

Table of Contents

Table of Contents	1
Интерфейс командной строки (CLI)	3
Общие положения	4
Общие положения (Описание)	5
Команды, доступные до первичной инициализации узла	7
Команды, доступные до первичной инициализации узла (Описание)	8
Первоначальная инициализация	9
Первоначальная инициализация (Описание)	10
Команды диагностики и мониторинга	12
Команды диагностики и мониторинга (Описание)	13
Режим конфигурации	22
Режим конфигурации (описание)	23
Настройка устройства	27
Настройка устройства (Описание)	28
Настройка кластеров	35
Настройка управления доступом к консоли NGFW	37
Настройка сертификатов	41
Настройка параметров устройства	44
Настройка телеметрии	46
Настройка прокси-сервера	47
Настройка параметров устройства	49
Настройки сети	51
Зоны	52
Интерфейсы	56
Шлюзы	69
DHCP	70
DNS-настройки	72
Настройка виртуальных маршрутизаторов	75
Настройка WCCP	88
Настройка правил с использованием UPL	90
Настройка правил с использованием UPL (Описание)	91
Настройка раздела Пользователи и устройства	93
Настройка групп пользователей	94
Настройки пользователей	95
Настройка серверов аутентификации	97
Настройка профилей аутентификации	101
Captive-портал	103
Настройка Captive-профилей	105
Настройка терминальных серверов	107
Настройка профилей MFA (мультифакторной аутентификации)	108
Настройка применения политик к пользователям	110
Настройка раздела Политики сети	111
Настройка правил межсетевого экрана	112
Настройка правил NAT и маршрутизации	115
Настройка балансировки нагрузки	122
Настройка правил пропускной способности	126
Настройка раздела Политики безопасности	128
Настройка фильтрации контента	129
Настройка веб-безопасности	132
Настройка правил инспектирования туннелей	134

Настройка инспектирования SSL	136
Настройка инспектирования SSH	139
Настройка COB	141
Настройка сценариев	143
Настройка правил защиты почтового трафика	148
Настройка правил ICAP	150
Настройка ICAP-серверов	152
Настройка правил защиты DoS	154
Настройка профилей DoS	156
Настройка глобального портала	157
Настройка веб-портала	158
Настройка правил reverse-прокси	160
Настройка серверов reverse-прокси	162
Настройка удалённого доступа (VPN)	163
Настройка серверных правил	164
Настройка клиентских правил	166
Настройка сетей VPN	168
Настройка профилей безопасности VPN	168
Настройка библиотек	172
Настройка библиотек (Описание)	173

Интерфейс командной строки (CLI)

Общие положения

Общие положения (Описание)

Documentation: ☒
Product: NGFW
Version: 7.0.1

UserGate NGFW имеет возможность управления через интерфейс командной строки — CLI (Command Line Interface). С помощью CLI администратор может выполнять команды диагностики и мониторинга, производить настройку устройства, а также перезагружать или выключать устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании NGFW), через последовательный порт или с помощью SSH по сети.

CLI имеет два режима работы — режим диагностики и мониторинга, и режим конфигурации.

В **режиме диагностики и мониторинга** доступны команды, позволяющие посмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.
- Мониторинг состояния кластера.
- Мониторинг заблокированных COB IP-адресов.
- Отображение системной информации.
- Диагностику работы протоколов динамической маршрутизации.
- Информацию об авторизованных пользователях.

Приглашение командной строки в режиме диагностики и мониторинга имеет следующий вид:

Admin@NGFW>

Настройка устройства производится в режиме конфигурации.

Для перехода в **режим конфигурации** используется команда:

Admin@NGFW> configure

После перехода в режим конфигурации приглашение командной строки будет выглядеть следующим образом:

Admin@NGFW#

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд в обоих режимах работы CLI необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

- * — обязательное поле в командах create и ряде других команд;
- + — необязательное/вариативное поле;
- > — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

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

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к NGFW.	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.

Наименование	Описание
Шаг 2. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к NGFW.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к NGFW.
Шаг 2. Запустить терминал.	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны.	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал.	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес NGFW, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: <code>ssh Admin@IPNGFW -p 2200</code>
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

После успешной авторизации в CLI пользователь попадает в режим диагностики и мониторинга, появляется строка, ожидающая ввода команды.

Для просмотра доступных команд, текущих возможных значений команды или автодополнения необходимо использовать клавишу **Tab**.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

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

где <action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter>: идентификатор объекта, к которому происходит обращение.

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

CLI поддерживает ввод команды в несколько строк (многострочный ввод). Для перехода на новую строку необходимо добавить "\n" в конце строки. Начиная со второй строки ввод "\n" необязателен; чтобы завершить ввод необходимо ввести одну пустую строку:

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

Команды, доступные до первичной инициализации узла

Команды, доступные до первичной инициализации узла (Описание)

Documentation: ☒

Product: NGFW

Version: 7.0.1

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации CLI — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу `radmin-emergency`.

Доступные команды в режиме диагностики

Команды диагностики позволяют просмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Мониторинг трафика.
- Информацию о маршрутах.
- Отображение системной информации.

Подробнее о синтаксисе и примерах использования команд диагностики читайте в разделе [Команды диагностики и мониторинга](#).

Доступные команды в режиме конфигурации

Для перехода в режим конфигурации используется команда:

```
Admin@NGFW> configure
```

После перехода в режим конфигурации приглашение командной строки будет выглядеть следующим образом:

```
Admin@NGFW#
```

В режиме конфигурации доступны команды *execute* (команды, которые не относятся к настройке конфигурации устройства — `ping`, `date`, `traceroute` и т.п.), команды настройки сети (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов), а также команды включения/отключения удалённого доступа к серверу `radmin-emergency`.

Подробнее о синтаксисе и примерах использования команд *execute* читайте в разделе [Режим конфигурации](#).

Подробнее о синтаксисе и примерах использования команд настройки сети читайте в следующих разделах:

- [Команды настройки зон](#).
- [Команды настройки интерфейсов](#).
- [Команды настройки шлюзов](#).
- [Команды настройки виртуальных маршрутизаторов](#).

Подробнее о синтаксисе и примерах использования команд включения/отключения удалённого доступа к серверу `radmin-emergency` читайте в разделе [Настройка управления устройством](#).

Подробнее о первоначальной инициализации устройства с помощью CLI читайте в разделе [Первоначальная инициализация](#).

Первоначальная инициализация

Первоначальная инициализация (Описание)

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Первоначальная инициализация

Первичную инициализацию NGFW с использованием интерфейса командной строки можно произвести несколькими способами.

Установка как главного узла.

Для настройки NGFW в качестве главного узла используется команда:

Admin@UGOS# execute install node master

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии Enter после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Установка как дополнительного узла кластера.

Для настройки NGFW в качестве дополнительного узла кластера используется команда:

Admin@UGOS# execute install node slave

Необходимо указать параметры:

Параметр	Описание
interface	Интерфейс для подключения к кластеру.
slave-ip	IP-адрес, который будет назначен на интерфейс, использующийся для подключения к кластеру.
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 NGFW.
password	Пароль учётной записи администратора.

Настройка через UGMC

Для настройки NGFW в качестве дополнительного узла кластера используется команда:

Admin@UGOS# execute install node mc

Необходимо указать параметры:

Параметр	Описание

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

После первичной инициализации будет доступно полное управление из CLI.

Команды диагностики и мониторинга

Команды диагностики и мониторинга (Описание)

Product: UserGate NGFW
Version: 7.0.1

Команды диагностики позволяют просмотреть следующее:

- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.

Статистика интерфейсов

Для отображения статистики интерфейса и информации о нём используется следующая команда:

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

Также доступно отображение только информации или только статистики интерфейса:

Admin@UGOS> show network interface <interface-name> info

Admin@UGOS> show network interface <interface-name> statistic

ARP-записи

Для просмотра информации о записях ARP:

Admin@UGOS> show network arp

При просмотре записей доступно использование фильтров. Параметры фильтрации:

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

Просмотр записей ARP также доступен в режиме конфигурации; команды идентичны командам в режиме диагностики и мониторинга.

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

Добавление статических ARP-записей доступно в режиме конфигурации с использованием следующей команды:

Admin@UGOS# set network arp

Необходимо указать:

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 NGFW.

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

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

- **clear**: удаление системных записей в режиме диагностики и мониторинга;
- **delete**: удаление статических записей в режиме конфигурации.

Далее будет представлен формат команд удаления на примере команд режима диагностики и мониторинга.

Для удаления системной записи:

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

Чтобы удалить запись на другом узле кластера:

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

Следующая команда позволяет удалить все системные записи на заданном интерфейсе (можно указать несколько интерфейсов):

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

Для удаления всех системных записей интерфейса другого узла:

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

Отслеживание пакетов

Чтобы произвести отслеживание пакетов, используется следующая команда:

```
Admin@UGOS> show network trace
```

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия портов источника и назначения NGFW, номера TCP/UDP портов источника и назначения. Команда также доступна в режиме конфигурации.

Чтобы выйти из режима отслеживания пакетов — **Ctrl+C**.

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации на уровне **network**. Для создания правила используется следующая команда:

```
Admin@UGOS# create network trace-rules
```

Далее указываются следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила отслеживания пакетов: • on. • off.
name	Название правила. Если название правила не было задано, то оно задаётся автоматически в формате: trace_rule_N (где N — порядковый номер создаваемого правила отслеживания пакетов).
zones-in	Список зон источников трафика.
source-ip-lists	Список групп IP-адресов источника пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов .
source-ip-addresses	Список IP-адресов источника пакета.
dest-ip-lists	Список групп IP-адресов назначения пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов .
dest-ip-addresses	Список IP-адресов назначения пакета.

Параметр	Описание
services	Тип сервиса. Подробнее читайте в разделе Настройка сервисов .

Для изменения правила:

```
Admin@UGOS# set network trace-rules <trace-rule-name>
```

Для изменения доступны параметры, представленные в таблице выше.

Для удаления правила отслеживания пакетов используется следующая команда:

```
Admin@UGOS# delete network trace-rules <trace-rule-name>
```

Также доступно удаление значений отдельных параметров правил. Для удаления доступны:

- **zones-in.**
- **source-ip-lists.**
- **source-ip-addresses.**
- **dest-ip-lists.**
- **dest-ip-addresses.**
- **services.**

Чтобы просмотреть существующие правила отслеживания пакетов:

```
Admin@UGOS# show network trace-rules
```

или

```
Admin@UGOS# show network trace-rules <trace-rule-name>
```

Мониторинг трафика

Следующая команда используется для мониторинга трафика:

```
Admin@UGOS> show traffic
```

Параметр	Описание
flows	Отображает информацию о входящем (IP и MAC-адреса источника и назначения, порты источника и назначения, протокол, тег VLAN, время жизни сессии, состояние сессии) и исходящем (IP-адреса источника и назначения, тег VLAN) потоках. Доступна фильтрация по: • source-ip — IP-адрес источника. • source-port — порт источника. • source-mac — MAC-адрес источника • dest-ip — IP-адрес назначения. • dest-port — порт назначения. • dest-mac — MAC-адрес назначения. • vlan-tag — тег VLAN.

Параметр	Описание
connections	Представлена информация 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.). Фильтрация доступна по: • protocol — протокол. • source-ip — IP-адрес источника. • dest-ip — IP-адрес назначения. • expect — отображение неустановленных соединений: ◦ on. ◦ off.

LLDP

Использованием следующей команды доступен просмотр информации LLDP:

```
Admin@UGOS> show lldp
```

Для просмотра доступны:

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

Маршруты

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

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

```
Admin@UGOS> show network route
```

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 Р в списке маршрутов.
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> all).

Мониторинг OSPF

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

Admin@UGOS> show network ospf

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, подключённых к его сегменту напрямую. • Summary Link States: пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • ASBR-Summary Link States: пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора (Autonomous System Border Router, ASBR) в других областях.

Параметр	Описание
neighbor	Отображение информации о соседях: - Идентификатор соседа (идентификатор маршрутизатора). - Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором — Designated Router, DR. Если приоритеты маршрутизаторов равны, то будет выбран маршрутизатор с наибольшим идентификатором. - Состояние, например, Full/DR, Full/BDR, Full/Drother. - Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. - IP-адрес интерфейса, к которому подключен сосед. - Интерфейс, на котором сформировано соседство маршрутизаторов. Доступно указание дополнительных параметров: interface-name — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. all — отображение таблицы со всеми соседями. detail — отображение подробной информации о соседях.
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@UGOS> clear network ospf

Параметр	Описание
virtual-router	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<vrf-name> all).
interface	Интерфейс, на котором необходимо перезапустить процесс OSPF.

Мониторинг BGP

В данном разделе представлены команды диагностики и мониторинга BGP.

Для отображения таблицы BGP маршрутизатора по умолчанию:

Admin@UGOS> show network bgp

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.

Параметр	Описание
neighbors	Отображение информации о BGP-соседах (доступно отображение информации об определённом соседе; необходимо указание IP-адреса соседа). Дополнительные параметры, доступные при указании соседа: • received-routes — принятые маршруты до применения к ним входящей политики (Routemap и фильтры). • advertised-routes — маршруты, которые анонсируются указанному соседу.
summary	Просмотр краткой информации о соседях.

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

Admin@UGOS> clear network bgp

Далее доступно указание параметров:

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

Мониторинг RIP

В данном разделе представлены команды диагностики и мониторинга RIP.

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

Admin@UGOS> show network rip

Далее доступно использование следующих параметров:

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

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

Admin@UGOS> show network mroute

Далее доступно использование следующих параметров:

Параметр	Описание
count	Отображение статистики о группе и источнике.
virtual-router	Выбор виртуального маршрутизатора: <vrf-name> all .

Параметр	Описание
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации.
fill	Таблица маршрутизации мультикаст-трафика. Доступно указание параметра: ip — отображение записи для определённого IP-адреса; далее необходимо указать IP-адрес.
ip	Отображение записи для определённого IP-адреса; необходимо указать IP-адрес.

Мониторинг IGMP

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

```
Admin@UGOS> show network igmp
```

Если необходимо отобразить информацию для определённого виртуального маршрутизатора или всех:

```
Admin@UGOS> show network igmp virtual-router <vrf-name> | all
```

Далее необходимо указать один из параметров:

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

Мониторинг PIM

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

является обязательным). Для отображения информации для маршрутизатора по умолчанию:

```
Admin@UGOS> show network pim
```

Если необходимо отобразить информацию для определённого виртуального маршрутизатора или всех:

```
Admin@UGOS> show network pim virtual-router <vrf-name> | all
```

Далее необходимо указать один из параметров:

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

Режим конфигурации (описание)

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Для перехода в режим конфигурации используется команда:

Admin@UGOS> configure

После перехода в режим конфигурации командная строка будет следующей:

Admin@UGOS#

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • execute — выполнение команд, которые не относятся к конфигурации NGFW (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • set — редактирование всех объектов, а также включение различных параметров, например, radmin. • end — переход на один уровень выше. • show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён над командной строкой. • top — возврат на самый верхний уровень конфигурации. • exit — выход из режима конфигурации. • export — экспорт конфигурации. • import — импорт конфигурации. • create — создание новых объектов. • delete — удаление объекта или параметра из списка параметров. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: Admin@UGOS# show network interface С использованием следующей команды производится переход на уровень network interface: Admin@UGOS# edit network interface Текущий уровень будет отображён над командной строкой: [network interface] Admin@UGOS# После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: [network interface] Admin@UGOS# show
<level>	Уровни в командной строке повторяют веб-интерфейс NGFW • security-policy — соответствует разделу веб-интерфейса Политики безопасности. • network — соответствует разделу веб-интерфейса Сеть. • settings — соответствует разделу веб-интерфейса NGFW. • global-portal — соответствует разделу веб-интерфейса Глобальный портал. • network-policy — соответствует разделу веб-интерфейса Политики сети. • vpn — соответствует разделу веб-интерфейса VPN. • users — соответствует разделу веб-интерфейса Пользователи и устройства.

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 <configuration_info> (рассмотрено далее в разделе). 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@UGOS# show network interface adapter port0</pre> то 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@UGOS# show network interface adapter (node-name another_nodename interface port0)</pre> Важно! Круглые скобки должны быть отделены пробелами с обеих сторон.
<configuration_info>	Набор пар: параметр-аргумент. 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@UGOS# create users group "VPN users"</pre> Множественные аргументы используются для установки множества значений какого-либо параметра; 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@UGOS# set users group "VPN users" users [user1 user2]</pre> Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

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

Доступны следующие команды:

Параметр	Описание
update	Обновление: software-updates — обновление программного обеспечения. libraries-updates — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: 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.
license	Команда регистрации продукта имеет следующую структуру: <pre>Admin@UGOS# execute license activate online <pin-code></pre> Укажите код активации продукта вместо <pin-code>.
terminate	Закрытие сессий администраторов. Подробнее читайте в разделе Настройка сессий администраторов.

Параметр	Описание
cache	Очистка кэша LDAP-записей: • ldap-clear.
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • count — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • numeric — не резолвить 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.
reboot	Перезагрузка NGFW.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение NGFW.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • 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 таймаут ожидания ответа от веб-сервера.
dig	Проверка записи DNS домена. • reverse-lookup — получение хоста по IP-адресу. • dns — указание IP-адреса DNS-сервера. • tcp — использование протокола TCP вместо UDP.
configuration-cluster	Генерирование секретного кода, необходимого для добавления нового узла в кластер конфигурации: <pre>Admin@UGOS# execute configuration-cluster generate-secret-key</pre> Важно! Для использования данной команды необходимо наличие лицензии на модуль Cluster, иначе будет отображена ошибка.

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@UGOS> <command-name>

Команды import

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

В разделе настроек NGFW доступен импорт сертификатов. Подробнее читайте в разделе [Настройка сертификатов](#).

В разделах **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN** доступен импорт правил, написанных на UPL. При использовании импорта, все существующие правила будут заменены на указанные; можно указать сразу несколько правил.

В разделе **Пользователи** доступен импорт правил Captive-портала. Подробнее о добавлении правил читайте в соответствующем разделе [Настройка Captive-портала](#).

В разделе **Сеть** доступен импорт правил DNS. Подробнее читайте в разделе [Настройка правил DNS](#).

В разделе **Политики сети** доступен импорт правил межсетевого экрана, NAT и маршрутизации, пропускной способности. Подробнее читайте

в соответствующих разделах [Настройка правил межсетевого экрана](#), [Настройка правил NAT и маршрутизации](#), [Настройка правил пропускной способности](#).

В разделе **Политики безопасности** доступен импорт правил контентной фильтрации, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, COB, 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 COB](#), [Настройка правил ICAP](#), [Настройка правил защиты DoS](#).

В разделе **Глобальный портал** доступен импорт правил веб-портала и reverse-прокси. Подробнее о создании правил читайте в разделах [Настройка веб-портала](#) и [Настройка правил reverse-прокси](#).

В разделе VPN доступен импорт серверных и клиентских правил, о добавлении которых написано в разделах [Настройка серверных правил](#) и [Настройка клиентских правил](#).

Команды export

Доступен экспорт сертификатов и элементов библиотек.

Подробнее об экспорте сертификатов смотрите в разделе [Настройка сертификатов](#).

Для экспорта доступны следующие элементы библиотек: IP-адреса, Useragent браузеров, списки URL, категории URL, изменённые категории URL, типы контента, морфология, почтовые адреса и номера телефонов. Для экспорта элемента библиотеки используется команда:

```
Admin@UGOS# export libraries <library-name> <list-name>
```

где <library-name> — название библиотеки элементов (IP-адреса, Списки URL и т.д.).

<list-name> — название элемента библиотеки.

Настройка устройства (Описание)

Documentation: ☒
Version: 7.0.1
Product: UserGate NGFW

Настройка CLI

Настройка интерфейса командной строки производится на уровне **settings cli**. Чтобы задать уровень детализации диагностики используется следующая команда:

Admin@UGOS# set settings cli log-level <off | error | debug | warning | info>

Уровни детализации:

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

Для отображения настроек CLI:

Admin@UGOS# show settings cli

Общие настройки NGFW

Общие настройки NGFW задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

Admin@UGOS# set settings general <settings-module>

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень settings general admin-console): • 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 авторизации веб-консоли: ◦ password: авторизацию по имени и паролю. ◦ cert: авторизация по X.509-сертификату. • web-ssl-profile: выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL смотрите в разделе Настройка профилей SSL. • response-page-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 смотрите в разделе Настройка профилей SSL.

Параметр	Описание
server-time	Настройка параметров установки точного времени (уровень settings general server-time): • ntp-enabled: включение/отключение использования NTP-серверов: ◦ on. ◦ off. • ntp-servers: указание серверов NTP (основного и запасного): <pre>Admin@UGOS# set settings general server-time ntp-servers [server1] Admin@UGOS# set settings general server-time ntp-servers [server1 server2]</pre> • time: установка времени на сервере; время указывается в часовом поясе UTC в формате уууу-мм-ддThh:mm:ss (например, 2022-02-15T12:00:00)
modules	Настройка модулей NGFW (уровень settings general modules): • proxy-port: указать нестандартный номер порта, который будет использоваться для подключения к встроенному прокси-серверу. • auth-captive: указать служебный домен, который используется NGFW при авторизации пользователей через Captive-портал. • logout-captive: указать служебный домен, который используется пользователями NGFW для окончания сессии (logout). • block-page-domain: указать служебный домен, который используется для отображения страницы блокировки пользователям. • ftp-enabled: включить/отключить модуль, позволяющий получать доступ к содержимому FTP-серверов из пользовательского браузера. • ftp-domain: указать служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. • zone-enabled: включить/отключить зону для инспектируемых туннелей: ◦ on. ◦ off. • tunnel-inspection-zone: выбрать зону для инспектируемых туннелей. • snmp-engine-id: настроить SNMP Engine ID: ◦ 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 SNMP Engine ID (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ value — значение идентификатора. • terminal-sever-agent password: настроить пароль агентов терминального сервиса. • lldp: настроить использование протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своём 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, изменение имени хоста или адреса управления. Может принимать значения от 1 до 3600; задаётся 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.

Параметр	Описание
cache	Настройка кэша прокси-сервера (уровень settings general cache): • caching-mode: включение или отключение кэширования. ◦ on. ◦ off. • exclusions: список URL, которые не будут кэшироваться. Для удаления исключений: Admin@UGOS# delete settings general cache exclusions [<URL>] • max-cacheable-size: максимальный размер объектов, которые будут кэшироваться (указывается в Мбайт). • ram-size: размер оперативной памяти, отведенный под кэширование (указывается в Мбайт).
log-analyzer	Настройки модуля Log Analyzer (уровень settings general log-analyzer): • use-local-stat-server — использование локального Log Analyzer: ◦ on. ◦ off.
proxy-portal	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (уровень settings general proxy-portal): • enabled: включение/отключение использования веб-портала: ◦ on. ◦ off. • hostname: имя хоста. • port: порт. • auth-profile: выбор профиля аутентификации. Подробнее о настройке профилей авторизации с использованием CLI читайте в разделе Настройка профилей аутентификации. • auth-template: выбор шаблона страницы авторизации. • portal-template: выбор шаблона портала. • enable-ldap: выбор домена AD/LDAP на странице авторизации: ◦ on. ◦ off. • use-captcha: показ CAPTCHA: ◦ on. ◦ off. • ssl-profile: выбор профиля SSL. Подробнее о настройке профилей аутентификации с использованием CLI читайте в разделе Настройка профилей SSL. • certificate: выбор сертификата. • auth-by-cert: включение/отключение авторизации пользователя по сертификату: ◦ on. ◦ off.

Параметр	Описание
pcap	Настройка захвата пакетов (уровень settings general pcap): • type: тип захвата: ◦ 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 учёта изменений (уровень settings general change-tracker): • enabled: включение/отключение учёта изменений. ◦ on. ◦ off. • event-tracker-types: типы изменений задаются администратором. Для удаления типа изменения используется команда: Admin@UGOS# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Настройка агента UGMC (уровень settings general management-center): • enabled: включение/отключение агента UGMC. ◦ on. ◦ off. • mc-address: адрес сервера UGMC. • device-code: уникальный код устройства для подключения устройства к UGMC.
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень settings general updates-schedule). Для расписания обновления программного обеспечения NGFW: <pre>Admin@UGOS# set settings general updates-schedule software-updates schedule advanced</pre> Расписание скачивания обновлений библиотек может быть единым: <pre>Admin@UGOS# set settings general updates-schedule libraries-updates all schedule advanced</pre> или может быть настроено отдельно для каждого элемента: <pre>Admin@UGOS# set settings general updates-schedule libraries-updates [lib-module ...] schedule advanced</pre> Время задаётся в Crontab-формате: (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". Команда для просмотра расписания обновлений: <pre>Admin@UGOS# show settings general updates-schedule</pre>

Настройка управления устройством

Настройка Radmin-emergency

Команда включения/отключения удалённого доступа к серверу для технической поддержки в случаях, когда NGFW не отвечает:

```
Admin@UGOS# set settings device-mgmt diagnostic radmin-emergency <on | off>
```

Далее необходимо указать параметры:

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

В случаях, когда произошла проблема с ядром NGFW, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации NGFW. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Настройка диагностики

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, задаются на уровне **device-mgmt diagnostic**. Текущие настройки можно просмотреть с использованием команды:

```
Admin@UGOS# show settings device-mgmt diagnostic
```

На уровне **settings device-mgmt diagnostic radmin** можно включить или отключить удалённый доступ к серверу для технической поддержки UserGate (**Radmin**). Команда включения/отключения Radmin:

```
Admin@UGOS# set settings device-mgmt diagnostic radmin <on | off>
```

Для просмотра состояния Radmin:

```
Admin@UGOS# show settings device-mgmt diagnostic radmin
```

На уровне **settings device-mgmt diagnostic details** с помощью следующей команды можно установить необходимый уровень детализации диагностики (отключено; только ошибки; ошибки и предупреждения; ошибки, предупреждения и дополнительная информация; максимум детализации):

```
Admin@UGOS# set settings device-mgmt diagnostic details <off | error | warning | info | debug>
```

Для просмотра состояния уровня детализации диагностики:

```
Admin@UGOS# show settings device-mgmt diagnostic details
```

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

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

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

```
Admin@UGOS# show settings device-mgmt updates-channel
```

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

```
Admin@UGOS# create settings device-mgmt settings-export
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек NGFW.
name	Название правила экспорта.
description	Описание правила экспорта.

Параметр	Описание
type	Выбор удалённого сервера для экспорта настроек: • ssh. • ftp.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (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".

Обновление существующего правила экспорта настроек NGFW производится с использованием следующей команды:

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

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

Команда для удаления правила экспорта настроек:

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

Команда для отображения правила экспорта настроек:

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

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием).
Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации (настроек) продукта от изменения используйте следующую команду:

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

Проверка целостности конфигурации происходит каждые несколько минут после загрузки NGFW.

- **log** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания изменений конфигурации. Требуется указания пароля, который был задан при активации режима отслеживания конфигурации.
- **block** — активирует режим отслеживания изменений конфигурации. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через NGFW.

Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего "замораживает" настройки (режим **log** или **block**). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений:

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

Настройка защиты исполняемых файлов от изменения

Чтобы настроить защиту параметры защиты исполняемого кода продукта от потенциального несанкционированного изменения:

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

Проверка целостности исполняемого кода происходит каждый раз после загрузки NGFW

- **log** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий. Требуется задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания несанкционированных изменений исполняемого кода. Требуется указания пароля, который был задан при активации режима отслеживания исполняемого кода.
- **block** — активирует режим отслеживания несанкционированных изменений исполняемого кода. Требуется задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через NGFW. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов:

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

Настройка кластеров

Version: 7.0.1
Documentation: ☒

Настройка кластера конфигурации

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

Команда обновления существующего узла кластера:

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

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера.
description	Обновить описание узла кластера.
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения настроек узла кластера:

```
Admin@UGOS# delete settings device-mgmt configuration-cluster <node-name>
Admin@UGOS# show settings device-mgmt configuration-cluster <node-name>
```

Настройка кластера отказоустойчивости

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

Для создания кластера отказоустойчивости:

```
Admin@UGOS# create settings device-mgmt ha-cluster
```

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).
master-node	Выбор Мастер-узла (будет отображён список узлов кластера, активных в данный момент).

Параметр	Описание
ha-cluster-id	Настройка синхронизации сессий в кластере: • <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. • off — отключение синхронизации пользовательских сессий.
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@UGOS# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info></pre> 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).

Для обновления настроек кластера:

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

Список параметров аналогичен списку параметров, доступных при создании кластера отказоустойчивости.

Для удаления кластера:

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

Также доступно удаление отдельных параметров:

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

Для отображения информации о всех кластерах отказоустойчивости:

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

Для отображения информации об определённом кластере:

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

Настройка управления доступом к консоли NGFW

Version: 7.0.1

Product: UserGate NGFW

Documentation: ☒

Настройка данного раздела производится на уровне **settings administrators**. В данном 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 необходимо использовать следующую команду

```
Admin@UGOS# set settings administrators general
```

Далее необходимо указать параметры, которые необходимо изменить:

Параметр	Описание
password	Изменить пароля текущего администратора.
unlock	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).
min-special-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
max-characters-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Для просмотра текущих параметров защиты учётных записей администраторов используйте команду:

```
Admin@UGOS# show settings administrators general
```

Настройка учётных записей администраторов

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

Для создания учётной записи администратора используется следующая команда:

```
Admin@UGOS# create settings administrators administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации)

и указать 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. • ldap-login: логин администратора. Структура команды при указании данного параметра: <code>Admin@UGOS# create settings administrators administrators ldap-user ... ldap-login connector <ldap-connector-name> user <domain\user> ...</code> • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее.
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. • ldap-login: логин администратора. Структура команды при указании данного параметра: <code>Admin@UGOS# create settings administrators administrators ldap-group ... ldap-login connector <ldap-connector-name> group <domain\group> ...</code> • description: описание учётной записи администратора. • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее.
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.

Следующая команда используется для обновления профиля (параметры аналогичны параметрам создания профиля администратора):

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

Для удаления учётной записи используется команда:

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

 Для отображения информации о всех учётных записях

администраторов:

Admin@UGOS# show settings administrators administrators

Для отображения информации об определённой учётной записи администратора:

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

Настройка прав доступа профилей администраторов

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

Для создания профиля администратора предназначена следующая команда:

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

Следующая команда используется для обновления профиля (параметры аналогичны параметрам создания профиля администратора):

Admin@UGOS# set settings administrators admin-profiles <profile-name>

Чтобы удалить профиль администратора:

Admin@UGOS# delete settings administrators admin-profiles <profile-name>

Для просмотра информации о всех профилях администраторов:

Admin@UGOS# show settings administrators admin-profiles

Для отображения информации об определённом профиле:

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

Настройка сессий администраторов

С использованием следующих команд возможен просмотр сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators 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@UGOS# show settings administrators 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@UGOS# show settings administrators 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@UGOS# execute terminate settings administrators sessions
```

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

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

Настройка сертификатов

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☒

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

Для импорта сертификатов предназначена команда:

```
Admin@UGOS# 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-console-cert-chain: цепочка сертификатов веб-консоли. • ssl-inspection-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • ssl-inspection-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-inspection-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 ftp-прокси. • web-console-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW. • saml: сертификат, который будет использован в SAML-клиенте. • none.

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

```
Admin@UGOS# export settings certificates <certificate | certificate-and-chain | csr> <certificate-name>
```

С использованием командной строки возможно создание сертификата и CSR:

Admin@UGOS# create settings certificates <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@UGOS# set settings certificates <certificate-name>

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: • web-console-cert-chain: цепочка сертификатов веб-консоли. • ssl-inspection-intermediate: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • ssl-inspection-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-inspection-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 ftp-прокси. • web-console-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW. • saml: сертификат, который будет использован в SAML-клиенте. • none.
user	Локальный пользователь, которому будет назначен пользовательский сертификат.

Параметр	Описание
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@UGOS# delete settings certificates <certificate-name>
```

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

```
Admin@UGOS# show settings certificates
```

```
Admin@UGOS# show settings certificates <certificate-name>
```

Чтобы удалить сертификат из кэша используется команда:

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

Настройка параметров устройства

Documentation: ☒
Version: 7.0.1
Product: UserGate NGFW

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

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

Доступно изменение следующих параметров:

Параметр	Описание
module_l7_enabled	Включение/отключение загрузки модуля L7: - on. - off По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка NGFW.
module_sip_enabled	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: - on. - off По умолчанию модуль выгружен. Важно! После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (кнопка Принудительно применить в разделе Политики сети → Межсетевой экран).
module_h323_enabled	Включение/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.
module_idps_enabled	Включение/отключение загрузки модуля IDPS: - on. - off По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка NGFW.
module_sunrpc_enabled	Включение/отключение загрузки модуля SunRPC: - on. - off По умолчанию модуль выгружен.
module_ftp_alg_enabled	Включение/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.

Параметр	Описание
ha_auth_type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • ah — включение подписи. • pass — отключение проверки.
fw_drop_invalid	Включение/отключение блокировки пакетов с невалидным 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/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • on. • off По умолчанию настройка выключена.
decrypt_bypass_optimization	Включение/отключение оптимизации инспектирования SSL: • on. • off По умолчанию настройка выключена.

Для просмотра текущих настроек используйте команду:

Admin@UGOS# show settings device

или

Admin@UGOS# show settings device <setting-name>

Настройка телеметрии

Version: 7.0.1

Product: UserGate NGFW

Documentation: 

Набор команд для просмотра и настройки режима работы телеметрии доступны на уровне **settings telemetry**. Телеметрия позволяет отправлять разработчику анонимную статистику, такую как популярность веб-сайтов, веб-сайты с неизвестной категорией, вирусные атаки, события COB, активность малваре. Данные телеметрии имеют вид обезличенных данных и не содержат персональную информацию.

Для включения/отключения телеметрии используйте команду:

```
Admin@UGOS# set settings telemetry enabled <on | off>
```

По умолчанию отправка телеметрии включена.

Для просмотра текущего режима:

```
Admin@UGOS# show settings telemetry
```

Настройка прокси-сервера

Version: 7.0.1

Product: UserGate 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@UGOS# set settings proxy <setting-name>
```

Для изменения доступны следующие параметры:

Параметр	Описание
add_via_enabled	Добавление HTTP заголовков Via: • on. • off. По умолчанию отключено.
add_forwarded_enabled	Добавление HTTP заголовков Forwarded: • on. • off. По умолчанию отключено.
add_xforwarded_enabled	Добавление HTTP заголовков X-Forwarded-For: • on. • off. По умолчанию отключено.
http_connection_timeout	Время ожидания, выделяемое на подключение HTTP. По умолчанию — 20 секунд.
http_loading_timeout	Время ожидания, выделяемое на загрузку контента HTTP. По умолчанию — 60 секунд.
proxy_host_rfc	Доступно: • relaxed — использование протокола HTTP PROXY 1.1 без указания параметра <code>host</code>. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • strict — соблюдать RFC. Данный режим используется по умолчанию.
fmode_enabled	Режим ускорения загрузки контента: • on. • off. Режим может быть несовместим с работой некоторых сайтов; по умолчанию отключен.
smode_enabled	Режим SYN Proxy: • on. • off. По умолчанию режим включен.
icap_wait_timeout	Время, которое NGFW 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 , NGFW отправит данные пользователю без модификации, если же действие правила Переслать , NGFW не отдаст данные пользователю. Значение по умолчанию — 10 секунд.

Для просмотра текущих настроек используйте команду:

```
Admin@UGOS# show settings proxy
```

или

```
Admin@UGOS# show settings proxy <setting-name>
```

Настройка параметров устройства

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☒

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

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

Доступно изменение следующих параметров:

Параметр	Описание
module_l7_enabled	Включение/отключение загрузки модуля L7: - on. - off По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка NGFW.
module_sip_enabled	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: - on. - off По умолчанию модуль выгружен.
module_h323_enabled	Включение/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.
module_idps_enabled	Включение/отключение загрузки модуля IDPS: - on. - off По умолчанию модуль загружен. Важно! После изменения данного параметра требуется перезагрузка NGFW.
module_sunrpc_enabled	Включение/отключение загрузки модуля SunRPC: - on. - off По умолчанию модуль выгружен.
module_ftp_alg_enabled	Включение/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.

Параметр	Описание
ha_auth_type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • ah - включение подписи. • pass - отключение проверки.
fw_drop_invalid	Включение/отключение блокировки пакетов с невалидным 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/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • on. • off По умолчанию настройка выключена.
decrypt_bypass_optimization	Включение/отключение оптимизации инспектирования SSL: • on. • off По умолчанию настройка выключена.

Для просмотра текущих настроек используйте команду:

Admin@UGOS# show settings device

или

Admin@UGOS# show settings device <setting-name>

Зоны

Documentation: ☒
Version: 7.0.1
Product: UserGate NGFW

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

Admin@UGOS# 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 NGFW 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 NGFW отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.

Параметр	Описание
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 NGFW отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса NGFW. • SNMP: доступ к NGFW 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 NGFW в кластер (TCP 4369, TCP 9000-9100). • VRRP: сервис, необходимый для объединения нескольких узлов NGFW в отказоустойчивый кластер (IP протокол 112). • "Admin Console": доступ к веб-консоли управления (TCP 8001). • DNS: доступ к сервису DNS-прокси (TCP 53, UDP 53). • "HTTP Proxy": доступ к сервису HTTP(S)-прокси (TCP 8090). • "Authorization agent": доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • "SMTP Proxy": сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "POP3 Proxy": сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • "PROXY PORTAL": сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • "SAML SERVER": выбор SAML-сервера в списке сервисов зоны и общих настройках NGFW. • "Log Analyzer": сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный узел в качестве LogAn (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 NGFW. • "Dynamic routing RIP": сервис динамической маршрутизации RIP.

Параметр	Описание
service-addresses	Указание разрешённых IP-адресов для сервисов: • service: выбор сервисов (список соответствует enabled-services). • allowed-addresses: разрешённые IP-адреса (задаются в формате IP/mask).
antispoof-enabled	Включение/отключение защиты от IP-спуфинга: • on. • off.
ip-spoofing-networks	Указание IP-адресов источников, допустимых в данной зоне; адреса указываются в формате <ip> или <ip/mask>. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены.
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.

Для обновления параметров зоны:

```
Admin@UGOS# set network zone <zone-name>
```

Для добавления новых сервисов к списку сервисов, разрешённым ранее используйте команду:

```
Admin@UGOS# set network zone <zone-name> ... enabled-services + [ <service-name> ... ] ...
```

Команда удаления зоны или её параметров:

```
Admin@UGOS# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.

Параметр	Описание
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • response-pages: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • rpc: XML-RPC для управления — позволяет управлять продуктом по API (TCP 4040). • ha: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • VRRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "Admin Console": доступ к веб-консоли управления (TCP 8001). • DNS: доступ к сервису DNS-прокси (TCP 53, UDP 53). • "HTTP Proxy": доступ к сервису HTTP(S)-прокси (TCP 8090). • "Authorization agent": доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • "SMTP Proxy": сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "POP3 Proxy": сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • "REVERSE PROXY": сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • "PROXY PORTAL": сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • "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 узел 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 NGFW. • "Dynamic routing RIP": сервис динамической маршрутизации RIP.
service-addresses	Разрешённые IP-адреса для сервисов: • service: выбор сервисов (список соответствует enabled-services). • allowed-addresses: разрешённые IP-адреса (задаются в формате IP/mask).
ip-spoofing-networks	При использовании защиты от IP-спуфинга администратор может указать IP-адреса источников, допустимых в данной зоне; адреса указываются в формате <ip> или <ip/mask>. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены.

Следующая команда отобразит настройки зоны:

```
Admin@UGOS# show network zone <zone-name>
```

Интерфейсы

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☒

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

Admin@UGOS> show network interface-mapping

Admin@UGOS# show network interface-mapping

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

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

Admin@UGOS> clear network interface-mapping

Admin@UGOS# delete network interface-mapping

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

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

Настройка adapter

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

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера:

Admin@UGOS# set network interface adapter

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: - on. - off.
description	Описание 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).
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: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_pvlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# set network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей читайте в разделе Настройка профилей LLDP .
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 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.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • enabled: включение/отключения релея: ◦ on. ◦ off. • utm-address: IP-адрес интерфейса NGFW, на который добавляется функция релея (принимает значения <ip none>). • server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

```
Admin@UGOS# delete network interface adapter <adapter-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.

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

Команда для отображения информации о всех сетевых адаптерах:

Admin@UGOS# show network interface adapter

Для отображения информации об адаптере:

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

Настройка VLAN

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

Команда для добавления нового VLAN-интерфейса:

Admin@UGOS# create network interface vlan

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • on. • off.
description	Описание 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).
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.

Параметр	Описание
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
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 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.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • enabled: включение/отключения релея: ◦ on. ◦ off. • utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея. • server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего VLAN:

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

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

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@UGOS# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

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

Чтобы отобразить информацию о всех интерфейсах VLAN:

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

или об определённом интерфейсе:

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

Настройка bond-интерфейса

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

Команда для создания бонд-интерфейса:

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

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • on. • off.
description	Описание интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# create network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
	Дополнительные параметры бонд-интерфейса: • aggr-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

Параметр	сетевая карта берет себе MAC-адрес вышедшей из строя карты).
bonding	Описание • 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 дойти 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 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 размер MTU.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • enabled: включение/отключения релея: ◦ on. ◦ off. • utm-address: IP-адрес интерфейса NGFW, на который добавляется функция релея. • server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего бонд-интерфейса:

Admin@UGOS# set network interface bond <bond-name>

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

Команда удаления бонд-интерфейса или его параметров:

Admin@UGOS# 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, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

Admin@UGOS# show network interface bond

или об определённом интерфейсе:

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

Настройка bridge-интерфейса

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

Чтобы добавить новый bridge-интерфейс:

Admin@UGOS# create network interface bridge

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: • on. • off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).
description	Описание bridge-интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.

Параметр	Описание
link-info	Настройка параметров сетевого интерфейса: • bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# create network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
bridging	Дополнительные параметры моста: • 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 использования STP (Spanning Tree Protocol) для защиты от петель: ◦ on. ◦ off. • forward-delay: задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP (указывается в секундах). • max-age: время, по истечении которого STP-соединение считается потерянным (указывается в секундах). • bypass-pair: пара интерфейсов, которая будет использована для построения байпас моста. Требуется поддержка оборудования ПАК NGFW.
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 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.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • enabled: включение/отключения релея: ◦ on. ◦ off. • utm-address: IP-адрес интерфейса NGFW, на который добавляется функция релея. • server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего bridge-интерфейса:

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

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

Команда удаления bridge-интерфейса или его параметров:

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

Параметры, доступные для удаления:

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

Чтобы отобразить информацию о всех bridge-интерфейсах:

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

или об определённом интерфейсе:

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

Настройка PPPoE

Настройка интерфейса PPPoE производится на уровне **network interface PPPoE**.

Для создания интерфейса PPPoE:

```
Admin@UGOS# network interface PPPoE
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса PPPoE: • on. • off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет ppp1).
description	Описание интерфейса PPPoE.
node-name	Имя узла кластера, на котором создаётся 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_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# create network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
pppoe-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: ◦ on. ◦ off. • 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: ◦ on. ◦ off. • lcp-echo-interval: интервал проверки соединения. • lcp-echo-failure: количество неуспешных проверок соединения, после которого UserGate считает, что соединение отсутствует и разрывает его. • providers-dns: использование DNS-серверов, выданных провайдером: ◦ on. ◦ off. • 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.

Обновление существующего интерфейса PPPoE:

```
Admin@UGOS# set network interface PPPoE <PPPoE-name>
```

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

Команда удаления интерфейса PPPoE:

```
Admin@UGOS# delete network interface PPPoE <PPPoE-name>
```

Чтобы отобразить информацию о всех интерфейсах PPPoE:

```
Admin@UGOS# show network interface PPPoE
```

или об определённом интерфейсе:

```
Admin@UGOS# show network interface PPPoE <PPPoE-name>
```

Настройка VPN-адаптера

VPN-адаптеры настраиваются на уровне **network interface vpn**.

Чтобы создать VPN-адаптер:

```
Admin@UGOS# network interface vpn
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VPN-интерфейса: - on. - off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет tunnel1).
description	Описание VPN-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_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# create network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow .
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN), то необходимо использовать статический IP-адрес. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. Для использования интерфейса, используемого в роли клиента, необходимо выбрать динамический режим.

Параметр	Описание
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.
mtu	Указание размера MTU для выбранного интерфейса.

Обновление существующего интерфейса VPN:

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

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

Команда для удаления интерфейса VPN или его параметров:

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

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех интерфейсах VPN:

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

или об определённом интерфейсе:

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

Настройка туннелей

Создание и настройка туннелей производится на уровне **network interface tunnel**.

Для создания туннелей используется команда:

```
Admin@UGOS# network interface tunnel
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение туннеля: • on. • off.
interface-name	Необходимо ввести номер, который будет отображён в названии туннеля (например 1, тогда название созданного интерфейса будет gre1).
description	Описание туннеля.
node-name	Узел кластера, на котором будет создан туннель.
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_vlan: механизм Proxy ARP. Параметр proxy_arp — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: <pre>Admin@UGOS# create network interface <iface-type> ... link-info [key/value]</pre> где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
mtu	Размер MTU для выбранного интерфейса.
tunnel-config	Дополнительные параметры интерфейса: • local-ip: локальный адрес Point-to-Point интерфейса. • remote-ip: удалённый 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). • vni: идентификатор VXLAN. Только для типа туннеля VXLAN.
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. 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.

Обновление существующего туннеля:

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

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

Команда для удаления интерфейса туннель или его параметров:

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

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех туннелях:

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

или об определённом интерфейсе:

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

Шлюзы

Version: 7.0.1

Product: UserGate NGFW

Documentation: 

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

```
Admin@UGOS# create network gateway
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • on. • off.
name	Название шлюза.
description	Описание шлюза.
node-name	Имя узла кластера, на котором создаётся шлюз.
interface	Интерфейс, использующийся для выхода в Интернет.
virtual-router	Выбор виртуального маршрутизатора, для которого настраивается шлюз.
ip	IP-адрес шлюза.
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@UGOS# set network gateway <gateway-name>
```

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза, кроме **node-name** (изменение значения данного параметра недоступно).

Команда для удаления шлюза:

```
Admin@UGOS# delete network gateway <gateway-name>
```

Чтобы отобразить информацию о всех шлюзах:

```
Admin@UGOS# show network gateway
```

или об определённом шлюзе:

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

DHCP

Version: 7.0.1

Product: UserGate NGFW

Documentation: ☒

Раздел находится на уровне **network dhcp**.

Для создания подсети DHCP, используется команда:

```
Admin@UGOS# 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.
node-name	Выбор узла кластера, на котором создается данный диапазон.
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-address	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@UGOS# set network dhcp <dhcp-name>
```

Параметры, информацию о которых можно обновить, аналогичны параметрам, доступным при создании, кроме параметров **node-name**, **interface** - изменение значений данных параметров недоступно.

Для удаления подсети:

```
Admin@UGOS# 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@UGOS# show network dhcp
```

или об определённой подсети DHCP:

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

DNS-настройки

Version: 7.0.1

Product: UserGate 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@UGOS# set network dns system-dns-servers + [ <ip> <ip> ... ] Admin@UGOS# set network dns system-dns-servers [ <ip> <ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin@UGOS# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin@UGOS# delete network dns system-dns-servers [ <ip> <ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin@UGOS# show network dns system-dns-servers
```

Настройка DNS-прокси

DNS-прокси настраивается на уровне **network dns proxy-settings**.

Для обновления настроек DNS-прокси используется следующая команда:

```
Admin@UGOS# 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.

Параметр	Описание
retries	Количество попыток DNS-запроса.
factory-defaults	Сброс до заводских настроек значения выбранного параметра (параметры представлены в данной таблице) или всех параметров (all).

Чтобы просмотреть настройки DNS-прокси:

```
Admin@UGOS# show network dns proxy-settings
```

Параметры, значения которых можно просмотреть, представлены в таблице выше.

Настройка правил DNS

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

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".
dns_server	Список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены. Для указания сервера: dns_server(1.2.3.4).

Настройка статистических записей DNS-прокси

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

Для добавления статической DNS-записи предназначена команда:

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

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статической записи: - on. - off.

Параметр	Описание
name	Название записи.
description	Описание DNS-записи.
domain	FQDN (Fully Qualified Name) статической записи, например, www.example.com .
static-dns-ips	Список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN.

Для обновления информации о статических DNS-записях:

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

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

Для удаления статической записи:

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

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

Команда

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

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

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

Настройка виртуальных маршрутизаторов

Technology: Routing

Version: 7.0.1

Product: UserGate 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@UGOS# create network virtual-router
```

Далее указываются параметры:

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора.
description	Описание виртуального маршрутизатора
node	Выбор узла NGFW, на котором будет создан виртуальный маршрутизатор (при наличии кластера).
interface	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.
route	Добавление маршрутов, которые будут применены к трафику в данном виртуальном маршрутизаторе. Подробнее читайте в разделе Настройка статических маршрутов .
ospf	Добавление динамических маршрутов, получаемых по протоколу маршрутизации OSPF. Подробнее читайте в разделе Настройка OSPF .
bgp	Добавление динамических маршрутов, получаемых по протоколу маршрутизации BGP. Подробнее смотрите в разделе Настройка BGP .
rip	Добавление динамических маршрутов, получаемых по протоколу маршрутизации RIP. Подробнее читайте в разделе Настройка RIP .
mcast-router	Настройка мультикастинга в данном виртуальном маршрутизаторе. Подробнее о настройке мультикастинга использованием интерфейса командной строки смотрите в разделе Настройка мультикаст-маршрутизации .

Следующая команда предназначена для изменения параметров виртуального маршрутизатора:

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

Параметры, доступные для обновления, аналогичны параметрам команды **create**, кроме:

- **name**.
- **node-name**.

Чтобы удалить виртуальный маршрутизатор используется команда:

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

Команда для отображения информации о виртуальном маршрутизаторе:

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

Настройка статических маршрутов

Для добавления нового статического маршрута используется команда:

```
Admin@UGOS# set network virtual-router <virtual-router-name> route 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-address	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с NGFW.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем приоритетней маршрут

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@UGOS# set network virtual-router <virtual-router-name> route <static-route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

```
Admin@UGOS# delete network virtual-router <virtual-router-name> route <static-route-name>
```

Для отображения статических маршрутов:

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

Настройка OSPF

Для настройки OSPF с использованием CLI используйте следующую команду:

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

Далее необходимо указать параметры OSPF-маршрутизатора:

Параметр	Описание
enabled	Включение/отключение OSPF-маршрутизатора: - on. - off.

Параметр	Описание
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 NGFW, относящимся к данному виртуальному маршрутизатору). При выключении OSPF (enabled off) значение router-id может быть удалено (none).
connected	Распространение другим роутерам OSPF маршрутов в непосредственно подключённые к NGFW сети: • on. • off.
kernel	Распространение другим роутерам OSPF маршрутов, которые были добавлены администратором: • on. • off.
metric	Метрика распространяемых маршрутов.
default-originate	Оповещение других маршрутизаторов о том, что у данного роутера настроен маршрут по умолчанию: • on. • off.
interface	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@UGOS# set network virtual-router <virtual-router-name> ospf interface new Admin@UGOS# set network virtual-router <virtual-router-name> ospf interface <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. • 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. • 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-key-id — идентификатор ключа. • key — ключ. Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.

Параметр	Описание
area	Настройка области OSPF. Для добавления новой области или изменения параметров созданной ранее области используются следующие команды: <pre>Admin@UGOS# set network virtual-router <virtual-router-name> ospf area new Admin@UGOS# set network virtual-router <virtual-router-name> ospf area <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 авторизации. Доступны следующие значения: • none — не требовать авторизацию 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. Идентификация на уровне интерфейсов имеет приоритет над авторизацией 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. • interface: 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.

Для удаления настроек OSPF используется команда:

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

Параметры, доступные для удаления:

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

Следующая команда используется для отображения конфигурации OSPF в виртуальном маршрутизаторе:

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

Настройка BGP

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

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

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение BGP-маршрутизатора: • on. • off.
router-id	IP-адрес маршрутизатора. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору. При выключении BGP (enabled off) значение router-id может быть удалено (none).
as-number	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/отключение балансировки трафика на маршруты с одинаковой стоимостью: • on. • off.
connected	Распространение другим роутерам BGP маршрутов в непосредственно подключённые к NGFW сети: • on. • off.
kernel	Распространение другим роутерам BGP маршрутов, которые были добавлены администратором: • on. • off.
ospf-redistribute	Распространение другим роутерам BGP маршрутов, полученных по протоколу OSPF: • on. • off.
network-addr	Список сетей, относящихся к данной автономной системе. Необходимо указать в формате <ip/mask>.

Параметр	Описание
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@UGOS# set network virtual-router <virtual-router-name> bgp routemaps new Admin@UGOS# 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. • match-by — условие применения routemap. Сравнивать по: ◦ ip — сравнение по IP-адресу. ◦ aspath — сравнение по AS пути. ◦ community — сравнение по Community. • 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. • 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 (<u> </u>), 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@UGOS# set network virtual-router <virtual-router-name> bgp filters new Admin@UGOS# 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. • filter-by — условия применения фильтра. Доступно: ◦ ip — фильтровать по IP-адресу. ◦ aspath — фильтровать по AS пути. • 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.

Параметр	Описание
neighbors	BGP-соседи. Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды: <pre>Admin@UGOS# set network virtual-router <virtual-router-name> bgp neighbors new Admin@UGOS# 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 — эта функция позволяет получать и обрабатывать маршруты, даже если маршрутизатор обнаруживает собственный номер автономной системы в AS Path в маршруте агрегации. ◦ on. ◦ off. • allows-in-number — количество раз, которое в AS Path может содержаться номер автономной системы BGP-соседа. Возможны значения от 0 до 10 (0 — origin) • 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-соседям: ◦ 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. • routemap-in — ограничение маршрутизирующей информации, которую BGP получает от соседей.

	• route-map-out — ограничение маршрутизирующей информации, которую BGP отдает соседям.
Параметр	Описание
Команда, используемая для удаления параметров BGP-маршрутизатора:	

Admin@UGOS# delete network virtual-router <virtual-router-name> bgp

Для удаления доступны следующие параметры:

- Адреса сетей, относящихся к данной автономной системе: **network-addr**s.
- Условия применения route-map: **route-maps <route-map-name> ip-match | community-match | as-path-match** .
- Условия применения фильтра: **filters <filter-name> ip-filter | as-path-filter** .
- Фильтры BGP-соседей и route-maps: **neighbors <host-ip> filter-in | filter-out | route-map-in | route-map-out** .

Следующая команда используется для отображения конфигурации BGP в виртуальном маршрутизаторе:

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

Настройка RIP

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

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

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: • on. • off.
rip-version	Версия протокола RIP: • 1. • 2. Как правило, используется 2-я версия протокола.
default-metric	Метрика RIP. По умолчанию метрика равна 1; максимальное значение — 15. Значение 16 считается бесконечным.
admin-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).
default-originate	Отправлять себя в качестве маршрута по умолчанию.
network-cidr	Указание сети в виде CIDR. Указывается в формате <ip/mask>.
network-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 NGFW 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-redistribute — распространение другим RIP-роутерам маршрутов, полученных по OSPF: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off. • bgp-redistribute — распространение другим RIP-роутерам маршрутов, полученных по BGP: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ off.

Параметр	Описание
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 отправляться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информацией по протоколу RIP, должны иметь одинаковый пароль. • split-horizon — метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который прибыло обновление. ◦ on. ◦ off. • poison-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, используемая для удаления параметров RIP-маршрутизатора:

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

Для удаления доступны следующие параметры:

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

Следующая команда используется для отображения конфигурации RIP в виртуальном маршрутизаторе:

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

Настройка мультикаст-маршрутизации

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

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

Далее указываются параметры:

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

Параметр	Описание
enabled	Включение/отключение мультикаст-маршрутизации: • on. • off.
use-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).
use-ecmp-rebalance	Использование ECMP rebalance: • on — если один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). • off — если один из интерфейсов, через который отсылался трафик, отключился, то перераспределяются только те потоки, которые передавались через отключенный интерфейс.
join-prune	Интервал отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.
register-suppress	Интервал, после которого маршрутизатор отправляет сообщение register suppress.
keep-alive	Интервал, через который маршрутизатор будет посылать сообщения keeralive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.
interfaces	Интерфейс, который будет использоваться для работы мультикаста; для указания доступны только интерфейсы, добавленные в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: <pre>Admin@UGOS# set network virtual-router <virtual-router-name> multicast-router interfaces new Admin@UGOS# set network virtual-router <virtual-router-name> multicast-router interfaces <interface-name></pre> 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. • 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.

Параметр	Описание
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.

Следующая команда предназначена для удаления параметров мультикаст-маршрутизатора:

```
Admin@UGOS# 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**.

Для отображения конфигурации мультикастинга в виртуальном маршрутизаторе используйте следующую команду:

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

Настройка WCCP

Version: 7.0.1

Product: UserGate NGFW

Documentation: ☒

Настройка WCCP производится на уровне **network wccp**. Для создания сервисной группы WCCP используется следующая команда:

```
Admin@UGOS# create network wccp
```

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 NGFW в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
fwd-type	Способ перенаправления трафика с серверов WCCP на NGFW: • l2 — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес NGFW. • gre — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
ret-type	Способ перенаправления трафика с NGFW на серверы WCCP: • l2 — используя перенаправление L2. В этом случае NGFW (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 NGFW 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-to-redirect	Порты для перенаправления (порты назначения трафика). При необходимости указываются несколько портов в формате: ports-to-redirect + [80 442] . Важно! NGFW может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на NGFW с другими портами, будет отправляться в интернет без фильтрации.
ports-source	Перенаправление трафика на основании значений портов источника: • on. • off.

Параметр	Описание
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. • wccp-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. • wccp-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@UGOS# set network wccp <service-group-name>
```

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

С использованием следующей команды доступно удаление сервисной группы полностью или некоторых её параметров:

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

Параметры, доступные для удаления:

- **routers-lists.**
- **routers-ips.**
- **ports-to-redirect.**

Следующая команда предназначена для просмотра информации о сервисной группе WCCP:

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

Настройка правил с использованием UPL

Настройка правил с использованием UPL (Описание)

Documentation: ☒

Product: NGFW

Version: 7.0.1

UPL — UserGate Policy Language — язык описания политик (конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента) UserGate.

Правила настраиваются с использованием действий, условий и свойств.

Для каждого правила настраивается одно из действий. Действия — настройки, которые управляют обработкой транзакции (**OK**, **WARNING**, **PASS**, **DENY**). При настройке правил, в которых не предусмотрено указание действия (например, правила DNS, NAT и маршрутизации, пропускной способности и т.п.), необходимо указать действия **PASS** или **OK**.

Условия задаются знаками равно (=) или не равно (!=), например, зоны, адреса, GeoIP источников и назначения, сервисы, приложения и т.д.; все условия в правиле проверяются по логическому И, т.е. правило сработает, если будут выполнены все условия.

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

Примечание При настройке правил сначала указывается действие, потом условия и затем свойства.

UPL используется для настройки правил в следующих разделах:

- Настройки DNS-прокси (уровень: **network dns dns-proxy dns-rules**).
- Captive-портал (уровень: **users captive-portal**).
- Межсетевой экран (уровень: **network-policy firewall**).
- NAT и маршрутизация (уровень: **network-policy nat-routing**).
- Пропускная способность (уровень: **network-policy traffic-shaping**).
- Фильтрация контента (уровень: **security-policy content-filtering**).
- Веб-безопасность (уровень: **security-policy web-browsing**).
- Инспектирование туннелей (уровень: **security-policy tunnel-inspection**).
- Инспектирование SSL (уровень: **security-policy ssl-inspection**).
- Инспектирование SSH (уровень: **security-policy ssh-inspection**).
- COV (уровень: **security-policy intrusion-prevention**).
- Защита почтового трафика (уровень: **security-policy mail-security**).
- ICAP-правила (уровень: **security-policy icap-rules**).
- Правила защиты DoS (уровень: **security-policy dos-rules**).
- Веб-портал (уровень: **global-portal web-portal**).
- Правила reverse-прокси (уровень: **global-portal reverse-proxy-rules**).
- Серверные правила (уровень: **vpn server-rules**).
- Клиентские правила (уровень: **vpn client-rules**).

Структура команды для создания правила:

```
Admin@UGOS# create <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо создать правило.

<position> — позиция, на которую будет помещено правило.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для обновления существующего правила:

```
Admin@UGOS# set <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо обновить правило.

<position> — номер правила, которое необходимо обновить.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для удаления правила:

```
Admin@UGOS# delete <level> <position | all>
```

где <level> — уровень, на котором необходимо удалить правило.

<position> — номер правила, которое необходимо удалить.

<all> — удалить все правила.

Структура команды для отображения правила:

```
Admin@UGOS# show <level> <position | all>
```

где <level> — раздел, правила которого нужно отобразить.

<position> — номер правила, которое необходимо отобразить.

<all> — отобразить все правила.

В качестве примера рассмотрим создание правила межсетевого экрана (использован многострочный ввод):

```
Admin@UGOS# create network-policy firewall 1 upl-rule \  
...DENY \  
...src.zone = Trusted \  
...dst.zone = Untrusted \  
...user = known \  
...service = HTTPS \  
...time = lib.time("Working hours") \  
...rule_log(session)\   
...name("Example of firewall rule created in CLI") \  
...enabled(true)
```

После создания правило отобразится в начале списка правил межсетевого экрана (на позиции 1). Данное правило запрещает HTTPS-трафик из зоны Trusted в зону Untrusted пользователям, идентифицированным системой; правило работает в соответствии с расписанием Working hours. При срабатывании правила в журнал будет записана информация о начале сессии.

Настройка раздела Пользователи и устройства

Настройка групп пользователей

Documentation: ☒

Version: 7.0.1

Product: UserGate NGFW

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

Для добавления новой группы пользователей используется команда:

```
Admin@UGOS# create users group
```

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

```
Admin@UGOS# set users group <group-name>
```

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

```
Admin@UGOS# delete users group <group-name>
```

Для удаления локальных пользователей:

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

Для удаления пользователей LDAP:

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

Для отображения настроек группы используется следующая команда:

```
Admin@UGOS# show users group <group-name>
```

Настройки пользователей

Version: 7.0.1

Product: UserGate NGFW

Documentation: 

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

Команда для добавления пользователей:

```
Admin@UGOS# create users user
```

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.
static-addresses	Указываются: • 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>.
emails	Почтовые адреса пользователя.
phones	Номера телефонов пользователя.

Для обновления параметров учётной записи пользователя:

```
Admin@UGOS# set users user <user-name>
```

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

Для удаления учётной записи пользователя используется следующая команда:

```
Admin@UGOS# 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**.

Команда для просмотра учётной записи пользователя:

```
Admin@UGOS# show users user <user-name>
```

Настройка серверов аутентификации

Version: 7.0.1

Product: UserGate NGFW

Documentation: 

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

Для сброса авторизации пользователя по IP-адресу используется команда:

```
Admin@UGOS# set settings userssession terminate <ip>
```

Настройка LDAP-коннектора

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

Для создания LDAP-коннектора используется команда:

```
Admin@UGOS# create users auth-servers ldap
```

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.
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.

Команда для обновления информации о существующем LDAP-коннекторе имеет следующую структуру:

```
Admin@UGOS# set users auth-servers ldap <ldap-server-name>
```

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

Для удаления LDAP-коннектора используется команда:

```
Admin@UGOS# delete users auth-servers ldap <ldap-server-name>
```

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

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

Структура команды для отображения информации о LDAP-коннекторе:

```
Admin@UGOS# show users auth-servers ldap <ldap-server-name>
```

Настройка RADIUS-сервера

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

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
Admin@UGOS# create users auth-servers radius
```

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

Следующая команда используется для обновления информации о сервере RADIUS:

```
Admin@UGOS# set users auth-servers radius <radius-server-name>
```

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

Для удаления сервера:

```
Admin@UGOS# delete users auth-servers radius <radius-server-name>
```

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

- **addresses.**

Структура команды для отображения информации о RADIUS-сервере:

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

Настройка сервера TACACS+

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

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

```
Admin@UGOS# create users auth-servers tacacs
```

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+.

Параметр	Описание
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Следующая команда используется для обновления информации о сервере TACACS+:

Admin@UGOS# set users auth-servers tacacs <tacacs-server-name>

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

Для удаления сервера:

Admin@UGOS# delete users auth-servers tacacs <tacacs-server-name>

Структура команды для отображения информации о сервере TACACS+:

Admin@UGOS# show users auth-servers tacacs <tacacs-server-name>

Настройка сервера NTLM

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

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

Admin@UGOS# create users auth-servers ntlm

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
win-domain	Имя домена Windows.

Следующая команда используется для обновления информации о NTLM-сервере:

Admin@UGOS# set users auth-servers ntlm <ntlm-server-name>

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

Для удаления сервера:

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

Структура команды для отображения информации о сервере NTLM:

Admin@UGOS# show users auth-servers ntlm <ntlm-server-name>

Настройка сервера SAML IDP

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

Для создания сервера аутентификации SAML IDP используется следующая команда:

Admin@UGOS# create users auth-servers saml-idp

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.

Параметр	Описание
metadata-url	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-url	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-url	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.

Следующая команда используется для обновления информации о сервере SAML IDP:

```
Admin@UGOS# set users auth-servers saml-idp <saml-idp-server-name>
```

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

Для удаления сервера:

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

Структура команды для отображения информации о сервере SAML IDP:

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

Настройка профилей аутентификации

Version: 7.0.1

Product: UserGate NGFW

Documentation: ☒

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

Для создания профиля аутентификации используется следующая команда:

```
Admin@UGOS# create users auth-profile
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
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-method	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.

Следующая команда предназначена для обновления настроек профилей аутентификации:

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

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

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@UGOS# 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@UGOS# delete users auth-profile <auth-profile-name> auth-method

Captive-портал

Product: UserGate NGFW
Version: 7.0.1
Documentation: ☒

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

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.

Параметр	Описание
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.

Настройка Captive-профилей

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☒

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

Для создания Captive-профиля необходимо использовать следующую команду:

Admin@UGOS# create users captive-profiles

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 авторизация; 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.

Параметр	Описание
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: уууу-мм-ддThh: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.

Для обновления профиля необходимо использовать следующую команду:

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

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

Для удаления профиля используется команда:

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

Команда для отображения настроек captive-профиля:

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

Настройка терминальных серверов

Version: 7.0.1

Product: UserGate NGFW

Documentation: ☒

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@UGOS# create users terminal-servers
```

Далее необходимо указать следующие параметры:

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

Следующая команда предназначена для обновления параметров (параметры приведены выше в таблице) терминального сервера:

```
Admin@UGOS# set users terminal-servers <terminal-server-name>
```

Команда удаления терминального сервера:

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

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

```
Admin@UGOS# delete users terminal-servers <terminal-server-name> host
```

Для отображения информации о терминальном сервере необходимо использовать команду:

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

Настройка профилей MFA (мультифакторной аутентификации)

Version: 7.0.1
Product: UserGate NGFW
Documentation: 

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.

Команда для удаления профиля мультифакторной аутентификации:

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

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

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

Настройка MFA через TOTP

В зависимости от выбранного способа получения первоначального кода для инициализации TOTP (на странице Captive-портала, по email, по SMS) будет доступен разный список параметров, которые необходимо указать. Получение возможно:

- по email:

```
Admin@UGOS# create users mfa-profiles mfa-totp smtp
```
- по SMS:

```
Admin@UGOS# create users mfa-profiles mfa-totp smpp
```
- отображение на странице Captive-портала после первой успешной авторизации:

```
Admin@UGOS# create users mfa-profiles mfa-totp key-on-captiveportal
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
totp-qr-code	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.
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 ("").

Для обновления параметров используется следующая команда:

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

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

Настройка MFA через email

Команда для добавления нового профиля мультифакторной аутентификации через email:

```
Admin@UGOS# create users mfa-profiles mfa-email smtp <smtp-profile>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
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.

Для обновления параметров используется следующая команда:

```
Admin@UGOS# set users mfa-profiles mfa-email <mfa-email-profile>
```

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

Настройка MFA через SMS

Команда для добавления нового профиля мультифакторной аутентификации через SMS:

```
Admin@UGOS# create users mfa-profiles mfa-sms smpp <smpp-profile>
```

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 будет заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Для обновления параметров используется следующая команда:

```
Admin@UGOS# set users mfa-profiles mfa-sms <mfa-sms-profile>
```

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

Настройка применения политик к пользователям

Version: 7.0.1

Product: NGFW

Documentation: 

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@UGOS# execute terminate usersession <IP-address>
```

Для очистки кэша используется команда:

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

Настройка раздела Политики сети

Настройка правил межсетевого экрана

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

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").
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 указание сервиса, использующего протокол TCP (подробнее о добавлении и настройке сервисов читайте в разделе ов). - 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.

Параметр	Описание
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.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 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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> 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.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.
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.

Настройка правил NAT и маршрутизации

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка правил NAT и маршрутизации происходит на уровне **network-policy nat-routing**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Настройка правил типа NAT

При настройке правил типа NAT, необходимо указать следующие параметры:

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 NAT. Например: name("NAT rule example") .
desc	Описание правила. Например: desc("NAT rule example set via CLI") .
nat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", 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, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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 . Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: src.ip = 02:00:00:00:00:00 .
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, 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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
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.

Настройка правил типа DNAT

При настройке правил типа **DNAT** необходимо указать следующие параметры.

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 DNAT. Например: name("DNAT rule example").
desc	Описание правила. Чтобы указать описание правила используется: desc("DNAT rule example created via CLI").
dnat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", 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. Чтобы указать зону источника трафика, например Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.

Параметр	Описание
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 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. 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 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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
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.
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1").
target_snat	Изменение IP-адреса источника на адрес NGFW: • target_snat(yes) или target_snat(true). • target_snat(no) или target_snat(false).

Настройка правил типа Порт-форвардинг

При настройке правил типа **Порт-форвардинг** необходимо указать:

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).

Параметр	Описание
name	Название правила Порт-форвардинга. Например: name("Port forwarding rule example") .
desc	Описание правила. Чтобы указать описание правила используется: desc("Port forwarding rule example created via CLI") .
port_mapping	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", 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 читайте 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 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 . 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 ISO 3166-1 . Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов, MAC-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 . Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00 .
port_map	Переопределение портов публикуемых сервисов: Для переопределения необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новые порты назначения. Например, port_map(tcp, 2000, 2100) . Важно! Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100.
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1") .

Параметр	Описание
target_snat	Изменение IP-адреса источника на адрес NGFW: • target_snat(yes) или target_snat(true). • target_snat(no) или target_snat(false).

Настройка правил типа **Policy-based routing**

Для настройки правил типа **Policy-based routing** нужно указать:

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 типа Policy-based routing. Например: name("Policy-based routing rule example") .
desc	Описание правила. Чтобы указать описание правила используется: desc("Policy-based routing rule example set via CLI") .
route	Тип правила (указывается в свойствах правила).
gateway	Выбор одного из существующих шлюзов: gateway("1.1.1.1") . О добавлении шлюзов через CLI читайте в разделе Настройка шлюзов .
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(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 читайте 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 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 . Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: src.ip = 02:00:00:00:00:00 .

Параметр	Описание
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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
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.

Настройка правил типа Network mapping

При настройке правил типа Network mapping необходимо указать следующие параметры:

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 типа Network mapping. Например: name("Network mapping rule example").
desc	Описание правила. Чтобы указать описание правила используется: desc("Network mapping rule example set via CLI").
netmap	Тип правила (указывается в свойствах 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.

Параметр	Описание
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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. 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 ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
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.
target_ip	Параметр подмены сетей; адрес сети, на которую будет производится замена, например: target_ip("1.1.1.0").
direction	Параметр подмены сетей. Направление: direction(input) — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении target_ip. direction(output) — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении target_ip.

Настройка балансировки нагрузки

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing**. Настройка балансировщиков нагрузки TCP/UDP, ICAP и reverse-прокси рассмотрена далее.

Для отображения информации о всех балансировщиках используется команда:

```
Admin@UGOS# 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@UGOS# create network-policy load-balancing tcp-udp
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Имя балансировщика.
enabled	Включение/отключение балансировщика.
description	Описание балансировщика.
virtual-ip	IP-адрес виртуального сервера.
port	Порт, для которого необходимо производить балансировку нагрузки.
protocol	Протокол — TCP или UDP, для которого необходимо производить балансировку нагрузки.
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 — leighted least connections — работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.

Параметр	Описание
real-servers	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 NGFW подменяет IP-адрес источника на свой. Важно! Задавать реальные серверы лучше последними, т.к. после задания параметров реального сервера невозможно вернуться к заданию остальных параметров балансировщика.

Для обновления существующего балансировщика нагрузки используется следующая команда:

```
Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>
```

Помимо параметров, доступных при создании балансировщика, доступно обновление следующих параметров:

Параметр	Описание
fallback	Настройка аварийного режима: • enabled — включение/отключение 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 NGFW подменяет IP-адрес источника на свой.
monitoring	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.

Для удаления существующего балансировщика нагрузки используется следующая команда:

```
Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>
```

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо уточнить один или несколько параметров реального сервера):

```
Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name> real-servers
```

Команды для отображения информации о всех балансировщиках TCP/UDP:

Admin@UGOS# set network-policy load-balancing tcp-udp

Для отображения информации об определённом балансировщике TCP/UDP:

Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>

Настройка балансировщика ICAP

Настройка данного раздела производится на уровне **network-policy load-balancing icap**.

Структура команды создания балансировщика нагрузки ICAP следующая:

Admin@UGOS# create network-policy load-balancing icap

Необходимо указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение балансировщика серверов ICAP: - on. - off.
name	Имя балансировщика.
description	Описание правила балансировки.
icap-server	Указание ICAP-профилей серверов, на которые будет распределяться нагрузка. Подробнее о создании и настройке ICAP-серверов с использованием CLI в разделе Настройка ICAP-серверов .

Команда для обновления параметров балансировщика нагрузки ICAP:

Admin@UGOS# create network-policy load-balancing icap <balancer-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании балансировщика серверов ICAP.

Для удаления существующего балансировщика нагрузки используется следующая команда:

Admin@UGOS# set network-policy load-balancing icap <balancer-name>

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо указать названия ICAP-серверов):

Admin@UGOS# set network-policy load-balancing icap <balancer-name> real-servers

Команды для отображения информации о всех балансировщиках ICAP:

Admin@UGOS# set network-policy load-balancing icap

Для отображения информации об определённом балансировщике серверов ICAP:

Admin@UGOS# set network-policy load-balancing icap <balancer-name>

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@UGOS# create network-policy load-balancing reverse-proxy

Необходимо указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение балансировщика серверов reverse-proxy: - on. - off.
name	Имя балансировщика.

Параметр	Описание
description	Описание правила балансировки.
reverse-proxy-servers	Выбор сервера reverse-прокси. Подробнее о создании и настройке серверов reverse-прокси с использованием CLI в разделе Настройка серверов reverse-прокси.

Команда для обновления параметров балансировщика нагрузки reverse-прокси:

```
Admin@UGOS# set network-policy load-balancing reverse-proxy <balancer-name>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании балансировщика серверов reverse-прокси.

Для удаления существующего балансировщика нагрузки используется следующая команда:

```
Admin@UGOS# delete network-policy load-balancing reverse-proxy <balancer-name>
```

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо указать названия серверов reverse-прокси):

```
Admin@UGOS# delete network-policy load-balancing reverse-proxy <balancer-name> real-servers
```

Команды для отображения информации о всех балансировщиках reverse-прокси:

```
Admin@UGOS# show network-policy load-balancing reverse-proxy
```

Для отображения информации об определённом балансировщике серверов reverse-прокси:

```
Admin@UGOS# show network-policy load-balancing reverse-proxy <balancer-name>
```

Настройка правил пропускной способности

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка правил пропускной способности производится на уровне **network-policy traffic-shaping**. О структуре команд подробнее читайте в разделе [Настройка правил с использованием UPL](#).
При настройке правил пропускной способности необходимо указать следующее:

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 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 .

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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.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.
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.

Настройка раздела Политики безопасности

Настройка фильтрации контента

Product: UserGate NGFW
Version: 7.0.1
Documentation: ☒

Настройка правил контентной фильтрации производится на уровне **security-policy content-filtering**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

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 .

Параметр	Описание
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). В следующей строке описано добавление локальных пользователей (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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.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.
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".

Параметр	Описание
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.

Настройка веб-безопасности

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка веб-безопасности производится на уровне **security-policy safe-browsing**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать следующие данные:

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 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	Инжектирование 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.

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> 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.
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 правил инспектирования туннелей

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил инспектирования туннелей производится на уровне **security-policy tunnel-inspection**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо задать следующие параметры:

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 .

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.

Настройка инспектирования SSL

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил инспектирования SSL производится на уровне **security-policy ssl-inspection**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

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.

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> 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.
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.
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, ...).

Параметр	Описание
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.

Настройка инспектирования SSH

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка правил SSH-инспектирования производится на уровне **security-policy ssh-inspection**. О структуре команд читайте подробнее в разделе [Настройка правил с использованием UPL](#).

Далее представлены 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.

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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.
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.
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.

Настройка COB

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка системы обнаружения и предотвращения вторжений производится на уровне **security-policy intrusion-prevention**.

Правила COB настраиваются на уровне **security-policy intrusion-prevention idps-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Доступны параметры:

Параметр	Описание
PASS WARNING DENY	Действие правила COB: • PASS — не блокировать трафик. • WARNING — не блокировать трафик и записать информацию в журнал. • DENY — блокировать трафик и записать информацию в журнал.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила системы обнаружения и предотвращения вторжений. Например: name("IDPS rule example") .
desc	Описание правила. Например: desc("Intrusion prevention rule example set via CLI") .
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, 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 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 . 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 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 трафика, 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, MAC-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. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: dst.ip = 02:00:00:00:00:00.
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.
idps_profiles	Профиля COB, которые будут использованы в данном правиле: idps_profiles("IDPS profile example"). Профили COB задаются для правил с действиями Сбросить и Журналировать. Для разрешающих правил задать профиль COB невозможно; такая реализация позволяет настроить исключения для определённого типа трафика.
idps-profiles_exclusions	Список профилей COB, сигнатуры которых будут исключены из сигнатур, указанных в профилях COB; могут быть использованы только в правилах с действием Сбросить или Журналировать: idps_profiles_exclusions("Example of IDPS profile with exclusions"). Данная возможность позволяет использовать централизованно создаваемые профили сигнатур, изменять содержимое которых администратор не может, но при этом исключить из этого профиля ряд сигнатур, которые избыточны или создают ложные срабатывания.

Только в CLI доступна настройка режима умного сканирования (сканирование только первых байт каждой сессии). Настройка режима производится на уровне **security-policy intrusion-prevention settings**. Для настройки используется команда:

```
Admin@UGOS# set security-policy intrusion-prevention settings
```

Доступны параметры:

Параметр	Описание
intelligent-mode	Включение/отключение режима умного сканирования: • on. • off.
intelligent-limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Для просмотра состояния режима:

```
Admin@UGOS# show security-policy intrusion-prevention settings
```

По умолчанию режим умного сканирования включен; проверяются первые 200 КБ каждой сессии.

Настройка сценариев

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка сценариев происходит на уровне **security-policy scenarios** с использованием UPL (подробнее об UserGate Policy Language читайте в разделе [Настройка правил с использованием UPL](#)).

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 работает, если выполнятся все условия; • operation_mode(any) — сценарий работает, 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@UGOS# create security-policy scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(2GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
```

... duration (1)

...

Для изменения, например, объема трафика:

```
Admin@UGOS# set security-policy 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
```

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
category	Категории или группы категорий сайтов: category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME).
scond_type	Тип условия: scond_type(url_category).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval().
max_event_count	Количество срабатываний: max_event_count().

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: scond_type(virus_detection).

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
application	Категории приложений или группы приложений: application = lib.applicationgroup(APP_GROUP) или application = lib.applicationgroup(all); application = lib.category(APPS_CATEGORY_NAME).
scond_type	Тип условия: scond_type(app).
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval().
max_event_count	Количество срабатываний: max_event_count().

Условие типа COB

Параметры условия типа **COB**:

Наименование	Описание
--------------	----------

Наименование	Описание
ips_tl	Уровень угрозы: • ips_tl(very_low) - очень низкий; • ips_tl(low) - низкий; • ips_tl(medium) - средний; • ips_tl(high) - высокий; • ips_tl(very_high) - очень высокий.
scond_type	Тип условия: scond_type(ips) .

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
response.header.Content-Type	Тип контента: response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST) .
scond_type	Тип условия: scond_type(mime_type) .
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): count_interval() .
max_event_count	Количество срабатываний: max_event_count() .

Условие типа Размер пакета

Для создания и настройки условия типа **Размер пакета** используются следующие параметры:

Наименование	Описание
packet_size	Размер пакета, при превышении которого выполняется условие; указывается следующим образом: • packet_size(1) - размер пакета 1 байт; • packet_size(1KB) - размер пакета 1 Кбайт; • packet_size(1MB) - размер пакета 1 Мбайт; • packet_size(1GB) - размер пакета 1 Гбайт.
scond_type	Тип условия: scond_type(net_packet_size) .

Условие типа Сессий с одного IP

При настройке условия типа **Сессий с одного IP** используются:

Наименование	Описание
scond_type	Тип условия: scond_type(sessions_per_ip) .
sessions_limit	Максимальное количество сессий, разрешённых с одного IP-адреса: sessions_limit() .

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: scond_type(traffic) .
traffic_limit	Ограничение объема трафика: • traffic_limit(1) - 1 байт трафика; • traffic_limit(1KB) - 1 Кбайт трафика; • traffic_limit(1MB) - 1 Мбайт трафика; • traffic_limit(1GB) - 1 Гбайт трафика.
period	Период времени: • period(minute) - минута; • period(hour) - час; • period(day) - день; • period(week) - неделя; • period(month) - 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() .

Наименование	Описание
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 правил защиты почтового трафика

Product: UserGate NGFW
Version: 7.0.1
Documentation: ☒

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать:

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") .
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 .

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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.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.
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.

Настройка правил ICAP

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

Необходимо указать:

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.

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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 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: <pre>response.header.Content-Type = lib.mime();</pre> 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.
service	Тип сервиса: HTTP, SMTP или POP3. Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...).

Настройка ICAP-серверов

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка ICAP-серверов производится на уровне **security-policy icap-server**.

Структура команды для создания ICAP-сервера:

```
Admin@UGOS# create security-policy icap-server
```

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. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
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-service	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Reqmod.
respmod-service	Использовать режим Respmode: • <text> — задать путь на сервере ICAP. • off — отключить использование режима Respmode.
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.

Параметр	Описание
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@UGOS# set security-policy icap-server <server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового ICAP-сервера.

Структура команды для удаления ICAP-сервера:

```
Admin@UGOS# delete security-policy icap-server <server-name>
```

Структура команды для отображения информации об ICAP-сервере:

```
Admin@UGOS# show security-policy icap-server <server-name>
```

Настройка правил защиты DoS

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка правил защиты DoS производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

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, "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 .

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> 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.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: src.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.
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 профилей DoS

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка профилей DoS производится на уровне **security-policy dos-profile**.

Структура команды для создания профиля DoS:

```
Admin@UGOS# create security-policy dos-profile
```

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.
dos-protection-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.
dos-protection-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.
dos-protection-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: • <num> — задать число сессий. • off — отключить ограничение числа сессий.

Структура команды для обновления существующих профилей DoS:

```
Admin@UGOS# set security-policy dos-profile <profile-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды добавления нового профиля DoS.

Структура команды для удаления профиля:

```
Admin@UGOS# delete security-policy dos-profile <profile-name>
```

Структура команды для отображения информации о профиле DoS:

```
Admin@UGOS# show security-policy dos-profile <profile-name>
```


Настройка веб-портала

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Настройка веб-портала производится на уровне **global-portal web-portal**. О структуре команд подробнее читайте в разделе [Настройка правил с использованием UPL](#).

При настройке закладок веб-портала

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 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, закодированное 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") .

Параметр	Описание
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). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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.

Настройка правил reverse-прокси

Documentation: ☒
Product: UserGate NGFW
Version: 7.0.1

Правила reverse-прокси настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд читайте в разделе [Настройка правил с использованием UPL](#).

При настройке правил reverse-прокси необходимо задать:

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 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 UserGate будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example") .
url.port	Порт, на котором UserGate 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	Авторизация 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 .

Параметр	Описание
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 локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> 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 сервера UserGate, 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").

Настройка серверов reverse-прокси

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка серверов reverse-прокси производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера reverse-прокси используется следующая команда:

```
Admin@UGOS# create global-portal reverse-proxy-servers
```

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.
check-cert	Проверка валидности SSL-сертификата, установленного на публикуемом сервере: • on: проверять. • off: не проверять.
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.

Следующая команда предназначена для обновления параметров сервера reverse-прокси:

```
Admin@UGOS# set global-portal reverse-proxy-servers <server-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для удаления сервера:

```
Admin@UGOS# delete global-portal reverse-proxy-servers <server-name>
```

Структура команды для отображения информации о сервере reverse-прокси:

```
Admin@UGOS# show global-portal reverse-proxy-servers <server-name>
```

Настройка удалённого доступа (VPN)

Настройка серверных правил

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе [Настройка правил с использованием UPL](#).

При настройке необходимо указать:

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). 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 .
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 .

Параметр	Описание
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): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> 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.

Настройка клиентских правил

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Клиентские правила настраиваются на уровне **vpn client-rules**. Подробнее о структурах команд настройки клиентских правил читайте в разделе [Настройка правил с использованием UPL](#).

При настройке правил необходимо указать:

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 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(tunnel1) . 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 сервере UserGate, выполняющего роль VPN-сервера. Задаётся в формате: server_address("1.2.3.4") .
service	Протокол VPN: • l2tp — L2TP. • cisco cryptomap — IPsec туннель. Указывается в формате: service = l2tp или service = "cisco cryptomap" .
subnet1	IP-адрес подсети, разрешённой со стороны UserGate; указывается в формате: subnet1("ip/mask") . Подсети указываются при выборе протокола VPN: IPsec туннель.
subnet2	IP-адрес подсети, разрешённой со стороны Cisco; указывается в формате: subnet2("ip/mask") . Подсети указываются при выборе протокола VPN: IPsec туннель.
user	Имя пользователя для авторизации сервера, выступающего в качестве клиента VPN. Указывается только для протокола L2TP в формате user() ; имя пользователя указывается в скобках.
password	Пароль пользователя VPN. Указывается только для протокола L2TP в формате password() ; пароль указывается в скобках.

При отображении правил, помимо заданных условий и свойств, будут показаны последняя ошибка VPN, статус подключения.

Настройка сетей VPN

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка VPN-сетей производится на уровне **vpn networks**.

Для создания сети VPN необходимо использовать следующую команду:

```
Admin@UGOS# create vpn networks
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название VPN-сети.
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 .

Следующая команда предназначена для обновления параметров сети:

```
Admin@UGOS# set vpn networks <network-name>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления сети VPN.

Структура команды для удаления сети VPN:

```
Admin@UGOS# delete vpn networks <network-name>
```

Также можно удалить отдельные параметры сети:

```
Admin@UGOS# delete vpn networks <network-name> <network-configuration-name>
```

Параметры, доступные для удаления:

- **dns-servers**.
- **routes-ip**.
- **routes-ip-list**.

Структура команды для отображения информации о сети VPN:

```
Admin@UGOS# show vpn networks <network-name>
```

Настройка профилей безопасности VPN

Documentation: 

Product: UserGate NGFW

Version: 7.0.1

Профили безопасности VPN настраиваются на уровне **vpn security-profile**.

Для создания профиля безопасности VPN предназначена следующая команда:

```
Admin@UGOS# create vpn security-profile
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
ike-version	Версия протокола IKE (Internet Key Exchange), использующегося для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1 (IKEv1).
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.
peer-auth	Аутентификация с пиром: psk — общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key).
psk	Общий ключ; должен совпадать на сервере и клиенте для успешного подключения.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
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).

Параметр	Описание
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: <pre>Admin@UGOS# create vpn security-profile ... phase1-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.
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-lifeseize	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Время жизни ключа может быть задано в байтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifeseize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off.

Параметр	Описание
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@UGOS# create vpn security-profile ... 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.

Установка значений профиля безопасности:

```
Admin@UGOS# set vpn security-profile <profile-name>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным для указания при создании профиля безопасности. Для добавления новой пары алгоритмов аутентификации и шифрования или группы Диффи-Хеллмана в профиль безопасности используются команды со структурой:

```
Admin@UGOS# set vpn security-profiles <profile-name> phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
Admin@UGOS# set vpn security-profiles <profile-name> phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
Admin@UGOS# set vpn security-profiles <profile-name> dh-groups + [ <dh-group1> <dh-group2> ... ]
```

Команда для удаления профиля безопасности:

```
Admin@UGOS# delete vpn security-profile <profile-name>
```

Также доступно удаление следующих параметров профиля безопасности VPN:

- **dh-groups**.
- **phase1-security**.
- **phase2-security**.

Для отображения информации о профиле безопасности VPN используется следующая команда:

```
Admin@UGOS# show vpn security-profile <profile-name>
```

Настройка библиотек

Настройка библиотек (Описание)

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

Настройка морфологии

Для создания списка морфологии используется следующая команда:

```
Admin@UGOS# create libraries morphology
```

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.
url	Если морфологический список является обновляемым, то необходимо указать адрес, с которого необходимо загружать обновления.
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: <pre>Admin@UGOS# create libraries morphology ... words new word "word or phrase" weight <weight></pre>

Чтобы обновить данные морфологического списка, необходимо использовать следующую команду:

```
Admin@UGOS# set libraries morphology <morphology-list-name>
```

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@UGOS# set libraries morphology <morphology-list-name> words new word "word or phrase" weight <weight>
```

Чтобы заменить слово в списке:

```
Admin@UGOS# 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@UGOS# delete libraries morphology <morphology-list-name>
```

```
Admin@UGOS# delete libraries morphology <morphology-list-name> words ( word "word or phrase" weight <weight> )
```

Команды отображения информации о всех имеющихся морфологических списках:

```
Admin@UGOS# show libraries morphology
```

Чтобы отобразить информацию об определённом списке, далее необходимо указать название интересующего морфологического списка.

Чтобы просмотреть содержание определённого морфологического списка:

Admin@UGOS# show libraries morphology <morphology-list-name> words

Настройка сервисов

Данный раздел настраивается на уровне **libraries services**.

Для добавления нового сервиса используется следующая команда:

Admin@UGOS# create libraries services

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название сервиса.
description	Описание сервиса.
protocols	Указание сетевого протокола и портов источника/назначения: • protocol — сетевой протокол. • dest-ports — порт(ы) назначения (указывается номер порта или диапазон портов). • source-ports — порт(ы) источника (указывается номер порта или диапазон портов). При создании сервиса для указания значений параметра protocols : Admin@UGOS# create libraries service ... protocols new Далее указываются параметры protocol , dest-ports , source-ports .

Для обновления существующего сервиса:

Admin@UGOS# set libraries services <service-name>

Для обновления сетевого протокола и портов источника/назначения сервиса:

Admin@UGOS# 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@UGOS# set libraries services <service-name> protocols new

Далее необходимо указать **protocol**, **dest-ports**, **source-ports**.

Чтобы удалить сервис используется следующая команда:

Admin@UGOS# delete libraries services <service-name>

Также возможно удаления из сервиса заданных сетевых протоколов:

Admin@UGOS# delete libraries services <service-name> protocols (<protocol-filter>)

Следующие команды предназначены для отображения информации о всех сервисах или об определённом сервисе:

Admin@UGOS# show libraries services

Admin@UGOS# show libraries services <service-name>

Настройка групп сервисов

Данный раздел находится на уровне **libraries service-groups**. Для создания группы сервисов предназначена следующая команда:

Admin@UGOS# create libraries service-groups

Далее указываются параметры:

Параметр	Описание
name	Название группы сервисов.

Параметр	Описание
description	Описание группы.
services	Сервисы, которые необходимо добавить в группу.

Для обновления информации о группе сервисов (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы):

```
Admin@UGOS# set libraries service-groups <service-group-name>
```

Чтобы добавить в группу сервисы:

```
Admin@UGOS# set libraries service-groups <service-group-name> + [ <service1> <service2> ... ]
```

Следующие команды используются для удаления группы сервисов или отдельных сервисов, содержащихся в ней:

```
Admin@UGOS# delete service-groups <service-group-name>
```

```
Admin@UGOS# delete service-groups <service-group-name> services [ <service> ... ]
```

Команды отображения информации о всех имеющихся списках:

```
Admin@UGOS# show libraries service-groups
```

об определённом списке:

```
Admin@UGOS# show libraries service-groups <service-group-name>
```

или списка сервисов, добавленных в группу:

```
Admin@UGOS# 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@UGOS# create libraries ip-list
```

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.
url	Если список адресов является обновляемым, то необходимо указать URL обновления.
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 обновления информации о списке (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@UGOS# set libraries ip-list <ip-list-name>
```

Чтобы добавить в список новые адреса:

```
Admin@UGOS# 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@UGOS# delete libraries ip-list <ip-list-name>
Admin@UGOS# delete libraries ip-list <ip-list-name> ips [ <ip> ... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@UGOS# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@UGOS# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@UGOS# show libraries ip-list <ip-list-name> ips
```

Настройка Useragent браузеров

Раздел настраивается на уровне **libraries useragents**.

Следующая команда используется для добавления нового списка Useragent браузеров:

```
Admin@UGOS# create libraries useragents
```

Далее указываются следующие данные:

Параметр	Описание
name	Название списка Useragent.
description	Описание списка.
url	Если список является обновляемым, то необходимо указать URL обновления.
patterns	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php .

Для обновления существующего списка:

```
Admin@UGOS# set libraries useragents <useragent-list-name>
```

Далее указываются параметры, которые необходимо обновить. Параметры представлены в таблице выше. Чтобы добавить новые Useragent браузеров:

```
Admin@UGOS# set libraries useragents <useragent-list-name> + [ <useragent1> <useragent2> ... ]
```

Следующие команды используются для удаления всего списка или отдельных Useragent браузеров, содержащихся в нём:

```
Admin@UGOS# delete libraries useragents <useragent-list-name>
Admin@UGOS# delete libraries useragents <useragent-list-name> patterns [ <useragent> ... ]
```

Команды отображения информации о всех имеющихся списках:

```
Admin@UGOS# show libraries useragents
```

Чтобы отобразить информацию об определённом списке, необходимо указать название списка Useragent браузеров. Чтобы просмотреть содержание списка Useragent браузеров:

```
Admin@UGOS# 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@UGOS# create libraries content-types
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.

Параметр	Описание
description	Описание списка.
url	Если список является обновляемым, то необходимо указать URL обновления.
types	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 обновления информации о списке используется следующая команда:

```
Admin@UGOS# set libraries content-types <content-types-list-name>
```

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

```
Admin@UGOS# delete libraries content-types <content-types-list-name>
```

Также доступно удаление отдельных типов контента из списка:

```
Admin@UGOS# delete libraries content-types <content-types-list-name> types [ <mime-type> ... ]
```

Следующие команды используются для отображения информации о списках типов контента:

```
Admin@UGOS# show libraries content-types
```

```
Admin@UGOS# show libraries content-types <content-types-list-name>
```

Для отображения типов контента, содержащихся в списке, используется команда:

```
Admin@UGOS# show libraries content-types <content-types-list-name> types
```

Настройка списков URL

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

```
Admin@UGOS# create libraries url-list
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка URL.
description	Описание списка URL.
url	Если список является обновляемым, то необходимо указать URL обновления.
urls	URL, которые необходимо добавить в список.

Для обновления информации о списке URL:

```
Admin@UGOS# set libraries url-list <url-list-name>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

```
Admin@UGOS# delete libraries url-list <url-list-name>
```

```
Admin@UGOS# delete libraries url-list <url-list-name> urls [ <url> ... ]
```

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

```
Admin@UGOS# show libraries url-list
```

```
Admin@UGOS# show libraries url-list <url-list-name>
```

```
Admin@UGOS# show libraries url-list <url-list-name> urls
```

Настройка календарей

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

Admin@UGOS# create libraries time-sets

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.

Параметр	Описание
time-set	Тип повторения: • daily — ежедневно: ◦ interval-name — название интервала. ◦ 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: ◦ interval-name — название интервала. ◦ 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: ◦ interval-name — название интервала. ◦ 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 — единовременно: ◦ interval-name — название интервала. ◦ 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). • repeating — повторяющиеся события: ◦ interval-name — название интервала. ◦ 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: ◦ interval-name — название интервала. ◦ 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). Admin@UGOS# create libraries time-sets ... time-set <time-set-type> new Далее указываются параметры, выбранного типа повторения.

Для обновления календаря:

Admin@UGOS# set libraries time-sets <time-sets-name>

Параметры, доступные для обновления, представлены в таблице выше.

Для обновления интервала, заданного в календаре:

Admin@UGOS# 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@UGOS# create libraries time-sets <time-sets-name> ... time-set <time-set-type> new

Команда для удаления группы элементов:

Admin@UGOS# delete libraries time-sets <time-sets-name>

Для удаления элемента календаря:

Admin@UGOS# delete libraries time-sets <time-sets-name> <time-set-type> (<time-set-filter>)

Для отображения информации о всех календарях:

Admin@UGOS# show libraries time-sets

Для отображения информации об определённом календаре:

Admin@UGOS# show libraries time-sets <time-sets-name>

Для отображения информации об элементах группы с одинаковым типом повторения:

Admin@UGOS# 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@UGOS# create libraries bandwidth-pools

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 для QoS (при указании будет прописываться в каждый IP-пакет: принимает значения от 0 до 63).

Для обновления параметров полосы пропускания:

Admin@UGOS# set libraries bandwidth-pools <bandwidth-name>

Параметры, доступные для изменения такие же, как и для команды создания полосы пропускания.

Чтобы удалить полосу пропускания:

Admin@UGOS# delete libraries bandwidth-pools <bandwidth-name>

С использованием **show** можно отобразить информацию о всех полосах пропускания:

Admin@UGOS# show libraries bandwidth-pools

или об определённой полосе:

Admin@UGOS# 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** — страница блокировки.
- **captiveportal-user-auth** — страница авторизации captive-портала.

- **captiveportal-user-session** — captive-портал, сессия пользователя.
- **content-warning** — содержание страницы предупреждения.
- **ftp-client** — страница отображения FTP поверх HTTP.
- **proxy-portal** — страница веб-портала.
- **pp-login-ssh** — страница SSH-логина веб-портала.
- **pp-login-rdp** — страница RDP-логина веб-портала.
- **totp-init-page** — страница инициализации TOTP.

Команда, используемая для создания шаблона страницы:

```
Admin@UGOS# create libraries response-pages type <response-page-type>
```

Необходимо указать параметры:

Параметр	Описание
name	Название шаблона страницы.
description	Описание шаблона.
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://logout.captive или http://USERGATE_IP/cps.

Параметр	captiveportal_user_session_ru — шаблон на русском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://localhost/captiveportal 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.
default	Использовать шаблон по умолчанию: on. off.

Для установки значений шаблона:

```
Admin@UGOS# set libraries response-pages type <response-page-type> response-page <response-page-name>
```

Далее необходимо указать значения параметров; параметры представлены в таблице выше.

Чтобы удалить шаблон страницы, используется следующая команда:

```
Admin@UGOS# delete libraries response-pages type <response-page-type> response-page <response-page-name>
```

Для просмотра информации о всех имеющихся шаблонах страниц:

```
Admin@UGOS# show libraries response-pages
```

Для просмотра информации об отдельном типе шаблонов страниц:

```
Admin@UGOS# show libraries response-pages type <response-page-type>
```

Для просмотра информации об отдельном шаблоне страницы:

```
Admin@UGOS# show libraries response-pages type <response-page-type> response-page <response-page-name>
```

Настройка категорий URL

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

```
Admin@UGOS# create libraries url-categories
```

Параметры, которые необходимо указать:

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для изменения параметров группы:

```
Admin@UGOS# set libraries url-categories <list-name>
```

Для добавления категорий URL в существующую группу:

```
Admin@UGOS# set libraries url-categories <list-name> categories + [ <url-category> ... ]
```

Команды для удаления группы URL-категорий:

```
Admin@UGOS# delete libraries url-categories <list-name>
```

или отдельных категорий из группы:

```
Admin@UGOS# delete libraries url-categories <list-name> categories [ <url-category> ... ]
```

Команды для просмотра информации о всех группах URL-категорий:

```
Admin@UGOS# show libraries url-categories
```

об определённой группе:

```
Admin@UGOS# show libraries url-categories <list-name>
```

Чтобы отобразить список категорий URL, входящих в группу:

```
Admin@UGOS# 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@UGOS# create libraries overridden-url-categories
```

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 изменения параметров:

```
Admin@UGOS# set libraries overridden-url-categories <domain>
```

Для удаления сайта с изменёнными категориями:

```
Admin@UGOS# delete libraries overridden-url-categories <domain>
```

Для отображения всего списка сайтов с изменёнными категориями:

```
Admin@UGOS# show libraries overridden-url-categories
```

Для отображения информации об определённом сайте с изменёнными категориями URL:

```
Admin@UGOS# show libraries overridden-url-categories <domain>
```

Настройка приложений

Данный раздел настраивается на уровне **libraries applications**.

Для создания группы приложений используется команда:

```
Admin@UGOS# create libraries applications
```

Далее указываются параметры:

Параметр	Описание
name	Название группы приложений.
description	Описание группы приложений.
apps	Приложения, которые необходимо добавить в группу.

Для изменения параметров:

```
Admin@UGOS# set libraries applications <app-group-name>
```

Чтобы добавить новые приложения в существующую группу, используется команда:

```
Admin@UGOS# set libraries applications <app-group-name> apps + [ <application> ... ]
```

Для удаления группы приложений полностью или отдельных приложений в ней используются команды:

```
Admin@UGOS# delete libraries applications <app-group-name>
```

```
Admin@UGOS# delete libraries applications <app-group-name> apps [ <application> ... ]
```

Следующие команды предназначены для отображения информации о всех созданных группах приложений:

```
Admin@UGOS# show libraries applications
```

или об определённой группе:

```
Admin@UGOS# show libraries applications <app-group-name>
```

Также доступно отображение приложений, входящих в определённый список:

```
Admin@UGOS# show libraries applications <app-group-name> apps
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@UGOS# create libraries email-list
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
url	Если список почтовых адресов является обновляемым, то необходимо указать URL обновления.
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для обновления информации о группе почтовых адресов:

```
Admin@UGOS# set libraries email-list <email-list-name>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@UGOS# delete libraries email-list <email-list-name>
```

```
Admin@UGOS# 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@UGOS# show libraries email-list
Admin@UGOS# show libraries email-list <email-list-name>
Admin@UGOS# 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@UGOS# create libraries phone-list

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
url	Если список почтовых адресов является обновляемым, то необходимо указать URL обновления.
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для обновления информации о группе телефонных номеров используется команда:

Admin@UGOS# set libraries phone-list <phone-list-name>

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

Admin@UGOS# delete libraries phone-list <phone-list-name>
Admin@UGOS# delete libraries phone-list <phone-list-name> phones [<phone> ...]

Следующие команды используются для просмотра информации о всех созданных группах:

Admin@UGOS# show libraries phone-list

или об определённых группах телефонных номеров:

Admin@UGOS# show libraries phone-list <phone-list-name>

Для просмотра номеров, содержащихся в группе, используется команда:

Admin@UGOS# show libraries phone-list <phone-list-name> phones

Настройка профилей COB

Настройка профилей COB производится на уровне **libraries ips-profiles**. Для создания профиля системы обнаружения вторжения используется команда:

Admin@UGOS# create libraries ips-profiles

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля COB.
description	Описание профиля COB.
signatures	Сигнатур, релевантные для защиты определенных сервисов.

Представленная ниже команда предназначена для обновления существующего профиля COB:

Admin@UGOS# set libraries ips-profiles <ips-profile-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании профиля.

С использованием **delete** возможно удаление сигнатур из профиля COB или профиля полностью:

```
Admin@UGOS# delete libraries ips-profiles <ips-profile-name> signatures
Admin@UGOS# delete libraries ips-profiles <ips-profile-name>
```

С использованием следующих команда возможно отображение информации о всех профилях COB:

```
Admin@UGOS# show libraries ips-profiles
```

или об одном профиле:

```
Admin@UGOS# show libraries ips-profiles <ips-profile-name>
```

Также доступен просмотр списка сигнатур, добавленных в профиль:

```
Admin@UGOS# show libraries ips-profiles <ips-profile-name> signatures
```

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@UGOS# create libraries notification-profiles smtp
```

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.
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@UGOS# create libraries notification-profiles smpp
```

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.

Параметр	Описание
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@UGOS# 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 обновления информации о профиле оповещения используется команда:

```
Admin@UGOS# set libraries notification-profiles <smtp | smpp> <profile-name>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@UGOS# set libraries notification-profiles <smtp | smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@UGOS# set libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1!phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@UGOS# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@UGOS# set libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@UGOS# show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка профилей NetFlow

Раздел находится на уровне **libraries netflow-profiles**.

Команда для создания профиля NetFlow:

```
Admin@UGOS# create libraries netflow-profiles
```

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.

Параметр	Описание
protocol	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): • netflow5. • netflow9. • netflow10.
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 обновить существующий профиль:

```
Admin@UGOS# set libraries netflow-profiles <profile-name>
```

Параметры, значения которых можно изменить, представлены в таблице выше.

Следующая команда предназначена для удаления профиля NetFlow:

```
Admin@UGOS# delete libraries netflow-profiles <profile-name>
```

Для отображения информации о всех профилях NetFlow или об отдельном профиле используются следующие команды:

```
Admin@UGOS# show libraries netflow-profiles
```

```
Admin@UGOS# 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@UGOS# create libraries lldp-profiles
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля LLDP.
description	Описание профиля.

Параметр	Описание
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 обновления информации о профиле:

```
Admin@UGOS# set libraries lldp-profiles <profile-name>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль LLDP, используя следующую команду:

```
Admin@UGOS# delete libraries lldp-profiles <profile-name>
```

Чтобы отобразить информацию о профилях:

```
Admin@UGOS# show libraries lldp-profiles
```

```
Admin@UGOS# 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@UGOS# create libraries ssl-profiles
```

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.
min-tls-version	Минимальная 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 обновления информации о профиле:

```
Admin@UGOS# set libraries ssl-profiles <profile-name>
```

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@UGOS# delete libraries ssl-profiles <profile-name>
Admin@UGOS# delete libraries ssl-profiles <profile-name> ssl-ciphers [ cipher ... ]
```

Чтобы отобразить информацию о профилях SSL:

```
Admin@UGOS# show libraries ssl-profiles
Admin@UGOS# 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@UGOS# create libraries ssl-forwarding-profiles
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля пересылки SSL.
description	Описание профиля пересылки.
forward-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.
target-mac	MAC-адрес назначения (указывается при использовании типа пересылки L2).
target-iface	Интерфейс UserGate, с которого будет производиться пересылка (указывается при использовании типа пересылки L2).
gre-source-ip	GRE IP-адрес источника (указывается при использовании типа пересылки L3).
gre-dest-ip	GRE IP-адрес назначения (указывается при использовании типа пересылки L3).

Следующая команда предназначена для обновления параметров профилей пересылки:

```
Admin@UGOS# set libraries ssl-forwarding-profiles <profile-name>
```

Для удаления профиля:

```
Admin@UGOS# delete libraries ssl-forwarding-profiles <profile-name>
```

Чтобы отобразить информацию о всех имеющихся профилях или об определённом профиле пересылки, используются следующие команды:

```
Admin@UGOS# show libraries ssl-forwarding-profiles
Admin@UGOS# show libraries ssl-forwarding-profiles <profile-name>
```

