых проблем.

Pcap-фильтры определяют условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол IPv4.

Для настройки pcap-фильтров используются команды на уровне **monitoring pcap-filter**:

Admin@nodename# edit monitoring pcap-filter <parameters>

В pcap-правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.

Для настройки pcap-правил используются команды на уровне **monitoring pcap-rule**:

Admin@nodename# edit monitoring pcap-rule <parameters>

Настройка профилей клиентских сертификатов

Product: NGFW
Documentation: 
Version: 7.x

Раздел **Профили клиентских сертификатов** находится на уровне **settings certificate-profiles**.

Для создания профиля клиентского сертификата предназначена команда:

Admin@nodename# create settings certificate-profiles <parameters>

Далее могут использоваться следующие параметры:

Параметр	Описание
name	Название профиля клиентского сертификата.
description	Описание профиля.
username-field	Выбор поля в сертификате, по которому определяется имя пользователя, используемое при аутентификации: common — доменное имя или имя хоста в поле Subject, для которых предназначен сертификат. email — для определения имени пользователя используется параметр с префиксом email в расширении SAN (Subject Alternative Name) . principal — для определения имени пользователя используется параметр Universal Principal Name (UPN), содержащийся в поле otherName в расширении SAN. Если в полях расширения SAN сертификата указано несколько имен UPN или несколько адресов email, берется первый, указанный в сертификате.
certificates	Сертификаты УЦ, назначаемые профилю.
crl	В списках отзыва сертификатов (CRL) содержатся сертификаты, которые были отозваны и больше не могут использоваться. В этот список входят сертификаты, срок действия которых истек или они были скомпрометированы. Параметр для проверки состояния отзыва сертификатов: off — не проверять ни один сертификат. on — проверять все сертификаты в цепочке и требовать, чтобы они все были валидными. peer — проверять только сертификат клиента. best-effort — если проверить CRL не удалось по какой-то причине, то сертификат считается валидным (при этом он всё равно проверяется и может вернуть статус invalid, если сертификат есть в списке отозванных).
receive-timeout	Интервал времени, по истечении которого UserGetе NGFW перестает ожидать ответа от службы отзыва сертификатов.

Для просмотра ранее созданных профилей клиентских сертификатов используются команды:

Admin@nodename# show settings certificate-profiles
Admin@nodename# show settings certificate-profiles <certificate-profile-name>

Для редактирования ранее созданного профиля используется команда:

Admin@nodename# set settings certificate-profiles <certificate-profile-name> <parameters>

Параметры, доступные для редактирования профиля, аналогичны параметрам создания профиля, рассмотренным ранее.

Для удаления ранее созданного профиля используется команда:

Admin@nodename# delete settings certificate-profiles <certificate-profile-name>

Настройка параметров управления телеметрией

Product: NGFW
Version: 7.x

Настройка параметров управления телеметрией устройства в интерфейсе командной строки производится на уровне settings telemetry.

Для редактирования параметров используется следующая команда:

Admin@nodename# set settings telemetry <parameters>

Возможна настройка следующих параметров:

Параметр	Описание
enabled	Включение/отключение сбора телеметрии на устройстве: - on, - off. По умолчанию сбор телеметрии включен.
hide-sensitive-data	Включение/отключение функции сокрытия персональных данных в телеметрии (доступно в версии ПО 7.4.0 и выше): - on, - off. По умолчанию функция отключена.

Посмотреть текущие настройки можно с помощью команды:

Admin@nodename# show settings telemetry

Экспорт и импорт конфигурации в текстовом формате

Product: NGFW
Version: 7.x

В версии 7.5.0 и выше UserGate NGFW поддерживает функцию экспорта и импорта конфигурации устройства в текстовом формате. С помощью этой функции вы можете:

- разворачивать новые устройства посредством клонирования конфигураций;
- добавлять однотипные параметры на устройства;
- быстро восстанавливать устройства после сбоев;
- проводить анализ, аудит или документирование изменений параметров устройств.

Экспорт и импорт конфигурации выполняется с помощью утилиты scp (Secure Copy Protocol) в приложении терминала на компьютере пользователя.

Экспорт конфигурации

Команда экспорта имеет следующий вид:

USER_KEY="<value>" scp -P 2200 -o 'SendEnv=USER_KEY' <user-name>@<IP-address>:sys_config <file-name>

Укажите имя пользователя, IP-адрес UserGate NGFW, название экспортируемого файла. Для шифрования чувствительных данных (паролей, ключей, сертификатов) при экспорте конфигурации задайте переменную окружения с собственной кодовой строкой (USER_KEY). Для импорта этого файла конфигурации необходимо будет использовать ту же кодовую строку.

Пример команды экспорта конфигурации:

USER_KEY="123123" scp -P 2200 -o 'SendEnv=USER_KEY' Admin@192.168.1.100:sys_config configfile1

ПримечаниеЕсли при выполнении команды экспорта или импорта конфигурации с помощью команды scp будет получено сообщение об ошибке вида subsystem request failed on channel 0, добавьте в указанную команду параметр -O.

Полученный файл содержит полную структурированную конфигурацию устройства в текстовом виде. В начале файла конфигурации находится блок метаданных:

```
-----
# Comment
author: "
product: NGFW
version: 7.X.X. YYYY
created: August 12, 2025, 08:04
secret: bamy2Bf6jcVTXWT6RkNbDIOAA=
factory-reset: off
-----
```

Назначение параметров в блоке метаданных:

- author — параметр, в котором вы можете указать имя автора подготовленной конфигурации.
- product — название продукта. Значение параметра устанавливается системой при экспорте данных.
- version — версия UGOS устройства. Значение параметра устанавливается системой при экспорте данных.
- created — время создания файла конфигурации. Значение параметра устанавливается системой при экспорте данных. Этот параметр не должен меняться пользователем.
- secret — ключ шифрования чувствительных данных. Значение параметра устанавливается системой при экспорте данных.
- factory-reset — параметр, определяющий порядок импорта данных из файла конфигурации:
 - off — параметры конфигурации из файла будут добавлены к существующей конфигурации на устройстве;
 - on — параметры конфигурации из файла заменят собой параметры существующей конфигурации.
- # — символ, с помощью которого вы можете добавлять произвольные комментарии в блоке метаданных.

Импорт конфигурации

Для импорта конфигурации на устройство используйте команду вида:

USER_KEY="<value>" scp -P 2200 -o 'SendEnv=USER_KEY' <file-name> <user-name>@<IP-address>:sys_config

Укажите имя пользователя, IP-адрес UserGate NGFW, название импортируемого файла, переменную окружения с той же кодовой строкой, которая была использована при экспорте конфигурации.

Пример команды импорта конфигурации:

USER_KEY="123123" scp -P 2200 -o 'SendEnv=USER_KEY' configfile1 Admin@192.168.1.100:sys_config

В зависимости от значения параметра factory-reset [в блоке метаданных](#) импортируемого файла параметры конфигурации будут добавлены к имеющейся конфигурации устройства или заменят ее.

Импортированные данные сразу же применяются на устройстве после импорта файла. Записи об изменениях параметров конфигурации отображаются в системном журнале событий (event log).

Просмотр журнала ошибок операций импорта и экспорта

Ошибки операций импорта и экспорта конфигурации можно просмотреть с помощью команды:

Admin@nodename> show logs transfer-logs <parameters>

Дополнительные параметры команды:

- direction — порядок отображения записей:
 - new-first — сначала новые записи;
 - old-first — сначала старые записи.
- raw — отображение полного списка записей журнала.

Зоны

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 ACU ТП-трафика. Необходим только при контроле ACU 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
----------	----------

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>

Интерфейсы

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: - l3 — 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). - ultp-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: - 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. - mirgor — 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	Тег 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
mtu	Размер MTU

Параметр	Описание
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). - ultm-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_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 »

Параметр	Описание
bonding	Дополнительные параметры bond-интерфейса: - agggr-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 загрузки 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 (miipton). Значение параметра должно быть кратным значениям miipton. - up-delay — время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miipton). Значение параметра должно быть кратным значениям miipton. - 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 дойти 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 ПИАК 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_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 »
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
node-name	Узел кластера, на котором будет создан туннельный интерфейс
zone	Зона, которой будет принадлежать интерфейс

Параметр	Описание
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.
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. - iipr — 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.
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 »

Параметр	Описание
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>
```

Шлюзы

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>

DHCP

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 proxy. 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").
url.domain	Список доменов, на которые необходимо перенаправлять. Допускается использование звёздочки (*) для указания шаблона доменов. Чтобы указать список доменов: url.domain = "*.example.com".

Параметр	Описание
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# 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 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 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 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 информацией 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 отсылает 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
  rendezvous-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: • l2 — 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: • l2 — 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.**

Настройка групп пользователей

Product: NGFW
Version: 7.x
Documentation: 

Настройка групп пользователей производится на уровне **users group**.

Для добавления новой группы пользователей используется команда:

Admin@nodename# create users group <parameter>

Возможно указать следующие параметры:

Параметр	Описание
name	Название группы пользователей.
description	Описание группы пользователей.
transient	Указать: • on — группа для гостевых пользователей. • off — не является группой для гостевых пользователей.
users	Добавление пользователей в группу.
ldap-users	Добавление пользователей LDAP. При добавлении пользователей LDAP необходимо указать LDAP-коннектор (ldap-users connector <ldap-server-name> users + [<domain\user1> <domain\user2> ...]).

Для редактирования информации о группе пользователей необходимо воспользоваться следующей командой (параметры, доступные для обновления, аналогичны с параметрами, доступными при создании группы):

Admin@nodename# set users group <group-name> <parameter>

Для отображения настроек группы используется следующая команда:

Admin@nodename# show users group <group-name>

Примеры команд создания и редактирования группы пользователей:

Admin@nodename# create users group name "Test user group" ldap-users connector "LDAP connector" users [testd.local\user1]
Admin@nodename# show users group "Test user group"

```
name      : Test user group
is-ldap   : off
is-transient : off
users     : user1 user1 (testd.local\user1)
Admin@nodename# set users group "Test user group" users [ user2 ]
Admin@nodename# show users group "Test user group"
```

```
name      : Test user group
is-ldap   : off
is-transient : off
users     : user2; user1 user1 (testd.local\user1)
```

С использованием следующих команд можно удалить группу пользователей или отдельных пользователей группы:

Admin@nodename# delete users group <group-name>

Для удаления локальных пользователей:

Admin@nodename# delete users group <group-name> users [<user1> <user2> ...]

Для удаления пользователей LDAP:

Admin@nodename# delete users group <group-name> ldap-users connector <ldap-server-name> users [<domain\user1> <domain\user2> ...]

Пример удаления из группы пользователя LDAP:

Admin@nodename# delete users group "Test user group" ldap-users connector "LDAP connector" users [testd.local\user1]

Настройки пользователей

Documentation: 
Product: NGFW
Version: 7.x

Настройка пользователей производится на уровне **users user**.

Команда для добавления пользователей:

Admin@nodename# create users user <parameter>

Доступно указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение пользователя.
name	Имя пользователя.
login	Логин пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
password	Пароль пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
expiration-date	Срок действия учётной записи пользователя. Указывается в формате YYYY-MM-DD.
groups	Группы, в которые будет добавлен пользователь.
ip	IP-адреса для идентификации пользователя; пользователь всегда должен получать доступ в сеть с указанных адресов.
mac	MAC-адреса для идентификации пользователей; пользователь всегда должен получать доступ в сеть с указанных адресов.
ip-range	Диапазон IP-адресов для идентификации пользователя; пользователь всегда должен получать доступ в сеть с адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>.
ip-mac	Идентификация пользователя с помощью комбинации MAC и IP-адресов; пользователь всегда должен получать доступ в сеть с указанных адресов. Указывается в формате <ip-mac>.
vlan-tag	Тег VLAN для идентификации пользователя.
emails	Почтовые адреса пользователя.
phones	Номера телефонов пользователя.

Для обновления параметров учётной записи пользователя:

Admin@nodename# set users user <user-name> <parameter>

Список доступных параметров аналогичен списку параметров, доступному при создании учётной записи пользователя.

Команда для просмотра учётной записи пользователя:

Admin@nodename# show users user <user-name>

Пример команд создания и редактирования учетной записи пользователя:

Admin@nodename# create users user name user_2 login user2 password 12345 expiration-date 2023-12-31 ip [192.168.100.112] enabled on
Admin@nodename# show users user user_2

name : user_2
login : user2
enabled : on
expiration-date : December 31, 2023, 00:00
ip : 192.168.100.112
Admin@nodename# set users user user_2 emails [example@example.org]
Admin@nodename# show users user user_2

name : user_2
login : user2
enabled : on
emails : example@example.org
expiration-date : December 31, 2023, 00:00
ip : 192.168.100.112

Для удаления учётной записи пользователя используется следующая команда:

Admin@nodename# delete users user <user-login>

Также имеется возможность удаления определённой информации из учётной записи. Для удаления доступны (при удалении требуется ввод значения параметра):

- groups.
- static-addresses.
- emails.
- phones.

Настройка серверов аутентификации

Documentation: ☒
Product: NGFW
Version: 7.x

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

Admin@nodename# create users auth-server ldap <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: on — использование SSL-соединения для подключения к LDAP-серверу. off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username @domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
cache-ttl	Время жизни записей LDAP-кэша. (Опция доступна начиная с релиза UGOS 7.1.3).
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

Admin@nodename# set users auth-server ldap <ldap-server-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

Admin@nodename# show users auth-server ldap <ldap-server-name>

Примеры команд создания и редактирования LDAP-коннектора:

Admin@nodename# create users auth-server ldap name "New LDAP connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains [testd.local] search-roots [dc=testd,dc=local] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

```
name      : New LDAP connector
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
Admin@nodename# set users auth-server ldap "New LDAP connector" description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"
```

```
name      : New LDAP connector
description : New LDAP connector description
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
```

Для удаления LDAP-коннектора используется команда:

Admin@nodename# delete users auth-server ldap <ldap-server-name> <parameter>

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- domains.**
- search-roots.**

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

Admin@nodename# create users auth-server radius <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.

Параметр	Описание
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin@nodename# set users auth-server radius <radius-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server" description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
description : New RADIUS server description
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server radius <radius-server-name> <parameter>
```

Также возможно удаление отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses.**

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
Admin@nodename# set users auth-server tacacs "New TACACS+ server" description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
description : New TACACS+ server description
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка сервера NTLM

Настройка сервера NTLM производится на уровне **users auth-server ntlm**.

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

```
Admin@nodename# create users auth-server ntlm <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
domain	IP-адрес или доменное имя сервера NLM.

Команда для обновления информации о NTLM-сервере:

```
Admin@nodename# set users auth-server ntlm <ntlm-server-name> <parameter>
```

Команда для отображения информации о сервере NTLM:

```
Admin@nodename# show users auth-server ntlm <ntlm-server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Примеры команд для создания и редактирования сервера NTLM:

```
Admin@nodename# create users auth-server ntlm name "New NTLM server" domain 10.10.0.12 enabled on
Admin@nodename# show users auth-server ntlm "New NTLM server"
```

```
name      : New NTLM server
enabled   : on
domain    : 10.10.0.12
```

```
Admin@nodename# set users auth-server ntlm "New NTLM server" description "New NTLM server description"
Admin@nodename# show users auth-server ntlm "New NTLM server"
```

```
name      : New NTLM server
description : New NTLM server description
enabled   : on
domain    : 10.10.0.12
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers ntlm <ntlm-server-name>
```

Настройка сервера SAML IDP

Настройка сервера SAML IDP производится на уровне **users auth-server saml-idp**.

Для создания сервера аутентификации SAML IDP используется следующая команда:

```
Admin@nodename# create users auth-server saml-idp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
metadata-uri	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML.
certificate	Сертификат, который будет использован в SAML-клиенте.
sso-uri	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
sso-binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-uri	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Команда для обновления информации о сервере SAML IDP:

```
Admin@nodename# set users auth-server saml-idp <saml-idp-server-name> <parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Команда для отображения информации о сервере SAML IDP:

```
Admin@nodename# show users auth-server saml-idp <saml-idp-server-name>
```

Примеры команд для создания и редактирования сервера SAML IDP:

```
Admin@nodename# create users auth-server saml-idp name "New SAML IDP server" slo-uri http://logout.example.org sso-uri http://login.example.org enabled on
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"
```

```
name      : New SAML IDP server
enabled   : on
certificate : Unused
sso-uri    : http://login.example.org
sso-binding : post
slo-uri    : http://logout.example.org
slo-binding : post
Admin@nodename# set users auth-server saml-idp "New SAML IDP server" description "New SAML IDP server description"
Admin@nodename# show users auth-server saml-idp "New SAML IDP server"
```

```
name      : New SAML IDP server
description : New SAML IDP server description
enabled   : on
certificate : Unused
sso-uri    : http://login.example.org
sso-binding : post
slo-uri    : http://logout.example.org
slo-binding : post
```

Для удаления сервера:

```
Admin@nodename# delete users auth-servers saml-idp <saml-idp-server-name>
```

Настройка профилей аутентификации

Product: NGFW
Documentation: 
Version: 7.x
Technology: Identification and Authentication

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
Admin@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
mfa	Указание профиля мультифакторной аутентификации (если её необходимо использовать). Для указания профиль MFA должен быть создан заранее. Подробнее о создании профилей MFA с использованием интерфейса командной строки читайте в разделе Настройка профилей MFA (мультифакторной аутентификации) .
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная авторизация пользователя на Captive-портале.
max-attempts	Число неудачных попыток авторизации через Captive-портал до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации; указывается в секундах.
auth-methods	Метод аутентификации: • local-user-auth: аутентификация по базе данных локально заведенных пользователей. • policy-accept: не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети; применяется совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • http-basic: аутентификация с помощью метода HTTP Basic. • ldap: аутентификация с использованием LDAP-коннектора. • radius: аутентификация с использованием RADIUS-сервера. • tacacs: аутентификация с использованием сервера TACACS+. • ntlm: аутентификация с использованием NTLM-сервера. • saml-idp: аутентификация с использованием сервера SAML IDP.

Команда для редактирования настроек профилей аутентификации:

```
Admin@nodename# set users auth-profile <auth-profile-name> <parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
Admin@nodename# create users auth-profile name "New LDAP auth profile" auth-methods ldap [ "New LDAP connector" ]
Admin@nodename# show users auth-profile "New LDAP auth profile"
```

```
name          : New LDAP auth profile
max-attempts   : 5
idle-time      : 900
expiration-time : 86400
lockout-time    : 300
mfa            : none
auth-methods   :
  http-basic    : off
  local-user-auth : off
  policy-accept : off
  ldap         : New LDAP connector
Admin@nodename# set users auth-profile "New LDAP auth profile" description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"
```

```
name          : New LDAP auth profile
description    : New LDAP auth profile description
max-attempts   : 5
idle-time      : 900
expiration-time : 86400
lockout-time    : 300
mfa            : none
auth-methods   :
  http-basic    : off
  local-user-auth : off
  policy-accept : off
  ldap         : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
Admin@nodename# delete users auth-profile <auth-profile-name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-method>
```

Настройка Captive-профилей

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Identification and Authentication

Настройка Captive-профилей производится на уровне **users captive-profiles**.

Для создания Captive-профиля необходимо использовать следующую команду:

```
Admin@nodename# create users captive-profiles <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название captive-профиля.
description	Описание captive-профиля.
auth-template	Шаблон страницы авторизации.
auth-mode	Метод идентификации, с помощью которого UserGate запомнит пользователя: - ip — Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относиться к данному пользователю; устанавливается по умолчанию. - cookie — Запоминать cookie. После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя.
auth-profile	Профиль аутентификации, определяющий методы аутентификации. Подробнее о настройке профилей авторизации с использованием CLI смотрите в разделе Настройка профилей аутентификации .
custom-redirect	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
use-cookie	Возможность сохранения авторизации в браузере на указанное время. Для сохранения информации используются cookie. - on. - off.
cookie-exptime	Время, на которое будет сохранена аутентификация; задаётся в часах.
enable-ldap	Возможность выбора домена AD/LDAP на странице авторизации: - on. - off.
use-captcha	Использование CAPTCHA: пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала: - on. - off.
use-https	Использование HTTPS при отображении страницы авторизации Captive-портала. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. - on. - off.
notification-profile	Профиль оповещения, который будет использоваться для отсылки гостевым пользователям информации о созданном пользователе и его пароле. Подробнее о настройке профилей оповещений с использованием CLI смотрите в разделе Настройка профилей оповещений .
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль. Текст оповещения обособляется кавычками ("").
exp-time	Дата и время, когда учетная запись временного пользователя будет отключена. Указывается в формате: yyyy-mm-ddThh:mm:ssZ.
session-ttl	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена; задаётся в часах.
password-len	Длина пароля 1 — 15 символов.
password-complexity	Сложность пароля: - num: использование только цифр. - alpha_num: использование букв и цифр. - alpha_num_special: использование букв, цифр и специальных символов.
ta-groups	Группа для временных пользователей, в которую будут помещены создаваемые пользователи.
captive-auth-mode	Выбор метода аутентификации Captive-профиля: - aaa - аутентификация посредством логина/пароля локального пользователя или через AAA-сервер. - pki - аутентификация посредством X.509 сертификатов.
uc-profile	Выбор профиля пользовательского сертификата при аутентификации методом pki.

Для редактирования профиля необходимо использовать следующую команду:

```
Admin@nodename# set users captive-profiles <captive-profile-name> <parameter>
```

При обновлении настроек captive-профиля доступны параметры, аналогичные параметрам, доступным при создании профиля.

Команда для отображения настроек captive-профиля:

```
Admin@nodename# show users captive-profiles <captive-profile-name>
```

Пример создания и редактирования captive-профиля:

```
Admin@nodename# create users captive-profiles name "New captive profile" auth-profile "LDAP auth profile" captive-auth-mode aaa enable-ldap on
Admin@nodename# set users captive-profiles "New captive profile" use-https on
```

Для удаления профиля используется команда:

```
Admin@nodename# delete users captive-profiles <captive-profile-name>
```

Также, с использованием следующей команды, доступно удаление групп для временных пользователей (всегда должна быть указана хотя бы одна группа для временных пользователей):

```
Admin@nodename# delete users captive-profiles <captive-profile-name> ta-groups
```

Captive-портал

Technology: Identification and Authentication
Version: 7.x
Documentation: 
Product: NGFW

В данном разделе описана настройка правил Captive-портала; настройка производится на уровне **users captive-portal**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Параметры правил captive-портала:

Параметр	Описание
OK PASS	Действия правила Captive-портала: OK - использовать аутентификацию. PASS - не использовать аутентификацию.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила captive-портала. Например: name("Captive rule example") .
desc	Описание правила captive-портала. Чтобы задать описание правила: desc("Captive portal rule example set via CLI") .
profile	Captive-профиль указывается при использовании аутентификации на captive-портале. Например, profile("Example Captive profile") . Подробнее о создании и настройке captive-профилей читайте в разделе Настройка Captive-профилей .
rule_log	Включение/отключение записи срабатывания в журнал правил: rule_log(yes) или rule_log(true). rule_log(no) или rule_log(false). Если параметр не указан, то функция журналирования отключена.
src.zone	Зона источника. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category() ; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL . Для указания категории URL: category = "URL category name" .
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url() ; в скобках необходимо указать название списка URL.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Пример создания и редактирования правила captive-портала с использованием UPL:

```
Admin@nodename# create users captive-portal 1 upl-rule OK \  
...profile("New captive profile") \  
...rule_log(true) \  
...name("Captive portal rule new") \  
...  
Admin@nodename# show users captive-portal 1  
% ----- 1 -----  
OK \  
rule_log(yes) \  
profile("New captive profile") \  
enabled(false) \  
id("676d2b1-03e9-42b2-8375-0b8f78c4c47c") \  
name("Captive portal rule new")
```

```
Admin@nodename# set users captive-portal 1 upl-rule OK \
...src.zone = Trusted \
...dst.zone = Untrusted
...
Admin@nodename# show users captive-portal 1
% ----- 1 -----
OK \
src.zone = Trusted \
dst.zone = Untrusted \
rule_log(yes) \
profile("New captive profile") \
enabled(false) \
id("676df2b1-03e9-42b2-8375-0b8f78c4c47c") \
name("Captive portal rule new")
```

Настройка терминальных серверов

Documentation: 
Product: NGFW
Version: 7.x
Technology: Identification and Authentication

В данном разделе описана настройка терминальных серверов с использованием интерфейса командной строки. Настройка производится на уровне **users terminal-servers**.

Для создания терминального сервера необходимо ввести следующую команду:

Admin@nodename# create users terminal-servers <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение терминального сервера: - on. - off.
name	Название терминального сервера.
description	Описание терминального сервера.
hosts	IP-адрес хоста. Для добавления нескольких адресов укажите их через пробел.

Команда для редактирования параметров (параметры приведены выше в таблице) терминального сервера:

Admin@nodename# set users terminal-servers <terminal-server-name> <parameter>

Команда для отображения информации о терминальном сервере:

Admin@nodename# show users terminal-servers <terminal-server-name>

Пример создания и редактирования терминального сервера:

Admin@nodename# create users terminal-servers name "Test terminal server" hosts [10.10.0.20] enabled on
Admin@nodename# show users terminal-servers "Test terminal server"

name : Test terminal server
enabled : on
hosts : 10.10.0.20

Admin@nodename# set users terminal-servers "Test terminal server" description "Test terminal server description"
Admin@nodename# show users terminal-servers "Test terminal server"

name : Test terminal server
description : Test terminal server description
enabled : on
hosts : 10.10.0.20

Команда удаления терминального сервера:

Admin@nodename# delete users terminal-servers <terminal-server-name>

Также возможно удаление отдельных хостов. Для удаления необходимо уточнить их адреса:

Admin@nodename# delete users terminal-servers <terminal-server-name> hosts

Настройка профилей MFA (мультифакторной аутентификации)

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Identification and Authentication

Данный раздел описывает настройку профилей мультифакторной аутентификации с использованием CLI. Настройка профилей MFA производится на уровне **users mfa-profiles**. Можно создать несколько типов профилей:

- MFA через TOTP**: использование токена TOTP (Time-based One Time Password) в качестве второго фактора аутентификации.
- MFA через email**: использование одноразового пароля, полученного по email, в качестве второго фактора аутентификации.
- MFA через SMS**: использование одноразового пароля, полученного по SMS, в качестве второго фактора аутентификации.

Для создания профиля мультифакторной аутентификации используется команда:

```
Admin@nodename# create users mfa-profiles <parameter>
```

Команда для удаления профиля мультифакторной аутентификации:

```
Admin@nodename# delete users mfa-profiles <mfa-name>
```

Для отображения информации о всех профилях или об определённом профиле MFA используются следующие команды:

```
Admin@nodename# show users mfa-profiles
Admin@nodename# show users mfa-profiles <mfa-name>
```

Настройка MFA через TOTP

Команда для добавления нового профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
show-qr-code	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.
notification-profile	Выбор профиля оповещения.
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").

Команда для редактирования параметров профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# set users mfa-profiles totp <mfa-totp-name> <parameter>
```

Параметры, доступные для редактирования, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через TOTP:

```
Admin@nodename# create users mfa-profiles totp name "Test TOTP MFA profile" notification-profile pass show-qr-code on
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"
```

```
name          : Test TOTP MFA profile
show-qr-code   : on
notification-profile : pass
notification-body : Your authentication code is {2fa_auth_code}! Do not share it with anybody!
Admin@nodename# set users mfa-profiles totp "Test TOTP MFA profile" description "Test TOTP MFA profile description"
Admin@nodename# show users mfa-profiles totp "Test TOTP MFA profile"
```

```
name          : Test TOTP MFA profile
description    : Test TOTP MFA profile description
show-qr-code   : on
notification-profile : pass
notification-body : Your authentication code is {2fa_auth_code}! Do not share it with anybody!
```

Настройка MFA через email

Команда для добавления нового профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-profile	Выбор профиля оповещения.
notification-sender	Email отправителя сообщения.
notification-subject	Тема оповещения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через email:

```
Admin@nodename# set users mfa-profiles smtp <mfa-email-profile> <parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через email:

```
Admin@nodename# create users mfa-profiles smtp name "Test SMTP MFA profile" notification-profile "Example SMTP profile" notification-sender sender@example.org notification-subject "Test notification subj" notification-body "Test notification text"
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"
```

```
name          : Test SMTP MFA profile
notification-profile : Example SMTP profile
notification-sender : sender@example.org
notification-subject : Test notification subj
notification-body   : Test notification text
code-lifetime      : 60
Admin@nodename# set users mfa-profiles smtp "Test SMTP MFA profile" code-lifetime 70
Admin@nodename# show users mfa-profiles smtp "Test SMTP MFA profile"

name          : Test SMTP MFA profile
notification-profile : Example SMTP profile
notification-sender : sender@example.org
notification-subject : Test notification subj
notification-body   : Test notification text
code-lifetime      : 70
```

Настройка MFA через SMS

Команда для добавления нового профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-sender	Имя отправителя сообщения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Команда для редактирования параметров профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# set users mfa-profiles smpp <mfa-sms-profile> <parameter>
```

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Пример создания и редактирования профиля мультифакторной аутентификации через SMS:

```
Admin@nodename# create users mfa-profiles smpp name "Test SMPP MFA profile" notification-profile "Example SMPP profile" notification-sender Tes_sender notification-body "Test notification text"
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"
```

```
name          : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender : Tes_sender
notification-body   : Test notification text
code-lifetime      : 60
Admin@nodename# set users mfa-profiles smpp "Test SMPP MFA profile" code-lifetime 80
Admin@nodename# show users mfa-profiles smpp "Test SMPP MFA profile"
```

```
name          : Test SMPP MFA profile
notification-profile : Example SMPP profile
notification-sender : Tes_sender
notification-body   : Test notification text
code-lifetime      : 80
```

Просмотр информации об авторизованных пользователях

Documentation: 

Product: NGFW

Version: 7.x

Для просмотра информации об авторизованных пользователях используется следующая команда интерфейса командной строки в режиме мониторинга:

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

Для просмотра деталей аутентификационной сессии определенного пользователя используется команда:

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

Для удаления сессии определенного пользователя используется команда:

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

где в качестве параметра может использоваться как имя пользователя, так и его IP-адрес.

Настройка применения политик к пользователям

Documentation: 

Product: NGFW

Version: 7.x

Для локальных пользователей UserGate политики применяются автоматически.

Если пользователи проходят аутентификацию через LDAP-коннектор, NTLM или Kerberos, то для применения политик к пользователям (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) необходимо сбросить сессии всех пользователей и произвести очистку кэша LDAP-записей на UserGate.

С помощью интерфейса командной строки CLI можно сбросить сессии отдельных пользователей. Команда выполняется в режиме конфигурации (configure), для выполнения команды необходимо знать IP-адрес пользователя:

```
Admin@nodename# execute termination user-sessions ip <IP-address>
```

Для очистки кэша используется команда:

```
Admin@nodename# execute cache ldap-clear
```

Настройка UserID-агента

Documentation: ☒
Product: NGFW
Version: 7.x

UserID-агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI), Syslog (посредством стандартизированного протокола syslog [RFC 3164](#), [RFC 5424](#), [RFC 6587](#)) и RADIUS (начиная с релиза ПО 7.2.0). Подробнее о схеме работы UserID-агента читайте в разделе [Пользователи и устройства](#) Руководства администратора NGFW.

Настройка UserID в CLI производится на уровне **users userid-agent**.

Настройка параметров UserID-агента

Общие параметры UserID-агента настраиваются с помощью команды:

Admin@nodename# set users userid-agent configurate-agent <parameters>

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию - 120 секунд.
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
radius-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей по RADIUS-логу. (Доступно в версии ПО 7.2.0 и выше.)
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале Агент UserID . Список может быть создан в разделе библиотек (IP-адреса) . Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID. Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.
tcp-enabled	Протокол TCP для приёма журналов по протоколу syslog: - on; - off.
udp-enabled	Протокол UDP для приёма журналов по протоколу syslog: - on; - off.

Настройка источника событий

Microsoft Active Directory

Для добавления Microsoft Active Directory в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent active-directory <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах AD.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий Active Directory предназначена команда:

Admin@nodename# set users userid-agent active-directory <source-name> <parameters>

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа Microsoft Active Directory в таблице выше.

Для просмотра параметров ранее созданных источников событий Active Directory предназначена команда:

Admin@nodename# show users userid-agent active-directory
Admin@nodename# show users userid-agent active-directory <source-name>

Для удаления ранее созданного источника событий Active Directory предназначена команда:

Admin@nodename# delete users userid-agent active-directory <source-name>

Syslog-sender

Для добавления отправителя syslog в качестве источника событий предназначена следующая команда:

Admin@nodename# create users userid-agent syslog-sender <parameters>

При настройке необходимо указать следующие параметры:

Параметр	Описание
----------	----------

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе Библиотеки → Syslog фильтры UserID-агента . Подробнее читайте в разделе Syslog фильтры UserID-агента .
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах syslog.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий отправителя syslog предназначена команда:

```
Admin@nodename# set users userid-agent syslog-sender <source-name> <parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа syslog-sender в таблице выше.

Для просмотра параметров ранее созданных источников событий syslog предназначена команда:

```
Admin@nodename# show users userid-agent syslog-sender
Admin@nodename# show users userid-agent syslog-sender <source-name>
```

Для удаления ранее созданного источника событий syslog предназначена команда:

```
Admin@nodename# delete users userid-agent syslog-sender <source-name>
```

RADIUS-server

Данная опция доступна начиная с релиза ПО 7.2.0.

Для добавления RADIUS-сервера в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent radius-server <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адреса хостов, с которых UserGate будет получать события по протоколу RADIUS.
server-secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
default-domain	Имя домена, в котором будет производиться поиск пользователя в случае, если в запросе не было явно указано какому домену принадлежит пользователь.
attribute-for-group	Номер radius attribute type, в котором находится группа пользователя, по умолчанию группа не проверяется.
attribute-for-name	Номер radius attribute type, в котором находится имя пользователя, по умолчанию 1.
auth-profile	Профиль аутентификации, с помощью которого производится поиск пользователей, найденных в журналах RADIUS.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию - 2700 секунд (45 минут).

Для редактирования ранее созданного источника событий RADIUS предназначена команда:

```
Admin@nodename# set users userid-agent radius-server <source-name> <parameters>
```

Параметры для редактирования аналогичны параметрам, используемым при создании источника событий типа RADIUS в таблице выше.

Для просмотра параметров ранее созданных источников событий RADIUS предназначена команда:

```
Admin@nodename# show users userid-agent radius-server
Admin@nodename# show users userid-agent radius-server <source-name>
```

Для удаления ранее созданного источника событий RADIUS предназначена команда:

```
Admin@nodename# delete users userid-agent radius-server <source-name>
```


Настройка правил межсетевого экрана

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Admin@nodename# create network-policy firewall

Параметры правил межсетевого экрана:

Параметр	Описание
PASS DENY	Действие правила межсетевого экрана: - PASS — разрешить трафик. - DENY — запретить трафик.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила межсетевого экрана. Например: name("Rule example").
desc	Описание правила. Например: desc("Firewall rule example configured in CLI").
ips_profile	Профиль СОВ. Подробнее о создании и настройке профилей СОВ с использованием интерфейса командной строки читайте в разделе Настройка профилей СОВ . Например: ips_profile("Test ips profile").
l7_profile	Профиль приложений. Подробнее о создании и настройке профилей приложений с использованием интерфейса командной строки читайте в разделе Настройка профилей приложений . Например: l7_profile("Test application-profile").
reject_with	Настройка доступна для правил с действием Запретить : - reject_with(no). - reject_with("host_unreach") — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. - reject_with("tcp_rst") — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указать сервиса, использующего протокол TCP. - reject_with("tcp_reset-both") — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. - rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. - rule_log(session) — журналировать начало сессии.
fragmented	Указание пакетов, к которым применяется правило межсетевого экрана: - fragmented(yes) или fragmented(true) — применить правило к только фрагментированным пакетам. - fragmented(no) или fragmented(false) — применить правило к только нефрагментированным пакетам. - fragmented(all) — применить правило ко всем пакетам. Если не указать fragmented при создании правила, то правило межсетевого экрана применяется ко всем пакетам.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geolp	Указание GeoIP источника; необходимо указать код страны (например, src.geolp = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило межсетевого экрана (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testId.local\user1" user = ("user", "testId.local\user1")
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) . Чтобы указать группу сервисов: service = lib.service() ; в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Пример создания правила межсетевого экрана с использованием UPL:

```
Admin@nodename# create network-policy firewall 1 upl-rule PASS \  
...src.zone = Trusted \  
...dst.zone = Untrusted \  
...user = known \  
...service = HTTP \  
...rule_log(session) \  
...name("Test firewall rule") \  
...enabled(true)  
...  
Admin@nodename# show network-policy firewall 1  
% ----- 1 -----  
PASS \  
  user = known \  
  src.zone = Trusted \  
  dst.zone = Untrusted \  
  service = HTTP \  
  rule_log(session) \  
  enabled(true) \  
  id("1505d309-621b-4f88-a2e4-98667c477535") \  
  name("Test firewall rule")
```

Настройка правил NAT и маршрутизации

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Правила NAT и маршрутизации настраиваются на уровне network-policy nat-routing. Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе [UserGate Policy Language](#).

Для создания правила используется команда:

Admin@nodename# create network-policy nat-routing <position> upl-rule <parameters>

Команда для редактирования ранее созданных правил:

Admin@nodename# set network-policy nat-routing <position> upl-rule <parameters>

Команда для просмотра ранее созданных правил:

Admin@nodename# show network-policy nat-routing <position>

Команда для удаления ранее созданных правил:

Admin@nodename# delete network-policy nat-routing <position>

Подробнее о применении правил NAT — в разделе « [NAT и маршрутизация](#) ».

Настройка правил NAT

При настройке правил NAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила NAT. Например, name("NAT rule example")
desc	Описание правила. Например, desc("NAT rule example set via CLI")
nat	Тип правила
snat_target_ip	IP-адрес, на который будет заменен адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src_zone	Зона источника трафика. Например, для указания зоны Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src_ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")
dst_zone	Зона назначения трафика. Для указания зоны назначения трафика, например Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
dst_ip	Добавление списков IP-адресов, доменов назначения, или MAC-адресов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов назначения используйте: dst.ip = 02:00:00:00:00:00
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках укажите название группы сервисов

Пример создания правила NAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...nat \
...rule_log(session) \
...name("Test NAT rule") \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 1
% ----- 1 -----
OK \
  src.zone = Trusted \
  dst.zone = Untrusted \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("0344640b-b392-4920-9853-77d85ec1338c") \
  name("Test NAT rule") \
  nat
```

Настройка правил NoNAT

При настройке правил NoNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила NAT. Например, name("NAT rule example")
desc	Описание правила. Например, desc("NAT rule example set via CLI")
nonat	Тип правила
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, указание зоны Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление адресов источника трафика в виде списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте строку вида: src.ip = 02:00:00:00:00:00
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")
dst.zone	Зона назначения трафика. Например, указание зоны Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL »
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов. Подробнее о создании сервисов или групп сервисов — в разделах « Настройка сервисов » и « Настройка групп сервисов ». Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках укажите название группы сервисов

Пример создания правила NoNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 6 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = "testd.local\user3" \
...rule_log(session) \
...name("NoNAT rule 1") \
...nonat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 6
% ----- 6 -----
OK \
```

```
user = "testd.local\\user3" \
src.zone = Trusted \
dst.zone = Untrusted \
rule_log(session) \
enabled(true) \
name("NoNAT rule 1")\
nonat
```

Настройка правил DNAT

При настройке правил DNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — включение правила
name	Название правила DNAT. Например, name("DNAT rule example")
desc	Описание правила. Для описание правила используйте: desc("DNAT rule example created via CLI")
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, чтобы указать зону Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание Geo IP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Список пользователей или групп, для которых применяется данное правило. Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unkown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\\user2"; - user = (user1, "testd.local\\user2")
dst.zone	Зона назначения трафика. Например, для указания зоны Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL »
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес UserGate: - target_snat(yes) или target_snat(true); - target_snat(no) или target_snat(false)
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »).
	Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
	Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Untrusted \
```

```
...target_ip("10.10.0.15") \
...dnat \
...rule_log(session) \
...name("Test DNAT") \
...enabled(yes)
...
Admin@nodename# show network-policy nat-routing 1
% ----- 1 -----
OK \
src.zone = Untrusted \
target_ip("10.10.0.15") \
direction(input) \
rule_log(session) \
enabled(true) \
id("00e60d4e-9b93-454b-a424-58e2102f84c2") \
name("Test DNAT") \
dnat
```

Настройка правил NoDNAT

При настройке правил NoDNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила DNAT. Например, name("DNAT rule example")
desc	Описание правила. Например, desc("DNAT rule example created via CLI")
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, чтобы указать зону Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL »
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес UserGate: - target_snat(yes) или target_snat(true); - target_snat(no) или target_snat(false)

Параметр	Описание
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »).
	Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
	Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...user = known \
...rule_log(session) \
...name("NoDNAT rule") \
...nodnat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 7
% ----- 7 -----
OK \
  user = known \
  src.zone = Untrusted \
  dst.zone = Trusted \
  rule_log(session) \
  enabled(true) \
  name("NoDNAT rule")\
  nodnat
```

Настройка правил трансляции портов

При настройке правил трансляции портов укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила трансляции портов. Например, name("Port forwarding rule example")
desc	Описание правила. Для создания описание правила используйте: desc("Port forwarding rule example created via CLI")
port_mapping	Тип правила.
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL »
port_map	Переназначение портов публикуемых сервисов. Для переназначения портов необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, port_map(tcp, 2000, 2100). Следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100

Параметр	Описание
target_ip	Адрес назначения DNAT. Например, target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес узла UserGate: - target_snat(yes) или target_snat(true); - target_snat(no) или target_snat(false)

Пример создания правила трансляции портов с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = Untrusted \
... dst.ip = lib.network(UG_IP) \
... target_ip("10.10.0.16") \
... port_map(top, 2222, 23) \
... rule_log(session) \
... name(port_fw1) \
... port_mapping \
...
Admin@nodename# show network-policy nat-routing 8
% ----- 8 -----
OK \
  src.zone = Untrusted \
  dst.ip = lib.network(UG_IP) \
  target_ip("10.10.0.16") \
  port_map(top, 2222, 23) \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("1af47c3f-96a3-4e65-90e3-debf169bb745") \
  name(port_fw1)\
  port_mapping
```

Настройка правил маршрутизации на основе политик

Для настройки правил маршрутизации на основе политик (policy-based routing, PBR) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила. Например, name("Policy-based routing rule example")
desc	Описание правила. Для создания описание правила используйте: desc("Policy-based routing rule example set via CLI")
route	Тип правила.
gateway	Выбор одного из существующих шлюзов. Например, gateway("1.1.1.1"). О добавлении шлюзов с использованием интерфейса командной строки — в разделе « Настройка шлюзов »
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария используйте: scenario = "Example of a scenario". Подробнее о настройке сценариев с использованием интерфейса командной строки — в разделе « Настройка сценариев »
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")

Параметр	Описание
dst.ip	Добавление списков IP-адресов, доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ».
dst.geoip	Указание GeoIP назначения; необходимо указать код страны. Например, dst.geoip = RU. Коды названий стран доступны по ссылке
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »).
	Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).
	Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов

Пример создания и редактирования правила PBR с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule OK \
... route \
... gateway("def") \
... name("testpbr1") \
... enabled(true) \
... rule_log(session) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... service = (HTTPS, HTTP) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... user = "CN=Users1,DC=LOCAL"
Admin@nodename# show network-policy nat-routing 7
% ----- 7 -----
OK \
  user = "CN=Users1,DC=LOCAL" \
  service = (HTTPS, HTTP) \
  gateway(def) \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("0585a95f-4707-4c11-840d-44643bc2c799") \
  name(testpbr1)\
  route
```

Настройка правил трансляции адресов сетей

При настройке правил трансляции адресов сетей (network mapping) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила. Например, name("Network mapping rule example").
desc	Описание правила. Для создания описание правила используйте: desc("Network mapping rule example set via CLI")
netmap	Тип правила.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена; - rule_log(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ».
	Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\user2"; - user = (user1, "testd.local\user2")

Параметр	Описание
dst_ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: <code>dst_ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst_ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL».
dst_geoip	Указание GeoIP назначения; необходимо указать код страны. Например, <code>dst_geoip = RU</code>. Коды названий стран доступны по ссылке.
target_ip	Параметр подмены сетей; адрес сети, на которую будет производится замена. Например, <code>target_ip("1.1.1.0")</code>
direction	Параметр подмены сетей. Направление: <code>direction(input)</code> — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>. <code>direction(output)</code> — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>.
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках необходимо указать название группы сервисов

Пример создания правила трансляции адресов сетей с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = External \
... target_ip("192.168.222.0/24") \
... direction(output) \
... netmap \
... rule_log(session) \
... name(netmap1) \
...
Admin@nodename# show network-policy nat-routing 8
% ----- 8 -----
OK \
src.zone = External \
target_ip("192.168.222.0/24") \
direction(output) \
rule_log(session) \
enabled(true) \
id("26cbd3e8-0210-494c-9fd4-57300b47a9fe") \
name(netmap1)\
netmap
```

Настройка балансировки нагрузки

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing** с использованием языка описания политик UPL. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Настройка балансировщиков нагрузки TCP/UDP и reverse-прокси рассмотрена далее.

Для отображения информации о всех балансировщиках используется команда:

Admin@nodename# show network-policy load-balancing

Настройка балансировщика TCP/UDP

Настройка данного раздела производится на уровне **network-policy load-balancing tcp-udp**.

Структура команды создания балансировщика нагрузки TCP/UDP следующая:

Admin@nodename# create network-policy load-balancing tcp-udp <position> upl-rule

Параметры правил балансировки нагрузки TCP/UDP:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
name	Название правила балансировки. Например: name("TCP_UDP balancer") .
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
desc	Описание правила. Например: desc("TCP_UDP balancing rule") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL . Например: src.ip = lib.network("Test ip-list") .
src.geoip	Указание Geo IP в качестве источника. Например: src.geoip = RU .
url.address	IP-адрес виртуального сервера. Например: url.address = 10.10.0.20 .
url.port	Порт, для которого необходимо производить балансировку нагрузки. Например: url.port = 1812 .
service	Протокол — TCP или UDP, для которого необходимо производить балансировку нагрузки. Например: service = udp .
scheduler	Методы распределения нагрузки на реальные серверы: rr — round robin — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. wrr — weighted round robin — работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. lc — least connections — новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. wlc — weighted least connections — работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. Например: scheduler(rr) .
real_server	Реальные сервера, на которые будет перенаправляться трафик. Для сервера необходимо указать: ip — IP-адрес сервера. port — порт сервера, на который будут перенаправлять запросы пользователей. weight — коэффициент, использующийся для неравномерного распределения нагрузки на реальные серверы. mode — режим: gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: real_server(masq, 10.10.0.9:1812, 50) .

Параметр	Описание
ipvs_fallback	Настройка аварийного режима: • ip — IP-адрес сервера. • port — порт сервера, на который будут пересылаться запросы пользователей. • mode — режим: ◦ gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: ipvs_fallback(masq, 10.10.100.100:1812) .
monitor	Настройка мониторинга реальных серверов: • kind — тип проверки: ◦ ping: проверка доступности узла с использованием утилиты ping. ◦ connect: проверка работоспособности узла путём установления TCP-соединения на определённый порт. ◦ negotiate: проверка работоспособности узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. • service — необходимо указать (HTTP или DNS) при использовании проверки типа negotiate. • request — запрос необходимо указать при использовании проверки типа negotiate. • response — ожидаемый ответ; необходимо указать при использовании проверки типа negotiate. • interval — интервал времени, через который должна выполняться проверка. • timeout — интервал времени ожидания ответа на проверку. • max-failures — количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки. Например: <pre>monitor_kind(ping) \ monitor_interval(60) \ monitor_timeout(60) \ monitor_failurecount(10) \</pre>

Для редактирования существующего правила балансировки нагрузки используется следующая команда:

```
Admin@nodename# set network-policy load-balancing tcp-udp <position> upl-rule
```

Команды для отображения информации о всех правилах балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp
```

Для отображения информации об определённом правиле балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp <position>
```

Пример создания правила балансировщика нагрузки с использованием UPL:

```
Admin@nodename# create network-policy load-balancing tcp-udp 1 upl-rule OK \  
...src.zone = Trusted \  
...url.address = 10.10.0.20 \  
...url.port = 1812 \  
...service = udp \  
...scheduler(rr) \  
...real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \  
...name(tcpudp_balancer1) \  
...enabled(true) \  
...  
Admin@nodename# show network-policy load-balancing tcp-udp
```

```
% ----- 1 -----  
OK \  
src.zone = Trusted \  
url.address = 10.10.0.20 \  
url.port = 1812 \  
service = udp \  
scheduler(rr) \  
real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \  
monitor_kind(ping) \  
monitor_interval(60) \  
monitor_timeout(60) \  
monitor_failurecount(10) \  
enabled(true) \  
id(cbed6ed7-901e-4641-83a1-a05f82dae177) \  
name(tcpudp_balancer1)
```

Для удаления существующего балансировщика нагрузки используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing tcp-udp <position>
```

Настройка балансировщика reverse-прокси

Настройка правил балансировки reverse-прокси производится на уровне **network-policy load-balancing reverse-proxy**.

Для создания правила балансировки reverse-прокси:

```
Admin@nodename# create network-policy load-balancing reverse-proxy <position> upl-rule
```

Параметры правил балансировки нагрузки reverse-proxy:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила балансировки. Например: name("RP balancer") .
desc	Описание правила. Например: desc("Test reverse-proxy balancing rule") .

Параметр	Описание
profile	Указание профилей серверов reverse-proxy, на которые будет распределяться нагрузка. Подробнее о создании и настройке серверов reverse-proxy с использованием CLI в разделе Настройка серверов reverse-прокси . Например, <code>profile("Reverse proxy server1", "Reverse proxy server2")</code> .

Команда для редактирования параметров правила балансировки reverse-прокси:

```
Admin@nodename# set network-policy load-balancing reverse-proxy <position> upl-rule
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании правила балансировки серверов reverse-прокси.

Команды для отображения информации о всех правилах балансировки reverse-proxy:

```
Admin@nodename# show network-policy load-balancing reverse-proxy
```

Для отображения информации об определённом правиле балансировки reverse-proxy:

```
Admin@nodename# show network-policy load-balancing reverse-proxy <position>
```

Пример создания правила балансировщика нагрузки reverse-proxy с использованием UPL:

```
Admin@nodename# create network-policy load-balancing reverse-proxy 1 upl-rule OK \
...profile("Reverse proxy server1", "Reverse proxy server2") \
...desc("Test reverse proxy balancing rule") \
...name(test_reversep1) \
...enabled(true)
...
Admin@nodename# show network-policy load-balancing reverse-proxy
```

```
% ----- 1 -----
OK \
  profile("Reverse proxy server1", "Reverse proxy server2") \
  desc("Test reverse proxy balancing rule") \
  enabled(true) \
  id("1ed892bb-26ee-4ab1-8a55-2f412ce8b55a") \
  name(test_reversep1)
```

Для удаления существующего правила балансировки нагрузки reverse-proxy используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing reverse-proxy <position>
```

Настройка правил управления пропускной способностью

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Настройка правил управления пропускной способностью производится на уровне **network-policy traffic-shaping** с использованием синтаксиса языка UPL. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Для создания правила управления пропускной способностью используется следующая команда:

Admin@nodename# create network-policy traffic-shaping <position> upl-rule

Параметры правил управления пропускной способностью:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила пропускной способности. Например: name("Traffic shaping rule example").
desc	Описание правила. Для задания описания правила: desc("The example of traffic shaping rule configured in CLI").
bandwidth_pool	Полоса пропускания, например, bandwidth_pool("1 Mbps"). Подробнее о создании и настройке полос пропускания читайте в разделе Настройка полос пропускания .
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario". Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. - rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. - rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило пропускной способности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило управления пропускной способностью: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
dst.zone	Зона назначения трафика. Для задания зоны назначения используется: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.

Параметр	Описание
application	Список приложений, для которых применяется данное правило. Доступно указание: • всех групп приложений: application = lib.category(All). • групп приложений: application = lib.applicationgroup(); в скобках необходимо указать название группы приложений. • категорий приложений: application = lib.category(); в скобках необходимо указать название категорий приложений.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правила управления пропускной способностью используется команда:

```
Admin@nodename# set network-policy traffic-shaping <position> upl-rule
```

Для просмотра всех созданных правил управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping
```

Для просмотра определенного правила управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping <position>
```

Пример создания правила управления пропускной способностью с использованием UPL:

```
Admin@nodename# create network-policy traffic-shaping 1 upl-rule OK \
...user = known \
...src.zone = Trusted \
...dst.zone = Untrusted \
...service = (HTTP, HTTPS) \
...time = lib.time("Working hours") \
...rule_log(session) \
...bandwidth_pool("1 Mbps") \
...name("Test traffic shaping rule") \
...desc("Test traffic shaping rule description") \
...enabled(true)
...
Admin@nodename# show network-policy traffic-shaping 1
```

```
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  dst.zone = Untrusted \
  service = (HTTP, HTTPS) \
  time = lib.time("Working hours") \
  desc("Test traffic shaping rule description") \
  rule_log(session) \
  bandwidth_pool("1 Mbps") \
  enabled(true) \
  id(e63c34e6-af7f-4a4d-a29d-b51d4070655c) \
  name("Test traffic shaping rule")
```

Для удаления правила управления пропускной способностью используется команда:

```
Admin@nodename# delete network-policy traffic-shaping <position>
```


Настройка фильтрации контента

Documentation: ☒
Version: 7.x
Product: NGFW

Настройка правил контентной фильтрации производится на уровне **security-policy content-filtering**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила контентной фильтрации используется команда:

Admin@nodename# create security-policy content-filtering <position> upl-rule

Параметры правил контентной фильтрации:

Параметр	Описание
PASS DENY WARNING	Действие правила контентной фильтрации: PASS — разрешить посещение веб-страницы. DENY — блокировать веб-страницу. WARNING — предупредить пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила контентной фильтрации. Для указания названия правила: name("Content filtering rule example") .
desc	Описание правила. Например: desc("Content filtering rule example set via CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. rule_log(yes) или rule_log(true) — включить журналирование.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
virus_usergate	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием Запретить , возможны значения: virus_usergate = yes или virus_usergate = true — использовать проверку потоковым антивирусом UserGate. virus_usergate = no или virus_usergate = false — не использовать проверку потоковым антивирусом UserGate.
Страница блокировки	Выбор страницы блокировки; если страница не указана, то используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например, DENY("Blockpage (RU)") . Подробнее о настройке страниц блокировки читайте в разделе Настройка шаблонов страниц . Можно использовать внешнюю страницу, задав внешний URL: redirect(302, "http://www.example.com") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило контентной фильтрации (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) . Чтобы указать группу сервисов: service = lib.service() ; в скобках необходимо указать название группы сервисов.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category() ; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL . Для указания категории URL: category = "URL category name" .
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url() ; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL .
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка типов контента: response.header.Content-Type = lib.mime() ; в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента .
morphology	Список баз словарей морфологии, по которым будут проверяться веб-страницы. Для задания списка баз словарей морфологии: morphology = lib.morphology() ; в скобках необходимо указать название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе "Настройка морфологии" и.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent() ; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров .
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET .
request.header.Referer	Список URL, в котором указаны рефереры для текущей страницы, или категория URL, к которой относится реферер. Чтобы указать список или категорию URL: request.header.Referer = lib.url() (в скобках необходимо указать название списка) или request.header.Referer = "URL category" Подробнее о настройке списков URL через CLI читайте в разделе Настройка списков URL ; о категориях URL — Настройка категорий URL .
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правил контентной фильтрации используется команда:

```
Admin@nodename# set security-policy content-filtering <position> upl-rule
```

Для просмотра всех созданных правил контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering
```

Для просмотра определенного правила контентной фильтрации используется команда:

```
Admin@nodename# show security-policy content-filtering <position>
```

Пример создания правила контентной фильтрации с использованием UPL:

```
Admin@nodename# create security-policy content-filtering 1 upl-rule PASS \
...src.zone = Trusted \
...url = lib.url("Test URL list") \
...user = known \
...rule_log(yes) \
...name("Test content-filtering rule") \
...desc("Test content-filtering rule description") \
...enabled(true)
...
Admin@nodename# show security-policy content-filtering 1
% ----- 1 --- "Content Rules" -----
PASS \
  user = known \
  url = lib.url("Test URL list") \
  src.zone = Trusted \
  desc("Test content-filtering rule description") \
  rule_log(yes) \
  enabled(true) \
  id("96b2ee34-528a-4b06-8726-69711ba639ba") \
  name("Test content-filtering rule")
```

Для удаления существующего правила контентной фильтрации используется команда:

```
Admin@nodename# delete security-policy content-filtering <position>
```

Настройка веб-безопасности

Version: 7.x Product: NGFW Documentation: 	
Настройка веб-безопасности производится на уровне security-policy safe-browsing . Подробнее о структуре команд читайте в разделе UserGate Policy Language .	
Для создания правила веб-безопасности используется команда: Admin@nodename# create security-policy safe-browsing <position> upl-rule	
Параметры правил веб-безопасности:	
Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила веб-безопасности. Например: name("Safe browsing rule example") .
desc	Описание правила, например, desc("Safe browsing rule example set via CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • rule_log(no) или rule_log(false) - отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. • rule_log(yes) или rule_log(true) - включить журналирование
enable_adblock	Блокировка рекламы • enable_adblock(yes) или enable_adblock(true). • enable_adblock(no) или enable_adblock(false).
url_list_exclusions	Список сайтов, для которых блокировать рекламу не требуется: url_list_exclusions("URL list name") . О создании и настройке списков URL с использованием CLI читайте в разделе Настройка списков URL .
enable_injector	Инъектирование кода в веб страницы: • enable_injector(yes) или enable_injector(true). • enable_injector(no) или enable_injector(false).
custom_injector	Код инжектора.
safe_search	Использование функции безопасного поиска: • safe_search(yes) или safe_search(true). • safe_search(no) или safe_search(false).
search_history_logging	Журналирование поисковых запросов пользователей: • search_history_logging(no) или search_history_logging(false) - отключить журналирование поисковых запросов пользователей. Если при создании правила search_history_logging не указано, функция журналирования отключена. • search_history_logging(yes) или search_history_logging(true) - включить журналирование поисковых запросов пользователей.
social_sites_block	Блокировка приложений социальных сетей: • social_sites_block(yes) или social_sites_block(true). • social_sites_block(no) или social_sites_block(false).
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 .
user	Пользователи и группы пользователей, для которых применяется правило веб-безопасности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\user1" user = ("user", "testd.local\user1")
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правил веб-безопасности используется команда:

Admin@nodename# set security-policy safe-browsing <position> upl-rule

Для просмотра всех созданных правил веб-безопасности используется команда:

Admin@nodename# show security-policy safe-browsing

Для просмотра определенного правила веб-безопасности используется команда:

```
Admin@nodename# show security-policy safe-browsing <position>
```

Пример создания правила веб-безопасности с помощью UPL:

```
Admin@nodename# create security-policy safe-browsing 1 upl-rule PASS \
...user = known \
...src.zone = Trusted \
...enable_adblock(yes) \
...safe_search(yes) \
...rule_log(yes) \
...name("Test safe browsing rule") \
...desc("Test safe browsing rule description") \
...enabled(true)
...
Admin@nodename# show security-policy safe-browsing 1
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  rule_log(yes) \
  enable_adblock(yes) \
  safe_search(yes) \
  desc("Test safe browsing rule description") \
  enabled(true) \
  id("406a2753-750e-4830-82a8-583043e72359") \
  name("Test safe browsing rule")
```

Для удаления правила веб-безопасности используется команда:

```
Admin@nodename# delete security-policy safe-browsing <position>
```

Настройка правил инспектирования туннелей

Version: 7.x
Product: NGFW
Documentation: 

Настройка правил инспектирования туннелей производится на уровне **security-policy tunnel-inspection**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила инспектирования туннелей используется команда:

Admin@nodename# create security-policy tunnel-inspection <position> upl-rule

Параметры правил инспектирования туннелей:

Параметр	Описание
OK PASS	Действие правила инспектирования туннелей: - OK — Инспектировать. - PASS — Не расшифровывать
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила инспектирования туннелей. Например: name("Tunnel inspection rule example").
desc	Описание правила. Например: desc("Tunnel inspection rule example configured via CLI").
service	Тип туннеля: - service = gre : инспектирование туннелей GRE. - service = gtpu : инспектирование туннелей GTP-U. - service = ipsec_null : инспектирование нешифрованных IPsec-туннелей
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика, например, dst.zone = "Tunnel inspection zone" . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Для редактирования правил инспектирования туннелей используется команда:

Admin@nodename# set security-policy tunnel-inspection <position> upl-rule

Для просмотра всех созданных правил инспектирования туннелей используется команда:

Admin@nodename# show security-policy tunnel-inspection

Для просмотра определенного правила инспектирования туннелей используется команда:

Admin@nodename# show security-policy tunnel-inspection <position>

Пример создания правила инспектирования туннелей:

```
Admin@nodename# create security-policy tunnel-inspection 1 upl-rule PASS \
...src.zone = Untrusted \
...dst.zone = Trusted \
...service = ipsec_null \
...name("Test tunnel-inspection rule") \
...desc("Test tunnel-inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy tunnel-inspection 1
% ----- 1 -----
PASS \
  src.zone = Untrusted \
  dst.zone = Trusted \
  service = ipsec_null \
  desc("Test tunnel-inspection rule description") \
  enabled(true) \
  id("051cf677-3d36-4d5c-968f-73c3421c2b28") \
  name("Test tunnel-inspection rule")
```

Для удаления правила инспектирования туннелей используется команда:

Admin@nodename# delete security-policy tunnel-inspection <position>

Настройка инспектирования SSL

Version: 7.x
Product: NGFW
Documentation: 

Настройка правил инспектирования SSL производится на уровне **security-policy ssl-inspection**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила инспектирования SSL используется команда:

Admin@nodename# create security-policy ssl-inspection <position> upl-rule

Параметры правил инспектирования SSL:

Параметр	Описание
OK PASS	Действие правила инспектирования SSL: OK — Расшифровать. PASS — Не расшифровывать OK ... forward — Расшифровать и переслать; forward указывается среди свойств правила. При настройке правила с действием Расшифровать и переслать необходимо указать профиль пересылки SSL. Подробнее о создании и настройке с использованием CLI профилей пересылки читайте в разделе Настройка профилей пересылки SSL.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила инспектирования SSL. Для указания названия правила: name("SSL inspection rule example") .
desc	Описание правила. Например: desc("SSL inspection rule example configured in CLI") .
ssl_forward_profile	Профиль пересылки SSL; профиль необходимо указать при настройке правила инспектирования SSL с действием Расшифровать и переслать. Указывается в формате: ssl_forward_profile("SSL forward profile example") .
ssl_profile	Профиль SSL; указывается: ssl_profile("Default SSL profile") . Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. rule_log(yes) или rule_log(true) — включить журналирование.
block_invalid_cert	Блокирование доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат отозван, выписан на другое доменное имя или недоверенным центром сертификации, срок действия сертификата истёк. Доступно в правилах с действием Расшифровать : block_invalid_cert(yes) или block_invalid_cert(true) — включение блокировки. block_invalid_cert(no) или block_invalid_cert(false) — отключение блокировки.
check_revoc_cert	Проверка сертификата сайта в списке отозванных сертификатов (CRL) и блокирование доступа, если он там найден. Доступно в правилах с действием Расшифровать : check_revoc_cert(yes) или check_revoc_cert(true) — включение проверки сертификата. check_revoc_cert(no) или check_revoc_cert(false) — отключение проверки сертификата.
block_expired_cert	Блокирование сертификатов с истёкшим сроком действия. Доступно в правилах с действием Расшифровать : block_expired_cert(yes) или block_expired_cert(true) — включить блокировку сертификатов с истёкшим сроком действия. block_expired_cert(no) или block_expired_cert(false) — отключить блокировку сертификатов с истёкшим сроком действия.
block_self_signed_cert	Блокирование самоподписанных сертификатов. Доступно в правилах с действием Расшифровать : block_self_signed_cert(yes) или block_self_signed_cert(true) — включить блокировку самоподписанных сертификатов. block_self_signed_cert(no) или block_self_signed_cert(false) — отключить блокировку самоподписанных сертификатов.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSL (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .

Параметр	Описание
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 .
service	Тип сервиса: HTTPS , SMTPS или POP3S . Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) .
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category() ; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL . Для указания категории URL: category = "URL category name" .
url	Списки доменных имён, для которых применяется правило инспектирования SSL. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена типа www.example.com , а не http://www.example.com/home/ . Для указания списка доменов: url = lib.url() ; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки читайте в разделе Настройка списков URL .
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Для редактирования правил инспектирования SSL используется команда:

```
Admin@nodename# set security-policy ssl-inspection <position> upl-rule
```

Для просмотра параметров всех созданных правил инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection
```

Для просмотра параметров определенного правила инспектирования SSL используется команда:

```
Admin@nodename# show security-policy ssl-inspection <position>
```

Пример создания правила инспектирования SSL:

```
Admin@nodename# create security-policy ssl-inspection 1 upl-rule OK \
...user = unknown \
...ssl_profile("Default SSL profile") \
...rule_log(yes) \
...name("Decrypt all test rule") \
...desc("Description for decrypt all rest rule") \
...enabled(true)
...
Admin@nodename# show security-policy ssl-inspection 1
% ----- 1 -----
OK \
  user = unknown \
  desc("Description for decrypt all rest rule") \
  rule_log(yes) \
  ssl_profile("Default SSL profile") \
  enabled(true) \
  id("134b7274-01ee-47db-9fc1-a2f06b340b94") \
  name("Decrypt all test rule")
```

Для удаления правила инспектирования SSL используется команда:

```
Admin@nodename# delete security-policy ssl-inspection <position>
```

Настройка инспектирования SSH

Version: 7.x
Product: NGFW
Documentation: 

Настройка правил SSH-инспектирования производится на уровне **security-policy ssh-inspection**. О структуре команд читайте подробнее в разделе [UserGate Policy Language](#).

Для создания правила инспектирования SSH используется команда:

Admin@nodename# create security-policy ssh-inspection <position> upl-rule

Параметры правил инспектирования SSH:

Параметр	Описание
OK PASS	Действие правила инспектирования SSH: - OK — Расшифровать. - PASS — Не расшифровывать
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила инспектирования SSH. Для указания названия правила: name("SSH inspection rule example") .
desc	Описание правила. Например: desc("SSH inspection rule example configured in CLI") .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: - rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. - rule_log(yes) или rule_log(true) — включить журналирование.
block_ssh_shell	Блокирование удалённого запуска shell (интерпретатора командной строки, оболочки). Доступно в правилах с действием Расшифровать : - block_ssh_shell(yes) или block_ssh_shell(true) — включить блокировку. - block_ssh_shell(no) или block_ssh_shell(false) -отключить блокировку.
block_ssh_exec	Блокирование удалённого выполнения по SSH. Доступно в правилах с действием Расшифровать : - block_ssh_exec(yes) или block_ssh_exec(true) — включить блокировку. - block_ssh_exec(no) или block_ssh_exec(false) — отключить блокировку.
ssh_command	Команда linux, которую требуется передать, в формате ssh user@host 'command' Например: ssh_command("ssh root@192.168.1.1 reboot") . Редактирование команды SSH доступно в правилах с действием Расшифровать .
block_sftp	Блокирование соединения SFTP (Secure File Transfer Protocol). Доступно в правилах с действием Расшифровать : - block_sftp(yes) или block_sftp(true) — включить блокировку соединения. - block_sftp(no) или block_sftp(false) — отключить блокировку соединения.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSH (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testld.local\user1" user = ("user", "testld.local\user1")
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) . Чтобы указать группу сервисов: service = lib.service() ; в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей.

Для редактирования правил инспектирования SSH используется команда:

```
Admin@nodename# set security-policy ssh-inspection <position> upl-rule
```

Для просмотра всех созданных правил инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection
```

Для просмотра определенного правила инспектирования SSH используется команда:

```
Admin@nodename# show security-policy ssh-inspection <position>
```

Пример создания правила инспектирования SSH с использованием UPL:

```
Admin@nodename# create security-policy ssh-inspection 1 upl-rule OK \
...service = ("Any TCP") \
...block_ssh_shell(yes) \
...block_sftp(yes) \
...rule_log(yes) \
...name("Test SSH inspection rule") \
...desc("Test SSH inspection rule description") \
...enabled(true)
...
Admin@nodename# show security-policy ssh-inspection 1
% ----- 1 -----
OK \
  service = "Any TCP" \
  block_ssh_shell(yes) \
  block_sftp(yes) \
  desc("Test SSH inspection rule description") \
  rule_log(yes) \
  enabled(true) \
  id(d703f390-896f-47c2-91bd-69c6d37aa6d2) \
  name("Test SSH inspection rule")
```

Для удаления правила инспектирования SSH используется правило:

```
Admin@nodename# delete security-policy ssh-inspection <position>
```

Настройка COB

Version: 7.x
Product: NGFW
Documentation: 

Настройка параметров [управления загрузкой](#) системы обнаружения и предотвращения вторжений производится на уровне security-policy intrusion-prevention.

Admin@nodename# set security-policy intrusion-prevention <parameter>

Доступны параметры:

Параметр	Описание
flow-control	Включение/отключение функции flow control (доступно в версии 7.4.0 и выше): - on — функция включена; - off — функция отключена.
mode	Включение/отключение режима умного сканирования (сканируется часть проходящих пакетов сессии в пределах установленного лимита): - on — режим включен; - off — режим отключен.
limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Посмотреть установленные настройки можно с помощью команды:

Admin@nodename# show security-policy intrusion-prevention

По умолчанию функция flow control и режим умного сканирования включены; проверяются первые 200 КБ каждой сессии.

[Профили COB](#) создаются в библиотеке элементов и добавляются в [правила межсетевое экрана](#) для активации системы обнаружения и предотвращения вторжений.

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка правил защиты почтового трафика

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила защиты почтового трафика используется следующая команда:

```
Admin@nodename# create security-policy mail-security <position> upl-rule
```

Параметры правил защиты почтового трафика:

Параметр	Описание
PASS WARNING DENY("with error") DENY	Действие правила защиты почтового трафика: PASS — Пропустить — пропустить трафик без изменения. WARNING — Маркировать — маркировать почтовые сообщения специальным тэгом в теме письма или дополнительном поле. DENY("with error") — Блокировать с ошибкой — блокировать письмо и сообщать об ошибке доставки письма серверу SMTP (для SMTP(S)-трафика) или клиенту (для POP3(S)-трафика). DENY — Блокировать без ошибки — блокировать письмо без уведомления о блокировке.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила защиты почтового трафика. Например: name("Mail security rule example") .
desc	Описание правила. Например: desc("Mail security rule example configured in CLI") .
rule_log	Запись в журнал информации о срабатывании правила защиты почтового трафика. Возможны варианты: rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. rule_log(yes) или rule_log(true) — включить журналирование.
antispam_usergate	Проверка почтового трафика антиспамом UserGate (задаётся для правил с действием Маркировать , Блокировать с ошибкой или Блокировать без ошибки): antispam_usergate(yes) или antispam_usergate(true) — включить проверку. antispam_usergate(no) или antispam_usergate(false) — отключить проверку.
dnsbl	Антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику в правилах с действием Маркировать , Блокировать с ошибкой или Блокировать без ошибки : dnsbl(yes) или dnsbl(true) — использовать антиспам-проверку. dnsbl(no) или dnsbl(false) — отключить использование антиспам-проверки. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам и вирусы.
mark_hdr	Заголовок. Поле куда помещать тег маркировки; задаётся для правил с действием Маркировать : mark_hdr(Subject) .
mark	Текст тега, который маркирует письмо; задаётся для правил с действием Маркировать , например, mark("Text for marking emails") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты почтового трафика (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\user1" user = ("user", "testd.local\user1")
dst.zone	Зона назначения трафика, например, dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
service	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило. Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) .
envelope_from	Почтовый адрес отправителя письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_from = "Sender email group" . Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов .
envelop_to	Почтовый адрес адресата письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: envelope_to = "Receiver email group" . Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов .

Для редактирования правила защиты почтового трафика используется команда:

```
Admin@nodename# set security-policy mail-security <position> upl-rule
```

Для просмотра параметров всех созданных правил защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security
```

Для просмотра параметров определенного правила защиты почтового трафика используется команда:

```
Admin@nodename# show security-policy mail-security <position>
```

Пример создания правила защиты почтового трафика:

```
Admin@nodename# create security-policy mail-security 1 upl-rule WARNING \
...src.zone = Untrusted \
...service = (SMTP, POP3, SMTPS, POP3S) \
...mark_hdr(Subject) \
...mark("SPAM") \
...antispam_usergate(yes) \
...rule_log(yes) \
...name("Test SMTP and POP3 filtering") \
...desc("Test SMTP and POP3 filtering description") \
...enabled(true)
...
Admin@nodename# show security-policy mail-security 1
% ----- 1 -----
WARNING \
src.zone = Untrusted \
service = (SMTP, POP3, SMTPS, POP3S) \
rule_log(yes) \
desc("Test SMTP and POP3 filtering description") \
mark_hdr(Subject) \
mark("SPAM") \
antispam_usergate(yes) \
enabled(true) \
id("7d86d348-9619-4097-94d1-bad4f3e85554") \
name("Test SMTP and POP3 filtering")
```

Для удаления правила защиты почтового трафика используется команда:

```
Admin@nodename# delete security-policy mail-security <position>
```

Настройка антиспама

Параметры антиспама настраиваются на уровне **security-policy mail-security-antispam**.

Для настройки параметров антиспама используется следующая команда:

```
Admin@nodename# set security-policy mail-security-antispam <parameters>
```

Параметры настройки антиспама:

Параметр	Описание
batv-enabled	on/off. Включение/выключение защиты BATV (Bounce Address Tag Validation), предотвращающей рассылку спам-сообщений в виде возвратных сообщений.
dnsbl-servers	Указание списка DNSBL-серверов для проверки SMTP-трафика.
dnsbl-black-list	Список запрещенных серверов в дополнение к тем, что есть в списках DNSBL. Возможно добавление списка по GeoIP, или списка IP-адресов.
dnsbl-white-list	Список серверов, исключенных из DNSBL проверки. Возможно добавление списка по GeoIP, или списка IP-адресов.

Для просмотра параметров антиспама используется следующая команда:

```
Admin@nodename# show security-policy mail-security-antispam <parameters>
```

Возможен просмотр всех настроек антиспама целиком (по нажатию Enter), или отдельно белого/черного списков DNSBL при указании параметров **dnsbl-white-list** или **dnsbl-black-list**.

Для удаления параметров антиспама используется следующая команда:

```
Admin@nodename# delete security-policy mail-security-antispam <parameters>
```

Возможно удаление серверов DNSBL, белого/черного списков DNSBL.

Настройка правил ICAP

Documentation: 
Product: NGFW
Version: 7.x

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Для создания правила ICAP используется команда:

Admin@nodename# create security-policy icap-rules <position> upl-rule

Параметры правил ICAP:

Параметр	Описание
PASS OK	Действие правила ICAP: PASS — Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. OK — Переслать — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера (стандартный режим работы большинства ICAP-серверов). OK ... ignore — Переслать и игнорировать — переслать данные ICAP-сервер и игнорировать ответ от ICAP-сервера (вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика); ignore указывается среди свойств правила.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила ICAP. Для указания названия правила: name("ICAP rule example") .
desc	Описание правила. Например: desc("ICAP rule example set via CLI") .
profile	ICAP-серверы, куда UserGate будет пересылать запросы; указывается в формате: profile("Example ICAP server") . О настройке серверов ICAP через CLI читайте в разделе Настройка ICAP-серверов .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило ICAP (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка: response.header.Content-Type = lib.mime() ; в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента .
category	Список категорий или категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: category = lib.category() ; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL . Для указания категории URL: category = "URL category name" .
url	Списки URL, для которых будет применяться правило. Для указания списка URL: url = lib.url() ; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL .
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: http.method = GET .

Параметр	Описание
service	Тип сервиса: HTTP , SMTP или POP3 . Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) .

Для редактирования правила ICAP используется команда:

```
Admin@nodename# set security-policy icap-rules <position> upl-rule
```

Для просмотра параметров всех созданных ICAP правил используется команда:

```
Admin@nodename# show security-policy icap-rules
```

Для просмотра параметров определенного правила ICAP:

```
Admin@nodename# show security-policy icap-rules <position>
```

Пример создания правила ICAP:

```
Admin@nodename# create security-policy icap-rules 1 upl-rule PASS \
...src.zone = Trusted \
...http.method = (GET, POST) \
...profile("ICAP server1") \
...name("Test ICAP rule") \
...desc("Test ICAP rule description") \
...enabled(true)
...
Admin@nodename# show security-policy icap-rules 1
% ----- 1 -----
PASS \
  src.zone = Trusted \
  http.method = (GET, POST) \
  desc("Test ICAP rule description") \
  profile("ICAP server1") \
  enabled(true) \
  id("80a7dca6-96f7-42c8-baad-8716be8d3b93") \
  name("Test ICAP rule")
```

Для удаления правила ICAP используется команда:

```
Admin@nodename# delete security-policy icap-rules <position>
```

Настройка ICAP-серверов

Product: NGFW
Documentation: 
Version: 7.x

Настройка ICAP-серверов производится на уровне **security-policy icap-server**.

Структура команды для создания ICAP-сервера:

Admin@nodename# create security-policy icap-server <parameter>

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя ICAP-сервера.
description	Задать описание ICAP-сервера.
ip	Задать IP-адрес ICAP-сервера.
port	Задать TCP-порт ICAP-сервера; значение по умолчанию: 1344.
max-msg-size	Определить максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установка значения поля в 0 может использоваться для проверки подключения к ICAP-серверу.
check-icap	Задать период проверки доступности сервера ICAP.
bypass	Если эта опция включена, то UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен.
reqmod-path	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Reqmod.
respmod-path	Использовать режим Respmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Respmod.
user-header	Установить отсылку имени пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. • off — не отсылать имя пользователя на ICAP-сервер.
user-encode	Установить кодировку имени пользователя в Base64: • on. • off.
ip-header	Установить отсылку IP-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. • off — не отсылать IP-адрес пользователя на ICAP-сервер.
mac-header	Установить отсылку MAC-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. • off — не отсылать MAC-адрес пользователя на ICAP-сервер.

Структура команды для обновления существующего ICAP-сервера:

Admin@nodename# set security-policy icap-server <server-name> <parameter>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового ICAP-сервера.

Структура команды для отображения информации об ICAP-сервере:

Admin@nodename# show security-policy icap-server <server-name>

Структура команды для удаления ICAP-сервера:

Admin@nodename# delete security-policy icap-server <server-name>

Настройка профилей DoS

Documentation: 
Product: NGFW
Version: 7.x

Настройка профилей DoS производится на уровне **security-policy dos-profile**.

Структура команды для создания профиля DoS:

Admin@nodename# create security-policy dos-profile <parameter>

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя профиля.
description	Задать описание профиля.
aggregate	Установить суммирование количества пакетов, проходящих в секунду для всех IP адресов или подсчёт индивидуально для каждого IP-адреса.
syn	Настройка защиты от сетевого флуда для протокола TCP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
udp	Настройка защиты от сетевого флуда для протокола UDP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
icmp	Настройка защиты от сетевого флуда для протокола ICMP. • enabled — установить конфигурацию от сетевого флуда для выбранного протокола. • alert-threshold — задать порог уведомлений. • drop-threshold — задать порог отбрасывания пакетов.
max-sessions	Установить ограничение количества сессий: • <limit> — задать число сессий. • off — отключить ограничение числа сессий.

Структура команды для редактирования существующих профилей DoS:

Admin@nodename# set security-policy dos-profile <profile-name> <parameter>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды добавления нового профиля DoS.

Структура команды для удаления профиля:

Admin@nodename# delete security-policy dos-profile <profile-name>

Структура команды для отображения информации о профиле DoS:

Admin@nodename# show security-policy dos-profile <profile-name>

Настройка правил защиты DoS

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка правил защиты от DoS атак производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Структура команды для создания правила защиты от DoS атак:

Admin@nodename# create security-policy dos-rules <position> upl-rule <parameters>

Параметры правил защиты от DoS атак:

Параметр	Описание
PASS WARNING DENY	Действие правила защиты DoS: PASS — разрешить трафик; защита от DoS атак не применяется. WARNING — применить профиль защиты от DoS атак. DENY — безусловно блокировать трафик.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название правила защиты DoS. Например: name("DoS rule example") .
desc	Описание правила. Например: desc("DoS rule example configured in CLI") .
profile	Профиль защиты DoS. Выбор профиля доступен только для правил с действием Защитить (WARNING) . Для указания профиля: profile("DoS profile example") . О создании и настройке профилей защиты читайте в разделе Настройка профилей DoS .
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. rule_log(session) — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты DoS (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...) . Чтобы указать группу сервисов: service = lib.service() ; в скобках необходимо указать название группы сервисов.

Параметр	Описание
time	Настройка расписания работы правила. Для установки расписания: time = lib.time() ; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей .

Структура команды для редактирования правила защиты от DoS атак:

```
Admin@nodename# set security-policy dos-rules <position> upl-rule <parameters>
```

Структура команды для просмотра правил защиты от DoS атак:

```
Admin@nodename# show security-policy dos-rules
Admin@nodename# show security-policy dos-rules <position>
```

Пример создания правила защиты от DoS атак с помощью UPL:

```
Admin@nodename# create security-policy dos-rules 1 upl-rule WARNING \
...src.zone = Untrusted \
...dst.zone = DMZ \
...service = (HTTP, HTTPS) \
...profile("Test DoS profile") \
...rule_log(session) \
...name("Test DoS rule") \
...desc("Test DoS rule description") \
...enabled(true)
...
Admin@nodename# show security-policy dos-rules 1
% ----- 1 -----
WARNING \
src.zone = Untrusted \
dst.zone = DMZ \
service = (HTTP, HTTPS) \
desc("Test DoS rule description") \
rule_log(session) \
profile("Test DoS profile") \
enabled(true) \
id("69da2f83-59ae-4a7d-b595-f6ff31bf34c6") \
name("Test DoS rule")
```

Структура команды для удаления правила защиты от DoS атак:

```
Admin@nodename# delete security-policy dos-rules <position>
```


Настройка веб-портала

Documentation: 
Product: NGFW
Version: 7.x

Настройка веб-портала производится на уровне **global-portal web-portal**. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Структура команды создания страницы веб-портала:

Admin@nodename# create global-portal web-portal <position> upl-rule <parameters>

Параметры настройки закладок веб-портала:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название закладки. Например: name("Example of bookmark publishing").
desc	Описание закладки. Например: desc("Example of bookmark publishing configured in CLI").
url	URL ресурса, который необходимо опубликовать через веб-портал. Необходимо указывать полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. URL указывается как url = "http://www.example.com" .
url.domain	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Для указания домена прямого доступа: url.domain = "example.com".
rdp_check_session_alive	Разрыв сессии RDP по завершению авторизации на веб-портале: - rdp_check_session_alive(yes) или rdp_check_session_alive(true) — разрывать сессию. - rdp_check_session_alive(no) или rdp_check_session_alive(false) — не разрывать сессию.
ssl_profile	Профиль SSL для построения защищенного канала для отображения веб-портала; указывается: ssl_profile("SSL profile example").
certificate	Сертификат, который будет использоваться для создания HTTPS-соединения. Чтобы задать сертификат: certificate("Certificate example").
icon	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку. Можно указать: - icon("Default icon name") — использовать штатную иконку (в скобках указывается название штатной иконки). - icon("Icon encoded with Base64") — использовать свою иконку. Необходимо указать содержимое файла, кодированное с использованием Base64. - icon("http://www.icon-url-example.com") — указать URL для использования сторонней иконки.
additional_url	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Для указания: additional_url("http://additional-url-example.com").
user	Пользователи и группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: user = known user = "user" user = "testd.local\user1" user = ("user", "testd.local\user1")

Для редактирования правила веб-портала используется команда:

Admin@nodename# set global-portal web-portal <position> upl-rule <parameters>

Для просмотра параметров правил веб-портала используется команда:

Admin@nodename# show global-portal web-portal <position>

Пример создания правила веб-портала с использованием UPL:

```
Admin@nodename# create global-portal web-portal 1 upl-rule OK \  
...user = "CN=Default Group,DC=LOCAL" \  
...url = "http://www.intranet.loc" \  
...name("Test web portal") \  
...desc("Test web portal description") \  
...enabled(true)  
...  
Admin@nodename# show global-portal web-portal 1  
% ----- 1 -----  
OK \  
  user = "CN=Default Group,DC=LOCAL" \  
  url = "http://www.intranet.loc" \  
  icon("default.svg") \  
  desc("Test web portal description") \  
  enabled(true) \  
  id("2fead5a1-29c3-4835-bbdb-1d0e07f84c28") \  
  name("Test web portal")
```

Для удаления правила веб-портала используется команда:

Admin@nodename# delete global-portal web-portal <position>

Настройка правил reverse-прокси

Documentation: ☒
Product: NGFW
Version: 7.x

Правила reverse-прокси настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд читайте в разделе [UserGate Policy Language](#).

Структура команды для создания правила reverse-прокси:

Admin@nodename# create global-portal reverse-proxy-rules <position> upl-rule <parameters>

Параметры настройки правил reverse-прокси:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название правила reverse-прокси. Например: name("Reverse proxy rule example") .
desc	Описание правила. Например: desc("Reverse proxy rule example set via CLI") .
profile	Сервер reverse-прокси, куда NGFW будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example") .
url.port	Порт, на котором NGFW будет слушать входящие запросы, например, url.port = 80 .
is_https	Поддержка HTTPS: - is_https(yes) или is_https(true) — использовать HTTPS. - is_https(no) или is_https(false) — не использовать HTTPS.
ssl_profile	Профиль SSL; указывается при использовании HTTPS: ssl_profile("Default SSL profile") . Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL .
certificate	Сертификат, используемый для поддержки HTTPS-соединения. Указывается при использовании HTTPS: certificate("Certificate example") .
cert_auth_enabled	Аутентификация по сертификату: - cert_auth_enabled(yes) или cert_auth_enabled(true) — включить авторизацию по сертификату. - cert_auth_enabled(no) или cert_auth_enabled(false) — отключить авторизацию по сертификату.
src.zone	Зона источника трафика. Для указания зоны источника, например, Untrusted: src.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов назначения: dst.ip = lib.url() ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
dst.geoip	Указание GeoIP; необходимо указать код страны (например, dst.geoip = RU). Коды названий стран доступны по ссылке ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent() ; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров .
rewrite_path	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2. Для этого необходимо указать: rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2") .

Для редактирования правила reverse-прокси используется команда:

```
Admin@nodename# set global-portal reverse-proxy-rules <position> upl-rule <parameters>
```

Для просмотра параметров правила reverse-прокси используется команда:

```
Admin@nodename# show global-portal reverse-proxy-rules <position>
```

Пример создания правила reverse-прокси:

```
Admin@nodename# create global-portal reverse-proxy-rules 1 upl-rule OK \
...url.port = 80 \
...src.zone = Untrusted \
...profile("Reverse proxy server1") \
...rewrite_path("example.com/path1", "example.local/path2") \
...name("Test reverse proxy rule") \
...desc("Test reverse proxy rule description") \
...enabled(true)
...
Admin@nodename# show global-portal reverse-proxy-rules 1
% ----- 1 -----
OK \
url.port = 80 \
src.zone = Untrusted \
desc("Test reverse proxy rule description") \
profile("Reverse proxy server1") \
rewrite_path("example.com/path1", "example.local/path2") \
enabled(true) \
id("7dc7041a-6538-400b-8f1e-9b18287218ac") \
name("Test reverse proxy rule")
```

Для удаления правила reverse-прокси используется команда:

```
Admin@nodename# delete global-portal reverse-proxy-rules <position>
```

Настройка серверов reverse-прокси

Documentation: 
Product: NGFW
Version: 7.x

Настройка серверов reverse-прокси производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера reverse-прокси используется следующая команда:

Admin@nodename# create global-portal reverse-proxy-servers <parameter>

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера reverse-прокси.
description	Описание сервера reverse-прокси.
address	Адрес или домен сервера reverse-прокси.
port	TCP-порт сервера reverse-прокси.
https	Использование протокола HTTPS до публикуемого сервера: • on: использовать. • off: не использовать.
keep-source-ip	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: • on: оставить оригинальный IP-адрес источника. • off: заменить IP-адрес источника на IP-адрес UserGate. Важно! Если в пакетах сохраняется оригинальный IP-адрес источника, для корректной работы необходимо настроить маршрутизацию таким образом, чтобы веб-сервер отвечал через тот же сетевой интерфейс UG NGFW, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UG NGFW или можно настроить статические маршруты через UG NGFW для «белых» IP-адресов источников.

Команда для редактирования параметров сервера reverse-прокси:

Admin@nodename# set global-portal reverse-proxy-servers <server-name> <parameter>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для отображения информации о сервере reverse-прокси:

Admin@nodename# show global-portal reverse-proxy-servers <server-name>

Структура команды для удаления сервера:

Admin@nodename# delete global-portal reverse-proxy-servers <server-name>

Настройка серверных правил

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

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе [UserGate Policy Language](#).

Для создания серверного правила VPN используется команда:

Admin@nodename# create vpn server-rules <position> upl-rule <parameters>

При настройке необходимо указать:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания.
name	Название серверного правила VPN. Например: name("VPN server rule example").
desc	Описание правила. Например: desc("VPN server rule example configured in CLI").
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile"). Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
vpn_network	Сеть VPN. Для указания сети: vpn_network("VPN network example"). О настройках сети VPN с использованием интерфейса командной строки читайте в разделе Настройка сетей VPN .
auth_profile	Профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль аутентификации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Чтобы указать профиль аутентификации: auth_profile("Example user auth profile"). Подробнее о создании и настройке профилей аутентификации с использованием интерфейса командной строки читайте в разделе Настройка профилей аутентификации .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel1). О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
ep_only	Опция (доступна начиная с релиза ПО 7.1.2) позволяет ограничить возможность подключения по данному правилу только для VPN-клиентов UserGate Client (true, false).
src.zone	Зона, с которой разрешено принимать подключения к VPN. Для указания зоны источника, например, Untrusted: src.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов, с которых разрешено принимать подключения к VPN. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов интерфейса, на который будет происходить подключение клиентов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов .

Пример создания серверного правила VPN:

```
Admin@nodename# create vpn server-rules 3 upl-rule OK\
...name("Test server VPN rule") \
...desc("Test server VPN rule description") \
...profile("New server VPN profile") \
...vpn_network("Test VPN network") \
...auth_profile(Local) \
...interface(tunnel3) \
...src.zone = Untrusted \
...dst.ip = lib.network("UG address") \
...user = ("CN=VPN servers,DC=LOCAL") \
...enabled(true) \
```

Для редактирования серверного правила VPN:

```
Admin@nodename# set vpn server-rules <position> upl-rule <parameters>
```

Для удаления серверных правил VPN:

```
Admin@nodename# delete vpn server-rules <position>
```

Для просмотра сконфигурированных серверных правил VPN:

```
Admin@nodename# show vpn server-rules <position>
```

Настройка клиентских правил

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: VPN

Клиентские правила настраиваются на уровне **vpn client-rules**. Подробнее о структурах команд настройки клиентских правил читайте в разделе [UserGate Policy Language](#).

Команда для создания клиентского правила VPN:

Admin@nodename# create vpn client-rules <position> upl-rule <parameters>

При настройке правил необходимо указать:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false).
name	Название клиентского правила VPN. Например, name("VPN client rule example").
desc	Описание клиентского правила VPN. Указывается, как desc("VPN client rule example set in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile"). Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel3). О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
server_address	IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на NGFW, выполняющего роль VPN-сервера. Задаётся в формате: server_address("1.2.3.4").

При отображении правил, помимо заданных условий и свойств, будут показаны последняя ошибка VPN и статус подключения.

Пример создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules 2 upl-rule OK\  
...name("Test VPN client rule") \  
...desc("Test VPN client rule description") \  
...profile("Client VPN profile") \  
...interface(tunnel3) \  
...server_address("10.10.0.1") \  
...enabled(true) \
```

Для редактирования клиентского правила VPN:

Admin@nodename# set vpn client-rules <position> upl-rule <parameters>

Для удаления клиентского правила VPN:

Admin@nodename# delete vpn client-rules <position>

Для просмотра параметров созданных клиентских правил VPN:

Admin@nodename# show vpn client-rules <position>

Настройка сетей VPN

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: VPN

Настройка VPN-сетей производится на уровне **vpn networks**.

Для создания сети VPN необходимо использовать следующую команду:

Admin@nodename# create vpn networks <parameters>

Настраиваемые параметры сети VPN:

Параметр	Описание
name	Название сети VPN.
description	Описание сети VPN.
ip-range	Диапазон IP-адресов, которые будут использованы клиентами и сервером; указывается в формате: <IP_start-IP_end>. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
mask	Маска сети, например, 255.255.255.0.
use-system-dns	Назначение клиенту DNS-серверов, которые использует UserGate: • on: использовать системных DNS-серверов. • off: не использовать системных DNS-серверов.
dns-servers	DNS-серверы, которые будут переданы клиенту.
routes-ip	Маршрут VPN. Необходимо указать IP-адрес в формате "A.B.C.D" или "A.B.C.D/m".
routes-ip-list	Маршрут VPN. Необходимо указать группу IP-адресов. Подробнее о создании групп IP-адресов через CLI читайте в разделе Настройка IP-адресов .
all-routes	Отсутствие ограничений на маршрутизацию по VPN соединению при использовании UserGate VPN клиента.
include-routes-ip	IP-адреса, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
include-routes-ip-list	Список IP-адресов, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip	IP-адреса, доступ к которым зарыт через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip-list	Список IP-адресов, доступ к которым закрыт через VPN соединение при использовании UserGate VPN клиента.
restrict-lan-access	Запрет доступа к локальной сети при использовании UserGate VPN клиента.

Пример команды создания сети VPN:

Admin@nodename# create vpn networks name "Test VPN network" description "This is a new test VPN network" ip-range 10.10.3.2-10.10.2.200 mask 255.255.255.0

Редактирование параметров сети:

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

Удаление сети VPN или отдельных параметров сети VPN:

Admin@nodename# delete vpn networks <network-name>

Просмотр информации о сети VPN:

Admin@nodename# show vpn networks <network-name>

Настройка профилей безопасности VPN

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: VPN

Начиная с версии nodename 7.1.0 определены два типа профилей безопасности VPN — серверные и клиентские.

Профили безопасности VPN настраиваются на уровне **vpn server-security-profiles** и **vpn client-security-profiles**.

Создание серверного профиля безопасности VPN

Для создания серверного профиля безопасности VPN предназначена следующая команда:

Admin@nodename# create vpn server-security-profiles <parameters>

Настраиваемые параметры серверного профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Версия протокола, используемого для создания защищённого канала связи между двумя сетями. Возможны следующие варианты: - ipsec — IPsec(IKEv1). - ipsec-l2tp — IPsec(IKEv1)/L2TP. - ikev2 — IPsec(IKEv2).
ike-mode	Режим IKE: - main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. - aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
local-id-type	Тип параметра IKE local ID. Необходим для валидации peer-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: - none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. - IPv4 — IP-адрес узла. - FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). - CIDR — Адрес узла в формате бесклассовой адресации (CIDR).
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
authentication-mode	Метод аутентификации. Возможна аутентификация с помощью логина и пароля посредством метода EAP (AAA) или посредством сертификатов (PKI).
user-certificate-profile	При выборе метода аутентификации с PKI необходимо указать сконфигурированный ранее профиль клиентских сертификатов.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: - off — Механизм отключен. DPD запросы не отсылаются. - always — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. - idle — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. - Group 1 Prime 768 bit. - Group 2 Prime 1024 bit. - Group 5 Prime 1536 bit. - Group 14 Prime 2048 bit. - Group 15 Prime 3072 bit. - Group 16 Prime 4096 bit. - Group 17 Prime 6144 bit. - Group 18 Prime 8192 bit.

Параметр	Описание
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: Admin@nodename# create vpn server-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name> Доступны: - auth-alg: выбор алгоритма аутентификации. - MD5. - SHA1. - SHA256. - SHA384. - SHA512. - encrypt-alg: выбор алгоритма шифрования. - DES. 3DES. - AES128. - AES192. - AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifetime-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifetime	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа , phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом , key-lifetime), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off .
nat-keepalive	Период отправки пакетов NAT kepalive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keeralive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keeralive в сторону реер-узла для поддержания сесси NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: Admin@nodename# create vpn server-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name> Доступны: - auth-alg: выбор алгоритма аутентификации. - MD5. - SHA1. - SHA256. - SHA384. - SHA512. - encrypt-alg: выбор алгоритма шифрования. - DES. 3DES. - AES128. - AES192. - AES256.

Создание клиентского профиля безопасности VPN

Для создания клиентского профиля безопасности VPN предназначена следующая команда:

Admin@nodename# create vpn client-security-profiles <parameter>

Настраиваемые параметры клиентского профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Протокол установления VPN канала. Возможны следующие варианты выбора поля: - ipsec-l2tp — IPsec(IKEv1)/L2TP VPN. - ipsec — IPsec(IKEv1) VPN с оборудованием сторонних производителей. - ikev2 — IPsec(IKEv2) VPN.
ike-mode	Режим IKE: - main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. - aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
local-id-type	Тип параметра IKE local ID. Необходим для валидации реер-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: - none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. - IPv4 — IP-адрес узла. - FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). - CIDR — Адрес узла в формате бесклассовой адресации (CIDR).

Параметр	Описание
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
authentication-login	Логин, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.
authentication-password	Пароль, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
vpn-local-network	IP-адрес разрешенной локальной подсети для организации VPN с узлом Cisco.
vpn-remote-network	IP-адрес разрешенной подсети со стороны удаленного VPN-сервера для организации VPN с узлом Cisco.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: • off — Механизм отключен. DPD запросы не отправляются. • always — DPD запросы всегда отправляются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отправляются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. • idle — DPD запросы не отправляются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отправляются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Group 1 Prime 768 bit. • Group 2 Prime 1024 bit. • Group 5 Prime 1536 bit. • Group 14 Prime 2048 bit. • Group 15 Prime 3072 bit. • Group 16 Prime 4096 bit. • Group 17 Prime 6144 bit. • Group 18 Prime 8192 bit.
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: Admin@nodename# create vpn client-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name> Доступны: • auth-alg: выбор алгоритма аутентификации. • MD5. • SHA1. • SHA256. • SHA384. • SHA512. • encrypt-alg: выбор алгоритма шифрования. • DES. • 3DES. • AES128. • AES192. • AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifetime-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifetime	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifetime), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off .
nat-keepalive	Период отправки пакетов NAT keepalive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону peer-узла для поддержания сессии NAT активной.

Параметр	Описание
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn client-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: auth-alg: выбор алгоритма аутентификации. - MD5. - SHA1. - SHA256. - SHA384. - SHA512. encrypt-alg: выбор алгоритма шифрования. - DES. 3DES. - AES128. - AES192. - AES256.

Примеры создания и редактирования профилей безопасности VPN

```
Создание нового профиля безопасности VPN:

Admin@nodename# create vpn server-security-profiles <profile-name> <parameters>
Admin@nodename# create vpn client-security-profiles <profile-name> <parameters>
...

Admin@nodename# create vpn server-security-profiles name "New server VPN profile"

Редактирование параметров профиля безопасности VPN:

Admin@nodename# set vpn server-security-profiles <profile-name> <parameters>
Admin@nodename# set vpn client-security-profiles <profile-name> <parameters>
...
Admin@nodename# set vpn server-security-profiles "New server VPN profile" phase1-security [ SHA1/AES128 SHA1/3DES ] phase2-security [ SHA1/AES128 SHA1/3DES ]
Admin@nodename# set vpn server-security-profiles "New server VPN profile" dh-groups [ "Group 16 Prime 4096 bit" ]
Admin@nodename# set vpn server-security-profiles "New server VPN profile" nat-keepalive 20

Удаление параметров профиля безопасности VPN:

Admin@nodename# delete vpn server-security-profiles <profile-name> <parameters>
Admin@nodename# delete vpn client-security-profiles <profile-name> <parameters>
...
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" phase1-security [ MD5/AES128 ]
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" phase2-security [ MD5/AES128 ]
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" dh-groups [ "Group 16 Prime 4096 bit" ]

Просмотр информации о сконфигурированных профилях безопасности VPN:

Admin@nodename# show vpn server-security-profiles <profile-name>
Admin@nodename# show vpn client-security-profiles <profile-name>
...
Admin@nodename# show vpn client-security-profiles "New client VPN profile"
```


Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В UserGate NGFW версии 7.5.0 и выше серверные правила VPN реализованы в виде модульной структуры, состоящей из трех отдельно настраиваемых объектов:

- [правил подключения](#);
- [правил аутентификации](#);
- [политик VPN](#).

Подробнее о структуре серверных правил — в разделе «[Общие понятия](#)».

Серверные правила создаются для двух сценариев:

- Защищенное соединение офисов (site-to-site VPN). Подробнее о создании site-to-site VPN — в разделе «[Настройка VPN для защищенного соединения офисов](#)».
- Удаленный доступ конечных устройств в сеть офиса (remote access VPN). Подробнее о создании remote access VPN — в разделе «[Настройка VPN для удаленного доступа в сеть](#)».

В интерфейсе командной строки серверные правила VPN настраиваются на уровне `vpn-server`.

Настройка правил подключения

Правила подключения описывают первый этап установления соединения. Он начинается с инициирования соединения VPN-клиентом (узлом-инициатором) и завершается ответом VPN-сервера (узла-ответчика) — предложением выполнить обмен ключами либо отказом с разрывом соединения. В правилах задаются проверки зоны источника, адреса инициатора и назначения, типа протокола, а также определяются параметры первой фазы установления защищенного соединения.

Команда для создания правила подключения:

Admin@nodename# create vpn-server connection-rules [ike|dtls] <parameters>

Дополнительные параметры команды.

Параметр	Описание
ike	Протокол подключения. Может использоваться в сценариях site-to-site и remote access VPN
dtls	Протокол подключения. Используется только при подключении конечных устройств с помощью UserGate Client в сценарии remote access VPN
name	Название правила подключения
description	Описание правила подключения
protocol	Версия протокола IKE: • ikev1; • ikev2
ike-mode	Режим работы протокола IKEv1: • main; • aggressive
psk	Значение общего ключа (pre-shared key)
src-zones	Зона источника трафика
src-ips	Адрес источника трафика (инициатора соединения): • ip — список IP-адресов; • url — список доменов; • geoip — GeoIP
dst-ips	Адрес назначения трафика (интерфейса, на который будут приходить подключения): • ip — список IP-адресов; • url — список доменов
key-lifetime	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1: • num+s[m h], например 1s, 2m, 3h
dpd-state	Режимы работы механизма Dead peer detection (DPD): • off — механизм отключен. DPD-запросы не отправляются. • always — DPD-запросы всегда отправляются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отправляются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается. • idle — DPD-запросы не отправляются, пока есть ESP-трафик через созданный канал. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отправляются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается
dpd-interval	Интервал отправки дополнительных запросов DPD. Указывается в секундах
dpd-max-failures	Количество повторов отправки DPD-запросов
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами
security	Алгоритмы аутентификации и шифрования
dtls-security	Алгоритмы аутентификации и шифрования для использования с протоколом DTLS.

Пример создания правила подключения с протоколом IKE:

Admin@nodename# create vpn-server connection-rules ike name Test1 description "Test connection rule #1" protocol ikev1 psk 123321 ike-mode main src-zones [Untrusted] dh-groups ["Group 2 Prime 1024 bit" "Group 14 Prime 2048 bit"] security
Repeat preshared key:
Admin@nodename# show vpn-server connection-rules ike Test1

name : Test1
description : Test connection rule #1

```
type      : ike
protocol  : ikev1
ike-mode   : main
src-zones : Untrusted
dh-groups  : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
security   :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256

key-lifetime : 1 h
dpd-state    : always
dpd-interval : 65
dpd-max-failures : 5
```

```
Admin@nodename#

Для изменения параметров правила подключения используется команда:
Admin@nodename# set vpn-server connection-rules [ike|dtls] [rule-name] <parameters>

Для просмотра созданных ранее правил подключения используется команда:
Admin@nodename# show vpn-server connection-rules [ike|dtls] <rule-name>

Для удаления правил подключения используется команда:
Admin@nodename# delete vpn-server connection-rules [ike|dtls] [rule-name]
```

Настройка правил аутентификации

Правила аутентификации описывают второй этап установления соединения. Он начинается с ответа узла-инициатора на предложение обмена ключами и завершается после успешной аутентификации. В этих правилах задаются проверки типа аутентификации и определяются параметры второй фазы установления защищенного соединения.

```
Команда для создания правила аутентификации:
Admin@nodename# create vpn-server authentication-rules [site-to-site|remote-access] <parameters>

Дополнительные параметры команды.
```

Параметр	Описание
ikev2	Протокол установления защищенного соединения IPsec IKEv2
ipsec	Протокол установления защищенного соединения IPsec IKEv1. Используется только в сценарии site-to-site
l2tp-ipsec	Протокол установления защищенного соединения L2TP/IPsec IKEv1
dtls	Протокол установления защищенного соединения DTLS. Используется только в сценарии remote access
name	Название правила аутентификации
description	Описание правила аутентификации
auth-ptofile	Профиль аутентификации для пользователей VPN
connection-rules	Выбор созданного ранее правила подключения
initiator-type	Выбор параметра идентификации узла-инициатора соединения: - ipv4; - fqdn
initiator-value	Значение параметра идентификации узла-инициатора: <ip> — например, 192.168.0.1; <domain> — например, example.com
responder-type	Выбор параметра идентификации узла-ответчика: - ipv4; - fqdn
responder-value	Значение параметра идентификации узла-ответчика: <ip> — например, 192.168.0.1; <domain> — например, example.com
auth-mode	Выбор режима аутентификации: - psk — аутентификации с помощью общего ключа (pre-shared key). - pki — аутентификации с помощью x.509 сертификатов. - aaa — аутентификации с помощью сервера AAA (логин и пароль). Только для сценария remote access
psk	Значение общего ключа (pre-shared key) для сценария site-to-site с IKEv2
certificate	Сертификат сервера. Сертификат используется для аутентификации сервера при установлении VPN-соединения.
client-certificate-profile	Профиль сертификата VPN-клиента. Профиль клиентского сертификата предназначен для получения имени пользователя из соответствующего атрибута в сертификате клиента, проверки иерархии доверия и подлинности сертификата по спискам отозванных сертификатов. Подробнее о создании профиля клиентского сертификата — в разделе « Настройка профилей клиентских сертификатов »
key-lifetime	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 2: num+s m h, например 1s, 2m, 3h
key-lifetime-enabled	Включение параметра указания максимального размера данных, шифруемых одним ключом: - on; - off

Параметр	Описание
key-lifeseize	Максимальный размер данных, шифруемых одним ключом: num+KB MB GB, например 1KB, 2MB, 3GB
nat-keepalive	NAT keepalive применяется в сценариях, когда IPsec-трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN-туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN-туннелю в дальнейшем не сможет проходить. С помощью функции NAT keepalive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keepalive в сторону VPN-клиентов для поддержания сессии NAT активной. Необходимо указать интервал отправки пакетов keepalive
local-networks remote-networks	Адреса локальных и удаленных подсетей. Используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Адреса указываются в формате [<ip/mask> <ip/mask> ...]
dont-check-initiator-announce	При активации этого параметра VPN-сервер не будет проверять подсети инициатора соединения в селекторе трафика при организации защищенного канала передачи данных. Функция удобна для подключения множества клиентов (инициаторов) по одному правилу
dynamic-routing	Разрешить для протокола IKEv2 работу протоколов динамической маршрутизации через туннель
security	Указание алгоритмов аутентификации и шифрования канала передачи данных

```
Пример создания правила аутентификации с протоколом L2TP/IPsec:

Admin@nodename# create vpn-server authentication-rules site-to-site l2tp-ipsec name Test2 description "Test authentication rule #2" initiator-type ipv4 initiator-value 172.16.1.10 responder-type ipv4 responder-value 172.16.1.1 auth-profile "Local a
Admin@nodename# show vpn-server authentication-rules site-to-site l2tp-ipsec Test2
```

```
name          : Test2
description   : Test authentication rule #2
connection-rules : CR1
initiator-type : ipv4
initiator-value : 172.16.1.10
responder-type : ipv4
responder-value : 172.16.1.1
auth-profile   : Local auth profile
key-lifetime   : 1 h
key-lifeseize-enabled : on
key-lifeseize  : 100.0 MB
nat-keepalive  : 0
security       :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256
```

```
Admin@nodename#

Для изменения параметров правила аутентификации используется команда:

Admin@nodename# set vpn-server authentication-rules [site-to-site|remote-access] [rule-name] <parameters>

Для просмотра созданных правил аутентификации используется команда:

Admin@nodename# show vpn-server authentication-rules [site-to-site|remote-access] [ikev2|ipsec|l2tp-ipsec] <rule-mane>

Для удаления правил аутентификации используется команда:

Admin@nodename# delete vpn-server authentication-rules [site-to-site|remote-access] [ikev2|ipsec|l2tp-ipsec] [rule-name]
```

Настройка политик VPN

Политики VPN описывают третий этап установления соединения. Он начинается с идентификации узла-инициатора и завершается назначением сетевых параметров подключения: туннельного интерфейса, пула IP-адресов внутри VPN-туннеля, маршрутов к ресурсам через туннель и адресов DNS-серверов.

Политики VPN создаются с помощью синтаксиса языка [UPL](#).

```
Команда для создания политик VPN:

Admin@nodename# create vpn-server vpn-policy [position] upl-rule
```

Дополнительные параметры команды.

Параметр	Описание
OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания
name	Название правила. Например: name("VPN rule example")
desc	Описание правила. Например: desc("VPN rule example configured in CLI")
auth_rules	Выбор созданного ранее правила аутентификации. Например: auth_rules("Authentication rule 1")
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Например, чтобы указать интерфейс tunnel1: interface(tunnel1).
ip_range	Диапазон IP-адресов туннеля, которые будут использованы VPN-клиентами. Например: ip_range("172.30.255.2-172.30.255.5")
mask	Маска сети VPN-туннеля. Например: mask(255.255.255.0)

Параметр	Описание
vpn_routes	Маршруты, передаваемые узлу-инициатору при установлении VPN-туннеля. Например: vpn_routes(10.10.0.0/24)
use_system_dns	Использование системных DNS-серверов для VPN-клиентов. Например: use_system_dns(true) или use_system_dns(false)
dns_server	Адрес DNS-сервера. Например: dns_server(10.10.0.100)
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор. Подробнее о настройке LDAP-коннектора через CLI — в разделе « Настройка LDAP-коннектора ». Пример добавления локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
type	Сценарий установления VPN-соединения. Возможные значения: • type(s2s_l2tp) — сценарий site-to-site, протокол L2TP/IPsec; • type(s2s_ipsec) — сценарий site-to-site, протокол IPsec; • type(ra_ep) — сценарий remote access, конечное устройство с установленным UserGate Client; • type(ra_native) — сценарий remote access, конечное устройство со встроенным VPN-клиентом операционной системы
include_routes	Для каждого включенного адреса в таблице маршрутизации конечного устройства добавляется маршрут вида н.п.н.п/с → VPN-шлюз с гарантированно минимальной метрикой 2. Например: include_routes(10.10.10.10/32)
exclude_routes	При добавлении IP-адресов в список исключаемых, в таблице маршрутизации конечного устройства будет добавлен маршрут по умолчанию вида 0.0.0.0/0 → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы. Для каждого исключаемого адреса добавляется свой маршрут через интерфейс с лучшей метрикой в обход VPN. Например: exclude_routes(10.10.10.10/32)
disable_lan	Если включен этот параметр (disable_lan(true)), то для каждой подсети локального интерфейса создается копия маршрута через VPN-шлюз с гарантированно минимальной метрикой 2. Такие же копии маршрутов создаются для всех адресов, которые имеют тип local interface
tunnel_all	Если включен этот параметр (tunnel_all(true)), в таблицу маршрутизации конечного устройства будет добавлен маршрут по умолчанию (default route) вида 0.0.0.0/0 → VPN-шлюз. Имеющийся ранее маршрут по умолчанию будет удален из таблицы маршрутизации конечного устройства

Пример политики VPN для сценария site-to-site с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-server vpn-policy 6 upl-rule \  
...OK  
...auth_rules(AR1) \  
...vpn_routes(10.10.0.0/24) \  
...ip_range("172.30.255.2-172.30.255.5") \  
...desc("Серверная политика VPN 1") \  
...mask(255.255.255.0) \  
...use_system_dns(false) \  
...user = "CN=VPN users,DC=LOCAL" \  
...dns_server(8.8.8.8) \  
...enabled(false) \  
...type(s2s_l2tp) \  
...interface(tunnel2) \  
...name(VR1)
```

Для изменения параметров политики VPN используется команда:

```
Admin@nodename# set vpn-server vpn-policy [position] upl-rule
```

Для просмотра созданных политик VPN используется команда:

```
Admin@nodename# show vpn-server vpn-policy <position>
```

Для удаления политик VPN используется команда:

```
Admin@nodename# delete vpn-server vpn-policy [position]
```

Просмотр журналов диагностики VPN-сервера

В режиме диагностики интерфейса командной строки вы можете просматривать события журналов диагностики VPN-сервера в статическом и динамическом режиме.

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

```
Admin@nodename> show logs log vpn-server static
```

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-server dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш Ctrl + C.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log vpn-server static | grep l2tp
```

Подробнее о функции фильтрации вывода — в разделе « [Общие положения](#) ».

Product: NGFW
Version: 7.x
Technology: VPN

Клиентские правила используются VPN-сервером, который инициирует подключение в сценарии site-to-site VPN. Подробнее о создании site-to-site VPN — в разделе « [Настройка VPN для защищенного соединения офисов](#) ».

В интерфейсе командной строки клиентские правила VPN настраиваются на уровне `vpn-client`.

Настройка параметров подключения клиента

При настройке VPN-подключения указываются используемые протоколы для установления соединения, выбираются методы аутентификации, а также определяются параметры обеих фаз формирования защищенного канала.

Команда для создания подключения клиента:

Admin@nodename# create vpn-client connections [ikev2|ipsec|l2tp-ipsec] <parameters>

Дополнительные параметры команды.

Параметр	Описание
name	Название подключения
description	Описание подключения
ike-mode	Режим работы IKEv1: - main; - aggressive
psk	Значение общего ключа (pre-shared key)
initiator-type	Параметр идентификации узла-инициатора: - ipv4; - fqdn
initiator-value	Значение параметра идентификации узла-инициатора: <ip> — например, 192.168.0.1; <domain> — например, example.com
responder-type	Параметр идентификации узла-ответчика: - ipv4; - fqdn
responder-value	Значение параметра идентификации узла-ответчика: <ip> — например, 192.168.0.1; <domain> — например, example.com
authentication-login	Логин для аутентификации узла-инициатора на узле-ответчике в сценарии с протоколом IPsec/L2TP
authentication-password	Пароль для аутентификации узла-инициатора на узле-ответчике в сценарии с протоколом IPsec/L2TP
check-ip	Параметр <code>check_ip</code> определяет, будет ли узел-инициатор соединения запрашивать проверку IP-адреса у VPN-сервера. VPN-сервер может принять предложенный IP-адрес или назначить другой. Если параметр разрешен, узел-инициатор соединения добавляет параметр Payload Configuration в сообщение <code>IKE_AUTH</code> и передает в поле <code>INTERNAL_IP4_ADDRESS</code> значение, зависящее от типа туннельного интерфейса: - Для туннельного интерфейса с динамическим назначением IP-адреса в поле <code>INTERNAL_IP4_ADDRESS</code> передается значение 0.0.0.0/0, что является запросом на динамическое выделение IP-адреса. VPN-сервер, получив значение 0.0.0.0/0, выделяет IP-адрес из собственного пула, заданного в параметрах соединения на сервере. - Для туннельного интерфейса со статическим IP-адресом в поле <code>INTERNAL_IP4_ADDRESS</code> передается его IP-адрес. VPN-сервер использует это значение для проверки соответствия политике подключения. Если параметр не разрешен, механизм согласования сетевых параметров для проверки IP-адреса туннельного интерфейса на VPN-сервере не применяется. Значение IP-адреса определяется настройками туннельного интерфейса на узле-инициаторе.
auth-mode	Режим аутентификации: - rki — режим аутентификации с помощью сертификата; - psk — режим аутентификации с помощью общего ключа
certificate	Сертификат узла-инициатора (клиента)
phase1-key-lifetime	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 1: num+s m h, например 1s, 2m, 3h
dpd-state	Режимы работы механизма Dead peer detection (DPD): - off — механизм отключен. DPD-запросы не отправляются. - always — DPD-запросы всегда отправляются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек. отправляются дополнительные запросы в количестве, указанном в параметре <code>dpd-max-failures</code>. Если ответ пришел, работа механизма возвращается к изначальному интервалу отправки DPD запросов. Если ответ не пришел, соединение завершается. - idle — DPD-запросы не отправляются, пока есть ESP-трафик через созданный канал. Если в течение двойного указанного интервала времени нет ни одного пакета, происходит отсылка DPD-запроса. При ответе новый DPD-запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек. отправляются дополнительные запросы в количестве, указанном в параметре <code>dpd-max-failures</code>. Если нет ни одного ответа, соединение завершается
dpd-interval	Интервал отсылки дополнительных запросов DPD. Указывается в секундах
dpd-max-failures	Количество повторов отправки DPD-запросов
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами
phase1-security	Алгоритмы аутентификации и шифрования для фазы 1

Параметр	Описание
phase2-key-lifetime	Время жизни ключа. По истечении этого времени происходит повторная аутентификация и согласование настроек фазы 2: num+s m h, например 1s, 2m, 3h
key-lifetime-enabled	Включение параметра указания максимального размера данных, шифруемых одним ключом: - on; - off
key-lifetime-size	Максимальный размер данных, шифруемых одним ключом: num+KB MB GB, например 1KB, 2MB, 3GB
dynamic-routing	Разрешить работу протоколов динамической маршрутизации через туннель (для протокола IKEv2)
local-networks remote-networks	Адреса локальных и удаленных подсетей. Используются для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В ходе фазы 2 стороны туннеля обмениваются своими предложениями по селекторам трафика. Для успешного установления туннеля сети в селекторах трафика от обеих сторон соединения должны совпасть или пересечься. Если нет совпадения хотя бы по одной из сторон, фаза 2 завершится ошибкой соединения. Адреса указываются в формате [<ip/mask> <ip/mask> ...]
phase2-security	Алгоритмы аутентификации и шифрования канала передачи данных (для фазы 2)

Пример настройки клиентского подключения с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-client connections l2tp-ipsec name Connection1 description "Test connection" ike-mode main authentication-login vpn_client1 authentication-password password111 psk 123321 initiator-type ipv4 initiator-value 172.1
Repeat preshared key:
```

Admin@nodename# show vpn-client connections l2tp-ipsec Connection1

```
name          : Connection1
description    : Test connection
ike-mode      : main
authentication-login : vpn_client1
phase1-key-lifetime : 1 h
phase2-key-lifetime : 1 h
key-lifetime-enabled : on
key-lifetime-size : 100.0 MB
initiator-type : ipv4
initiator-value : 172.16.1.10
responder-type : ipv4
responder-value : 172.16.1.1
dpd-state     : off
dpd-interval  : 60
dpd-max-failures : 5
dh-groups     : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
phase1-security :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256

phase2-security :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256
```

Admin@nodename#

Для изменения параметров клиентского подключения используется команда:

```
Admin@nodename# set vpn-client connections [ikev2|ipsec|l2tp-ipsec] <connection-name>
```

Для просмотра параметров клиентских подключений используется команда:

```
Admin@nodename# show vpn-client connections [ikev2|ipsec|l2tp-ipsec] <connection-name>
```

Для удаления клиентского подключения используется команда:

```
Admin@nodename# delete vpn-client connections [ikev2|ipsec|l2tp-ipsec] <connection-name>
```

Настройка клиентских правил

Клиентское правило в сценарии site-to-site VPN используется для инициирования подключения к VPN-серверу (узлу-ответчику).

Клиентские правила VPN создаются с помощью синтаксиса языка [UPL](#).

Команда для создания клиентских правил:

```
Admin@nodename# create vpn-client rules [position] upl-rule
```

Дополнительные параметры команды.

Параметр	Описание
OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true). - enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания
name	Название правила. Например: name("VPN rule example")
desc	Описание правила. Например: desc("VPN rule example configured in CLI")
connection	Название ранее созданного клиентского подключения. Например: connection(Connection1)
interface	VPN-интерфейс, который будет использоваться для подключения. Например, чтобы указать интерфейс tunnel3: interface(tunnel3)

Параметр	Описание
server_address	Адрес VPN-сервера (IP-адрес или доменное имя). Например: server_address("172.16.1.1")

Пример клиентского правила с протоколом L2TP/IPsec:

```
Admin@nodename# create vpn-client rules 5 upl-rule \  
...OK  
...server_address(172.16.1.1)  
...connection(Connection1)  
...interface(tunnel3)  
...enabled(false)  
...name(Rule1)
```

Для изменения параметров правила используется команда:

```
Admin@nodename# set vpn-client rules [position] upl-rule
```

Для просмотра созданных правил используется команда:

```
Admin@nodename# show vpn-client rules <position>
```

Для удаления правил используется команда:

```
Admin@nodename# delete vpn-client rules [position]
```

Просмотр журналов диагностики VPN-сервера, работающего в режиме инициатора соединения

В режиме диагностики интерфейса командной строки вы можете просматривать события журналов диагностики VPN-сервера (когда UserGate NGFW выступает в роли узла-инициатора соединения в сценарии site-to-site VPN), в статическом и динамическом режиме.

Для вывода всего журнала диагностики VPN-сервера в консоль используйте команду:

```
Admin@nodename> show logs log vpn-client static
```

Для вывода событий журнала диагностики VPN-сервера в консоль в реальном времени используйте команду:

```
Admin@nodename> show logs log vpn-client dynamic
```

Для отключения вывода событий журнала используйте комбинацию клавиш **Ctrl + C**.

В командах раздела может использоваться фильтрация вывода. Пример команды с фильтрацией вывода:

```
Admin@nodename> show logs log vpn-client static | grep l2tp
```

Подробнее о функции фильтрации вывода — в разделе « [Общие положения](#) ».

Product: NGFW
Version: 7.x
Technology: VPN

Администратор UserGate NGFW версии 7.5.1 в режиме диагностики интерфейса командной строки может просматривать и принудительно завершать активные VPN-сессии, а также блокировать доступ пользователей к VPN-серверу.

Принудительное завершение активных VPN-сессий

Для просмотра активных VPN-сессий используется команда:

```
Admin@nodename> show vpn-sessions
```

Команда для принудительного завершения активных сессий:

```
Admin@nodename> clear vpn-sessions <remote-access | site-to-site> [ session1 session2 ... ]
```

Блокировка пользователей VPN

В некоторых случаях требуется оперативная блокировка доступа пользователей к VPN-серверу, например:

- при компрометации учетных данных;
- утере или краже устройства пользователя;
- выявлении критически опасных уязвимостей VPN-клиента;
- ограничении лицензий или квот.

Для добавления локальных пользователей в список заблокированных используется команда:

```
Admin@nodename> block-vpn-user users [ user_name1 user_name2 ... ]
```

Для добавления доменных пользователей в список заблокированных используется команда:

```
Admin@nodename> block-vpn-user ldap-users connector "Connector name" users [ domain\user_name1 domain\user_name2 ... ]
```

Команда для просмотра списка заблокированных пользователей VPN:

```
Admin@nodename> show blocked-vpn-users
```

Команда для удаления пользователей из списка заблокированных:

```
Admin@nodename> clear blocked-vpn-users users [ user_name1 user_name2 ... ]
```


Настройка библиотек (Описание)

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка морфологии

Для создания списка морфологии используется следующая команда:

Admin@nodename# create libraries morphology <parameter>

Далее необходимо указать:

Параметр	Описание
name	Название морфологического списка.
description	Описание списка.
threat-lvl	Уровень угрозы: very-low — очень низкий уровень угрозы. low — низкий уровень угрозы. medium — средний уровень угрозы. high — высокий уровень угрозы. very-high — высокий уровень угрозы.
threshold	Вес морфологической категории, при превышении которого сработает правило.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (uri). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
words	Слова и фразы, которые необходимо добавить в список. word — слова и фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. weight — вес слова или фразы. Если вес не задан, то автоматический устанавливается значение 100. Для добавления слов и фраз: Admin@nodename# create libraries morphology ... words new word "word or phrase" weight <weight>

Чтобы редактировать список, необходимо использовать следующую команду:

Admin@nodename# set libraries morphology <morphology-list-name> <parameter>

Далее указываются параметры, значения которых необходимо обновить (список параметров представлен в таблице выше). Для добавления в список новых слов или фраз необходимо использовать команду:

Admin@nodename# set libraries morphology <morphology-list-name> words new word "word or phrase" weight <weight>

Чтобы заменить слово в списке:

Admin@nodename# set libraries morphology <morphology-list-name> words (word "old word or phrase" weight <weight>) word "new word or phrase" weight <weight>

Следующие команды используются для удаления всего морфологического списка или отдельных слов, содержащихся в нём:

Admin@nodename# delete libraries morphology <morphology-list-name>

Admin@nodename# delete libraries morphology <morphology-list-name> words (word "word or phrase" weight <weight>)

Команды отображения информации о всех имеющихся морфологических списках:

Admin@nodename# show libraries morphology

Чтобы отобразить информацию об определённом списке, далее необходимо указать название интересующего морфологического списка. Чтобы просмотреть содержание определённого морфологического списка:

Admin@nodename# show libraries morphology <morphology-list-name> words

Настройка сервисов

Данный раздел настраивается на уровне **libraries services**.

Для добавления нового сервиса используется следующая команда:

Admin@nodename# create libraries services <parameter>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название сервиса.
description	Описание сервиса.
protocols	Указание сетевого протокола и портов источника/назначения: protocol — сетевой протокол. alg — L7 шлюз, только для TCP или UDP (поддерживается SIP, H323, FTP, TFTP — для протокола UDP). dest-ports — порт(ы) назначения (указывается номер порта или диапазон портов). source-ports — порт(ы) источника (указывается номер порта или диапазон портов).

Для редактирования существующего сервиса:

Admin@nodename# set libraries services <service-name> <parameter>

Для обновления сетевого протокола и портов источника/назначения сервиса:

Admin@nodename# set libraries services <service-name> protocols (<protocol-filter>)

<protocol-filter> — фильтр, настроенный с использованием значений параметра protocols.

Далее указываются новые значения параметра **protocols**.

Для добавления сетевого протокола и портов источника/назначения в существующий сервис:

```
Admin@nodename# set libraries services <service-name> protocols new <parameter>
```

Далее необходимо указать **protocol, dest-ports, source-ports**.

Чтобы удалить сервис используется следующая команда:

```
Admin@nodename# delete libraries services <service-name>
```

Также возможно удаления из сервиса заданных сетевых протоколов:

```
Admin@nodename# delete libraries services <service-name> protocols ( <protocol-filter> )
```

Следующие команды предназначены для отображения информации о всех сервисах или об определённом сервисе:

```
Admin@nodename# show libraries services
Admin@nodename# show libraries services <service-name>
```

Настройка групп сервисов

Данный раздел находится на уровне **libraries service-groups**. Для создания группы сервисов предназначена следующая команда:

```
Admin@nodename# create libraries service-groups <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы сервисов.
description	Описание группы.
services	Сервисы, которые необходимо добавить в группу.

Для редактирования группы сервисов (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы):

```
Admin@nodename# set libraries service-groups <service-group-name> <parameter>
```

Чтобы добавить в группу сервисы:

```
Admin@nodename# set libraries service-groups <service-group-name> [ <service1> < service2> ... ]
```

Следующие команды используются для удаления группы сервисов или отдельных сервисов, содержащихся в ней:

```
Admin@nodename# delete libraries service-groups <service-group-name>
Admin@nodename# delete libraries service-groups <service-group-name> services [ <services> ... ]
```

Команды отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries service-groups
```

об определённом списке:

```
Admin@nodename# show libraries service-groups <service-group-name>
```

или списка сервисов, добавленных в группу:

```
Admin@nodename# show libraries service-groups <service-group-name> services
```

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: very-low — очень низкий уровень угрозы. low — низкий уровень угрозы. medium — средний уровень угрозы. high — высокий уровень угрозы. very-high — высокий уровень угрозы.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> ips [ <ip1> <ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка Useragent браузеров

Раздел настраивается на уровне **libraries useragents**.

Следующая команда используется для добавления нового списка Useragent браузеров:

```
Admin@nodename# create libraries useragents <parameter>
```

Далее указываются следующие данные:

Параметр	Описание
name	Название списка Useragent.
description	Описание списка.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
patterns	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php .

Для редактирования существующего списка:

```
Admin@nodename# set libraries useragents <useragent-list-name> <parameter>
```

Далее указываются параметры, которые необходимо обновить. Параметры представлены в таблице выше. Чтобы добавить новые Useragent браузеров:

```
Admin@nodename# set libraries useragents <useragent-list-name> [ <useragent1> <useragent2> ... ]
```

Следующие команды используются для удаления всего списка или отдельных Useragent браузеров, содержащихся в нём:

```
Admin@nodename# delete libraries useragents <useragent-list-name>
Admin@nodename# delete libraries useragents <useragent-list-name> patterns [ <useragent> ... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries useragents
```

Чтобы отобразить информацию об определённом списке, необходимо указать название списка Useragent браузеров. Чтобы просмотреть содержание списка Useragent браузеров:

```
Admin@nodename# show libraries useragents <useragent-list-name> patterns
```

Настройка типов контента

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

```
Admin@nodename# create libraries content-types <parameter>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.
description	Описание списка.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
mime	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml .

Для редактирования списка используется следующая команда:

```
Admin@nodename# set libraries content-types <content-types-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

```
Admin@nodename# delete libraries content-types <content-types-list-name>
```

Также доступно удаление отдельных типов контента из списка:

```
Admin@nodename# delete libraries content-types <content-types-list-name> mime [ <mime-type> ... ]
```

Следующие команды используются для отображения информации о списках типов контента:

```
Admin@nodename# show libraries content-types
Admin@nodename# show libraries content-types <content-types-list-name>
```

```
Admin@nodename# show libraries content-types <content-types-list-name> mime
```

Настройка списков URL производится на уровне **libraries url-list**.

```
Admin@nodename# create libraries url-list <parameter>
```

Далее указывается следующая информация:

Для редактирования списка URL:

```
Admin@nodename# set libraries url-list <url-list-name> <parameter>
```

Параметры, значения которых можно обновить, представлены в таблице выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

```
Admin@nodename# delete libraries url-list <url-list-name>
Admin@nodename# delete libraries url-list <url-list-name> [url [url ... ]
```

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список URL:

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

```
Admin@nodename# create libraries time-sets <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.

Параметр	Описание
time-set	interval-name — название интервала повторения. type — тип интервала повторения: daily — ежедневно: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. weekly — каждую неделю: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. days [Mon Tue Wed Thu Fri Sat Sun] — дни недели. monthly — каждый месяц: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. days — числа месяца (от 1 до 31). fixed — одновременно: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. fixed-date — нужная дата (указывается в формате YYYY-MM-DD). span — повторяющиеся события: time-from — время начала (указывается в формате HH:MM). time-to — время окончания (указывается в формате HH:MM). all-day on — весь день. fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). range — диапазон дат: time-from-enabled <on off> — включение/отключение указания даты начала интервала. fixed-date-from — дата начала (указывается в формате YYYY-MM-DD). time-from — время начала (указывается в формате HH:MM). time-to-enabled <on off> — включение/отключение указания даты окончания интервала. fixed-date-to — дата окончания (указывается в формате YYYY-MM-DD). time-to — время окончания (указывается в формате HH:MM).

Для редактирования календаря:

Admin@nodename# set libraries time-sets <time-sets-name> <parameter>

Параметры, доступные для обновления, представлены в таблице выше.

Для редактирования интервала, заданного в календаре:

Admin@nodename# set libraries time-sets <time-sets-name> ... time-set <time-set-type> (<time-set-filter>)

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

Admin@nodename# create libraries time-sets <time-sets-name> ... time-set <time-set-type> new

Команда для удаления группы элементов:

Admin@nodename# delete libraries time-sets <time-sets-name>

Для удаления элемента календаря:

Admin@nodename# delete libraries time-sets <time-sets-name> <time-set-type> (<time-set-filter>)

Для отображения информации о всех календарях:

Admin@nodename# show libraries time-sets

Для отображения информации об определённом календаре:

Admin@nodename# show libraries time-sets <time-sets-name>

Для отображения информации об элементах группы с одинаковым типом повторения:

Admin@nodename# show libraries time-sets <time-sets-name> <time-set-type>

Настройка полос пропускания

Раздел находится на уровне **libraries bandwidth-pools**.

Для добавления новой полосы пропускания используется следующая команда:

Admin@nodename# create libraries bandwidth-pools <parameter>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название полосы пропускания.
description	Описание полосы пропускания.
rate	Скорость передачи данных; указывается в Кбит/с.
dscp	Значение DSCP QoS (при указании будет прописываться в каждый IP-пакет: принимает значения от 0 до 63).

Для редактирования параметров полосы пропускания:

Admin@nodename# set libraries bandwidth-pools <bandwidth-name> <parameter>

Параметры, доступные для изменения такие же, как и для команды создания полосы пропускания.

Чтобы удалить полосу пропускания:

```
Admin@nodename# delete libraries bandwidth-pools <bandwidth-name>
```

С использованием **show** можно отобразить информацию о всех полосах пропускания:

```
Admin@nodename# show libraries bandwidth-pools
```

или об определённой полосе:

```
Admin@nodename# show libraries bandwidth-pools <bandwidth-name>
```

Настройка шаблонов страниц

Раздел находится на уровне **libraries response-pages**. Доступно создание следующих типов шаблонов страниц (<response-page-type>):

- **blockpage** — шаблоны страниц блокировки;
- **captiveportal-user-auth** — шаблоны страниц авторизации captive-портала;
- **captiveportal-user-session** — шаблоны страниц captive-портала, сессия пользователя;
- **content-warning** — шаблоны страниц предупреждения;
- **ftp-client** — шаблоны страниц отображения FTP поверх HTTP;
- **proxy-portal** — шаблоны страниц веб-портала;
- **pp-login-ssh** — шаблоны страниц SSH-логина веб-портала;
- **pp-login-rdp** — шаблоны страниц RDP-логина веб-портала;
- **totp-init-page** — шаблоны страниц инициализации TOTP;
- **network-error-page** — шаблоны страниц сетевых ошибок от прокси-сервера (доступно в версии ПО 7.4.0 и выше).

Команда, используемая для создания шаблона страницы:

```
Admin@nodename# create libraries response-pages <response-page-type> <parameter>
```

Необходимо указать параметры:

Параметр	Описание
name	Название шаблона страницы.
description	Описание шаблона.

Параметр	Описание
original-template	Выбор базового шаблона. Базовые шаблоны для страницы блокировки (blockpage): blockpage-en — шаблон страницы блокировки на английском языке; blockpage-ru — шаблон страницы блокировки на русском языке. Базовые шаблоны для страницы авторизации captive-портала (captiveportal-user-auth): captiveportal_user_auth-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке; captiveportal_user_auth-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке; captiveportal-user-auth-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; captiveportal-user-auth-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа; captiveportal-user-auth-email-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; captiveportal-user-auth-email-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email; captiveportal-user-auth-sms-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; captiveportal-user-auth-sms-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS; captiveportal-user-policy-en — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации; captiveportal-user-policy-ru — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в профиле авторизации. Базовые шаблоны для страницы captive-портал, сессия пользователя (captiveportal-user-session): captiveportal-user-session-en — шаблон на английском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://USERGATE_IP/cps: captiveportal-user-session-ru — шаблон на русском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps. Базовые шаблоны для страницы предупреждения (content-warning): content-warning-en — шаблон страницы предупреждения на английском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить; content-warning-ru — шаблон страницы предупреждения на русском языке, отображаемый при срабатывании правила контентной фильтрации с действием Предупредить. Базовые шаблоны для страницы отображения FTP поверх HTTP (ftp-client): ftp-client-en — шаблон на английском языке для отображения контента FTP-серверов поверх HTTP; ftp-client-ru — шаблон на русском языке для отображения контента FTP-серверов поверх HTTP. Базовые шаблоны для страницы веб-портала (proxy-portal): proxy-portal-en — шаблон на английском языке для отображения страницы веб-портала; proxy-portal-ru — шаблон на русском языке для отображения страницы веб-портала. Базовые шаблоны для страницы SSH-логина веб-портала (pp-login-ssh): pp-login-ssh-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал; pp-login-ssh-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. Базовые шаблоны для страницы RDP-логина веб-портала (pp-login-rdp): pp-login-rdp-en — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал; pp-login-rdp-ru — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. Базовые шаблоны для страницы инициализации TOTP (totp-init-page): totp-init-page-en — шаблон на английском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей; totp-init-page-ru — шаблон на русском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей. Базовые шаблоны для страницы сетевых ошибок от прокси-сервера (network-error-page). Доступно в версии ПО 7.4.0 и выше: network-error-page-en — шаблон на английском языке для отображения страницы сетевых ошибок от прокси-сервера; network-error-page-ru — шаблон на русском языке для отображения страницы сетевых ошибок от прокси-сервера.
default	Использовать шаблон по умолчанию: on; off.

```
Для редактирования значений шаблона:
Admin@nodename# set libraries response-pages <response-page-type> <response-page-name> <parameters>

Далее необходимо указать значения параметров; параметры представлены в таблице выше.

Чтобы удалить шаблон страницы, используется следующая команда:
Admin@nodename# delete libraries response-pages <response-page-type> <response-page-name>

Для просмотра информации о всех имеющихся шаблонах страниц:
Admin@nodename# show libraries response-pages

Для просмотра информации об отдельном типе шаблонов страниц:
Admin@nodename# show libraries response-pages <response-page-type>

Для просмотра информации об отдельном шаблоне страницы:
Admin@nodename# show libraries response-pages type <response-page-type> <response-page-name>
```

Настройка категорий URL

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

```
Admin@nodename# create libraries url-categories <parameter>
```

Параметры, которые необходимо указать:

Параметр	Описание

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для редактирования параметров группы:

Admin@nodename# set libraries url-categories <list-name> <parameter>

Для добавления категорий URL в существующую группу:

Admin@nodename# set libraries url-categories <list-name> categories [<url-category> ...]

Команды для удаления группы URL-категорий:

Admin@nodename# delete libraries url-categories <list-name>

или отдельных категорий из группы:

Admin@nodename# delete libraries url-categories <list-name> categories [<url-category> ...]

Команды для просмотра информации о всех группах URL-категорий:

Admin@nodename# show libraries url-categories

об определённой группе:

Admin@nodename# show libraries url-categories <list-name>

Чтобы отобразить список категорий URL, входящих в группу:

Admin@nodename# show libraries url-categories <list-name> categories

Настройка изменённых категорий URL

Настройка раздела **Изменённые категории URL** производится на уровне **overridden-url-categories**.

Для добавления новой изменённой категории URL:

Admin@nodename# create libraries overridden-url-categories <parameter>

Далее необходимо указать параметры:

Параметр	Описание
domain	Доменное имя проверяемого ресурса.
description	Описание изменяемого домена.
categories	Новые категории сайта (можно указать не более 2-х категорий).

Для редактирования параметров:

Admin@nodename# set libraries overridden-url-categories <domain> <parameter>

Для удаления сайта с изменёнными категориями:

Admin@nodename# delete libraries overridden-url-categories <domain>

Для отображения всего списка сайтов с изменёнными категориями:

Admin@nodename# show libraries overridden-url-categories

Для отображения информации об определённом сайте с изменёнными категориями URL:

Admin@nodename# show libraries overridden-url-categories <domain>

Настройка групп приложений

Данный раздел настраивается на уровне **libraries application-groups**.

Для создания группы приложений используется команда:

Admin@nodename# create libraries application-groups

Далее указываются параметры:

Параметр	Описание
name	Название группы приложений.
description	Описание группы приложений.
apps	Приложения, которые необходимо добавить в группу.

Для редактирования параметров:

Admin@nodename# set libraries application-groups <app-group-name>

Чтобы добавить новые приложения в существующую группу, используется команда:

Admin@nodename# set libraries application-groups <app-group-name> apps [<application> ...]

Для удаления группы приложений полностью или отдельных приложений в ней используются команды:

Admin@nodename# delete libraries application-groups <app-group-name>

Admin@nodename# delete libraries application-groups <app-group-name> apps [<application> ...]

Следующие команды предназначены для отображения информации о всех созданных группах приложений:

Admin@nodename# show libraries application-groups

или об определённой группе:

Admin@nodename# show libraries application-groups <app-group-name>

Также доступно отображение приложений, входящих в определённый список:

Admin@nodename# show libraries application-groups <app-group-name> apps

Настройка профилей приложений

Настройка профилей приложений производится на уровне **libraries application-profile**.

Для создания профиля приложений используется команда:

Admin@nodename# create libraries application-profile <parameter>

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля приложений.
description	Описание профиля приложений.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур приложений.
unknown-application-settings	Параметры сигнатуры для неизвестных приложений.

Представленная ниже команда предназначена для редактирования существующего профиля приложений:

```
Admin@nodename# set libraries application-profile <application-profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании профиля.

С использованием следующих команда возможен просмотр информации о всех профилях приложений:

```
Admin@nodename# show libraries application-profile
```

или об одном профиле:

```
Admin@nodename# show libraries application-profile <application-profile-name>
```

Пример создания профиля приложений:

```
Admin@nodename# create libraries application-profile name "Test app profile 1" description "Test app profile 1 description" filters new action drop value "category = Games" enabled on
Admin@nodename# show libraries application-profile "Test app profile 1"
```

```
name      : Test app profile 1
description : Test app profile 1 description
filters   :
  enabled  : on
  value    : category = Games
  enable-setting : on
  action   : drop
  pcap     : off
  track-by : src
  duration : 0 days 0 hours 5 minutes
```

Для удаления профиля приложений используется команда:

```
Admin@nodename# delete libraries application-profile <application-profile-name>
```

Подробнее о профилях приложений читайте в статье [Профили приложений](#) Руководства администратора.

Настройка сигнатур приложений

На уровне **libraries application-signature** возможно создание и настройка пользовательских кастомизированных сигнатур приложений.

Для создания пользовательской сигнатуры приложений используется команда:

```
Admin@nodename# create libraries application-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. - on -включить. - off — отключить.
categories	Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен. - Media streaming - Email - Coin Miners - TunnelingGames - Remote access - Conferencing - Trojan Horses - Business - Mobile - Proxies and anonymizers - Standard networks - VOIP - Web posting - Software update - File storage and backup - Web browsing - File sharing P2P - Instant messaging - Social networking

Параметр	Описание
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • very-low — очень низкий. • low — низкий. • medium — средний. • high — высокий. • very-high — очень высокий.
technology	Технология приложения. • browser-based — браузерное веб-приложение. • client-server — клиент-серверное приложение. • network-protocol — сетевой протокол. • peer-to-peer — приложение точка-точка.
type	Тип сигнатуры: • app — сигнатура приложения. • proto — сигнатура протокола. • support — вспомогательная сигнатура.
uasl	Описание сигнатуры приложений с помощью синтаксиса UASL.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры приложений:

```
Admin@nodename# set libraries application-signature <application-signature-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команда возможен просмотр информации о всех сигнатурах приложений:

```
Admin@nodename# show libraries application-signature
```

или об одной сигнатуре:

```
Admin@nodename# show libraries application-signature <application-signature-name>
```

Пример создания сигнатуры приложений:

```
Admin@nodename# create libraries application-signature name "Test app signature 2" description "Test app signature 2 description" categories [ "Web browsing" ] signature-id 2 technology browser-based threat low type app uasl "UASL(.dst_addr=
Admin@nodename# show libraries application-signature "Test app signature 2"
```

```
signature-id : 2
name         : Test app signature 2
threat       : low
technology   : browser-based
categories   : Web browsing
uasl         : UASL(.dst_addr=192.168.10.1;)
owner        : You
type         : custom
description  : Test app signature 2 description
```

Для удаления созданной ранее сигнатуры приложений используется команда:

```
Admin@nodename# delete libraries application-signature <application-signature-name>
```

Подробнее о сигнатурах приложений читайте в статье [Приложения](#) Руководства администратора.

Настройка тайм-аутов приложений

Значение пользовательского тайм-аута бездействия для приложения настраивается в интерфейсе командной строки (CLI) на уровне libraries application-signature.

Для проприетарных сигнатур приложений (сигнатур, созданных UserGate) значение тайм-аута бездействия устанавливается с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout <num>
```

Значение тайм-аута указывается в секундах в диапазоне от 60 до 604 800.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```
Admin@nodename# show libraries application-signature <"signature-name">
```

Пример:

```
Admin@nodename# set libraries application-signature "1C" idle-timeout 400
Admin@nodename# show libraries application-signature "1C"

signature-id : 188
name         : 1C
type         : app
description  : 1C is a Russian company specializing in the distribution, support and development of computer programs
              and databases for business and home use.
threat       : very-low
technology   : Client-server
categories   : Business
idle-timeout : 400
```

Вернуть значение тайм-аута по умолчанию можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout default
```

Примеч:

```
Admin@oulmetioeth# set libraries application-signature "1C" idle-timeout default
Admin@oulmetioeth# show libraries application-signature "1C"
```

```
signature-id : 188
name         : 1C
type         : app
description  : 1C is a Russian company specializing in the distribution, support and development of computer programs
              and databases for business and home use.
threat       : very-low
technology   : Client-server
categories   : Business
idle-timeout : default
```

В пользовательских сигнатурах (сигнатурах, созданных самими пользователями) значение тайм-аута бездействия можно указать при создании сигнатуры:

```
Admin@nodename# create libraries application-signature name <signature-name> uasl <"uasl-code"> idle-timeout <num>
```

Значение тайм-аута указывается в секундах.

Посмотреть установленное значение тайм-аута можно с помощью команды:

```
Admin@nodename# show libraries application-signature <"signature-name">
```

Пример создания пользовательской сигнатуры с указанием тайм-аута бездействия:

```
Admin@nodename# create libraries application-signature name test_sig1 uasl "UASL(.name="EXAMPLE2")" idle-timeout 500
Admin@nodename# show libraries application-signature "test_sig1"
```

```
signature-id : 1050002
name : test_sig1
type : app
threat : very-low
idle-timeout : 500
uasl : UASL(.name="EXAMPLE2");
```

В ранее созданных пользовательских сигнатурах можно менять значение тайм-аута с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout <num>
```

Пример:

```
Admin@oulmetioeth# set libraries application-signature "test_sig1" idle-timeout 700
Admin@oulmetioeth# show libraries application-signature "test_sig1"
```

```
signature-id : 1050002
name : test_sig1
type : app
threat : very-low
idle-timeout : 700
uasl : UASL(.name="EXAMPLE2");
```

Установить значение тайм-аута по умолчанию (в зависимости от протокола транспортного уровня) можно с помощью команды:

```
Admin@nodename# set libraries application-signature <"signature-name"> idle-timeout default
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@nodename# create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails [ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка сигнатур COB

На уровне **libraries ips-signature** возможно создание и настройка пользовательских кастомизированных сигнатур системы обнаружения вторжения (COB).

Для создания пользовательской сигнатуры COB используется команда:

```
Admin@nodename# create libraries ips-signature <parameters>
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
description	Описание сигнатуры COB. Не может быть изменено для сигнатур, созданных UserGate.
signature-id	Идентификатор группы сигнатур. Не может быть изменен для сигнатур, созданных UserGate.
enabled	Индикатор включения сигнатуры. - on — включить. - off — отключить.
threat	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: - very-low — очень низкий. - low — низкий. - medium — средний. - high — высокий. - very-high — очень высокий. Не может быть изменен для сигнатур, созданных UserGate.
action	Действие на срабатывание сигнатуры. Определены следующие значения: - none — действие не определено. - pass — пропустить пакет. - drop — отбросить пакет. - rst — отбросить пакет с разрывом TCP соединения (отправка TCP reset). - block — блокировать IP-адрес источника и/или назначения.
log	Журналирование: - on — включить запись в журнал. - off — отключить запись в журнал.
os	Тип операционной системы, для которой определена сигнатура: - windows - linux - bsd - macos - solaris - cisco - ios - android - other Не может быть изменено для сигнатур, созданных UserGate.
pcap	Трассировка срабатывания сигнатуры с записью в файл формата pcap. - on — включить. - off — отключить.
track-by	Применимость действий типа block или rst на срабатыване сигнатуры: - src — действия block или rst применяются к адресу источника отправления пакетов. - dst — действия block или rst применяются к адресу назначения отправления пакетов. - both — действия block или rst применяются и к источнику, и к назначению.
duration	Длительность блокировки для действия block .
uasl	Описание сигнатуры с помощью синтаксиса UASL. Не может быть изменено для сигнатур, созданных UserGate.
cve	Идентификатор уязвимостей по реестру CVE.

Параметр	Описание
bdu	Идентификатор уязвимостей по реестру BDU.
uri	Оptionальная ссылка на ресурс с описанием уязвимости.
category	Категория сигнатуры — группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup. • attack_response — сигнатуры, определяющие ответы на известные сетевые атаки. • coinminer — скачивание, установка, деятельность известных майнеров. • dns — известные уязвимости DNS. • dos — сигнатуры известных Denial of services атак. • exploit — сигнатуры известных exploits. • ftp — известные FTP-уязвимости. • imap — известные IMAP-уязвимости. • info — потенциальная утечка информации. • ldap — известные LDAP-уязвимости. • malware — скачивание, установка, деятельность известных malware. • misc — другие известные сигнатуры. • netbios — известные уязвимости протокола NETBIOS. • phishing — сигнатуры известных phishing атак. • pop3 — известные уязвимости протокола POP3. • rpc — известные уязвимости протокола RPC. • scada — известные уязвимости протокола SCADA. • scan — сигнатуры, определяющие попытки сканирования сети на известные приложения. • shellcode — сигнатуры, определяющие известные попытки запуска программных оболочек. • smtp — известные уязвимости протокола SMTP. • snmp — известные уязвимости протокола SNMP. • sql — известные уязвимости SQL. • telnet — известные попытки взлома по протоколу telnet. • tftp — известные уязвимости протокола TFTP. • user_agents — сигнатуры подозрительных Useragent. • voip — известные уязвимости протокола VoIP. • web_client — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps — сигнатуры, определяющие известные попытки взлома различных веб-приложений. • worm — сигнатуры, определяющие сетевую активность известных сетевых червей. Не может быть изменена для сигнатур, созданных UserGate.
classtype	Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Список классов может быть пополнен. • arbitrary-code-execution — попытка запуска произвольного кода. • attempted-admin — попытка получения административных привилегий. • attempted-dos — попытка совершения атаки Denial of Service. • attempted-recon — попытка атаки, направленной на утечку данных. • attempted-user — попытка получения пользовательских привилегий. • bad-unknown — потенциально плохой трафик. • command-and-control — попытка общения с C&C центром • default-login-attempt — попытка логина с именем/паролем по умолчанию. • denial-of-service — обнаружена атака Denial of Service. • exploit-kit — обнаружен exploit kit • misc-activity — прочая активность. • misc-attack — обнаружена атака. • shellcode-detect — обнаружен исполняемый код. • string-detect — обнаружена подозрительная строка. • suspicious-login — попытка логина с использованием подозрительного имени пользователя. • trojan-activity — обнаружен сетевой троян. • web-application-attack — обнаружена атака на веб-приложение. Не может быть изменен для сигнатур, созданных UserGate.

Представленная ниже команда предназначена для редактирования ранее созданной сигнатуры COB:

```
Admin@nodename# set libraries ips-signature <ips-signature-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании сигнатуры.

С использованием следующих команд возможен просмотр информации о сигнатурах COB:

```
Admin@nodename# show libraries ips-signature
```

или об определенной сигнатуре:

```
Admin@nodename# show libraries ips-signature <ips-signature-name>
```

Пример создания сигнатуры COB:

```
Admin@nodename# create libraries ips-signature name "Test signature" action none threat low description "Test signature description" log on pcap on url example.org uasl "UASL(.name="EXAMPLE");" enabled off
Admin@nodename# show libraries ips-signature "Test signature"
```

```
signature-id : 5
name         : Test signature
enabled      : off
description  : Test signature description
threat       : low
action       : none
log          : on
```

pcap : on
track-by : src
duration : 0 days 0 hours 5 minutes
uasl : UASL(.name="EXAMPLE";)
url : example.org
owner : You
type : custom

Для удаления созданной ранее сигнатуры COB используется команда:

Admin@nodename# delete libraries ips-signature <ips-signature-name>

Подробнее о сигнатурах COB читайте в статье [Сигнатуры COB](#) Руководства администратора.

Настройка профилей COB

Настройка профилей COB производится на уровне **libraries ips-profile**.

Для создания профиля системы обнаружения вторжения используется команда:

Admin@nodename# create libraries ips-profile <parameter>

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля COB.
description	Описание профиля COB.
filters	Фильтр для выбора релевантных сигнатур из библиотеки сигнатур COB. new — создание нового фильтра в профиле; value — SQL-подобное выражение для выбора сигнатур из библиотеки; enabled — активация фильтра в профиле; settings — задание свойств отобранных фильтром сигнатур: action — предпринимаемое действие, если сигнатура сработала, т.е. была найдена в трафике. Действия могут быть следующие: пропустить пакет (pass), отбросить пакет (drop), сбросить пакет с разрывом TCP соединения (reset), заблокировать IP-адрес источника и/или назначения (block-ip). Значение default (по умолчанию) оставляет для всех сигнатур то действие, которое было определено в самих сигнатурах по умолчанию. enabled — возможность включить/отключить сигнатуры. log — включение/отключение журналирования срабатывания сигнатуры. pcap-file — включение/отключение записи в PCAP-файл, если сигнатура сработала.

Пример создания профиля COB:

Admin@nodename# create libraries ips-profile name 222 filters new value "protocol = 'http' AND (category = 'exploit') AND (os = 'Linux')\" settings action drop log on pcap-file on enabled on

Команда для редактирования существующего профиля COB:

Admin@nodename# set libraries ips-profile <ips-profile-name> <parameter>

Список настраиваемых параметров аналогичен списку параметров, используемых при создании профиля (таблица выше).

Пример редактирования созданного ранее профиля COB:

Admin@nodename# set libraries ips-profile 222 filters 1 settings action reset

С помощью следующей команды можно перенастроить параметры системных сигнатур COB, входящих в правило:

Admin@nodename# set libraries ips-profile <ips-profile-name> override signature <signature-name> <parameters>

Следующая команда позволяет вернуть перенастроенные ранее параметры системной сигнатуры COB в первоначальное значение:

Admin@nodename# set libraries ips-profile <ips-profile-name> override signature <signature-name> restore-default

С использованием следующих команд возможен просмотр информации о профилях COB:

Admin@nodename# show libraries ips-profile

или об определенном профиле:

Admin@nodename# show libraries ips-profile <ips-profile-name>

Пример просмотра определенного фильтра в ранее созданном профиле COB:

Admin@nodename# show libraries ips-profile 222 filters 1

enabled : on
value : protocol = 'http' AND (category = 'exploit') AND (os = 'Linux')
settings :
enabled : on
action : reset
pcap-file : on
duration : 5
track-by : both
log : on

Для удаления профиля COB используется команда:

Admin@nodename# delete libraries ips-profile <ips-profile-name>

Для удаления определенного фильтра в ранее созданном профиле COB используется команда:

Admin@nodename# delete libraries ips-profile <ips-profile-name> filters <filter-number>

Подробнее о профилях COB читайте в статье [Профили COB](#) Руководства администратора.

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

Admin@nodename# create libraries notification-profiles smtp <parameter>

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.

Параметр	Описание
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):
Admin@nodename# create libraries notification-profiles smpp <parameter>
Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7/8]
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).

Параметр	Описание
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: 0 — Unknown. 1 — ISDN/telephone numbering plan (E.163/E.164). 3 — Data numbering plan (X.121). 4 — Telex numbering plan (F.69). 6 — Land Mobile (E.212). 8 — National numbering plan. 9 — Private numbering plan. 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). 13 — Internet (IP). 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp> <profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1|phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка профилей Netflow

Раздел находится на уровне **libraries netflow-profiles**.

Команда для создания профиля NetFlow:

```
Admin@nodename# create libraries netflow-profiles <parameter>
```

Далее необходимо указать параметры профиля:

Параметр	Описание
name	Название профиля NetFlow.
description	Описание профиля.
ip	IP-адрес NetFlow коллектора, куда сенсор будет отправлять статистику.
port	UDP порт, на котором NetFlow коллектор будет принимать статистику.
protocol	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): 5 — Netflow версии 5. 9 — Netflow версии 9. 10 — Netflow версии 10.
active-timeout	Время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока (например, передача большого файла через сеть). Задаётся в секундах; значение по умолчанию: 1800 секунд, максимальное значение — 3600 секунд.
inactive-timeout	Время, резервируемое на завершение неактивного потока; указывается в секундах. Значение по умолчанию — 15 секунд; максимальное значение — 3600 секунд.
max-flows	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. После достижения указанного количества все последующие потоки не будут учитываться (ограничение необходимо для защиты от DoS-атак); значение по умолчанию — 2000000; для снятия ограничения установить 0.
nat-events	Включить/отключить отправку информации о NAT преобразованиях в статистику NetFlow: on. off.
refresh-rate	Количество пакетов, после которого шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
timeout-rate	Время, через которое старый шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Чтобы редактировать существующий профиль:

```
Admin@nodename# set libraries netflow-profiles <profile-name>
```

Параметры, значения которых можно изменить, представлены в таблице выше.

Следующая команда предназначена для удаления профиля NetFlow:

```
Admin@nodename# delete libraries netflow-profiles <profile-name>
```

Для отображения информации о всех профилях NetFlow или об отдельном профиле используются следующие команды:

```
Admin@nodename# show libraries netflow-profiles
Admin@nodename# show libraries netflow-profiles <profile-name>
```

Настройка профилей LLDP

Создание и настройка профилей LLDP (Link Layer Discovery Protocol) производятся на уровне **libraries lldp-profiles**.

Команда для создания профиля LLDP:

```
Admin@nodename# create libraries lldp-profiles <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля LLDP.
description	Описание профиля.
port-status	Режимы: - rx — только приём данных LLDP — UserGate не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. - tx — только передача данных LLDP — UserGate будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей. - rx-tx — приём и передача данных LLDP — UserGate будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.

Следующая команда предназначена для редактирования информации о профиле:

```
Admin@nodename# set libraries lldp-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль LLDP, используя следующую команду:

```
Admin@nodename# delete libraries lldp-profiles <profile-name>
```

Чтобы отобразить информацию о профилях:

```
Admin@nodename# show libraries lldp-profiles
Admin@nodename# show libraries lldp-profiles <profile-name>
```

Настройка профилей SSL

Создание и настройка профилей SSL производятся на уровне **libraries ssl-profiles**.

Команда для создания профиля SSL:

```
Admin@nodename# create libraries ssl-profiles <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля SSL.
description	Описание профиля.
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: - tls1. - tls1.1. - tls1.2.
max-tls-version	Максимальная версия TLS, которая может быть использована в данном профиле: - tls1. - tls1.1. - tls1.2. - tls1.3.
ssl-ciphers	Выбор необходимых алгоритмов шифрования и цифровой подписи.
ssl-ciphers-suite	Установка алгоритмов шифрования для стандартных протоколов. Параметр предназначен для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS; необходимо указать версию: - tls1. - tls1.1. - tls1.2. - tls1.3.

Следующая команда предназначена для редактирования информации о профиле:

```
Admin@nodename# set libraries ssl-profiles <profile-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль SSL полностью или удалить отдельные алгоритмы шифрования и цифровой подписи, заданные в нём:

```
Admin@nodename# delete libraries ssl-profiles <profile-name>
Admin@nodename# delete libraries ssl-profiles <profile-name> ssl-ciphers [ cipher ... ]
```

Чтобы отобразить информацию о профилях SSL:

```
Admin@nodename# show libraries ssl-profiles
Admin@nodename# show libraries ssl-profiles <profile-name>
```

Настройка профилей пересылки SSL

Данный раздел находится на уровне **libraries ssl-forwarding-profiles**.

Для создания профиля пересылки используется команда:

```
Admin@nodename# create libraries ssl-forwarding-profiles <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля пересылки SSL.
description	Описание профиля пересылки.
type	Тип пересылки: - I2. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. - I3. Копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.

Параметр	Описание
mac	MAC-адрес назначения (указывается при использовании типа пересылки L2).
iface	Интерфейс UserGate, с которого будет производиться пересылка (указывается при использовании типа пересылки L2).
source-ip	GRE IP-адрес источника (указывается при использовании типа пересылки L3).
dest-ip	GRE IP-адрес назначения (указывается при использовании типа пересылки L3).

Следующая команда предназначена для обновления параметров профилей пересылки:

```
Admin@nodename# set libraries ssl-forwarding-profiles <profile-name> <parameter>
```

Для удаления профиля:

```
Admin@nodename# delete libraries ssl-forwarding-profiles <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом профиле пересылки, используются следующие команды:

```
Admin@nodename# show libraries ssl-forwarding-profiles
Admin@nodename# show libraries ssl-forwarding-profiles <profile-name>
```

Настройка объектов HIP

Данный раздел находится на уровне **libraries hip-object**

Для создания объекта HIP используется команда:

```
Admin@nodename# create libraries hip-object <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название объекта HIP.
description	Описание объекта HIP.
process	Проверка процессов, запущенных на конечном устройстве.
running-services	Проверка служб, запущенных на конечном устройстве.
installed-updates	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.
os-version	Версия операционной системы устройства пользователя.
products	Проверка на соответствие статуса: • antimalware — антивирусное ПО на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • firewall — межсетевой экран на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • backup — ПО для резервного копирования ◦ products — название продукта. ◦ vendor — производитель продукта. • disk-encryption — ПО шифрования диска на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • dlp — система предотвращения утечек информации на конечном устройстве. ◦ products — название продукта. ◦ vendor — производитель продукта. • patch-management — ПО для установки обновлений на конечном устройстве. ◦ products — название продукта ◦ vendor — производитель продукта.
registry-keys	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце. • REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft .
security	Проверка активных компонентов: • firewall — межсетевой экран (да, нет, не проверять). • virus-protection — антивирусное ПО (да, нет, не проверять). • automatic-update — автоматическая установка обновлений (да, нет, не проверять). • bitlocker — шифрование дисков (да, нет, не проверять).
ug-client-version	Версия ПО UserGate Client.

Команда для редактирования параметров объектов HIP:

```
Admin@nodename# set libraries hip-object <hip-object-name> <parameters>
```

Для удаления объекта:

```
Admin@nodename# delete libraries hip-object <hip-object-name>
```

Чтобы отобразить информацию о всех имеющихся объектах или об определённом объекте, используются следующие команды:

```
Admin@nodename# show libraries hip-object
Admin@nodename# show libraries hip-object <hip-object-name>
```

Настройка профилей HIP

Данный раздел находится на уровне **libraries hip-profile**

Для создания профиля HIP используется команда:

```
Admin@nodename# create libraries hip-profile <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля HIP.
description	Описание профиля HIP.
enabled	Включение/отключение использования профиля..
hip-objects	Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP. Подробнее о создании объектов HIP читайте в разделе Настройка объектов HIP .

Следующая команда предназначена для обновления параметров HIPprofiles:

```
Admin@nodename# set libraries hip-profile <hip-profile-name> <parameters>
```

Для удаления профиля:

```
Admin@nodename# delete libraries hip-profile <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом HIP profiles, используются следующие команды:

```
Admin@nodename# show libraries hip-profile
Admin@nodename# show libraries hip-profile <hip-profile-name>
```

Настройка профилей BFD

Данный раздел находится на уровне **libraries bfd-profile**

Для создания профиля BFD используется команда:

```
Admin@nodename# create libraries bfd-profile
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля BFD.
description	Описание профиля.
detect-multiplier	Множитель времени обнаружения; влияет на время обнаружения неисправностей соединения.
receive-interval	Интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами); указывается в миллисекундах.
transmit-interval	Интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами; указывается в миллисекундах.
echo-receive-interval	Минимальный интервал, через который данная система способна принимать echo-пакеты; указывается в миллисекундах.
echo-transmit-interval	Минимальный интервал, через который система будет способна отправлять echo-пакетов BFD; указывается в миллисекундах.
echo-mode	Включить или выключить режим передачи Echo mode .
pessive-mode	Включить или выключить режим Passive .
ttl	Минимальное ожидаемое TTL для входящего управляющего пакета BFD. Может принимать значения от 1 до 254.

Следующая команда предназначена для обновления параметров BFD profiles:

```
Admin@nodename# set libraries bfd-profile <profile-name> <parameter>
```

Для удаления профиля:

```
Admin@nodename# delete libraries bfd-profile <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом BFD profiles, используются следующие команды:

```
Admin@nodename# show libraries bfd-profile
Admin@nodename# show libraries bfd-profile <profile-name>
```

Настройка Syslog фильтров UserID агента

Создание и настройка syslog-фильтров производится на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

```
Admin@nodename# create libraries syslog-filters <parameters>
```

Далее необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.

Параметр	Описание
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-филтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameters>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка сценариев

Общие правила создания сценариев

Настройка сценариев происходит на уровне **libraries scenarios** с использованием UPL (подробнее о написании правил с помощью UserGate Policy Language читайте в разделе [Типы правил](#)).

Для задания условий сценариев и их объединения используются определения (definitions). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слэша (как при использовании многострочного ввода).

Для создания/изменения условий сценариев используется функция **def scenario_cond**, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
<scenario_conditions>
end
```

Параметры, использующиеся для задания разных типов условий, будут рассмотрены в следующих разделах.

Далее, после указания условий, указываются общие свойства сценария, представленные в таблице ниже:

Наименование	Описание
OK	Действие для создания сценария.
scenario_cond	Пользовательское имя определения, содержащего список условий сценария: scenario_cond = condition_example .
enabled	Включить/отключить использование сценария: enabled(true); enabled(false).
name	Задать имя сценария: name("Example scenario name") .
desc	Задать описание сценария: desc("Description for scenario created as an example") .
trigger	Применение: trigger(one_user) — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; trigger(all_users) — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила.
duration	Задать период активности сценария; указывается в минутах.
operation_mode	Задать режим активации сценария: operation_mode(all) — сценарий сработает, если выполнятся все условия; operation_mode(any) — сценарий сработает, если выполнится хотя бы одно из условий.

Примечание!При обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием **Объём трафика**. Сценарий будет применён ко всем пользователям в течение минуты; ограничение объёма трафика: 1 ГБ/день:

```
Admin@nodename# create libraries scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(1GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
...
```

Для изменения, например, объёма трафика:

```
Admin@nodename# set libraries scenarios 3 upl-rule \
...def scenario_cond scenario_cond_test
...traffic_limit(2GB) \
...period(day) \
...scond_type(traffic)
...end
...OK \
...scenario_cond = scenario_cond_test
```

Типы условий, используемых при создании сценариев

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
scond_type	Тип условия: scond_type(url_category) .

Наименование	Описание
category	Категории или группы категорий сайтов: <code>category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(virus_detection)</code> .

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(app)</code> .
application	Категории приложений или группы приложений: <code>application = lib.applicationgroup(APP_GROUP)</code> или <code>application = lib.applicationgroup(all)</code>; <code>application = lib.category(APPS_CATEGORY_NAME)</code>.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа COB

Параметры условия типа **COB**:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(ips)</code> .
ips_tl	Уровень угрозы: <code>ips_tl(very_low)</code> - очень низкий; <code>ips_tl(low)</code> - низкий; <code>ips_tl(medium)</code> - средний; <code>ips_tl(high)</code> - высокий; <code>ips_tl(very_high)</code> - очень высокий.

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(mime_type)</code> .
response.header.Content-Type	Тип контента: <code>response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST)</code> .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): <code>count_interval()</code> .
max_event_count	Количество срабатываний: <code>max_event_count()</code> .

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: <code>scond_type(traffic)</code> .
traffic_limit	Ограничение объёма трафика: <code>traffic_limit(1)</code> - 1 байт трафика; <code>traffic_limit(1KB)</code> - 1 Кбайт трафика; <code>traffic_limit(1MB)</code> - 1 Мбайт трафика; <code>traffic_limit(1GB)</code> - 1 Гбайт трафика.
period	Период времени: <code>period(minute)</code> - минута; <code>period(hour)</code> - час; <code>period(day)</code> - день; <code>period(week)</code> - неделя; <code>period(month)</code> - месяц.

Условие типа Проверка состояния

Для настройки условия типа **Проверка состояния** предназначены параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(health_check) .
health_check_method	Метод проверки: health_check_method(ping) - ping; health_check_method(dns) - DNS-запрос; health_check_method(get) - HTTP-метод GET.
url.address	Адрес, на который будут выполняться ping и DNS-запрос: url.address = "1.1.1.1" .
url.domain	FQDN для проверки состояния путём выполнения DNS-запроса или URL для метода HTTP GET: url.domain = "example.ru" .
gateway	Название используемого шлюза: gateway() . Важно! Шлюз должен быть предварительно создан.
health_result	Результат выполнения проверки: health_result(positive) - положительный; health_result(negative) - отрицательный.
health_request_timeout	Тайм-аут подключения (в секундах): health_request_timeout() .
health_answer_timeout	Время ожидания ответа на запрос HTTP GET (в секундах): health_answer_timeout() .
health_type_request	Тип DNS-запроса: health_type_request(a). health_type_request(aaaa). health_type_request(cname). health_type_request(ns). health_type_request(ptr).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Настройка тегов

Использование тегов доступно в версии ПО 7.3.0 и выше.

Создание и настройка тегов производятся на уровне **libraries tags**.

Команда для создания тегов:

Admin@nodename# create libraries tags <parameters>

Далее необходимо указать:

Параметр	Описание
name	Название тега.
description	Описание тега.
color	Выбор цветовой маркировки тега для отображения в веб-интерфейсе: no-color (Значение по умолчанию); red; orange; yellow; green; aqua; blue; violet; pink; purple; light-gray; light-green; light-blue; black; rose; magenta; wood;

Команда для редактирования информации о теге:

Admin@nodename# set libraries tags <tag-name> <parameters>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании тега.

Чтобы отобразить информацию о тэгах:

Admin@nodename# show libraries tags <tag-name>

Пользователь может удалить тег, используя следующую команду:

Admin@nodename# delete libraries tags <tag-name>

Примеры работы с тэгами в библиотеке:

Admin@nodename# create libraries tags name "Test tag 6" description "Tag made with CLI" color magenta
Admin@nodename# show libraries tags

Test tag 6
name : Test tag 6
description : Tag made with CLI
color : magenta

Tag 5
name : Tag 5
description : Test tag #5
color : green

Tag 1
name : Tag 1
description : Test tag #1
color : no-color

Admin@nodename# show libraries tags "Test tag 6"

name : Test tag 6
description : Tag made with CLI
color : magenta

Admin@nodename# set libraries tags "Test tag 6" description "Update tag from cli"
Admin@nodename# show libraries tags "Test tag 6"

name : Test tag 6
description : Update tag from cli
color : magenta

Admin@nodename# delete libraries tags "Test tag 6"

Настройка экспорта журналов

Documentation: ☒
Product: NGFW
Version: 7.x

Функция экспортирования журналов позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM.

Для создания нового правила экспорта журналов используется команда:

```
Admin@nodename# create logs logs-export <parameters>
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение правила: - on. - off.
name	Название правила.
description	Описание правила.
server-type	Тип сервера: - ssh; - ftp; - syslog. При выборе типа сервера доступны следующие дополнительные настройки: - port — Порт сервера, на который следует отправлять данные. - login — Имя учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). - password — Пароль учетной записи для подключения к удаленному серверу (не применяется к методу отправки syslog). - path — Каталог на сервере для копирования файлов журналов (не применяется к методу отправки syslog). - passive — Пассивный режим ftp. - transport — Только для типа серверов syslog. TCP или UDP. - protocol — Только для типа серверов syslog. RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. - severity — Только для типа серверов syslog. Критичность. Возможны следующие значения: alert, critical, error, warning, notice, info. - facility — Только для типа серверов syslog. Объект. Возможны следующие значения: user-level, system-daemons, security-auth, log-audit, log-alert, local- (0-7). - hostname — Только для типа серверов syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN). - app-name — Только для типа серверов syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
target	IP-адрес или доменное имя сервера.
logs	Журналы для экспорта: - dns — Журнал DNS. - events — Журнал событий. - webaccess — Журнал веб-доступа. - idps — Журнал COB. - mailsecurity — Журнал почтового трафика. - ssh — Журнал инспектирования SSH. - traffic — Журнал трафика. - userid — Журнал UserID. Для каждого журнала можно выбрать синтаксис выгрузки: - cef; - cef-compact; - json; - cee-json; - off.
schedule	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. cron-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Для редактирования ранее созданных правил используется команда:

```
Admin@nodename# set logs logs-export <log-export-rule-name>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил экспорта.

Для просмотра параметров созданных ранее правил экспорта используется команда:

```
Admin@nodename# show logs logs-export
Admin@nodename# show logs logs-export <log-export-rule-name>
```

Для удаления созданных ранее правил экспорта используется команда:

```
Admin@nodename# delete logs logs-export <log-export-rule-name>
```

Для настройки параметров разового экспорта журналов используется команда:

```
Admin@nodename# execute logs send-once <log-export-rule-name> <parameters>
```

Параметр	Описание

Параметр	Описание
fresh	Экспортировать свежие логи.
range	Указать диапазон экспорта: • start-export-range — начало диапазона в формате: 2022-12-31T23:59:59 • end-export-range — конец диапазона в формате: 2022-12-31T23:59:59

Настройка отчетов

Product: NGFW
Version: 7.x

Настройка отчетов в интерфейсе командной строки CLI (доступно в версии 7.4.0 и выше) происходит в режиме конфигурации на уровне `reports`. С помощью команд этого раздела можно просматривать имеющиеся на устройстве шаблоны отчетов, создавать и редактировать правила отчетов, просматривать ранее созданные отчеты.

Шаблоны отчетов

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией UserGate.

Для просмотра имеющихся шаблонов отчетов используется команда:

```
Admin@nodename# show reports report-templates
```

Правила отчетов

Правила отчётов задают параметры создаваемого отчета, а также расписание запуска отчетов и способы их доставки пользователям.

Для создания нового правила отчетов используется команда:

```
Admin@nodename# create reports report-rules <parameters>
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение правила: - on; - off.
name	Название правила.
description	Описание правила.
language	Выбор языка создания отчета: - ru; - en.
time-range	Диапазон времени в секундах, за который необходимо подготовить отчет.
format	Выбор формата, в котором будет создан отчет: - pdf; - html.
query-limit	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
query-limit-by	Задание ограничения числа записей, которые будут выводиться в отчетах с ограничением по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчётов, которые содержат группирование.
templates	Список шаблонов, которые будут использоваться для построения отчёта. Обязательно необходимо добавить хотя бы один шаблон.
email-sender	Отправитель письма с созданным отчётом.
email-recipients	Список получателей письма с отчётом. Получатели должны быть добавлены в списки библиотеки «Почтовые адреса» (<code>email-list</code>).
email-subject	Тема письма с отчетом.
email-body	Содержимое письма с отчетом.
smtp-profile	Профиль SMTP, который будет использован для отправки отчетов.
schedule	Выбор расписания для отправки отчетов. Crontab-подобный формат, при котором строка выглядит как шесть полей, разделённых пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0 — воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звёздочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, 5-7 будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделённые запятыми. Например, 1,5,10,11 или 1-11,19-23. - Звёздочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, выражение «2-10/2» будет значить: «2,4,6,8,10», а выражение: «*/2» в поле «часы» будет означать каждые два часа.

Для редактирования ранее созданных правил используется команда:

```
Admin@nodename# set reports report-rules <report-rule-name> <parameters>
```

Параметры, доступные для редактирования, аналогичны параметрам создания правил отчетов.

Для просмотра параметров созданных ранее правил отчетов используется команда:

```
Admin@nodename# show reports report-rules
Admin@nodename# show reports report-rules <report-rule-name>
```

Для удаления созданных ранее правил отчетов используется команда:

```
Admin@nodename# delete reports report-rules <report-rule-name>
```

Созданные отчеты

Для просмотра информации о созданных отчетах используется команда:

```
Admin@nodename# show reports generated-reports
Admin@nodename# show reports generated-reports <generated-report-name>
```

