

Table of Contents

Table of Contents	1
Настройка устройства	2
Настройка устройства (Описание)	3
Настройка кластеров	10
Настройка управления доступом к консоли NGFW	12
Настройка сертификатов	16
Настройка параметров устройства	19
Настройка телеметрии	21
Настройка прокси-сервера	22
Настройка параметров устройства	24

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.
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]</pre><pre>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)

Параметр	Описание
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.
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.

Параметр	Описание
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.
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: <pre>Admin@UGOS# delete settings general change-tracker event-tracker-types [type1 ...]</pre>

Параметр	Описание
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.
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.

Параметр	Описание
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 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).
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.

Параметр	Описание
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.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: • on. • off.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
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: Admin@UGOS# create settings administrators administrators ldap-user ... ldap-login connector <ldap-connector-name> user <domain\user> ... • 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: Admin@UGOS# create settings administrators administrators ldap-group ... ldap-login connector <ldap-connector-name> group <domain\group> ... • 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.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • user: имя пользователя в формате domain\user. • connector: выбор LDAP сервера.

Параметр	Описание
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>

