

Table of Contents

Table of Contents	1
Настройка удалённого доступа (VPN)	2
Настройка серверных правил	3
Настройка клиентских правил	5
Настройка сетей VPN	7
Настройка профилей безопасности VPN	7

Настройка удалённого доступа (VPN)

Настройка серверных правил

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

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

При настройке необходимо указать:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания.
name	Название серверного правила VPN. Например: name("VPN server rule example") .
desc	Описание правила. Например: desc("VPN server rule example configured in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
vpn_network	Сеть VPN. Для указания сети: vpn_network("VPN network example") . О настройках сети VPN с использованием интерфейса командной строки читайте в разделе Настройка сетей VPN .
auth_profile	Профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль аутентификации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Чтобы указать профиль аутентификации: auth_profile("Example user auth profile") . Подробнее о создании и настройке профилей аутентификации с использованием интерфейса командной строки читайте в разделе Настройка профилей аутентификации .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel1) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
src.zone	Зона, с которой разрешено принимать подключения к VPN. Для указания зоны источника, например, Untrusted: src.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов, с которых разрешено принимать подключения к VPN. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .

Параметр	Описание
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов интерфейса, на который будет происходить подключение клиентов. Для указания списка IP-адресов: dst.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов.

Настройка клиентских правил

Documentation: ☒

Product: UserGate NGFW

Version: 7.0.1

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

При настройке правил необходимо указать:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название клиентского правила VPN. Например, name("VPN client rule example") .
desc	Описание клиентского правила VPN. Указывается, как desc("VPN client rule example set in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel1) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
server_address	IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на сервере UserGate, выполняющего роль VPN-сервера. Задаётся в формате: server_address("1.2.3.4") .
service	Протокол VPN: • l2tp — L2TP. • cisco cryptomap — IPsec туннель. Указывается в формате: service = l2tp или service = "cisco cryptomap" .
subnet1	IP-адрес подсети, разрешённой со стороны UserGate; указывается в формате: subnet1("ip/mask") . Подсети указываются при выборе протокола VPN: IPsec туннель.
subnet2	IP-адрес подсети, разрешённой со стороны Cisco; указывается в формате: subnet2("ip/mask") . Подсети указываются при выборе протокола VPN: IPsec туннель.
user	Имя пользователя для авторизации сервера, выступающего в качестве клиента VPN. Указывается только для протокола L2TP в формате user() ; имя пользователя указывается в скобках.
password	Пароль пользователя VPN. Указывается только для протокола L2TP в формате password() ; пароль указывается в скобках.

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

Настройка сетей VPN

Documentation: 

Product: UserGate NGFW

Version: 7.0.1

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

Для создания сети VPN необходимо использовать следующую команду:

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

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название VPN-сети.
description	Описание сети VPN.
ip-range	Диапазон IP-адресов, которые будут использованы клиентами и сервером; указывается в формате: <IP_start-IP_end>. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
mask	Маска сети, например, 255.255.255.0.
use-system-dns	Назначение клиенту DNS-серверов, которые использует UserGate: • on: использовать системных DNS-серверов. • off: не использовать системных DNS-серверов.
dns-servers	DNS-серверы, которые будут переданы клиенту.
routes-ip	Маршрут VPN. Необходимо указать IP-адрес в формате "A.B.C.D" или "A.B.C.D/m".
routes-ip-list	Маршрут VPN. Необходимо указать группу IP-адресов. Подробнее о создании групп IP-адресов через CLI читайте в разделе Настройка IP-адресов .

Следующая команда предназначена для обновления параметров сети:

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

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

Структура команды для удаления сети VPN:

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

Также можно удалить отдельные параметры сети:

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

Параметры, доступные для удаления:

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

Структура команды для отображения информации о сети VPN:

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

Настройка профилей безопасности VPN

Documentation: 

Product: UserGate NGFW

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

Для создания профиля безопасности VPN предназначена следующая команда:

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

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
ike-version	Версия протокола IKE (Internet Key Exchange), использующегося для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1 (IKEv1).
ike-mode	Режим IKE: main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
peer-auth	Аутентификация с пиром: psk — общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key).
psk	Общий ключ; должен совпадать на сервере и клиенте для успешного подключения.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. Group 1 Prime 768 bit. Group 2 Prime 1024 bit. Group 5 Prime 1536 bit. Group 14 Prime 2048 bit. Group 15 Prime 3072 bit. Group 16 Prime 4096 bit. Group 17 Prime 6144 bit. Group 18 Prime 8192 bit.

Параметр	Описание
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@UGOS# create vpn security-profile ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifsize	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Время жизни ключа может быть задано в байтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifsize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@UGOS# create vpn security-profile ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.

Установка значений профиля безопасности:

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

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

команды со структурой:

```
Admin@UGOS# set vpn security-profiles <profile-name> phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
```

```
Admin@UGOS# set vpn security-profiles <profile-name> phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
```

```
Admin@UGOS# set vpn security-profiles <profile-name> dh-groups + [ <dh-group1> <dh-group2> ... ]
```

Команда для удаления профиля безопасности:

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

Также доступно удаление следующих параметров профиля безопасности VPN:

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

Для отображения информации о профиле безопасности VPN используется следующая команда:

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


