Table of Contents

Table of Contents 1
Общие положения 2
Общие положения 3

Общие положения

Product: SWG
Version: 7.5.x

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

С помощью CLI вы можете:

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

Подключение к интерфейсу командной строки

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

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

Для подключения с помощью монитора и клавиатуры:

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

Для подключения с помощью консольного порта:

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

Для подключения с помощью протокола SSH:

1. Разрешите доступ для протокола CLI по SSH в параметрах зоны, к которой вы собираетесь подключаться (доступ по порту TCP 2200). Подробнее о настройке зоны в CLI — в разделе «Зоны».
2. Запустите на компьютере SSH-терминал, например SSH для Linux или Putty для Windows.
3. Укажите IP-адрес устройства, порт для подключения (по умолчанию — 2200), имя пользователя с правами администратора (по умолчанию — Admin).

   Пример команды подключения для Linux: ssh Admin@<IP-address> -p 2200.
3. Войдите в CLI, используя пароль пользователя, указанного на предыдущем шаге.

Для подключения к CLI по SSH поддерживаются следующие алгоритмы:

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

Режимы работы интерфейса командной строки

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

После авторизации вы попадаете в режим диагностики.

В режиме диагностики доступны команды:

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

Приглашение командной строки в режиме диагностики имеет следующий вид:

Admin@nodename>

Настройка параметров устройства выполняется в режиме конфигурации.

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

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

Если система находится в состоянии до первичной инициализации, в CLI доступны команды режима диагностики и ограниченный набор команд режима конфигурации, позволяющий выполнить настройку сетевых параметров устройства. Приглашение командной строки в режиме диагностики по умолчанию имеет вид: <user-name>@<product-type>> (например, Admin@SWG>), а в режиме конфигурации — <user-name>@<product-type># (например, Admin@SWG#). Подробнее — в разделе «Команды, доступные до первичной инициализации узла».

Если система находится в аварийном состоянии, для восстановления рабочего состояния в неё можно войти в режиме emergency под учетной записью корневого администратора, которая была создана при инициализации устройства. Обычно это учетная запись Admin. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора. Приглашение командной строки в режиме emergency по умолчанию имеет вид: <user-name>@emergency@<product-type># (например, Admin@emergency@SWG#). Подробнее о режиме emergency — в разделе « Настройка устройства».

Формат команд

Команды интерфейса командной строки имеют следующий формат:

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

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

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

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

В интерфейсе командной строки поддерживается последовательное исполнение нескольких команд, вставленных из буфера обмена. Исключением являются многострочные команды, например команды, написанные с помощью синтаксиса UPL. Импортировать многострочные команды можно с помощью команды import.

Фильтрация вывода команд

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

Фильтрация может применяться к различных типам команд просмотра, включая:

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

Формат команд с фильтрацией вывода:

<cli-command> | grep <pattern> -f <include|exclude> -BA <Num>:<Num>

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

Пример фильтрации вывода команд просмотра состояния интерфейсов:

```
Admin@nodename> show network interface

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

Пример фильтрации вывода команд поиска правил межсетевого экрана:

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

```
    enabled(false) \
    name("VPN for remote access to Trusted and Untrusted")
--------------------------------------------------
    src.zone = "VPN for Site-to-Site" \
    dst.zone = (Untrusted, Trusted) \
    desc("Example firewall rule which allows traffic from VPN for Site-to-Site zone to Trusted and Untrusted zones. This is an example rule which can be changed or deleted if necessary.") \
    enabled(false) \
    name("VPN for Site-to-Site to Trusted and Untrusted")
--------------------------------------------------
```

Пример фильтрации вывода команды просмотра событий журнала:

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

Пример фильтрации вывода команды с динамическим выводом:

```
Admin@nodename> show traffic capture | grep ICMP

  92 0.305709456 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping) request  id=0x0e30, seq=3/768, ttl=30
  93 0.305739062 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping) reply    id=0x0e30, seq=3/768, ttl=64 (request in 92)
 706 1.329727201 172.26.147.146 → 172.26.147.145 ICMP 100 Echo (ping) request  id=0x0e30, seq=4/1024, ttl=30
 707 1.329755455 172.26.147.145 → 172.26.147.146 ICMP 100 Echo (ping) reply    id=0x0e30, seq=4/1024, ttl=64 (request in 706)
```

Горячие клавиши

В интерфейсе командной строки вы можете использовать следующие горячие клавиши:

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

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

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

Например:

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