Table of Contents

Table of Contents 1
Настройка устройства в CLI 2
- Настройка общих параметров устройства 3
- Настройка кластеров 13
- Настройка управления доступом к консоли UserGate SWG 18
- Настройка сертификатов 22
- Настройка прокси-сервера 25
- Настройка работы с вышестоящими прокси-серверами 26
- Настройка параметров мониторинга устройства 30
- Настройка профилей клиентских сертификатов 33
- Настройка параметров управления телеметрией 34

Настройка устройства в CLI

Product: SWG
Version: 7.5.x

Настройка параметров работы CLI

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

С помощью команд этого уровня вы можете:

- настроить вид системного приглашения консоли CLI;
- уровень детализации журналирования действий в CLI;
- уровень детализации журналирования операций экспорта и импорта конфигурации CLI.

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

Admin@nodename# show settings cli

Пример выполнения команды:

Admin@mynode1# show settings cli

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

Настройка системного приглашения

Для настройки вида системного приглашения консоли CLI используется команда:

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

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

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

Вернуть системное приглашение в первоначальное состояние можно с помощью команды:

Admin@nodename# set settings cli custom-prompt default

Пример выполнения команды:

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

Настройка уровня детализации журналирования действий в CLI

Чтобы задать уровень детализации журналирования действий в CLI используется команда:

Admin@nodename# set settings cli log-level

Вы можете установить следующие уровни детализации:

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

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

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

Пример выполнения команды:

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

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

Настройка уровня детализации журналирования операций экспорта и импорта конфигурации

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

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

Вы можете установить следующие уровни детализации:

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

Пример выполнения команды:

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

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

Настройка базовых параметров устройства

Базовые параметры UserGate SWG настраиваются на уровне settings general.

Структура команд для настройки базовых параметров устройства:

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

Базовые параметры устройства сгруппированы в разделы.

Раздел	Описание

admin-console	Параметры консоли управления:
	• timezone — часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т. п.
	• language — язык интерфейса:
	  ◦ ru — русский;
	  ◦ en — английский.
	• webaccess — режим аутентификации веб-консоли:
	  ◦ password — аутентификация по имени и паролю;
	  ◦ cert — аутентификация по X.509-сертификату.
	• uc-profile — выбор профиля пользовательских сертификатов.
	• web-ssl-profile — выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL — в разделе «Настройка профилей SSL».
	• response-pages-ssl-profile — выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации captive-портала. Подробнее о профилях SSL — в разделе «Настройка профилей SSL».
	• api-session-lifetime — время ожидания сеанса администратора в минутах. По истечении этого времени при вводе команды CLI, использующей API-вызовы (команды создания объектов, изменения параметров, просмотра параметров, удаления объектов или параметров), сессия администратора будет завершена сообщением Authentication session expired. Restart CLI

server-time	Параметры установки точного времени: • ntp-enabled — включение и отключение использования NTP-серверов. • primary-ntp-server — адрес основного NTP-сервера. • second-ntp-server — адрес запасного NTP-сервера. • time — установка времени на устройстве. Время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)

Раздел	Описание
modules	Настройка работы модулей устройства: • proxy-port — указание нестандартного номера порта, который будет использоваться для подключения к встроенному прокси-серверу. • auth-captive — указание служебного домена, который будет использоваться UserGate SWG при авторизации пользователей через captive-портал. • logout-captive — указание служебного домена, который будет использоваться пользователями UserGate SWG для окончания сессии. • cert-captive — указание служебного домена, который будет использоваться UserGate SWG при авторизации пользователей через captive-портал с помощью сертификатов. • block-page-domain — указание служебного домена, который будет использоваться для отображения страницы блокировки. • ftp-enabled — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. • ftp-domain — указание служебного домена, который будет использоваться для предоставления пользователям сервиса FTP поверх HTTP. • snmp-engine-id — настройка идентификатора SNMP устройства: ◦ length <fixed | dynamic> — длина идентификатора. Фиксированная (не более 8 байт), только для типа text или динамическая (не более 27 байт). ◦ type <ip4 | ip6 | mac | text | octets> — формат идентификатора SNMP (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ value — значение идентификатора. • terminal-sever-agent — настройка пароля для подключения агентов авторизации терминального сервера. • lldp — настройка использования протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своем существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: ◦ transmit-delay — задержка передачи. Указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например после изменения имени узла или адреса управления. Может принимать значения от 1 до 3600. Указывается в секундах. ◦ transmit-hold — значение мультипликатора удержания. Произведение значений transmit-delay и transmit-hold определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100
cache	Параметры кэширования прокси-сервера: • caching-mode — включение или отключение режима кэширования. • exclusions — список URL, которые не будут кэшироваться. Для удаления исключений используйте команду: Admin@nodename# delete settings general cache exclusions [<URL>] • max-cacheable-size — максимальный размер объектов, которые будут кэшироваться (МБ). • ram-size: размер оперативной памяти, отведенный под кэширование (МБ)
log-analyzer	Параметры модуля сбора статистики: • use-local-stat-server — использование локальной службы журналирования

Раздел	Описание
proxy-portal	Параметры предоставления доступа к внутренним ресурсам компании с помощью веб-портала: • enabled — включение или отключение использования веб-портала. • hostname — имя узла, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. • port — порт TCP, который будет использоваться сервисом веб-портала. • auth-profile — указание профиля аутентификации, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей аутентификации». • auth-template — выбор шаблона страницы аутентификации. • portal-template — выбор шаблона веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. • enable-ldap — выбор домена AD или LDAP на странице аутентификации: ◦ on — показывать; ◦ off — не показывать. • use-captcha — показывать на странице аутентификации веб-портала код для ввода пользователем: ◦ on — показывать; ◦ off — не показывать. • ssl-profile — выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробнее о настройке профилей аутентификации с использованием CLI — в разделе «Настройка профилей SSL». • certificate — выбор сертификата, который будет использоваться для создания HTTPS-соединения. • auth-mode — выбор метода аутентификации: ◦ aaa — аутентификация через логин и пароль локальных пользователей или аутентификация пользователей на AAA-сервере; ◦ pki — аутентификация посредством X.509-сертификатов. • user-cert-profile — выбор профиля пользовательских сертификатов при аутентификации посредством сертификатов
pcap	Настройка захвата пакетов. Команда для настройки: Admin@nodename# set settings general pcap packet-capture-mode <parameters> Параметры: • no-capture — без захвата; • one-packet — один пакет; • previous — предшествующие пакеты; • previous-and-following — предшествующие и последующие пакеты: ◦ previous-packets — количество предшествующих пакетов (от 4 до 30 пакетов); ◦ following-packets — количество последующих пакетов (от 2 до 15 пакетов)
change-tracker	Настройка учета изменений параметров устройства: • enabled — включение или отключение учета изменений параметров. • event-tracker-types — типы изменений (например, приказ, регламентные работы и т. д.). Для удаления типа изменения используется команда: Admin@nodename# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Настройка агента UserGate Management Center. Команда для настройки: Admin@nodename# set settings general management-center <parameters> Параметры: • enabled — включение или отключение агента UserGate Management Center; • mc-address — адрес сервера UserGate Management Center; • device-code — уникальный код устройства для подключения устройства к UserGate Management Center

Раздел	Описание
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек. Расписание для обновления программного обеспечения задается командой: Admin@nodename# set settings general updates-schedule software schedule <schedule|disabled> Единое расписание для скачивания обновлений библиотек задается командой: Admin@nodename# set settings general updates-schedule all-libraries schedule <schedule|disabled> Расписание для скачивания обновлений отдельных библиотек задается командой: Admin@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule/disabled> Время задается в crontab-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Каждое из полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что проверка обновления программного обеспечения должна выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями. Команда для просмотра расписания обновлений: Admin@nodename# show settings general updates-schedule
metrics-collection	Настройка параметров передачи метрик телеметрии. • enabled — включение или выключение отправки метрик телеметрии. По умолчанию отправка метрик телеметрии включена. • masking-sensitive-data — маскирование чувствительных данных в отправляемых метриках. К чувствительным данным относятся IP-адреса, MAC-адреса, URL, адреса эл. почты и т. д. По умолчанию маскирование чувствительных данных отключено.

Управление подключаемыми модулями

Управление подключаемыми модулями устройства в CLI выполняется на уровне settings device.

Для управления модулями используется команда:

Admin@nodename# set settings device <parameters>

Укажите параметры команды.

Параметр	Описание
sip	Включение или отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: Admin@nodename# set settings device sip enabled • on; • off. По умолчанию модуль выгружен. Для разрешения передачи медиа-трафика напрямую между конечными участниками разговора: Admin@nodename# set settings device sip direct-media • on; • off **Важно!**После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (нажать «Принудительно применить» в разделе «Политики сети» → «Межсетевой экран»).
h323	Включение или отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • on; • off. По умолчанию модуль выгружен

Параметр	Описание
sunrpc	Включение или отключение загрузки модуля SunRPC: • on; • off. По умолчанию модуль выгружен
ftp-alg	Включение или отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • on; • off. **Важно!**Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен
auth-type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • ah — включение подписи; • pass — отключение проверки
fw-drop-invalid	Включение или отключение блокировки пакетов с некорректным набором параметров в полях заголовка: • on; • off. По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной
fw-established	Включение или отключение создания одного общего правила межсетевого экрана для обратных пакетов: • on; • off. По умолчанию настройка выключена
bypass-optimization	Включение или отключение оптимизации инспектирования SSL: • on; • off. При включённом параметре bypass-optimization для снижения нагрузки на прокси-сервер инспекция SSL не будет происходить, если на узле нет запрещающих правил инспектирования SSL. При этом в журнале веб-доступа при включённой опции журналирования будет присутствовать только информация уровней L3/L4. По умолчанию настройка выключена

Команда для просмотра текущих параметров:

Admin@nodename# show settings device

Настройка управления устройством

Настройка диагностики

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

Параметры диагностики задаются на уровне settings loglevel.

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

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

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

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

Для просмотра состояния уровня детализации диагностики используется команда:

Admin@nodename# show settings loglevel

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

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

Для просмотра состояния удаленного помощника используется команда:

Admin@nodename# show settings radmin

Режим emergency

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

Команда входа в режим emergency CLI выглядит следующим образом:

ssh Admin@emergency@<SWG_IP> -p 2200

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

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

В команде указываются следующие сетевые параметры:

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

В режиме emergency доступна команда возврата устройства в первоначальное состояние:

Admin@emergency@SWG# execute factory-reset

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

Настройка получения обновлений

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

Канал обновлений устанавливается с помощью команды:

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

Для просмотра наличия обновлений и выбранного канала обновления используется команда:

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

Управление резервным копированием

Правила резервного копирования создаются на уровне settings device-mgmt.

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

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

Параметры правил резервного копирования.

Параметр	Описание
enabled	Включение или отключение правила создания резервной копии устройства
name	Название правила резервного копирования
description	Описание правила резервного копирования
type	Выбор типа удаленного сервера для экспорта файлов: • ssh; • ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере

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

Для изменения существующего правила резервного копирования используется команда:

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

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

Для удаления правила резервного копирования используется команда:

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

Для просмотра параметров правила резервного копирования используется команда:

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

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

Экспорт параметров

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

Для создания правила экспорта параметров используется команда:

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

Параметры правила экспорта.

Параметр	Описание
enabled	Включение или отключение правила экспорта параметров устройства
name	Название правила экспорта
description	Описание правила экспорта
type	Тип удаленного сервера для экспорта параметров: • ssh; • ftp
address	IP-адрес удаленного сервера
port	Порт сервера
login	Учетная запись на удаленном сервере
password	Пароль учетной записи на удаленном сервере
path	Путь на сервере, куда будут выгружены параметры

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

Для изменения существующего правила экспорта параметров устройства используется команда:

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

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

Для удаления правила экспорта параметров используется команда:

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

Для просмотра параметров правила экспорта используется команда:

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

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

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации устройства от изменения используется команда:

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

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

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

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

Для просмотра текущего режима защиты конфигурации от изменений используется команда:

Admin@nodename# show settings change-control config

Настройка защиты исполняемых файлов от изменения

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

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

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

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

Для просмотра текущего режима защиты исполняемых файлов используется команда:

Admin@nodename# show settings change-control code

Настройка режима ускоренной обработки сетевого трафика

Для включения или отключения режима ускоренной обработки трафика используется команда:

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

Для просмотра параметров режима ускоренной обработки трафика используется команда:

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

Version: 7.5.x
Product: SWG

Настройка кластера конфигурации

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

Для изменения параметров существующего узла кластера используется команда:

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

Доступно изменение следующих параметров:

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

Команды для удаления и отображения параметров узла кластера:

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

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

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

Настройка кластера отказоустойчивости

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

Для создания кластера отказоустойчивости используется команда:

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

Далее необходимо задать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • on, • off
name	Название кластера отказоустойчивости
description	Описание кластера отказоустойчивости
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
delivery-mode	Выбор режима отправки служебного трафика: • Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. • Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
virtual-ips	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • ip — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask); • ha-interfaces — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)

Параметр	Описание
mode	Выбор режима работы кластера: • active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен); • active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
advertise-time	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
master-down-timer	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
preemption-delay	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
use-vmac	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
no-preempt	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
heartbeat	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
ha-cluster-multicast-id	<num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически
session-sync	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
vrid	Идентификатор виртуального маршрутизатора (VRID)
node-sync	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
unicast-sync-ip	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-sync-port	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-ip	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-port	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
track-interfaces-enabled	Включение/отключение проверки интерфейсов

Параметр	Описание
track-interfaces	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • change-priority — понизить приоритет узла кластера. • fault — считать узел недоступным

Пример команды создания кластера отказоустойчивости:

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

Команда для редактирования параметров кластера:

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

Команда для настройки кластера отказоустойчивости в облачной среде Yandex Cloud

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

Параметры для редактирования:

Параметр	Описание
heartbeat	Указание интерфейсов кластера, по которым будет проходить многоадресная передача сообщений синхронизации сессий и VRRP-объявлений (мультикастовый режим). По умолчанию для отправки VRRP-объявлений назначены интерфейсы кластера конфигурации
mode	Выбор режима работы кластера: • active-passive: режим работы «активный — пассивный» (трафик обрабатывается только мастер-узлом и переводится на резервный узел в случае, если основной недоступен). • active-active: режим работы «активный — активный» (нагрузка распределяется мастер-узлом на остальные узлы кластера)
name	Название кластера отказоустойчивости
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости
delivery-mode	Выбор режима отправки служебного трафика: • Multicast — многоадресная передача сообщений синхронизации сессий и VRRP-объявлений. • Unicast — одноадресная передача сообщений синхронизации сессий и VRRP-объявлений между мастер-узлом и резервным узлом. При выборе этого способа передачи следует указать IP-адреса и интерфейсы, по которым будет происходить общение между узлами. Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
enabled	Включение/отключение кластера отказоустойчивости: • on, • off
description	Описание кластера отказоустойчивости
virtual-ips	Задание общего виртуального IP-адреса интерфейсам узлов кластера, находящимся в одной зоне: • ip — задание IP-адреса для кластера отказоустойчивости (указывается в формате IP/mask); • ha-interfaces — задание интерфейсов для узлов кластера (указываются в формате node-name/interface)
advertise-time	Выбор интервала в секундах между VRRP-объявлениями, в которых мастер-узел сообщает остальным узлам о своем состоянии. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 120
master-down-timer	Выбор количества интервалов, в течение которых резервный узел не получает подтверждения того, что мастер-узел находится в сети. Один из параметров переключения роли мастер-узла на резервный узел. По достижении этого значения начнется переключение роли мастер-узла на резервный узел. Можно указывать значения от 0 до 100
preemption-delay	Указание времени, на которое будет задержано переключение роли после того, как приоритет мастер-узла понизится. Один из параметров переключения роли мастер-узла на резервный узел. Можно указывать значения от 0 до 900
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный

Параметр	Описание
use-vmac	Назначение/отключение виртуального MAC-адреса кластера узлу с ролью мастер-узла. Может назначаться, если назначены виртуальные IP-адреса и выбран режим работы кластера «активный — пассивный»
allow-non-vip-traffic	Включение/отключение обработки транзитного трафика резервным узлом. Отключение транзита трафика доступно только в режиме работы кластера «активный — пассивный
no-preempt	Управление переключением мастер-роли на резервный узел. Если включено, понижение приоритета мастер-узла учитываться не будет, а переключение мастер-роли на резервный узел будет происходить только в случае, если основной узел выйдет из строя
master-node	Назначение мастер-узла кластера отказоустойчивости
ha-cluster-multicast-id	<num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически
session-sync	Включение/отключение синхронизации пользовательских сессий между узлами кластера по протоколам TCP, SCTP, DCCP
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии
vrid	Идентификатор виртуального маршрутизатора (VRID)
node-sync	Выбор интерфейсов, через которые будет выполняться синхронизация пользовательских сессий в мультикастовом режиме. В свойствах зоны, в которой находятся выбранные интерфейсы, необходимо разрешить синхронизацию сессий.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий. Доступно для мультикастового режима
unicast-sync-ip	Указание IP-адресов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-sync-port	Указание интерфейсов, по которым будет происходить одноадресная передача сообщений между мастер-узлом и резервным узлом (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-ip	Указание IP-адресов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
unicast-vrrp-port	Указание интерфейсов, по которым будет происходить обмен VRRP-объявлениями между узлами кластера (юникастовый режим). Доступно только в режиме работы кластера «активный — пассивный» после выбора узлов кластера
track-interfaces-enabled	Включение/отключение проверки интерфейсов
track-interfaces	Выбор действия в случае недоступности интерфейса (доступно, если включена проверка интерфейсов): • change-priority — понизить приоритет узла кластера. • fault — считать узел недоступным

Параметр	Описание
checkers	Настройка диагностики узлов кластера. Проверка доступности шлюзов • gateway-availability — проверка доступности шлюзов: ◦ enabled — включение/включение/отключение проверки доступности шлюзов. Чтобы помимо проверки самих шлюзов также выполнялась проверка доступа в интернет, необходимо включить проверку сети. ◦ action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). ◦ fall-count — количество последовательных неудовлетворительных результатов проверки, после которых шлюз признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ interval-time — регулярная проверка шлюзов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ rise-count — количество последовательных положительных результатов проверки, подтверждающее, что работоспособность шлюза восстановлена и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. • resource-availability — проверка доступности ресурсов: ◦ enabled — включение/включение/отключение проверки доступности ресурсов. ◦ action — выбор действия в случае неудовлетворительных результатов проверки (change-priority — понизить приоритет узла кластера, fault — считать узел недоступным). ◦ fall-count — количество последовательных неудовлетворительных результатов проверки, после которых узел признается недоступным или приоритет узла понижается. Можно указывать значения от 0 до 10. ◦ interval-time — регулярная проверка ресурсов через указанный промежуток времени. Можно указывать значения от 0 до 300. ◦ rise-count — количество последовательных положительных результатов проверки, подтверждающее, что доступ к ресурсу восстановлен и узел можно признать доступным или повысить его приоритет. Можно указывать значения от 0 до 10. ◦ resources — указание IP-адресов или FQDN тех ресурсов, доступ к которым будет проверяться
cloud	Параметры кластера: • destination-prefix — укажите префикс маршрута по умолчанию для таблицы статической маршрутизации Yandex Cloud. • next-hops — IP-адреса интерфейсов узлов кластера. • route-table-id — идентификатор созданной ранее таблицы статической маршрутизации Yandex Cloud

Примеры редактирования настроек кластера:

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

Для удаления кластера:

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

Также доступно удаление отдельных параметров:

- nodes,
- virtual-ips.

Для отображения информации о всех кластерах отказоустойчивости:

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

Для отображения информации об определённом кластере:

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

Настройка управления доступом к консоли UserGate SWG

Version: 7.5.x
Product: SWG

Настройка управления доступом к консоли UserGate SWG выполняется на уровне settings administrators. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Настройка общих параметров доступа выполняется на уровне settings administrators general.

Для изменения параметров используется команда:

Admin@nodename# set settings administrators general <parameters>

Параметры, доступные для редактирования.

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

Пример редактирования параметров учетных записей:

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

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

Admin@nodename# show settings administrators general

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

Настройка учётных записей администраторов

Учётные записи администраторов настраиваются на уровне settings administrators administrators.

Для создания учётной записи администратора используется команда:

Admin@nodename# create settings administrators administrators <parameters>

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

Параметр	Описание
local	Добавить локального администратора: • enabled: включение/отключение учётной записи администратора: ◦ on; ◦ off. • login: логин администратора; • description: описание учётной записи администратора; • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее; • password: пароль администратора
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on; ◦ off. • login: логин администратора в формате domain\user; • connector: название сконфигурированного ранее LDAP-коннектора; • description: описание учётной записи администратора; • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • enabled: включение/отключение учётной записи администратора: ◦ on; ◦ off. • login: логин администратора; • connector: название используемого LDAP-коннектора; • description: описание учётной записи администратора; • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • enabled: включение/отключение учётной записи администратора: ◦ on; ◦ off. • login: логин администратора; • description: описание учётной записи администратора; • admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее; • auth-profile: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации

Для редактирования параметров профиля используется команда:

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

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Команда для отображения информации о всех учётных записях администраторов:

Admin@nodename# show settings administrators administrators

Команда для отображения информации об определённой учётной записи администратора:

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

Пример выполнения команды:

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

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

Команда для удаления учётной записи:

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

Пример команды:

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

Настройка прав доступа профилей администраторов

Права доступа профилей администраторов настраиваются на уровне settings administrators profiles.

Для создания профиля администратора используется следующая команда:

Admin@nodename# create settings administrators profiles <parameters>

Далее необходимо указать следующие параметры.

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

Команда для редактирования профиля:

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

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Команда для просмотра информации о всех профилях администраторов:

Admin@nodename# show settings administrators profiles

Команда для отображения информации об определённом профиле:

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

Команда для удаления профиля администратора:

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

Управление сессиями администраторов

Просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий выполняется на уровне settings administrators admin-sessions.

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

Admin@nodename# show settings administrators admin-sessions

Для отображения сессий доступно использование фильтра:

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

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

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

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

Пример выполнения команд:

Admin@nodename# show settings administrators admin-sessions

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

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

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

Admin@nodename# show settings administrators admin-sessions

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

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

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

Настройка сертификатов

Version: 7.5.x
Product: SWG

Управление сертификатами выполняется на уровне settings certificates.

Для импорта сертификатов используется команда:

Admin@nodename# import settings certificates <parameters>

Далее необходимо указать параметры.

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

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

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

С использованием командной строки возможно создание сертификата и CSR:

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

Далее необходимо указание следующие параметры.

Параметр	Описание
name	Название сертификата.

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

Команда для управления сертификатом:

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

Доступные параметры.

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

Команда для удаления сертификата:

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

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

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

Чтобы удалить сертификат из кэша используется команда:

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

Настройка прокси-сервера

Version: 7.5.x
Product: SWG

Команды для просмотра и настройки параметров прокси-сервера доступны на уровне settings proxy.

Вы можете настроить такие параметры, как добавление заголовков HTTP — via и forwarded, а также настройки тайм-аутов на подключение к сайтам и на загрузку контента.

Для изменения параметров прокси-сервера используется команда:

Admin@nodename# set settings proxy <parameters>

Параметр	Описание
via	Добавление HTTP заголовков Via: • **on**. • **off**. По умолчанию отключено
forwarded	Добавление HTTP заголовков Forwarded: • **on**. • **off**. По умолчанию отключено
xforwarded	Добавление HTTP заголовков X-Forwarded-For: • **on**. • **off**. По умолчанию отключено
connection-timeout	Время ожидания, выделяемое на подключение HTTP. По умолчанию — 20 секунд
loading-timeout	Время ожидания, выделяемое на загрузку контента HTTP. По умолчанию — 60 секунд
smode	Режим SYN Proxy: • **on**. • **off**. По умолчанию режим включен
icap-wait-timeout	Время, которое сервер UserGate ждет ответа от ICAP-сервера; указывается в секундах. Значение по умолчанию — 10 секунд
proxy_host_rfc	Доступно: • **relaxed** — использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • **strict** — соблюдать RFC. Данный режим используется по умолчанию.

Команда для просмотра текущих параметров:

Admin@nodename# show settings proxy

Настройка работы с вышестоящими прокси-серверами

Version: 7.5.x
Product: SWG

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

Настройка состоит из следующих основных шагов:

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

Настройка подключения к вышестоящему прокси-серверу

Для создания подключения к вышестоящему прокси-серверу используется команда:

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

Параметры для настройки подключения.

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

Команда для редактирования параметров ранее созданного подключения к вышестоящему прокси-серверу:

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

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

Команда для просмотра настроек ранее созданного подключения:

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

Команда для удаления ранее созданное подключения к вышестоящему прокси-серверу:

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

Создание профиля подключения

Для создания профиля подключения к вышестоящему прокси-серверу используется команда:

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

Параметры для настройки профиля.

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

Команда для редактирования параметров ранее созданного профиля подключения к вышестоящему прокси-серверу:

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

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

Команда для просмотра настройки ранее созданного профиля:

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

Команда для удаления ранее созданного профиля:

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

Создание правила вышестоящего прокси

Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе « UserGate Policy Language ».

Команда для создания правила подключения к вышестоящему прокси-серверу:

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

Команда для редактирования ранее созданных правил:

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

Команда для просмотра ранее созданных правил:

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

Команда для удаления ранее созданных правил:

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

Параметры для настройки правил.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: • enabled(yes) или enabled(true) — включение правила; • enabled(no) или enabled(false) — отключение правила
name	Название правила. Например, name("Rule 1")

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

Настройка активации лицензии и обновления ПО

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

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

Дополнительные параметры команды.

Параметр	Описание

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

Команда для просмотра созданных настроек активации лицензии и обновления ПО узла UserGate через внешний прокси-сервер:

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

Подробнее о функциональности Upstream Proxy, сценариях использования и настройках в веб-консоли администратора — в разделе « Настройка работы с вышестоящими прокси-серверами».

Настройка параметров мониторинга устройства

Version: 7.5.x
Product: SWG

Настройка параметров мониторинга устройства в интерфейсе командной строки выполняется в режиме конфигурации на уровне monitoring.

Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений — в разделе «Оповещения».

Настройка параметров SNMP устройства

Параметры SNMP устройства настраиваются на уровне monitoring snmp-parameter.

Для настройки параметров используется команда:

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

Далее необходимо указать следующие параметры.

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

Подробнее о параметрах SNMP устройства UserGate — в разделе « SNMP».

Настройка правил мониторинга по SNMP

Правила мониторинга устройства по SNMP настраиваются на уровне monitoring snmp.

Для создания правила используется команда:

Admin@nodename# create monitoring snmp <parameters>

Далее необходимо указать следующие параметры.

Параметр	Описание
name	Название правила
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3

Параметр	Описание
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений
security-profile	Только для SNMP v3. Подробнее — в разделе « Профили безопасности SNMP »
events	Выбор типов параметров, доступных для мониторинга по правилу.

Команда для изменения параметров ранее созданного правила:

Admin@nodename# set monitoring snmp <rule-name>

Для работы SNMP-менеджера с UserGate SWG необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис SNMP в настройках контроля доступа. Подробнее о настройке зон в CLI — в разделе «Настройки сети».

Настройка профилей безопасности SNMP

Профили безопасности для аутентификации SNMP-менеджеров настраиваются на уровне monitoring snmp-security-profile.

Для создания профиля используется команда:

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

Далее необходимо указать следующие параметры.

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

Команда для изменения параметров ранее созданного профиля:

Admin@nodename# set monitoring snmp-security-profile <profile-name>

Настройка правил оповещений

Правила оповещений настраиваются на уровне monitoring alert-rules.

Для создания правила оповещения используется команда:

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

Далее необходимо указать следующие параметры.

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

Команда для изменения параметров ранее созданного правила:

Admin@nodename# set monitoring alert-rules <rule-name>

Настройка захвата пакетов

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

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

Pcap-фильтры настраиваются на уровне monitoring pcap-filter.

Для создания pcap-фильтра используется команда:

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

Команда для изменения параметров ранее созданного фильтра:

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

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

Pcap-правила настраиваются на уровне monitoring pcap-rule.

Для создания правила используется команда:

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

Команда для изменения параметров ранее созданного правила:

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

Настройка профилей клиентских сертификатов

Version: 7.5.x
Product: SWG

Профили клиентских сертификатов настраиваются на уровне settings certificate-profiles.

Для создания профиля клиентского сертификата используется команда:

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

Далее необходимо указать следующие параметры.

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

Команды для просмотра ранее созданных профилей клиентских сертификатов:

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

Команда для изменения параметров ранее созданного профиля:

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

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

Команда для удаления ранее созданного профиля:

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

Настройка параметров управления телеметрией

Version: 7.5.x
Product: SWG

Параметры управления телеметрией устройства настраиваются на уровне settings telementry.

Для редактирования параметров используется команда:

Admin@nodename# set settings telemetry <parameters>

Далее необходимо указать следующие параметры.

Параметр	Описание
enabled	Включение или отключение сбора телеметрии на устройстве: • on, • off. По умолчанию сбор телеметрии включен
hide-sensitive-data	Включение или отключение функции сокрытия персональных данных в телеметрии: • on, • off. По умолчанию функция отключена

Команда для просмотра текущих параметров:

Admin@nodename# show settings telemetry