

Table of Contents

Table of Contents	1
Удаленный доступ	2
Настройка Remote Access VPN на ОС Linux	3
Настройка VPN	5
Настройка роутера MikroTik для установки VPN-соединения с UserGate	7
Использование двухфакторной аутентификации через Контур.ID в настройках UserGate RA VPN	10
Настройка GRE over IPsec между UserGate и Cisco	13
Настройка VPN туннеля между UserGate NGFW и CheckPoint	17
Настройка VPN туннеля между UserGate и NSX Edge	25
Настройка IPsec VPN-туннеля между UserGate и Linux-сервером	28
Настройка IPsec туннеля между S-Terra Gate и UserGate NGFW	32
Настройка Site-to-Site VPN между UserGate и Cisco	35
Настройка VPN-соединения между UserGate и FortiGate	39
Настройка VPN туннеля между UserGate NGFW и Cisco ASR1002-X	42
Настройка VPN с передачей маршрутов по OSPF для своевременного переключения активного туннеля	47
Особенности настройки Site-to-Site VPN в конфигурации с кластером отказоустойчивости	50
Настройка GRE over IPsec с OSPF	51
Создание отказоустойчивого Site-to-Site VPN-соединения через сети двух провайдеров	54
Настройка VPN для удалённого доступа клиентов (Remote access VPN) при использовании двух провайдеров	56
Настройка IPsec over GRE с OSPF	59
Настройка GRE-туннеля	61
Пример настройки Remote access VPN с IPsec(IKEv2)	62
Пример настройки Remote access VPN с IPsec(IKEv2) с аутентификацией через EAP для OS Linux	74
Пример настройки Remote access VPN с L2TP/IPSec(IKEv1)	86
Пример настройки Site-to-Site VPN с IPSec(IKEv2)	96
Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1) с помощью интерфейса CLI	106
Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1)	111
L2TP VPN-подключение между UserGate и macOS	120

Product: NGFW
Version: 6.x, 7.x
Technology: VPN

Для разных дистрибутивов процедура установки VPN соединения отличается.

Для Fedora/RedHat/CentOS

Для начала необходимо установить необходимые пакеты:

```
sudo dnf install xl2tpd
sudo dnf install NetworkManager-l2tp
sudo dnf install NetworkManager-l2tp-gnome
```

Так как эти дистрибутивы используют `libreswan`, для корректной работы его нужно заменить. Для этого выполните команды:

```
sudo dnf remove libreswan
sudo dnf install strongswan
sudo service NetworkManager restart
```

Далее необходимо вывести `l2tp` из черного списка. Для этого в файле `/etc/modprobe.d/l2tp_netlink-blacklist.conf` закомментируйте следующую строку:

```
blacklist l2tp_netlink
```

Затем в файле `/etc/modprobe.d/l2tp_ppp-blacklist.conf` закомментируйте строки:

```
blacklist l2tp_ppp
```

Теперь можно переходить к созданию VPN подключения.

Для Debian/Ubuntu

Выполните следующие команды:

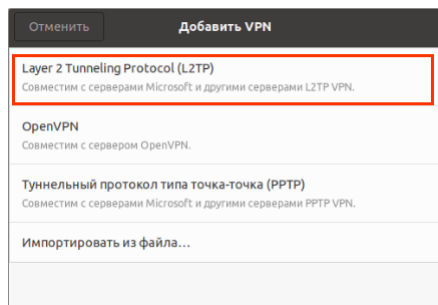
```
sudo add-apt-repository ppa:nm-l2tp/network-manager-l2tp
sudo apt update
sudo apt install network-manager-l2tp network-manager-l2tp-gnome
```

Примечание. В версиях Ubuntu ниже 22й, возможно придется обновить `xl2tpd`, для этого нужно выполнить следующие команды

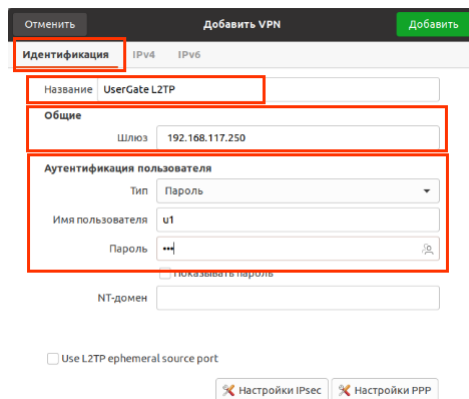
```
sudo apt remove xl2tpd
sudo add-apt-repository ppa:racb/fixes
sudo apt install xl2tpd network-manager-l2tp-gnome
```

Настройка VPN подключения через GUI (Графический интерфейс)

После выполнения команд выше появится возможность добавления L2TP VPN-подключения. Перейдите в **Настройки → Сеть**. Добавьте **Layer 2 Tunneling Protocol (L2TP)**.



Далее настройте параметры подключения и укажите данные для аутентификации:



Перейдите в настройки IPsec нажатием одноимённой кнопки. В настройках IPsec укажите:

- **Type:** Pre-shared key (PSK).
- **Pre-shared key**, указанный на UserGate.
- **Phase1 Algorithms:** aes128-sha1-modp1024!
- **Phase2 Algorithm:** aes128-sha1!

Сохраните настройки IPsec. Перейдите в настройки PPP. В качестве метода аутентификации укажите PAP и отключите все виды компрессии:

Сохраните изменения. На этом настройка Ubuntu для подключения Remote Access VPN закончена.

Настройка через командную строку (CLI)

Выполните следующие действия для настройки L2TP VPN с использованием командной строки.

1. Выполните команду

```
sudo nmcli connection add connection.id vpnName con-name vpnName type VPN vpn-type l2tp connection.autoconnect no ipv4.method auto vpn.data "gateway = server_address, ipsec-enabled = yes, ipsec-esp = "aes128-sha1!", ipsec-ike = "aes1
```

где **server_address** - IP-адрес VPN-сервера;
username - имя пользователя, выполняющего подключение;
pass - пароль учётной записи пользователя;
key - общий ключ для установления VPN-соединения.

2. Организуйте туннель с помощью следующей команды:

```
nmcli c up vpnName
```

Настройка VPN

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

UserGate позволяет создавать VPN-подключения двух типов:

- Remote access VPN - режим подключения, обеспечивающий доступ в сеть предприятия удалённым пользователям. В этом случае UserGate выступает в качестве сервера, а пользователи других устройств - клиентов VPN.
- Site-to-Site VPN - VPN для защищённого объединения офисов в одну общую сеть. В этом случае один UserGate выступает в качестве сервера, а другой - VPN-клиента.

Рассмотрим настройку серверных правил при создании на UserGate одновременно двух VPN-подключений: Remote access VPN и Site-to-Site VPN. При настройке Site-to-Site VPN настраиваемый UserGate выступает в качестве сервера. С настройкой VPN-подключений более подробно можно ознакомиться в [UserGate 6. Руководство администратора](#).

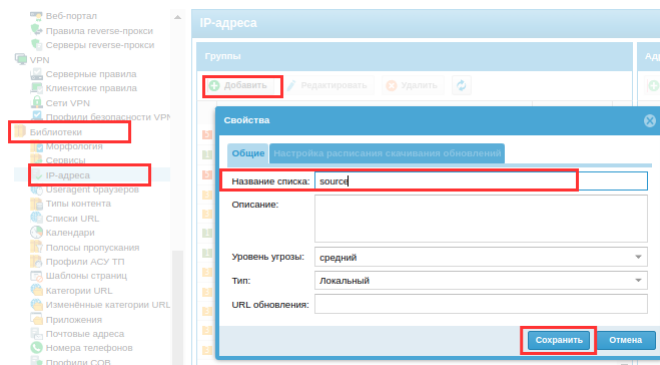
Примечание Если при настройке в свойствах серверных правил была указана одинаковая зона, то при попытке подключения на разные VPN-сервера будет срабатывать только первое (верхнее) правило, даже если в правилах были указаны разные пользователи. Такое происходит по причине того, что UserGate изначально не знает, какое правило необходимо применить для обработки запроса на подключение, потому что пользователя узнаёт в процессе установки соединения на этапе авторизации.

В таком случае нужно уточнить серверные правила. Уточнение возможно сделать по адресу/зоне источника или по адресу назначения.

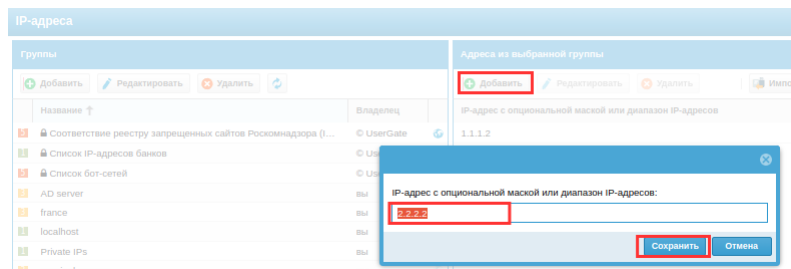
По адресу источника. Обычно Site-to-Site VPN настраивается между удалёнными офисами, роутеры которых имеют белые статические IP-адреса. Поэтому в серверном правиле для Site-to-Site VPN-подключения во вкладке **Источник** необходимо добавить IP-адрес стороны, с которой происходит подключение.

Для уточнения списка IP-адресов источника необходимо:

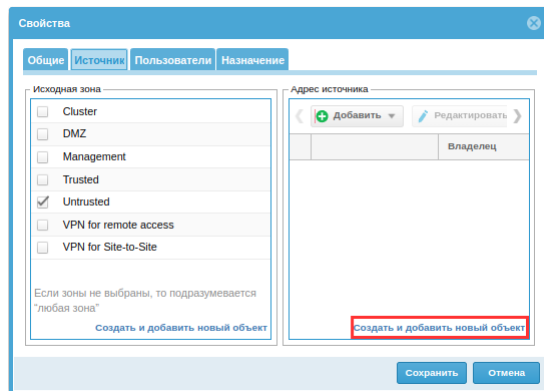
1. В разделе **Библиотеки** → **IP-адреса** создать группу.



2. В созданную группу добавить нужные IP-адреса.



Создать список IP-адресов источников также можно при настройке серверных правил во вкладке **Источник** с использованием кнопки **Создать и добавить новый объект**.

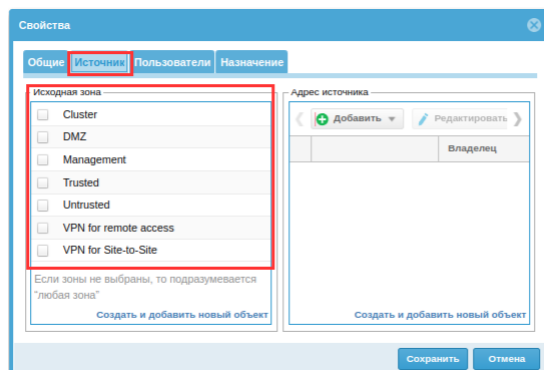


Т.к. правила выполняются по очереди сверху вниз, то данное правило необходимо поместить выше правил, в которых в качестве источника указана только зона Untrusted. Благодаря такому уточнению UserGate поймет, что VPN-соединения из зоны Untrusted от указанных IP-адресов должно происходить по правилу Site-to-Site VPN, а все другие соединения, например подключения удалённых сотрудников, будут обрабатываться следующим правилом.

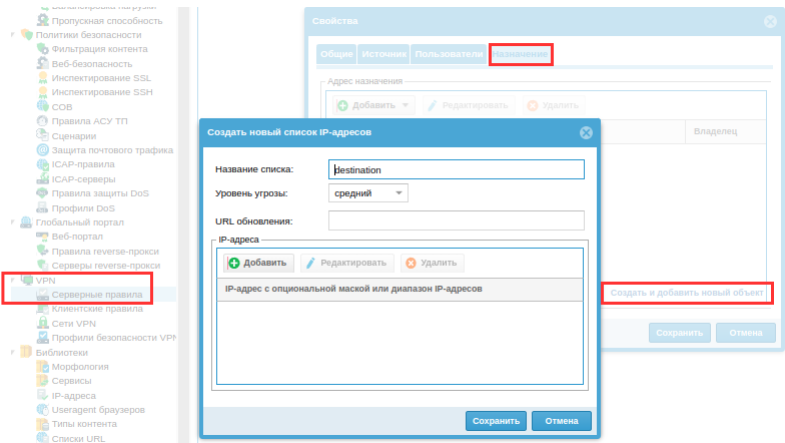
Можно сделать и наоборот: указать адреса, с которых будут происходить подключения удалённых пользователей (Remote Access VPN), если они известны.

По зоне источника. Если для выхода во внешнюю сеть используются несколько интерфейсов, то в свойствах интерфейсов в разделе **Сеть** → **Интерфейсы** во вкладке **Общие** им необходимо назначить разные зоны.

Далее в свойствах серверных правил во вкладке **Источник**, необходимо выбрать зону, из которой будет происходить подключение.



По адресу назначения. Если на внешнем интерфейсе настроены 2 и более IP-адресов, то возможно уточнение серверных правил по адресу назначения (вкладка **Назначение**) - указывается один из IP-адресов интерфейса, по которому должно происходить соединение.



Данное правило необходимо поместить наверх списка правил.

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

(Про настройку VPN на UserGate читайте в соответствующей документации: [UserGate 6. Руководство администратора](#)).

Настройка подключения L2TP VPN

Настройка роутера MikroTik с использованием WinBox.

1. В разделе **PPP → Profiles** создать профиль с обязательной настройкой USE Encryption - YES.
2. В разделе **PPP → Interfaces** добавить L2TP Client. Заполняем во вкладке **Dial Out** следующие поля:
 - **Connect To**: адрес интерфейса UserGate, через который будет происходить соединение.
 - **User**: указываем ранее созданного пользователя.
 - **Password**: пароль пользователя.
 - **Use IPsec**: да.
 - **IPsec Secret**: ввести pre-shared key, указанный при настройке UserGate.
 - **Allow**: pap.

Во вкладке **General** указываем:

- **Max MTU**: 1400.
 - **Max MRU**: 1400.
3. В разделе **IP → IPsec → Proposals** необходимо произвести настройку в соответствии с:

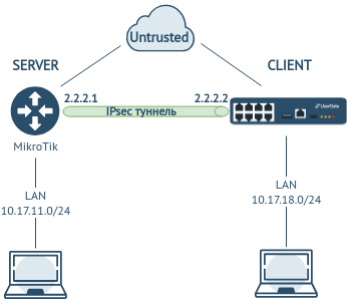
default	
Enabled	☒
Name	default
Auth. Algorithms	☒ md5 ☒ sha1 ☐ null ☐ sha256 ☐ sha512
Encr. Algorithms	☐ null ☐ des ☐ 3des ☒ aes-128 cbc ☐ aes-192 cbc ☐ aes-256 cbc ☐ blowfish ☐ twofish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256 ☐ aes-128 ctr ☐ aes-192 ctr ☐ aes-256 ctr ☐ aes-128 gcm ☐ aes-192 gcm ☐ aes-256 gcm
Lifetime	▼
PFS Group	none

4. В разделе **IP → IPsec → Profiles** необходимо произвести настройку в соответствии с:

Name	default
Hash Algorithms	sha1
Encryption Algorithm	☐ des ☒ 3des ☒ aes-128 ☐ aes-192 ☐ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256
DH Group	☐ modp768 ☐ modp1024 ☐ ec2h155 ☐ ec2h185 ☐ modp1536 ☒ modp2048 ☒ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ grp256 ☐ grp384 ☐ grp521
Proposal Check	obey
Lifetime	1d 00:00:00
Lifeytes	▼
NAT Traversal	☒
DPD Interval	120 s
DPD Maximum Failures	5

Алгоритмы авторизации и шифрования должны совпадать с алгоритмами, указанными при создании профилей безопасности на UserGate.
В данном случае алгоритмы авторизации и шифрования совпадают с алгоритмами, используемыми в настройках профиля безопасности UserGate, созданном по умолчанию.

Настройка IPsec VPN-подключения.



Файл конфигурации MikroTik доступен по [ссылке](#). Данный скрипт прописывает необходимые для UserGate настройки, также файл можно открыть с помощью текстового редактора и вручную перенести нужные настройки.

Настройка MikroTik.

1. Произвести настройку профиля IPsec; для этого перейдите в раздел **IP → IPsec → Profiles**.

Name	UG
Hash Algorithms	sha1
Encryption Algorithm	☐ des ☒ 3des ☒ aes-128 ☐ aes-192 ☐ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256
DH Group	☐ modp768 ☐ modp1024 ☐ ec2n155 ☐ ec2n185 ☐ modp1536 ☒ modp2048 ☐ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ ec256 ☐ ec384 ☐ ec521
Proposal Check	obey
Lifetime	1d 00:00:00
Lifeytes	
NAT Traversal	☒
DPD Interval	120 s
DPD Maximum Failures	5

2. Настроить IPsec-пир.

Для настройки перейдите во вкладку **IP → IPsec → Peers** и укажите адрес интерфейса UG, через который будет происходить соединение профиль, созданный ранее. Отключите параметр "Send INITIAL_CONTACT".

Enabled	☒
Name	peer1
Address	2.2.2.2/32
Port	
Local Address	2.2.2.1
Profile	UG
Exchange Mode	main
Passive	☐
Send INITIAL_CONTACT	☐

3. Указать общий ключ.

Чтобы указать общий ключ, перейдите во вкладку **IP → IPsec → Identities** (укажите общий ключ в поле **Secret**):

Enabled	☒
Peer	peer1
Auth. Method	pre shared key
Secret	*****
Policy Template Group	default
Notrack Chain	
My ID Type	auto
Remote ID Type	auto
Match By	remote id
Mode Configuration	
Generate Policy	no

4. Перейдите в раздел **IP → IPsec → Proposals** для настройки параметров второй фазы согласования.

default	
Enabled	☒
Name	default
Auth. Algorithms	☒ md5 ☒ sha1 ☐ null ☐ sha256 ☐ sha512
Encr. Algorithms	☐ null ☐ des ☐ 3des ☒ aes-128 cbc ☐ aes-192 cbc ☐ aes-256 cbc ☐ blowfish ☐ twofish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256 ☐ aes-128 ctr ☐ aes-192 ctr ☐ aes-256 ctr ☐ aes-128 gcm ☐ aes-192 gcm ☐ aes-256 gcm
Lifetime	
PFS Group	none

5. Настроить политики IPsec. Политики задаются во вкладке **IP → IPsec → Policies**.

Enabled	☒
Peer	peer1
Tunnel	☒
Src. Address	10.17.11.0/24
Src. Port	
Dst. Address	10.17.18.0/24
Dst. Port	
Protocol	255 (all)
Template	☐
Action	encrypt
Level	unique
IPsec Protocols	esp
Proposal	default

6. Разрешить трафик в межсетевом экране.

	#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Src. Address List	Dst. Address List	Bytes
	0	 accept	input			50 (ipsec)										10.3 KiB
	1	 accept	input			17 (udp)		500,4500								180.7 KiB

Настройка UserGate.

1. Разрешить сервис **VPN** на зоне, через которую происходит соединение.
2. Создать или использовать созданный по умолчанию туннельный интерфейс.

Во вкладке **Сеть** настроек VPN-адаптера укажите статический IP-адрес туннельного VPN-интерфейса, используемого в правиле VPN; IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32.
3. Разрешить прохождение трафика между зонами правилом межсетевого экранами (из зоны, которой принадлежит VPN-интерфейс, в зоны Trusted и Untrusted).
4. Настроить профиль безопасности в соответствии с настройками MikroTik (алгоритмы авторизации и шифрования, общий ключ).
5. Создать клиентское правило, указав:
 - **Профиль безопасности VPN**, настроенный ранее.
 - **Интерфейс**.
 - **Адрес сервера**.
 - **Протокол VPN**: IPsec туннель.
 - **Подсети, разрешённые со стороны MikroTik и UserGate**.

Свойства

Включено:

☒

Название:

Client VPN rule

Описание:

Профиль безопасности VPN:

Site-to-Site VPN profile

Интерфейс:

tunnel2

Адрес сервера:

2.2.2.1

Протокол VPN:

IPsec туннель

Подсети для Cisco VPN

Разрешённая подсеть со стороны UserGate:

10.17.18.0/24

Разрешённая подсеть со стороны Cisco:

10.17.11.0/24

Аутентификация

Пользователь:

Пароль:

Сохранить

Отмена

В случае успешного подключения в разделе **VPN → Клиентские правила** отобразится индикатор зелёного цвета:

Client VPN rule	2.2.2.1	 tunnel2	 Site-to-Site VPN profile	
-----------------	---------	---	--	---

KnowledgeBase: 
Product: NGFW
Version: 6.x, 7.x
Technology: VPN

Ресурс Контур.ID предоставляет сервис двухфакторной аутентификации для VPN. Для реализации сервиса используется RADIUS Proxy, который интегрируется с VPN-сервером и контроллером домена AD:

Рассмотрим пример использования сервиса двухфакторной аутентификации от Контур.ID в настройках VPN удаленного доступа UserGate.

Настройки на стороне Контур.ID

1. На сайте Контур перейти в раздел **Ресурсы** и выбрать **OpenVPN**:



2. Произвести настройку конфигурации сервиса в соответствии со своими требованиями:



По окончании настройки нажать кнопку **Скачать** и сохранить файлы для запуска RADIUS Proxy.

3. Запустить сервис RADIUS Proxy на сетевом хосте согласно рекомендациям поставщика сервиса.

Настройки на стороне UserGate

1. Контроллер домена AD должен быть интегрирован с UserGate NGFW посредством LDAP-коннектора. Подробнее читайте в разделе [Серверы аутентификации](#) руководства администратора.

В свойствах LDAP-коннектора в списке доменов необходимо указать используемые домены в виде:

2. Необходимо настроить VPN для удаленного доступ в сеть согласно [описанию в руководстве администратора](#).

3. Создать сервер аутентификации RADIUS. В свойствах RADIUS-сервера указать в качестве IP-адреса сервера — IP-адрес хоста с установленным RADIUS Proxy, в качестве порта и секрета использовать значения из настроек ресурса Контур (см. [пункт 2 в настройках Контура](#)):

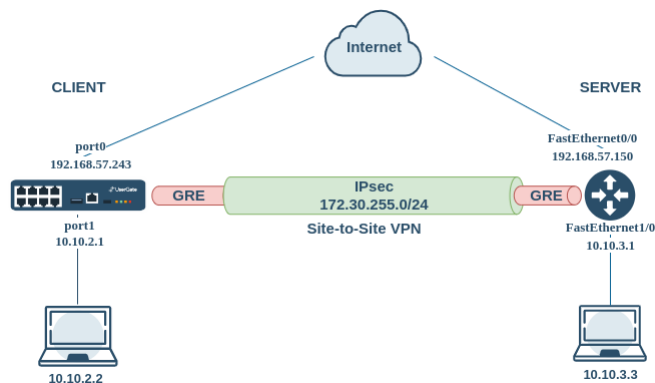
4. На UserGate NGFW создать профиль аутентификации (RADIUS-Kontur), указав в качестве метода аутентификации созданный на предыдущем шаге RADIUS-сервер KonturID:

5. В свойствах созданного ранее серверного правила VPN для удаленного доступа необходимо в качестве профиля аутентификации указать созданный на предыдущем шаге профиль RADIUS-Kontur:

Настройки завершены.

KnowledgeBase: ☒
 Product: UserGate NGFW
 Version: 6.1.8, 6.1.9

В данной статье рассматривается настройка между UserGate и Cisco зашифрованного канала связи (IPsec) с использованием GRE-туннеля.



Адресация на UserGate:

- Выход в интернет настроен через интерфейс port0 с IP-адресом 192.168.57.243 (шлюз по умолчанию: 192.168.57.1).
- Локальная сеть подключена через port1 с IP-адресом 10.10.2.1.

Адресация на Cisco:

- Выход в интернет настроен через интерфейс FastEthernet0/0 с IP-адресом 192.168.57.150 (шлюз по умолчанию: 192.168.57.1).
- Локальная сеть подключена через FastEthernet1/0 с IP-адресом 10.10.3.1.

Конфигурация IPsec на Cisco.

- Настроить интерфейс Loopback0:

```
interface Loopback0
ip address 11.11.3.1 255.255.255.0
```
- Настроить политику ISAKMP:

```
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
```
- Определить Pre-Shared ключ (указать вместо <psk>):

```
crypto isakmp key <psk> address 192.168.57.243
```
- Создать расширенный ACL:

```
ip access-list extended <list-name>
permit ip 11.11.3.0 0.0.0.255 11.11.2.0 0.0.0.255
```
- Создать набор преобразований (Transform Set):

```
crypto ipsec transform-set <TS-name> esp-aes esp-sha-hmac
mode tunnel
```
- Создать Crypto Map:

```
crypto map <CMAP-name> 10 ipsec-isakmp
set peer 192.168.57.243
set transform-set <TS-name>
match address <list-name>
```
- Применить Crypto Map к интерфейсу FastEthernet0/0:

```
interface FastEthernet0/0
ip address 192.168.57.150 255.255.255.0
duplex full
crypto map <CMAP-name>
```

Настройка IPsec на UserGate.

- В разделе **Сеть → Интерфейсы** добавить VPN интерфейс tunnel с произвольным номером, и назначить на него IP-адрес, например, 11.11.2.1/24. В данном случае интерфейс tunnel будет являться loopback-интерфейсом со стороны UserGate.
- Произвести настройки для VPN-подключения Site-to-Site.

Перейдите в раздел **Сеть → Интерфейсы** и активируйте интерфейс **tunnel2**. Данный интерфейс находится в зоне **VPN for Site-to-Site** и имеет IP-адрес 172.30.255.1/24.

Далее необходимо произвести настройку профиля безопасности в разделе **VPN → Профили безопасности VPN**. Можно создать новый профиль безопасности или использовать созданный по умолчанию (**Client VPN profile**).

Во вкладке **Общие** укажите:

- Название** профиля безопасности VPN.
- Описание** (опционально).
- IKE версия**: IKEv1.
- Режим IKE**: Основной.
- Аутентификация с пиром**: Общий ключ.
- Общий ключ**: общий ключ, указанный при настройке оборудования Cisco - <psk>.

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Название: Client VPN profile

Описание: Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be

IKE версия: IKEv1

Режим IKE: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

Во вкладке **Фаза 1**:

- **Diffie-Hellman группы**: Группа 2 Prime 1024 бит.
- **Алгоритмы авторизации и шифрования**: SHA1 - AES128.

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Время жизни ключа: 1 часов

Интервал проверки dead peer detection: 60 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

Добавить Удалить

Группа 2 Prime 1024 бит

Безопасность

Добавить Редактировать Удалить Выше Ниже

Авторизация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Во вкладке **Фаза 2**:

- **Алгоритмы авторизации и шифрования**: SHA1 - AES128.

Свойства профиля безопасности VPN

Общие Фаза 1 **Фаза 2**

Время жизни ключа: 1 часов

Максимальный размер данных, шифруемых одним ключом: Отключено

100 MB

Безопасность

Добавить Редактировать Удалить

Авторизация	Шифрование
SHA1	AES128

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Перейдите в раздел **VPN → Клиентские правила**. Для подключения можно использовать правило, созданное по умолчанию (**Client VPN rule**), или создать новое. Укажите:

- **Включено** — поставьте флажок.
- **Название** правила.
- **Описание** (опционально).
- **Профиль безопасности**, настроенный ранее.
- **Интерфейс**: tunnel2.
- **Адрес сервера**: 192.168.57.150.
- **Протокол VPN**: IPsec-туннель.
- **Разрешённые подсети со стороны UserGate**: 11.11.2.0/24.
- **Разрешённые подсети со стороны Cisco**: 11.11.3.0/24.

Настройка IPsec-туннеля между UserGate и Cisco завершена, далее настройка GRE.

Настройка GRE-туннеля на Cisco.

- Создать туннельный интерфейс и назначить ему адрес из сети 172.30.222.0/24; в качестве адреса источника укажите адрес интерфейса Loopback0 Cisco, в качестве адреса назначения — secondary адрес интерфейса UserGate **port1**:

```
interface Tunnel0
ip address 172.30.222.2 255.255.255.0
tunnel source 11.11.3.1
tunnel destination 11.11.2.1
```
- Добавить статический маршрут в сеть 10.10.2.0/24 со шлюзом 172.30.222.1:

```
ip route 10.10.2.0 255.255.255.0 172.30.222.1
```

Настройка GRE-туннеля на UserGate.

- Перейдите в раздел **Сеть** → **Интерфейсы** нажмите **Добавить** и выберите **Добавить туннель**.
- Во вкладке **Общие** укажите:
 - Порядковый номер туннельного интерфейса.
 - Описание** (опционально).
 - Зону**, которой будет относиться интерфейс: VPN for Site-to-Site.

Перейдите во вкладку **Сеть** и задайте следующие параметры (в качестве локального и удалённого IP-адресов используются IP-адреса VPN-интерфейсов):

- MTU**.
- Локальный IP**: 11.11.2.1 - IP-адрес loopback-интерфейса со стороны UserGate.
- Удалённый IP**: 11.11.3.1 - IP-адрес loopback-интерфейса со стороны Cisco.
- Режим**: GRE.
- IP-адрес интерфейса и маску**: 172.30.222.1/24.

- Перейдите в раздел **Сеть** → **Виртуальные маршрутизаторы** и настройте статический маршрут в сеть с IP-адресом 10.10.3.0/24 и шлюзом 172.30.222.2.

- Создайте правило межсетевого экрана, разрешающее трафик из зоны **VPN for Site-to-Site** в зону **Trusted** и обратно.

ПРОВЕРКА.

В случае успешного подключения в разделе **VPN** → **Клиентские правила** отобразится индикатор зелёного цвета.

Клиентские правила				
Добавить Редактировать Удалить Включить Отключить				
Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN
Client VPN rule	192.168.57.150	VPN2	Client VPN profile	

Во вкладке **Диагностика и мониторинг** в разделе **Мониторинг** → **Ping** возможна проверка сетевой доступности узлов.

Проверка IPsec-туннеля на UserGate:

PING 11.11.3.1 (11.11.3.1) from 11.11.2.1 : 56(84) bytes of data.

64 bytes from 11.11.3.1: icmp_seq=1 ttl=255 time=9.59 ms
64 bytes from 11.11.3.1: icmp_seq=2 ttl=255 time=4.19 ms
64 bytes from 11.11.3.1: icmp_seq=3 ttl=255 time=8.90 ms
64 bytes from 11.11.3.1: icmp_seq=4 ttl=255 time=2.68 ms
64 bytes from 11.11.3.1: icmp_seq=5 ttl=255 time=7.62 ms
64 bytes from 11.11.3.1: icmp_seq=6 ttl=255 time=2.14 ms

--- 11.11.3.1 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 2.140/5.857/9.596/2.974 ms

Проверка IPsec-туннеля на Cisco:

R1#show crypto session
Crypto session current status
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 192.168.57.243 port 500
IKEv1 SA: local 192.168.57.150/500 remote 192.168.57.243/500 Active
IPSEC FLOW: permit ip 11.11.3.0/255.255.255.0 11.11.2.0/255.255.255.0
Active SAs: 2, origin: crypto map

R1#ping 11.11.2.1 source 11.11.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.2.1, timeout is 2 seconds:
Packet sent with a source address of 11.11.3.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/14/24 ms

Проверка сетевой доступности туннельного интерфейса на UserGate:

PING 172.30.222.2 (172.30.222.2) from 172.30.222.1 : 56(84) bytes of data.

64 bytes from 172.30.222.2: icmp_seq=1 ttl=255 time=10.6 ms
64 bytes from 172.30.222.2: icmp_seq=2 ttl=255 time=5.04 ms
64 bytes from 172.30.222.2: icmp_seq=3 ttl=255 time=8.96 ms
64 bytes from 172.30.222.2: icmp_seq=4 ttl=255 time=2.65 ms
64 bytes from 172.30.222.2: icmp_seq=5 ttl=255 time=7.08 ms
64 bytes from 172.30.222.2: icmp_seq=6 ttl=255 time=11.2 ms

--- 172.30.222.2 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 2.652/7.611/11.232/3.055 ms

Проверка доступности локальных шлюзов на UserGate:

PING 10.10.3.1 (10.10.3.1) from 10.10.2.1 : 56(84) bytes of data.

64 bytes from 10.10.3.1: icmp_seq=1 ttl=255 time=16.5 ms
64 bytes from 10.10.3.1: icmp_seq=2 ttl=255 time=10.6 ms
64 bytes from 10.10.3.1: icmp_seq=3 ttl=255 time=5.23 ms
64 bytes from 10.10.3.1: icmp_seq=4 ttl=255 time=9.93 ms
64 bytes from 10.10.3.1: icmp_seq=5 ttl=255 time=3.65 ms
64 bytes from 10.10.3.1: icmp_seq=6 ttl=255 time=7.37 ms

--- 10.10.3.1 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 3.656/8.893/16.546/4.197 ms

Проверка доступности конечных узлов:

C:\Users\admin>ping 10.10.3.3 -S 10.10.2.2

Обмен пакетами с 10.10.3.3 по с 10.10.2.2 с 32 байтами данных:

Ответ от 10.10.3.3: число байт=32 время=17мс TTL=62

Ответ от 10.10.3.3: число байт=32 время=20мс TTL=62

Ответ от 10.10.3.3: число байт=32 время=21мс TTL=62

Ответ от 10.10.3.3: число байт=32 время=21мс TTL=62

Статистика Ping для 10.10.3.3:

Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)

Приблизительное время приема-передачи в мс:

Минимальное = 17мсек, Максимальное = 21 мсек, Среднее = 19 мсек

Настройка VPN туннеля между UserGate NGFW и CheckPoint

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.x, 7.x
Technology: VPN

Описание

Рассмотрим ситуацию, при которой необходимо объединить две сети, одна из которых защищена с помощью UserGate NGFW, а другая - с помощью CheckPoint.
В данном примере предполагается использование следующих адресов:

- Адрес сети, защищенной UserGate NGFW: 172.21.10.0/24.
- IP-адрес внешнего интерфейса UserGate NGFW: 91.107.67.230.
- Адрес сети, защищенной CheckPoint: 10.10.10.0/24.
- IP-адрес внешнего интерфейса CheckPoint: 91.107.67.228.

Схема сети



Настройка на стороне CheckPoint

1. Указать параметры сетевых интерфейсов:

Name	Topology	IP
eth0	This network	10.10.10.1/24
eth1	External	91.107.67.228/29

2. Активировать блейд IPSec VPN:

Machine Name: CP, Color: Black

IPv4 Address: 10.10.10.1

Platform: Hardware: Open server, Version: R81.10, OS: Gaia

Network Security (2): Firewall, IPSec VPN

3. Выбрать внешний адрес для подключения IPsec:

IP Selection by Remote Peer

Locally managed VPN peers determine this gateway's IP address using the following method:

☒ Always use this IP address:

- ☐ Main address
- ☒ Selected address from topology table: 91.107.67.228
- ☐ Statically NATed IP:

☐ Calculate IP based on network topology

☐ Use DNS resolving:

- ☒ Full hostname:
- ☐ Gateway's name and domain name (specified in Global Properties)

☐ Use probing, Link redundancy mode:

- ☒ High Availability:
- ☐ Load Sharing:

Outgoing Route Selection

Determine the outgoing interface using one of the following methods:

When initiating a tunnel

- ☒ Operating system routing table
- ☐ Route based probing

4. Указать VPN-домен объектом локальной сети CheckPoint:

Check Point Gateway - CP

General Properties

VPN Domain

VPN Domain

All IP Addresses behind Gateway based on Topology information

User defined 10.10.10.0/24 View...

Set Specific VPN Domain for Gateway Communities: Set...

5. Создать Interoperable Device с именем UserGate:

Interoperable Device - UserGate

General Properties

Machine

Name: UserGate Color: Black

IPv4 Address: 91.107.67.230 Resolve from Name Dynamic Address

IPv6 Address:

Comment:

SmartConsole

Interoperable Devices 1

UserGate

6. Указать топологию объектом локальной сети за UserGate:

Interoperable Device - UserGate

General Properties

Topology

IPSec VPN

Type to Search

Name	Network ...	IPv4 Address	IPv4 Netmask	IPv6 Address	Topology

VPN Domain

All IP Addresses behind Gateway based on Topology information

User defined UG2_172.21.10.0/24 View...

SmartConsole

Interoperable Devices 1

UserGate

7. Добавить сетевые устройства CheckPoint и UserGate в Meshed Community:

Meshed Community

MyIntranet

Enter Object Comment

Gateways

Encrypted Traffic

Encryption

Tunnel Management

Excluded Services

Shared Secret

Wire Mode

Advanced

Participating Gateways

All the connections between the VPN Domains of the gateways below will be encrypted.

2 Items

Gateway	Gateway Comments	VPN Domain
CP		10.10.10.0/24
UserGate		UG2_172.21.10.0/24

Add Tag

OK Cancel

8. Задать параметры первой и второй фаз согласования туннеля:

Meshed Community

MyIntranet

Enter Object Comment

Gateways

Encrypted Traffic

Encryption

Tunnel Management

Excluded Services

Shared Secret

Wire Mode

Advanced

Encryption Method

Encryption Method: IKEv1 for IPv4 and IKEv2 for IPv6 only

Encryption Suite

Use this encryption suite: Suite-B-GCM-256 (AES-GCM-256, SHA-384, EC Di...

Custom encryption suite:

IKE Security Association (Phase 1)

Encryption Algorithm: AES-128

Data Integrity: SHA1

Diffie-Hellman group: Group 2 (1024 bit)

IKE Security Association (Phase 2)

Encryption Algorithm: AES-128

Data Integrity: SHA1

☐ Use Perfect Forward Secrecy

Diffie-Hellman groups: Group 2 (1024 bit)

Override Encryption for Externally Managed Gateways

+ | - | X

Search...

No items found

Internal	External	IKE Version	Ciphers
----------	----------	-------------	---------

Add Tag

OK

Cancel

Meshed Community

MyIntranet

Enter Object Comment

Gateways

Encrypted Traffic

Encryption

Tunnel Management

Excluded Services

Shared Secret

Wire Mode

Advanced

Permanent Tunnels

☐ Set Permanent Tunnels:

On all tunnels in the community

On all tunnels of specific gateways

On specific tunnels in the community

Enable Route Injection Mechanism (RIM)

Select Gateways...

Select Permanent Tunnels...

Settings...

Tunnel down track: Log

Tunnel up track: Log

VPN Tunnel Sharing

One VPN tunnel per each pair of hosts

One VPN tunnel per subnet pair

One VPN tunnel per Gateway pair

Add Tag

OK

Cancel

Meshed Community

MyIntranet

Enter Object Comment

Gateways

Encrypted Traffic

Encryption

Tunnel Management

Excluded Services

Shared Secret

Wire Mode

Advanced

Shared Secret

☒ Use only Shared Secret for all external members

Each external member will have the following with all internal members in this community

Peer Name	Shared Secret
UserGate	****

Add Tag

OK

Cancel

Meshed Community

MyIntranet

Enter Object Comment

Gateways

Encrypted Traffic

Encryption

Tunnel Management

Excluded Services

Shared Secret

Wire Mode

Advanced

IKE (Phase 1)

Renegotiate IKE security associations every (minutes): 1440

IPsec (Phase 2)

Renegotiate IPsec security associations every (seconds): 3600

Properties

Disable NAT inside the VPN community

Use aggressive mode

Support IP Compression

Reset

Reset All VPN Properties

Add Tag

OK

Cancel

9. Создать правило для взаимодействия удаленных сегментов:

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
4	vpn	10.10.10.0/24 UG2_172.21.10.0/24	10.10.10.0/24 UG2_172.21.10.0/24	MyIntranet	* Any	Accept	Log

Настройка на стороне CheckPoint завершена.

Настройка на стороне UserGate

1. В разделе **Сеть** → **Зоны** разрешить доступ по VPN для зоны Untrusted:

Свойства сетевой зоны

Общие

Контроль доступа

Защита от IP-спуфинга

Разрешённые сервисы

Разрешённые адреса

☒ Ping
☐ SNMP
☐ Captive-портал и страница блокировки
☐ Кластер
☐ VRRP
☐ Консоль администрирования
☐ DNS
☐ HTTP(S)-прокси
☐ Агент аутентификации
☐ SMTP(S)-прокси
☐ POP3(S)-прокси
☐ CLI по SSH
☒ VPN
☐ SCADA
☐ Reverse-прокси
☐ Веб-портал
☐ Log Analyzer
☐ OSPF

Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой
Любой

Сохранить

Отмена

2. В разделе **Сеть** → **Интерфейсы** создать или использовать созданный по умолчанию интерфейс VPN for Site-to-Site:

Настройка VPN-адаптера

Общие

Сеть

Включено: ☒

Название: tunnel3

Описание: Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN interface which can be changed or deleted if necessary.

Зона: VPN for Site-to-Site

Профиль netflow: Не выбран

Сохранить

Отмена

Назначить данному интерфейсу IP-адрес. IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32:

Настройка VPN-адаптера

Общие

Сеть

Режим:

Статический

MTU:

1420

IP интерфейса

Добавить

Редактировать

Удалить

IP интерфейса	Маска
169.254.0.1	255.255.255.0

Сохранить

Отмена

3. В разделе **VPN → Профили безопасности VPN** создать профиль безопасности VPN. В свойствах профиля указать общий ключ (pre-shared key) и указать параметры первой и второй фаз согласования туннеля, заданные на CheckPoint:

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Название:

CheckPoint S2S

Описание:

ИКЕ версия:

IKEv1

Режим IKE:

Основной

Аутентификация с пиром:

Общий ключ

Общий ключ:

Общий ключ (повтор):

Сохранить

Отмена

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

24

часов

Интервал проверки dead peer detection:

120

(в секундах)

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 2 Prime 1024 бит

Безопасность

Добавить

Редактировать

Удалить

Выше

Ниже

Аутентификация	Шифрование
SHA1	AES128

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить

Отмена

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

Безопасность

Добавить

Редактировать

Удалить

Выше

Ниже

Аутентификация	Шифрование
SHA1	AES128

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить

Отмена

4. В разделе **VPN → Клиентские правила** создать правило, выбрав созданный ранее профиль безопасности VPN. В поле адреса сервера указать IP-адрес внешнего интерфейса CheckPoint, через который происходит соединение. В поле протокола VPN выбрать IPsec-туннель. Далее указать разрешенные подсети со стороны UserGate и CheckPoint:

Клиентские правила

Добавить

Редактировать

Удалить

Включить

Отключить

✓

Название	Адрес сервера	Интерфейс	Профиль безопасности VPN
CheckPoint IPsec	91.107.67.228	tunnel3	CheckPoint S2S

Свойства

Общие

Включено:

✓

Название:

CheckPoint IPsec

Описание:

Профиль безопасности VPN:

CheckPoint S2S

Интерфейс:

tunnel3

Адрес сервера:

91.107.67.228

Протокол VPN:

IPsec туннель

Подсети для VPN

Локальная подсеть:

172.21.10.0/24

Удаленная подсеть:

10.10.10.0/24

Аутентификация

Пользователь:

Пароль:

Сохранить

Отмена

6. В разделе **Политики сети → Межсетевой экран** создать двустороннее правило доступа с указанием Trusted и VPN Site-to-Site зон. Разрешить трафик между Trusted и S2S:

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

✓

#	Статус журнал...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначе...
1		VPN S2S	Разрешить	Trusted VPN for Site-to-Site	Любой	Trusted VPN for Site-to-Site	Любой

Свойства правила межсетевого экрана

Общие Источник Пользователи Назначение Сервис Приложения Время Использование История

Включено:

☒

Название:

VPN S2S

Описание:

Действие:

Разрешить

Отбросить и:

Не выбран

Сценарий:

Не использовать сценарии

Журналирование:

☒ Журналировать начало сессии

Включить лимит журналирования:

☒

Ограничить число событий, записываемых в журнал:

3 / час

Максимальное количество пакетов, журналируемых на событие:

5

Применить правило к:

Все пакеты

Вставить:

Наверх списка правил

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источник Пользователи Назначение Сервис Приложения Время Использование История

Зона источника

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Tunnel inspection zone

☐ Untrusted

☐ VPN for remote access

☒ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инvertировать

Адрес источника

+ Добавить

Редактировать

Удалить

Название списка ↑

Владелец

Создать и добавить новый объект

☐ Инvertировать

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источник Пользователи Назначение Сервис Приложения Время Использование История

Зона назначения

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Tunnel inspection zone

☐ Untrusted

☐ VPN for remote access

☒ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инvertировать

Адрес назначения

+ Добавить

Редактировать

Удалить

Название списка ↑

Владелец

Создать и добавить новый объект

☐ Инvertировать

Сохранить Отмена

7. В разделе **VPN** → **Клиентские правила** включить правило CheckPoint IPsec. При успешном подключении должен гореть зеленый индикатор:

Клиентские правила

Добавить

Редактировать

Удалить

Включить

Отключить

✓

Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN
CheckPoint IPsec	91.107.67.228	tunnel3	CheckPoint S2S	
Client VPN rule	10.10.10.10	tunnel3	Client VPN profile	Подключено с: 06 июля 2022 г., 16:59

8. В разделе **Диагностика и мониторинг** → **VPN** проверить статус туннеля:

UserGate

Дашборд

Диагностика и мониторинг

Журналы и отчеты

Настройки

Гостевой портал

Помощь

Русский

Admin

Мониторинг

Мониторинг трафика

Маршруты

VPN

Веб-портал

Сеть

Захват пакетов

Запросы в белый список

Трассировка правил

VPN

utmcore@essediarfree

3 секунды

Пользователь ↑	Роль этого сервера	Время сессии	Туннельный IP	IP адрес	Geo IP	Шифрование
IPSEC tunnel	Клиент	06 июля 2022 г., 16:...	—	91.107.67.228	RU	aes128

Настройка на стороне UserGate завершена.

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.x, 7.x
Technology: VPN

Описание

Рассмотрим ситуацию, при которой необходимо объединить две сети, одна из которых защищена с помощью UserGate NGFW, а другая NSX Edge.

Предполагаем использование следующих адресов в данной ситуации:

- Адрес сети защищенной UserGate : 172.21.10.0/24.
- IP-адрес внешнего интерфейса UserGate NGFW: 91.107.67.230.
- Адрес сети защищенной NSX Edge: 192.168.1.0/24.
- IP-адрес внешнего интерфейса NSX Edge: 178.20.233.46.

Схема сети



Настройка на стороне NSX Edge

Для настройки VPN туннеля на стороне NSX Edge, необходимо в меню:

vCloud Director → Networking → EDGE → Services → VPN → IPsec VPN Sites, установить следующие значения:

Параметр	Значение
Enabled	True
PFS	False
Local ID и Local Endpoint	178.20.233.46
Local Subnets	192.168.1.0/24
Peer ID и Peer Endpoint	91.107.67.230
Peer Subnets	172.21.10.0/24
Encryption Algorithm	AES256
Authentication	PSK
Pre-Shared Key	*****
Diffie-Hellman Group	DH14
Digest Algorithm	SHA-256
IKE Option	IKEv1
Session Type	Policy Based Session

Настройка на стороне UserGate

На стороне UserGate необходимо изменить базовые настройки фаз IPsec, поскольку данные параметры зашиты в NSX Edge и не подлежат изменению.

Параметр	Значение
ikelifetime	28800s
type	tunnel
lifetime	3600s
dpddelay	30
dpdaction	restart

Порядок настройки VPN соединения на стороне UserGate следующий:

1. Разрешить сервис **VPN** на зоне, через которую происходит соединение.
 2. Создать или использовать созданный по умолчанию туннельный интерфейс.
Во вкладке **Сеть** настроек VPN-адаптера указать статический IP-адрес туннельного VPN-интерфейса, используемого в правиле VPN; IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32.
 3. Разрешить прохождение трафика между зонами правилом межсетевого экранами (из зоны, которой принадлежит VPN-интерфейс, в зоны Trusted и Untrusted).
1. Создать профиль безопасности VPN в разделе **VPN → Профили безопасности VPN**:

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Название: NSX S2S

Описание:

IKE версия: IKEv1

Режим IKE: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: *****

Общий ключ (повтор): *****

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Время жизни ключа: 8 часов

Интервал проверки dead peer detection: 30 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

+ Добавить ✖ Удалить

Группа 14 Prime 2048 бит

Безопасность

+ Добавить ✎ Редактировать ✖ Удалить ⬆ Выше ⬇ Никже

Авторизация	Шифрование
SHA256	AES256

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить Отмена

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Время жизни ключа: 1 часов

Максимальный размер данных, шифруемых одним ключом: Отключено

100 МБ

Безопасность

+ Добавить ✎ Редактировать ✖ Удалить ⬆ Выше ⬇ Никже

Авторизация	Шифрование
SHA256	AES256

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить Отмена

2. В разделе **VPN → Клиентские правила** нужно создать правило, выбрав профиль безопасности VPN, указав адрес сервера (IP-адрес внешнего интерфейса NSX Edge, через который происходит соединение) и протокол VPN: IPsec-туннель. Указываем локальные сети со стороны UserGate и NSX Edge, трафик которых должен шифроваться данным туннелем:

Клиентские правила

+ Добавить ✎ Редактировать ✖ Удалить ⬆ Выше ⬇ Никже

✓

Название: CheckPoint IPsec, Client VPN rule, NSX IPsec

Свойства

Включено: ☒

Название: NSX IPsec

Описание:

Профиль безопасности VPN: NSX S2S

Интерфейс: tunnel3

Адрес сервера: 178.20.233.46

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешённые подсети со стороны UserGate: 172.21.10.0/24

Разрешённые подсети со стороны Cisco: 192.168.1.0/24

Аутентификация

Пользователь:

Пароль: *****

Сохранить Отмена

3. Создание правила Межсетевго экрана:

Межсетевой экран						
Добавить Редактировать Удалить Переместить Копировать Включить Отключить						
✓						
#	Название	Действие	Зона источника	Адрес...	Зона назначения	
1	VPN S2S	Разрешить	Trusted VPN for Site-to-Site	Любой	Trusted VPN for Site-to-Site	

4. Создание маршрута в локальную сеть за NSX Edge:

Виртуальные маршрутизаторы						
Свойства виртуального маршрутизатора						
Статические маршруты						
Добавить Редактировать Удалить Включить Отключить						
Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика	
192.168.1.0/24	unicast	192.168.1.0/24		tunnel3	0	

Примечание При наличии нескольких сетей защищаемых NSX Edge и UserGate NGFW, следует создавать маршруты для каждой из них. Плохой идеей будет создавать VPN туннель для каждой из таких сетей.

5. Проверка состояния туннеля: в разделе **VPN → Клиентские правила** в нормальном состоянии должен гореть зеленый индикатор:

Клиентские правила					
Добавить Редактировать Удалить Включить Отключить ↺					
✓					
Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN	
CheckPoint IPsec	91.107.67.228	tunnel3	CheckPoint S2S		
Client VPN rule	10.10.10.10	tunnel3	Client VPN profile		
NSX IPsec	178.20.233.46	tunnel3	NSX S2S		

6. В разделе **Диагностика и мониторинг → VPN** должна быть информация о работающем туннеле:

Дашборд Диагностика и мониторинг Журналы и отчёты Настройки Гостевой портал Помощь Русский						
VPN						
UG-230 10 секунд						
Пользователь	Роль этого сервера	Время сессии	Туннельный IP ↑	IP адрес	Geo IP	Шифрование
IPSEC tunnel	Клиент	12 августа 2022 г., 12:1...	—	178.20.233.46	RU	aes256

Настройка на стороне UserGate завершена.

KnowledgeBase: ☒
 Product: UserGate NGFW
 Version: 6.1.8, 6.1.9
 Technology: VPN

Подключение производится по следующей схеме:



Далее будут рассмотрены настройки серверов Linux и UserGate для настройки IPsec-туннеля между сетями 172.16.0.0/24 и 10.0.5.0/24.

Настройка Linux-сервера

Для реализации IPsec на Linux-сервере использовалось ПО LibreSwan (ПО и подробная информация о нём доступны по следующей ссылке: <https://libreswan.org/>).

- Установить ПО LibreSwan.

```
sudo apt update
sudo apt install -y -q libreswan
```

После установки LibreSwan будет доступна команда **ipsec**.

Файлы конфигурации для настройки политики подключения:

- создание политик подключения: / etc/ ipsec. conf и файлы / etc/ ipsec. d/* conf.
- хранение PSK: / etc/ ipsec. secrets и файлы / etc/ ipsec. d/* . secrets.

- Сгенерировать Pre-shared key.

Для генерации PSK была использована команда (в привилегированном режиме):

```
# openssl rand -base64 18
```

Был сгенерирован ключ: WXj72QDymXs1inggnYVSBuox

Сохраните общий ключ в файл / etc/ ipsec.secrets. Общий формат файлов *. secrets следующий:

- для конкретного Peer-to-Peer соединения:

```
<Source_IP> <Destination_IP> : PSK <PSK>
```

- для любых подключений, которые не попадают в заданные правила:

```
: PSK <PSK>
```

```
# cat /etc/ipsec.secrets
: PSK "WXj72QDymXs1inggnYVSBuox"
include /etc/ipsec.d/* . secrets
```

- Создать файл конфигурации VPN-подключения.

Файл необходимо создать в каталоге / etc/ ipsec.d/ vpn.conf. Подробное описание конфигурационных параметров доступно по ссылке: <https://libreswan.org/man/ipsec.conf.5.html>.

Далее представлена базовая конфигурация:

```
config setup
logfile=/var/log/pluto.log
```

Дайте название подключению, например **vpn**:

```
conn vpn
```

Укажите IP-адрес удалённого пира (UserGate):

```
right=192.168.2.168
```

или укажите «%any» для автоматического заполнения этого параметра в процессе установки сессии:

```
right=%any
```

Укажите адрес подсети, подключённой к удалённому пиру:

```
rightsubnet=172.16.0.0/24
```

Укажите адрес пира - Linux-сервера и подсети, подключённой к нему:

```
left=172.17.1.73
leftsubnet=10.0.5.0/24
```

Задайте способ аутентификации - Общий ключ:

```
authby=secret
```

В текущих версиях UserGate не поддерживается PFS (Perfect Forward Secrecy) и IKEv2:

```
pfs=no
ikev2=no
rekey=yes
keyingtries=3
```

Тип подключения туннельный (значение по умолчанию)

```
type=tunnel
auto=start
```

Далее задайте алгоритмы, которые будут использоваться на первой и второй фазах согласования:

```
ike=aes256-sha1-modp1536,aes128-sha1-modp1536,3des-sha1-modp1536,aes128-sha1,modp1536,aes128-sha1,modp1536
esp=aes256-sha256,aes256-sha1,3des-sha1
nat-ikev1-method=none
```

- Запустить IPsec:

```
# ipsec start
```

- Создайте правило SNAT (Source Network Address Translation), для корректного прохождения трафика, предназначенного для сети, расположенной за удалённым пиrom:

```
# iptables -t nat -A POSTROUTING -d 172.16.0.0/24 -j SNAT --to-source 10.0.5.1
```

Настройка UserGate

- Настройка сетевых интерфейсов.

Особенностью данной настройки является необходимость создания виртуального туннельного VPN интерфейса. Интерфейс необходим для инкапсуляции трафика в модуль VPN (при активации подключения создаётся маршрут в указанную сеть за удаленным пиrom через туннельный VPN интерфейс).

Для добавления интерфейса перейдите в раздел **Сеть → Интерфейсы**, нажмите **Добавить** и выберите **Добавить VPN**. Далее укажите:

- отметьте чекбокс **Включено**;
- порядковый номер, использующийся в названии интерфейса;
- Описание** (опционально);
- Зона**, которой принадлежит интерфейс;
- IP-адрес** может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32. Используемая подсеть должна быть согласована в рамках туннельного подключения. В данном примере назначен IP-адрес интерфейса: 172.16.0.0/24.

2. Настроить профиль безопасности VPN.

Настройка профилей безопасности производится в разделе **VPN → Профили безопасности VPN** веб-интерфейса UserGate. Настройка профиля безопасности необходима для согласования следующих параметров:

- режим IKE;
- общий ключ;
- алгоритмы шифрования, проверки целостности и обмена ключами первой фазы;
- алгоритмы шифрования, проверки целостности второй фазы.

Алгоритмы шифрования и авторизации, указанные на сервере Linux и UserGate, должны совпадать. Можно задать несколько комбинаций алгоритмов, из совпадающих вариантов хосты выберут наиболее защищённую комбинацию.

Для данного примера профиль безопасности VPN имеет следующие настройки:

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Название:

Linux

Описание:

ИКЕ версия:

IKEv1

Режим IKE:

Основной

Аутентификация с пиром:

Общий ключ

Общий ключ:

Общий ключ (повтор):

Сохранить

Отмена

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Интервал проверки dead peer detection:

60

(в секундах)

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 5 Prime 1536 бит

Безопасность

Добавить

Редактировать

Удалить

Вверх

Вниз

Авторизация

Шифрование

SHA1

AES128

SHA1

3DES

MD5

AES128

MD5

3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

1

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

100

МБ

Безопасность

Добавить

Редактировать

Удалить

Вверх

Вниз

Авторизация

Шифрование

SHA256

AES256

SHA1

AES256

SHA1

3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

3. Создать клиентское правило VPN.

Чтобы добавить правило перейдите в раздел **VPN → Клиентские правила**, нажмите **Добавить** и укажите:

- отметьте чекбокс **Включено**;
- **Название** правила;
- **Описание** (опционально);
- **Профиль безопасности**, настроенный ранее;
- **Интерфейс**, созданный в пункте 1;
- **Адрес сервера**: адрес интерфейса Linux-сервера, через который происходит подключение;
- **Протокол VPN**: IPsec туннель;
- согласовать сети с каждой стороны туннеля (rightsubnet и leftsubnet).

Свойства

Включено: ☒

Название: linux_libreswan

Описание:

Профиль безопасности VPN: Linux

Интерфейс: tunnel3

Адрес сервера: 172.17.1.73

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешённая подсеть со стороны UserGate: 172.16.0.0/24

Разрешённая подсеть со стороны Cisco: 10.0.5.0/24

Аутентификация

Пользователь:

Пароль:

Сохранить Отмена

В случае успешного подключения напротив правила отобразится зелёный индикатор.

Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN
linux_libreswan	172.17.1.73	tunnel3	Linux	

Новый маршрут отобразится в таблице маршрутизации системы (вкладка **Диагностика и мониторинг** раздел **Мониторинг** → **Маршруты**):

```
VRF default:
K> * 0.0.0.0/0 [0/0] via 192.168.2.1, port0, 02:04:13
K> * 10.0.5.0/24 [0/0] via 172.16.0.254, tunnel3, 00:03:18
```

Диагностика и мониторинг соединения

Для поиска неисправностей инструментами UserGate используйте функцию захвата пакетов на интерфейсе и расширенные логи.

Для создания правила захвата пакетов на интерфейсе перейдите во вкладку **Диагностика и мониторинг** раздел **Сеть** → **Захват пакетов**. В качестве фильтра используйте IP-адрес хоста, укажите интерфейс и настроенный фильтр в правиле PCAP.

Правило PCAP

Название: isakmp

Размер файла, МБ: 100

Файл: isakmp

Интерфейсы

Добавить Удалить

port0

Фильтры

Добавить Удалить

udp|isakmp

Сохранить Отмена

Запустите запись, нажав **Начать запись**.

Измените уровень детализации журналов диагностики на **Debug** во вкладке **Настройки** в разделе **UserGate** → **Управление устройством**.

Попробуйте установить соединение, включив необходимое правило. Соединение не было установлено:

Название	Адрес сервера	Интерфейс	Профиль без...	Последняя ошибка VPN
linux_libres...	172.17.1.73	tunnel3	Linux	Ошибка подключения VPN-клиента - неверный общий ключ

Отключите правило, измените уровень детализации журналов на **Error** и остановите захват пакетов. Скачайте файл PCAP и журналы работы системы.

В архиве с файлами необходимо найти каталог **utm-vpn-server** или **utm-vpn-client** в зависимости от роли UserGate.

В каталоге откройте файл, например, utm-vpn-client.log. В соответствии с ошибкой подключения в файле необходимо найти ключи шифрования первой фазы IKE. Чтобы их найти, например, на ОС Windows, можно воспользоваться утилитой findstr. Ключевое слово для фильтрации - WIRESHARK.

```
2022-07-21 14:17:15.4241650.10011.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 7ad0be8d3cf1870f,095ca
d88bce3378b60ed792f0b12801
2022-07-21 14:17:30.4613430.10028.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: b0ea1c8b5e52cc3d,4bf2e
3cda1d20fc2c5a3ed4f9fad074c
2022-07-21 14:17:45.4978110.10045.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 186009079318008f,ef39e
d82a540dd362caca2aafdd89c6
2022-07-21 14:18:00.5504940.10060.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 6f24dc0b79142f671,d27af
19f560ad5d6c808ae40732ca3
2022-07-21 14:18:15.5925770.10077.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 9fc76cd0b2cdf913f,41d00
6e7a7867ec60d0d328056db5fb0
2022-07-21 14:18:30.6453000.10095.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: ab361330ea9acd8f,954e1
5f9f1bd0f32af3004fbc7bab988
2022-07-21 14:18:45.6779510.10119.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 63bcf774c525fd2b,8d49a
85b4bfbb31e8e061d09507a7b2ce
2022-07-21 14:19:00.7380500.10135.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 71881490b65a5d81,646fc
51eb334bc4d347f107fc03a15
2022-07-21 14:19:15.7665940.10152.0> [critical][vpn] vpn:setup_phase1_main/1:482 WIRESHARK key: 2422a3e837bbdb64,47d5c
d7bec86a8ff6f28f75f9c028a98
PS C:\Users\chef\Downloads\logs-21-07-2022 14_19_30>utm-vpn-client>
```

Сохраните ключи в отдельный файл. Далее запустите программу Wireshark и в настройках найдите опции протокола ISAKMP. Выберите редактирование IKEv1 Decryption Table и пропишите сохранённые ранее ключи шифрования:

Wireshark - Preferences

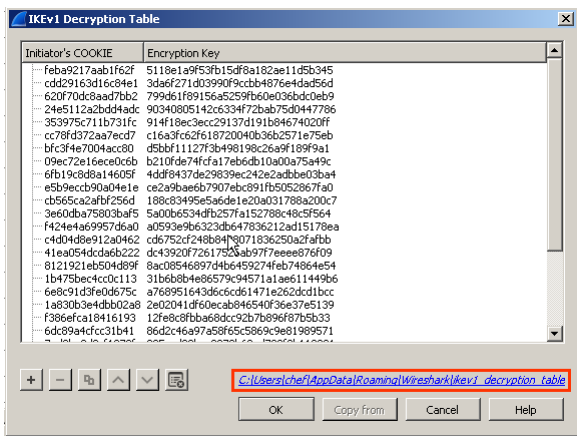
Internet Security Association and Key Management Protocol

IKEv1 Decryption Table Edit...

IKEv2 Decryption Table Edit...

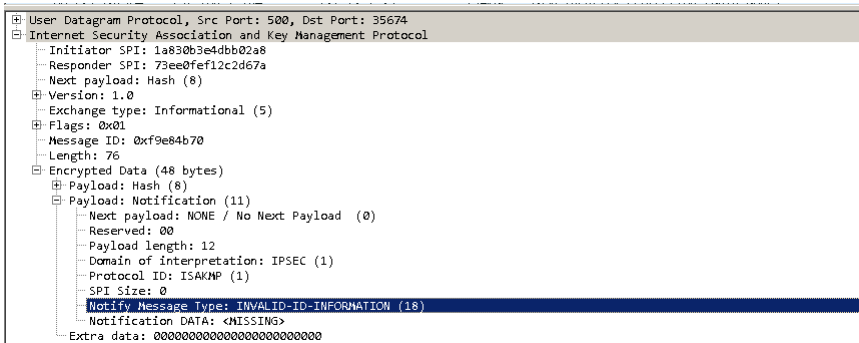
ISAKMP UDP port 500

ISAKMP TCP port 500



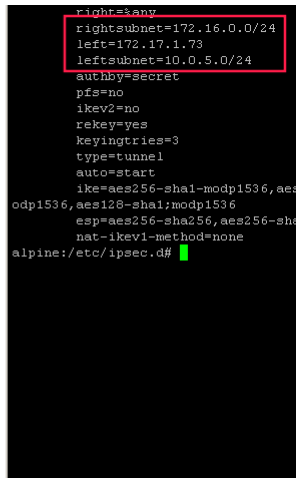
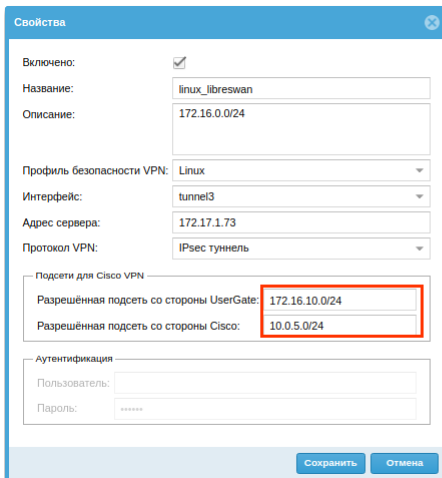
Если ключей много, то можно создать одну запись, далее сохранить настройки, ещё раз вернуться в редактор ключей, посмотреть название файла, в который программа сохраняет ключи (путь к файлу выделен на рисунке), и добавить все ключи в файл.

После добавления ключей откройте файл захвата пакетов, созданный на UserGate, зашифрованная часть трафика будет доступна для изучения.



Отследив конкретные UDP сессии, можно увидеть коды ответа удаленного хоста. Если протокол реализован в соответствии с RFC, то по коду ответа можно яснее понять, в чем именно заключается проблема. Например, из кода ответа 18 (INVALID-ID-INFORMATION), можно сделать вывод, что объявляемые сети с обеих сторон не совпадают.

Если посмотреть предыдущий пакет либо внимательнее сравнить сети, прописанные на UserGate, и сети, прописанные на удаленном хосте, то мы обнаружим их несовпадение.

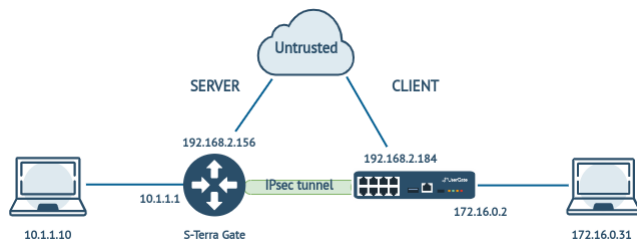


KnowledgeBase: ☒
 Product: UserGate NGFW
 Version: 6.x, 7.x
 Technology: VPN

Настройка S-Terra Gate

В данном разделе рассматривается только настройка VPN-соединения. Считается, что базовые настройки устройств уже были произведены.

Далее будет рассмотрена настройка Site-to-Site VPN между устройствами UserGate и S-Terra Gate; S-Terra Gate выступает в качестве сервера, UserGate - клиента. При настройке VPN-соединения используется основной режим IKE, который является более защищённым по сравнению с агрессивным режимом.



Адресация на S-Terra Gate:

- локальная сеть подключена к интерфейсу FastEthernet 0/1 с адресом 10.1.1.1;
- внешний интерфейс FastEthernet 0/0 с адресом 192.168.2.156.

Адресация на UserGate:

- локальная сеть подключена к интерфейсу с адресом 172.16.0.2;
- внешний интерфейс имеет адрес 192.168.2.184.

Настройка S-Terra Gate

```
sterragate#sh run
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
```

1. Настроить политики ISAKMP, задать алгоритмы, которые будут использоваться на первой фазе согласования (например, MD5/AES128):

```
crypto isakmp policy 7
encr aes
hash md5
authentication pre-share
group 1
```

2. Указать общий ключ для конкретного удалённого хоста:

```
crypto isakmp key < PRESHARED_KEY> address 192.168.2.184
```

3. Задать алгоритмы аутентификации и шифрования второй фазы согласования, например, SHA1/AES128:

```
crypto ipsec transform-set test esp-aes esp-sha-hmac
```

4. Создать список доступа, разрешающий трафик между сетями 10.0.0.0/24 и 172.16.0.0/24:

```
ip access-list extended test
permit ip 10.1.1.0 0.0.0.255 172.16.0.0 0.0.0.255
```

5. Настроить crypto map и применить её к внешнему интерфейсу шлюза:

```
crypto map s2s_map 10 ipsec-isakmp
match address test
set transform-set test
set security-association lifetime seconds 86400
set peer 192.168.2.184
reverse-route
!
interface FastEthernet0/0
ip address 192.168.2.156 255.255.255.0
crypto map s2s_map
!
interface FastEthernet0/1
ip address 10.1.1.1 255.255.255.0
!
end
```

Настройка UserGate NGFW

1. Разрешить сервис **VPN** на зоне, через которую происходит соединение.
2. Создать новый или использовать созданный по умолчанию туннельный интерфейс.
 Во вкладке **Сеть** настроек VPN-адаптера укажите статический IP-адрес туннельного VPN-интерфейса, используемого в правиле VPN; IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32.
3. Разрешить прохождение трафика между зонами правилом межсетевого экранами (из зоны, которой принадлежит VPN-интерфейс, в зоны Trusted и Untrusted).
4. Настроить профиль безопасности VPN, определяющий общий ключ и алгоритмы шифрования и аутентификации.

Перейдите в раздел **VPN → Профили безопасности** веб-интерфейса UserGate и укажите необходимые данные. Во вкладке **Общие** укажите:

- **Название** профиля безопасности VPN;
- **Описание** (опционально);
- **IKE версия**: IKEv1;
- **Режим IKE**: основной;
- **Аутентификация с пиром**: общий ключ;
- **Общий ключ** для установки соединения, указанный при настройке S-Terra Gate.

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Название: VPN Site-to-Site with S-Terra Gate

Описание:

ИКЕ версия: IKEv1

Режим ИКЕ: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: ***

Общий ключ (повтор): ***

Сохранить Отмена

Во вкладке **Фаза 1** укажите алгоритмы шифрования и аутентификации первой фазы согласования:

- **Время жизни ключа**, по истечении которого происходят повторные аутентификация и согласование настроек;
- **Diffie-Hellman группы**: Группа 1 Prime 768 бит;
- **Безопасность**: алгоритмы авторизации и шифрования, указанные при настройке S-Terra Gate - в данном примере MD5/AES128.

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 1000 секунд

Интервал проверки dead peer detection: 60 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

Добавить Удалить

Группа 1 Prime 768 бит

Безопасность

Добавить Редактировать Удалить Выше Ниже

Авторизация Шифрование

MD5 AES128

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

- Во вкладке **Фаза 2** укажите алгоритмы шифрования и аутентификации второй фазы согласования:
- **Время жизни ключа** второй фазы;
- **Безопасность**: алгоритмы авторизации и шифрования. Алгоритмы должны быть согласованы между устройствами - SHA1/AES128.

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 1000 секунд

Максимальный размер данных, шифруемых одним ключом: Отключено

100 МБ

Безопасность

Добавить Редактировать Удалить Выше Ниже

Авторизация Шифрование

SHA1 AES128

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Примечание Так как UserGate NGFW является клиентом, задавать сеть, из которой будут выдаваться IP-адреса для подключённых удалённых хостов, не требуется.

5. Настроить клиентское правило.

Для настройки клиентского правила VPN перейдите в раздел **VPN → Клиентские правила** и укажите:

- **Название** клиентского правила;
- **Описание** (опционально);
- **Профиль безопасности VPN**, созданный ранее;
- **Интерфейс**, который используется для клиентского VPN Site-to-Site подключения (в данном случае используется интерфейс **tunnel1**);
- **Адрес сервера**: 192.168.2.156;
- **Протокол VPN**: IPsec туннель, т.е. оригинальный пакет данных будет полностью инкапсулироваться в новый IP пакет со своими адресами источника и назначения (SourceIP и DestinationIP);
- **Разрешённые подсети со стороны UserGate**: 172.16.0.0/24;
- **Разрешённые подсети со стороны S-Terra Gate**: 10.1.1.0/24.

Свойства

Включено: ☒

Название: Client VPN rule

Описание:

Профиль безопасности VPN: VPN Site-to-Site with S-Terra Gate

Интерфейс: tunnel1

Адрес сервера: 192.168.2.156

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешённые подсети со стороны UserGate: 172.16.0.0/24

Разрешённые подсети со стороны Cisco: 10.1.1.0/24

Аутентификация

Пользователь: vpn

Пароль:

Сохранить

Отмена

В случае успешного установления соединения сервера отобразится индикатор зелёного цвета.

Клиентские правила

Добавить

Редактировать

Удалить

Включить

Отключить

✓

Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN	
Client VPN profile	192.168.2.156	tunnel1	VPN Site-to-Site with S-Terra Gate		

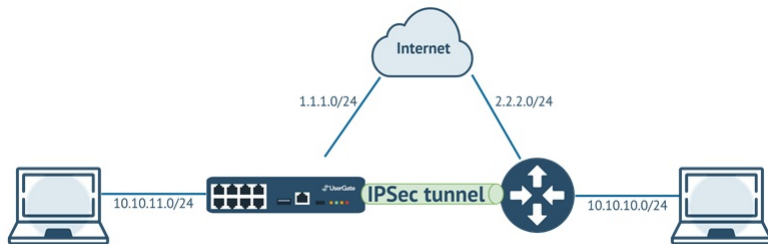
Настройка Site-to-Site VPN между UserGate и Cisco

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

Site-to-Site VPN (Site-to-Site Virtual Private Network) - один из способов реализации технологии VPN, предназначенный для создания защищённого виртуального туннеля между несколькими частными сетями. Site-to-Site VPN часто используется компаниями, имеющими филиалы в разных городах для объединения их в виртуальную частную сеть.

Для создания постоянного безопасного туннеля используется протокол IPsec.

Рассмотрим создание Site-to-Site VPN подключения между UserGate и Cisco.



Адреса:

- IP-адрес сети за UserGate: 10.10.11.0/24.
- IP-адрес интерфейса, через который происходит подключение к UserGate: 1.1.1.2.
- IP-адрес сети оборудованием Cisco: 10.10.10.0/24.
- IP-адрес интерфейса, через который происходит подключение к Cisco: 2.2.2.1.

Настройка оборудования Cisco (с использованием crypto-map).

На маршрутизаторе произведены настройки интерфейсов, есть выход в сеть Интернет.

1. Настроить политику IKE/ISAKMP (Internet Key Exchange/Internet Security Association and Key Management Protocol), использующуюся для обеспечения защищённого взаимодействия в виртуальных частных сетях. При запуске согласования IKE происходит поиск общей политики на узлах.

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
```

2. Указать pre-shared key (общего ключа), который будет использоваться при аутентификации:

```
crypto isakmp key cisco address 1.1.1.2
```

3. Указать трафик между сетями, который необходимо шифровать и настроить список доступа для разрешения Site-to-Site VPN.

В данном примере должен шифроваться трафик между сетями 10.10.10.0/24 и 10.10.11.0/24.

```
ip access-list extended map_vpn
permit ip 10.10.10.0 0.0.0.255 10.10.11.0 0.0.0.255
deny ip any any
```

4. Произвести настройку политики для защиты передаваемых данных (transform-set):

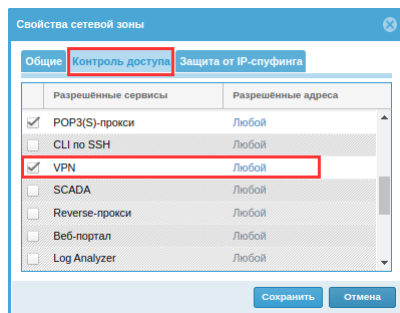
```
crypto ipsec transform-set map_set128 esp-aes esp-sha-hmac
```

5. Настроить crypto map (объект, в котором находятся наборы правил, относящиеся к разным туннелям IPsec) и её применение на внешнем интерфейсе GigabitEthernet0/0:

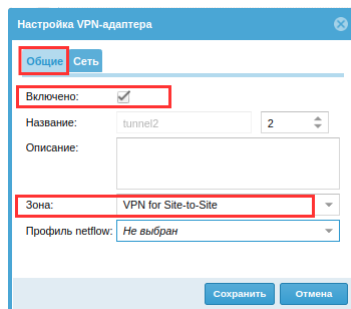
```
crypto map map1 10 ipsec-isakmp
set peer 1.1.1.2
set transform-set map_set128
match address map_vpn
interface GigabitEthernet0/0
ip address 2.2.2.1 255.255.255.0
duplex auto
speed auto
crypto map map1
```

Настройка UserGate.

1. В разделе **Сеть** → **Зоны** разрешить доступ по VPN для зоны, из которой будет происходить соединение.



2. В разделе **Сеть** → **Интерфейсы** создать или использовать созданный по умолчанию интерфейс VPN для Site-to-Site.



Во вкладке **Сеть** настроек VPN-адаптера укажите статический IP-адрес туннельного VPN-интерфейса, используемого в правиле VPN; IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32.

3. Добавить или использовать существующее правило VPN Site-to-Site to Trusted and Untrusted в разделе **Политики сети** → **Межсетевой экран** для разрешения трафика по VPN Site-to-Site. В свойствах правила можно указать

пользователей/группу пользователей, которым будет разрешено подключение, сервис, приложения и время.

Далее представлены свойства созданного по умолчанию правила VPN Site-to-Site to Trusted and Untrusted.

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Включено: ☒

Название: VPN for Site-to-Site to Trusted and Untrusted

Описание: 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.

Действие: ☒ Разрешить

Отбросить и: Не выбран

Сценарий: Не использовать сценарии

Журналирование: Нет

Включить лимит журналирования: ☒

Ограничить число событий, записываемых в журнал: 3 / час

Максимальное количество пакетов, журналируемых на событие: 5

Применить правило к: Все пакеты

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Исходная зона

☐ Cluster

☐ DMZ

☐ Management

☐ Trusted

☐ Untrusted

☐ VPN for remote access

☒ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес источника

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Зона назначения

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☒ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес назначения

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

4. Создать или использовать созданные по умолчанию профили безопасности VPN в разделе VPN → Профили безопасности VPN.

Если используется **UserGate 6.1.6** и **ниже**: в свойствах профиля указать общий ключ (pre-shared key) и во вкладке **Безопасность** задать тип авторизации и шифрования, заданные на Cisco.

Свойства профиля безопасности VPN

Общие Безопасность

Название: Client VPN profile

Описание: Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

Свойства профиля безопасности VPN

Общие **Безопасность**

Добавить Редактировать Удалить Выше Ниже

Авторизация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

При использовании **UserGate 6.1.7 и выше** в настройках профиля безопасности согласуйте настройки безопасности, заданные на оборудовании Cisco: режим IKE, DH-группы, алгоритмы аутентификации и шифрования; далее представлены настройки профиля безопасности VPN для данного примера:

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Название: Cisco compatible VPN profile

Описание:

IKE версия: IKEv1

Режим IKE: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

Свойства профиля безопасности VPN

Общие **Фаза 1** Фаза 2

Время жизни ключа: 1 часов

Интервал проверки dead peer detection: 60 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

Добавить Удалить

Группа 2 Prime 1024 бит

Безопасность

Добавить Редактировать Удалить Выше

Аутентификация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Свойства профиля безопасности VPN

Общие Фаза 1 **Фаза 2**

Время жизни ключа: 1 часов

Максимальный размер данных, шифруемых одним ключом: Отключено

100 МБ

Безопасность

Добавить Редактировать Удалить Выше

Аутентификация	Шифрование
SHA1	AES128

Поддерживаемые алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

5. В разделе **VPN → Клиентские правила** необходимо создать правило, выбрав профиль безопасности VPN, указав адрес сервера (IP-адрес интерфейса на роутере Cisco, через который происходит соединение) и протокол VPN: IPsec туннель. Далее необходимо указать разрешённые подсети со стороны UserGate и Cisco.

Свойства

Включено: ☒

Название: Client VPN rule

Описание: Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.

Профиль безопасности VPN: Client VPN profile

Интерфейс: tunnel3

Адрес сервера: 2.2.2.1

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешённая подсеть со стороны UserGate: 10.10.11.0/24

Разрешённая подсеть со стороны Cisco: 10.10.10.0/24

Аутентификация

Пользователь: vpn

Пароль:

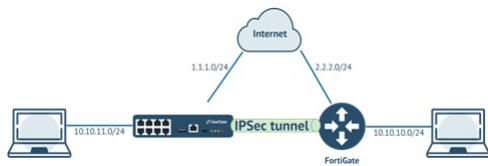
Сохранить

Отмена

Настройка VPN-соединения между UserGate и FortiGate

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

В данном разделе рассмотрена настройка VPN-соединения между UserGate и FortiGate. Соединение происходит по следующей схеме:



Адреса:

- IP-адрес сети за UserGate: 10.10.11.0/24.
- IP-адрес интерфейса, через который происходит подключение к UserGate: 1.1.1.2.
- IP-адрес сети оборудованием FortiGate: 10.10.10.0/24.
- IP-адрес интерфейса, через который происходит подключение к FortiGate: 2.2.2.1.

О настройке VPN на продуктах FortiGate читайте в соответствующей документации. При настройке необходимо:

1. Установить режим, используемый для создания защищенного канала, **Aggressive**.
2. Указать группу Диффи — Хеллмана (Diffie-Hellman group, DH group) 1.

Настройка UserGate.

1. В разделе **Сеть** → **Зоны** разрешить доступ по VPN для зоны, из которой будет происходить соединение.

2. В разделе **Сеть** → **Интерфейсы** создать или использовать созданный по умолчанию интерфейс VPN for Site-to-Site.

Во вкладке **Сеть** настроек VPN-адаптера укажите статический IP-адрес туннельного VPN-интерфейса, используемого в правиле VPN; IP-адрес может быть любым при условии, что он не будет пересекаться с адресами других подсетей, с любой маской, за исключением маски с префиксом /32.

3. Добавить или использовать существующее правило VPN Site-to-Site to Trusted and Untrusted в разделе **Политики сети** → **Межсетевой экран** для разрешения трафика по VPN Site-to-Site. В свойствах правила можно указать пользователей/группу пользователей, которым будет разрешено подключение, сервис, приложения и время.

Далее представлены свойства созданного по умолчанию правила VPN Site-to-Site to Trusted and Untrusted.

Свойства правила межсетевого экрана

Общие **Источник** Пользователи Назначение Сервис Приложения Время

Исходная зона

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☐ Trusted
- ☐ Untrusted
- ☐ VPN for remote access
- ☒ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес источника

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источник Пользователи **Назначение** Сервис Приложения Время

Зона назначения

- ☐ Cluster
- ☐ DMZ
- ☐ Management
- ☒ Trusted
- ☒ Untrusted
- ☐ VPN for remote access
- ☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес назначения

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

4. Создать или использовать созданные по умолчанию профили безопасности VPN в разделе **VPN → Профили безопасности VPN**. В свойствах профиля указать общий ключ (pre-shared key) и во вкладке **Безопасность** задать тип авторизации и шифрования, заданные на FortiGate.

Свойства профиля безопасности VPN

Общие **Безопасность**

Название: Client VPN profile

Описание: Example VPN security profile for client VPN rule. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

Свойства профиля безопасности VPN

Общие **Безопасность**

Добавить Редактировать Удалить Выше Ниже

Авторизация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх или вниз

Сохранить Отмена

5. В разделе **VPN → Клиентские правила** необходимо создать правило, выбрав профиль безопасности VPN, указав адрес сервера (IP-адрес интерфейса FortiGate, через который происходит соединение) и протокол VPN: IPsec туннель. Далее необходимо указать разрешенные подсети со стороны UserGate и FortiGate.

Свойства

Включено: ☒

Название: Client VPN rule

Описание: Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.

Профиль безопасности VPN: Client VPN profile

Интерфейс: tunnel3

Адрес сервера: 2.2.2.1

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешённая подсеть со стороны UserGate: 10.10.11.0/24

Разрешённая подсеть со стороны Cisco: 10.10.10.0/24

Аутентификация

Пользователь: vpn

Пароль: *****

Сохранить Отмена

При подключении FortiGate и UserGate версии 6.1.7 и выше :

1. На FortiGate отключите опцию Perfect Forward Secrecy (PFS).
2. Согласуйте настройки безопасности между UserGate и Fortinet (режим IKE, DH-группы, алгоритмы авторизации и шифрования).

На UserGate, по умолчанию, создан профиль безопасности **Fortinet compatible VPN profile**, определяющий следующие настройки:

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Название: Fortinet compatible VPN profile

Описание:

ИКЕ версия: IKEv1

Режим ИКЕ: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: *****

Общий ключ (повтор): *****

Сохранить Отмена

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 24 часов

Интервал проверки dead peer detection: 60 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

Добавить Удалить

Группа 14 Prime 2048 бит

Группа 5 Prime 1536 бит

Безопасность

Добавить Редактировать Удалить Выше

Авторизация	Шифрование
MD5	DES
SHA1	DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 12 часов

Максимальный размер данных, шифруемых одним ключом: Отключено

4500 MB

Безопасность

Добавить Редактировать Удалить Выше

Авторизация	Шифрование
MD5	DES
SHA1	DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.x, 7.x
Technology: VPN

Описание

Рассмотрим ситуацию, при которой необходимо объединить две сети, одна из которых защищена с помощью UserGate NGFW, а другая - с помощью Cisco ASR1002-X.

В данном примере предполагается использование следующих адресов:

- Адрес сети, защищенной UserGate NGFW: 172.21.10.0/24.
- IP-адрес внешнего интерфейса UserGate NGFW: 91.107.67.230.
- IP-адрес туннельного интерфейса tunnel4: 172.21.10.254/24.
- Адрес сети, защищенной Cisco ASR1002-X: 172.22.10.0/24.
- IP-адрес внешнего интерфейса Cisco ASR1002-X: 91.107.67.229.

Схема сети



Настройка на стороне Cisco ASR1002-X

1. Задать параметры 1-й фазы соласования туннеля:

```
crypto isakmp policy 235
encr aes
authentication pre-share
group 14
```

2. Задать pre-shared key:

```
crypto isakmp key <PSK ключ> address 91.107.67.230
```

3. Задать параметры 2-й фазы соласования туннеля:

```
crypto ipsec transform-set UserGate_TEST esp-aes 256 esp-sha256-hmac
mode tunnel
```

4. Создать фильтр для сетей, между которыми будет шифроваться трафик (src/dst):

```
ip access-list extended UserGate_TEST
permit ip 172.22.10.0 0.0.0.255 172.21.10.0 0.0.0.255
```

5. Создать криптокарту, которая будет назначена на исходящий интерфейс:

```
crypto map IPSEC 100 ipsec-isakmp
description UserGate_TEST
set peer 91.107.67.230
set transform-set UserGate_TEST
match address UserGate_TEST
```

6. Эмуляция внутренней сети:

```
interface Port-channel1.3970
description UserGate_TEST
encapsulation dot1Q 3970
ip address 172.22.10.1 255.255.255.0
```

7. Создать маршрут до локальной сети за туннелем UserGate:

```
ip route 172.21.10.0 255.255.255.0 91.107.67.225
```

8. Назначить созданную криптокарту на исходящий интерфейс:

```
interface Port-channel1.100
crypto map IPSEC
```

Настройка на стороне Cisco завершена.

Настройка на стороне UserGate NGFW

1. В разделе **Сеть** → **Зоны** разрешить доступ по VPN для зоны Untrusted:

Свойства сетевой зоны

Общие

Контроль доступа

Защита от IP-спуфинга

Разрешённые сервисы	Разрешённые адреса
☒ Ping	Любой
☐ SNMP	Любой
☐ Captive-портал и страница блокировки	Любой
☐ Кластер	Любой
☐ VRRP	Любой
☐ Консоль администрирования	Любой
☐ DNS	Любой
☐ HTTP(S)-прокси	Любой
☐ Агент аутентификации	Любой
☐ SMTP(S)-прокси	Любой
☐ POP3(S)-прокси	Любой
☐ CLI по SSH	Любой
☒ VPN	Любой
☐ SCADA	Любой
☐ Reverse-прокси	Любой
☐ Веб-портал	Любой
☐ Log Analyzer	Любой
☐ OSPF	Любой

Сохранить

Отмена

2. В разделе **Сеть** → **Интерфейсы** создать интерфейс tunnel4 и назначить адрес из пула локальной сети 172.21.10.254:

Интерфейсы

Добавить

Редактировать

Добавить VLAN

Добавить бонд-интерфейс

Добавить мост

Добавить PPPoE

Добавить VPN

Добавить туннель

Настройка туннельного интерфейса

Общие

Сеть

Включено: ☒

Название: gre4 4

Описание:

Имя узла: UG-230

Зона: VPN for Site-to-Site

Настройка VPN-адаптера

Общие

Сеть

Режим: Статический

MTU: 1420

IP интерфейса

Добавить

Редактировать

Удалить

IP интерфейса	Маска
172.21.10.254	255.255.255.0

Интерфейсы

Добавить

Редактировать

Удалить

Включить

Отключить

Показать Все

	Тип	Название	Режим	IP интерфейса	MAC-адрес	Зона	MTU	D
Узел кластера: cluster								
VPN	tunnel1	Статический	172.19.2.1/255.255.255.0			VPN for r...	1420	
VPN	tunnel2	Статический	172.30.255.1/255.255.255.0			VPN for S...	1420	
VPN	tunnel3	Статический	203.0.113.1/255.255.255.0			VPN for S...	1420	
VPN	tunnel4	Статический	172.21.10.254/255.255.255.0			VPN for S...	1420	
Узел кластера: UG-230 (текущий узел)								
Cerebo...	port0	Статический	172.21.10.1/255.255.255.0	00:50:56:01:10:ac		Trusted	1500	—
Cerebo...	port1	Без адреса	Нет		00:50:56:01:14:2b	Trusted	1500	—
Cerebo...	port2	Статический	91.107.67.230/255.255.255.248		00:50:56:01:1d:93	Untrusted	1500	—
Cerebo...	port3	Без адреса	Нет		00:50:56:01:3a:d8	DMZ	1500	—
VPN	tunnel1	Статический	172.19.2.1/255.255.255.0			VPN for r...	1420	

3. В разделе VPN → Профили безопасности VPN создать новый профиль безопасности VPN со следующими параметрами:

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Название: Cisco S2S

Описание:

IKE версия: IKEv1

Режим IKE: Основной

Аутентификация с пиром: Общий ключ

Общий ключ: *****

Общий ключ (повтор): *****

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 24 часов

Интервал проверки dead peer detection: 120 (в секундах)

Неудачных попыток: 5

Diffie-Hellman группы

+ Добавить - Удалить

Группа 14 Prime 2048 бит

Безопасность

+ Добавить Редактировать - Удалить Выше Ниже

Авторизация	Шифрование
SHA256	AES256

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить Отмена

Свойства профиля безопасности VPN

Общие Фаза 1 Фаза 2

Время жизни ключа: 1 часов

Максимальный размер данных, шифруемых одним ключом: Отключено

4500 МБ

Безопасность

+ Добавить Редактировать - Удалить Выше Ниже

Авторизация	Шифрование
SHA256	AES256

4. В разделе **VPN** → **Клиентские правила** создать правило Cisco IPsec, выбрав созданный ранее профиль безопасности VPN. В поле адреса сервера указать IP-адрес внешнего интерфейса Cisco ASR1002-X. В поле протокола VPN выбрать IPsec-туннель. Далее указать разрешенные подсети со стороны UserGate и Cisco:

Свойства

Включено: ☒

Название: CISCO IPsec

Описание:

Профиль безопасности VPN: Cisco S2S

Интерфейс: tunnel4

Адрес сервера: 185.98.84.26

Протокол VPN: IPsec туннель

Подсети для Cisco VPN

Разрешенные подсети со стороны UserGate: 172.21.10.0/24

Разрешенные подсети со стороны Cisco: 172.22.10.0/24

Аутентификация

Пользователь:

Пароль: *****

Сохранить Отмена

Клиентские правила

+ Добавить Редактировать - Удалить Включить Отключить ↺

name="CISCO IPsec"

Название	Адрес сервера	Интерфейс	Профиль безопасности VPN	Последняя ошибка VPN
CISCO IPsec	185.98.84.26	tunnel4	Cisco S2S	

5. В разделе **Сеть** → **Виртуальные маршрутизаторы** → **Виртуальный маршрутизатор по умолчанию** прописать статический маршрут к удаленной локальной сети Cisco через tunnel4:

Виртуальные маршрутизаторы

+ Добавить Редактировать - Удалить ↺

Название ↑

Интерфейсы Статические маршруты OSPF BGP RIP Мультикаст маршрутизации

Узел кластера: UG-230 (текущий)

Виртуальный маршрутизатор по умолчанию

Свойства виртуального маршрутизатора

Статические маршруты

+ Добавить Редактировать - Удалить Включить Отключить

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
172.22.10.0/24	unicast	172.22.10.0/24		tunnel4	0

6. В разделе **Политики сети** → **Межсетевой экран** создать двустороннее правило доступа с указанием Trusted и VPN Site-to-Site зон. Разрешить трафик между Trusted и S2S:

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

✓

#	Статус журнал...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначе...
1		VPN S2S	✓ Разрешить	Trusted VPN for Site-to-Site	Любой	Trusted VPN for Site-to-Site	Любой

Свойства правила межсетевого экрана

Общие

Источник

Пользователи

Назначение

Сервис

Приложения

Время

Использование

История

Включено:

Название:

Описание:

Действие:

Отбросить и:

Сценарий:

Журналирование:

Включить лимит журналирования:

Ограничить число событий, записываемых в журнал:

Максимальное количество пакетов, журналируемых на событие:

Применить правило к:

Вставить:

☒

VPN S2S

✓ Разрешить

Не выбран

Не использовать сценарии

Журналировать начало сессии

☒

3 / час

5

Все пакеты

Наверх списка правил

Сохранить

Отмена

Свойства правила межсетевого экрана

Общие

Источник

Пользователи

Назначение

Сервис

Приложения

Время

Использование

История

Зона источника

Адрес источника

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Tunnel Inspection zone

☐ Untrusted

☐ VPN for remote access

☒ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инvertировать

Добавить

Редактировать

Удалить

Название списка ↑	Владелец
-------------------	----------

Создать и добавить новый объект

☐ Инvertировать

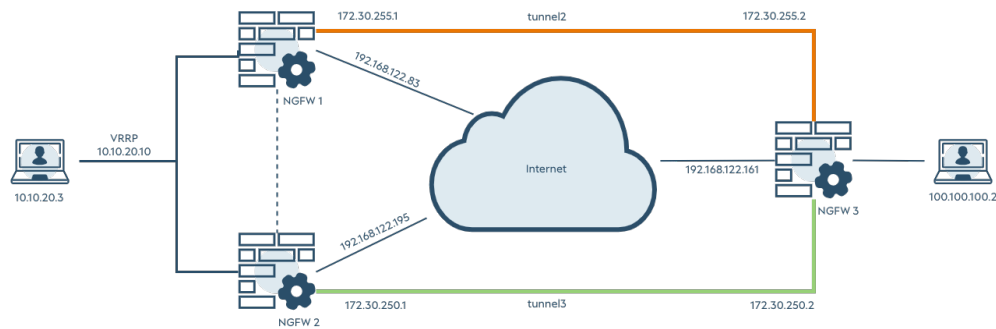
Сохранить

Отмена

KnowledgeBase: ☒
Product: NGFW
Version: 6.x, 7.x
Technology: VPN

Конфигурация

В данном примере рассматривается кластер из двух узлов (NGFW 1, NGFW 2), которые являются vpn-серверами и один удаленный узел (NGFW 3), выполняющий роль vpn-клиента. В примере использована версия ПО UserGate 6.1.9.



Информацию по общим настройкам соединения Site-to-Site можно найти в статье: [VPN для защищенного соединения офисов \(Site-to-Site VPN\)](#).

Для корректной работы схемы понадобятся два клиентских и два серверных правила.

Настройки на стороне VPN-сервера

- В разделе **Сеть** → **Зоны** в зоне, через которую будет строиться туннель, разрешить сервис **VPN**.
- В разделе **Политики сети** → **Межсетевой экран** создать разрешающие правила из нужных зон в зону VPN и обратно.
- В разделе **VPN** → **Профили безопасности** создать профиль безопасности, как указано в статье [VPN для защищенного соединения офисов \(Site-to-Site VPN\)](#). (**ВАЖНО!** Интервал проверки Dead Peer Detection необходимо поставить равным 0)
- В разделе **Сеть** → **Интерфейсы** включить/создать интерфейсы **tunnel2** и **tunnel3**, режим адресации — статический. Указать IP-адреса для этих интерфейсов из разных подсетей, например: 172.30.255.1 и 172.30.250.1, маска 255.255.255.252. Выбрать зону **VPN for Site-to-Site**.

VPN	tunnel2	Статический	172.30.255.1/255.255.255.252	VPN for Site-to-Site
VPN	tunnel3	Статический	172.30.250.1/255.255.255.252	VPN for Site-to-Site

- В разделе **VPN** → **Сети VPN** создать сети VPN, в которых необходимо указать диапазоны подсетей, в которых находятся туннельные интерфейсы, например:

Название	Диапазон IP-адресов	Маска
For tunnel2	172.30.255.1 – 172.30.255.2	255.255.255.252
For tunnel3	172.30.250.1 – 172.30.250.2	255.255.255.252

- В разделе **VPN** → **Серверные правила** создать два серверных правила: зона источника — **Untrusted**, в качестве адреса назначения указывается физический IP-адрес внешнего интерфейса. На каждое правило разный узел. Указать на каждое правило свой интерфейс **tunnel** и соответствующую ему сеть, например:

Адрес назначения	Интерфейс	Профиль безопасности VPN	Сеть VPN	Профиль аутентификации	Пользователи
192.168.122.83	tunnel2	Site-to-Site VPN profile	For tunnel2	Example user auth profile	VPN servers
192.168.122.195	tunnel3	Site-to-Site VPN profile	For tunnel3	Example user auth profile	VPN servers

Настройки на стороне VPN-клиента

- Аналогично стороне VPN-сервера, разрешить сервис **VPN** в зоне **Untrusted** и создать правила межсетевого экрана.
- Создать профиль безопасности, аналогичный серверному.
- Настроить туннельные интерфейсы, обязательно с адресацией в статическом режиме:

VPN	tunnel2	Статиче...	172.30.255.2/255.255.255.252	VPN for Site-to-Site
VPN	tunnel3	Статиче...	172.30.250.2/255.255.255.252	VPN for Site-to-Site

- Создать два клиентских правила до каждого VPN-сервера по соответствующему туннелю.

Адрес сервера	Интерфейс	Профиль безопасности VPN
192.168.122.83	tunnel2	Site-to-Site VPN profile
192.168.122.195	tunnel3	Site-to-Site VPN profile

- Чтобы туннели корректно работали, необходимо, чтобы они строились с разных IP-адресов. На узле VPN-клиента можно использовать secondary адрес или адрес второго провайдера. Также можно создать VIP-адрес с помощью кластера отказоустойчивости. Необходимо создать правило NAT, где в SNAT IP указывается второй (запасной) IP-адрес, а в назначении указать один из VPN-серверов. Таким образом строится два независимых туннеля.

Роль этого устройства	Время сессии	Туннельный IP	IP адрес
Сервер	24 января 2024 г., 02:27 (37 м 13 с)	172.30.255.2	192.168.122.160
Сервер	24 января 2024 г., 02:26 (37 м 53 с)	172.30.250.2	192.168.122.161

Роль этого устройства	Время сессии	Туннельный IP	IP адрес
Клиент	24 января 2024 г., 09:14 ()	172.30.255.2	192.168.122.83
Клиент	24 января 2024 г., 09:13 ()	172.30.250.2	192.168.122.195

OSPF

Необходимо настроить OSPF, чтобы на мастер-узле метрики были автоматически в 2 раза ниже, чем на резервном узле. Так при переходе мастера на клиент придут актуальные маршруты. Общее описание настройки OSPF смотрите в статье [Виртуальные маршрутизаторы](#).

Настройки на стороне VPN-сервера

- В разделе **Сеть** → **Зоны** разрешить **OSPF** в зоне с VPN.
- В разделе **Сеть** → **Виртуальные маршрутизаторы** выбрать **Виртуальный маршрутизатор по умолчанию**, сверху в выпадающем меню **Настройки** выбрать **OSPF**. Поставить флажок **Включить**. В поле **Идентификатор маршрутизатора** можно указать физический адрес узла; главное, что он должен быть уникален для каждого узла. Значение раздела **Redistribute** по документации, кратко: **connected** — маршруты до подключенных сетей; **kernel** — маршруты, прописанные статически.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизаторИнтерфейсыОбласти

Включено:

☒

Идентификатор маршрутизатора:

192.168.122.195

Redistribute

☐ connected☐ kernel

Метрика:

1

☐ Default originate

- Во вкладке **Интерфейсы** добавить интерфейс **tunnel**, соответствующий данному узлу. В данном примере для узла 192.168.122.83 добить интерфейс **tunnel2**. Также, если мы хотим передавать маршрут в подсеть за конкретным интерфейсом, добавить и его. В примере добавили **port2**, за которым находится сеть 10.10.20.0/24.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизаторИнтерфейсыОбласти

Добавить

Редактировать

Включить

Отключить

Удалить

Интерфейс	Стоимость	Приоритет	Аутентификация
tunnel3	1	1	Отключено
port2	1	1	Отключено

- Во вкладке **Области** добавить область, в поле **Идентификатор области** поставить 0.

Свойства

ОбщиеИнтерфейсыВиртуальные линки

Включено:

☒

Название:

area0

Описание:

Стоимость:

1

Идентификатор области:

0

Тип аутентификации:

Нет

Тип области:

Нормальная

☐ Не суммировать

- Во вкладке **Интерфейсы** выбираем добавленные интерфейсы.

Свойства

ОбщиеИнтерфейсыВиртуальные линки

Интерфейс	Описание
☒ tunnel3	
☒ port2	

- На втором узле делаем аналогичные действия, но в поле **Идентификатор маршрутизатора** указываем его физический адрес, а во вкладке **Интерфейсы** — его туннель.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизаторИнтерфейсыОбласти

Включено:

☒

Идентификатор маршрутизатора:

192.168.122.83

Redistribute

☐ connected☐ kernel

Метрика:

1

☐ Default originate

Настройки на стороне VPN-клиента

- Алгоритм такой же, как и для сервера, но необходимо добавить уже оба туннеля сразу. Также в примере добавили **port2**, за которым находится сеть 100.100.100.0/24
- После этого соседство должно установиться.
- Проверка работы туннелей из CLI клиентского узла:

```
PING 172.30.255.1 (172.30.255.1) 56(84) bytes of data.  
64 bytes from 172.30.255.1: icmp_seq=1 ttl=64 time=2.55 ms  
64 bytes from 172.30.255.1: icmp_seq=2 ttl=64 time=3.46 ms  
  
--- 172.30.255.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 2.550/3.007/3.465/0.460 ms  
UTM> ping 172.30.250.1  
PING 172.30.250.1 (172.30.250.1) 56(84) bytes of data.  
64 bytes from 172.30.250.1: icmp_seq=1 ttl=64 time=2.13 ms  
64 bytes from 172.30.250.1: icmp_seq=2 ttl=64 time=1.10 ms  
  
--- 172.30.250.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 1.102/1.616/2.130/0.514 ms  
UTM> _
```

4. На узле VPN-клиента перейти в раздел **Диагностика и мониторинг** —> **Маршруты**. Нажать на значок фильтра и добавить OSPF, после чего должны появиться маршруты полученные посредством OSPF:

```
VRF default:  
O>* 10.10.20.0/24 [110/2] via 172.30.250.1, tunnel3, weight 1, 00:34:35  
O 100.100.100.0/24 [110/1] is directly connected, port2, weight 1, 22:15:29  
O 172.30.250.1/32 [110/1] via 172.30.250.1, tunnel3 inactive, weight 1, 00:34:35  
O>* 172.30.250.2/32 [110/0] is directly connected, tunnel3, weight 1, 22:15:45  
O 172.30.255.1/32 [110/1] via 172.30.255.1, tunnel2 inactive, weight 1, 00:34:02  
O>* 172.30.255.2/32 [110/0] is directly connected, tunnel2, weight 1, 22:15:45
```

Как видно на примере выше, клиент получил маршрут в подсеть 10.10.20.0/24, находящуюся за сервером. Маршрут ведет в интерфейс **tunnel3**, который на данный момент соответствует активному узлу.

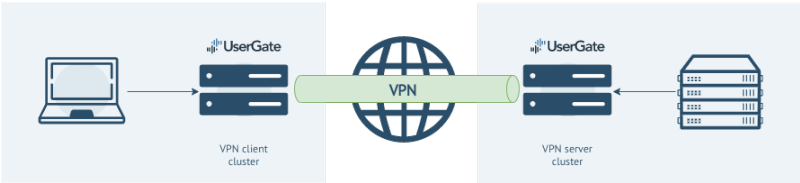
Результат просмотра маршрутов после инициации отключения мастер-узла:

```
VRF default:  
O>* 10.10.20.0/24 [110/2] via 172.30.255.1, tunnel2, weight 1, 00:00:20  
O 100.100.100.0/24 [110/1] is directly connected, port2, weight 1, 22:19:39  
O 172.30.250.1/32 [110/1] via 172.30.250.1, tunnel3 inactive, weight 1, 00:38:45  
O>* 172.30.250.2/32 [110/0] is directly connected, tunnel3, weight 1, 22:19:55  
O 172.30.255.1/32 [110/1] via 172.30.255.1, tunnel2 inactive, weight 1, 00:38:12  
O>* 172.30.255.2/32 [110/0] is directly connected, tunnel2, weight 1, 22:19:55
```

Маршрут был перестроен в другой туннель, который теперь соответствует новому мастер-узлу.

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.x, 7.x
Technology: VPN

Подробнее о настройке [Site-to-Site VPN](#) и [кластера отказоустойчивости](#) читайте в Руководстве администратора.



При настройке соединения Site-to-Site VPN между двумя кластерами отказоустойчивости каждый узел кластера, выступающий в роли VPN-клиента, создает своё соединение с активным узлом кластера VPN-сервера. Необходимо привязать ответный трафик со стороны серверов к узлу, через который подключился клиент.

1. На узлах кластера VPN-сервера необходимо проверить настройки сети VPN, для этого в разделе **VPN → Сети VPN** открыть свойства VPN-сети и проверить размер диапазона IP-адресов. Количества IP-адресов должно быть достаточно для подключения всех узлов VPN-клиентов.

Свойства VPN-сети

Общие

Сеть

Маршруты VPN

Диапазон IP:

172.30.255.2-172.30.255.4

Маска:

255.255.255.0

☒ Использовать системные DNS-серверы

Серверы DNS:

Добавить

Редактировать

Удалить

IP-адрес

Сохранить

Отмена

2. На узлах кластера VPN-клиента необходимо создать два правила NAT:
- Правило NAT из всех разрешенных зон в зону интерфейса tunnel, используемого в клиентском правиле.
 - Правило NAT из зоны интерфейса tunnel, используемого в клиентском правиле, во все разрешенные зоны.

Настройка правил NAT необходима для того, чтобы сервер для отправки ответов клиенту использовал тот же узел, на котором были получены запросы от клиента. Поле SNAT в правилах должно оставаться пустым.

NAT и маршрутизация							
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи							
✓							
#	Тип	Статус журналирования	Название	Зона источника	Адрес источника	Пользователи	Зона назначения
1	NAT		Allowed to VPN	Trusted	Любой	—	VPN for Site-to-Site
2	NAT		VPN to allowed	VPN for Site-to-Site	Любой	—	Trusted

3. При работе с кластерами отказоустойчивости Актив-Актив на узлах кластера VPN-сервера необходимо дополнительно создать правило NAT из зоны интерфейса tunnel, используемого в серверном правиле, во все разрешенные зоны без указания адреса SNAT.

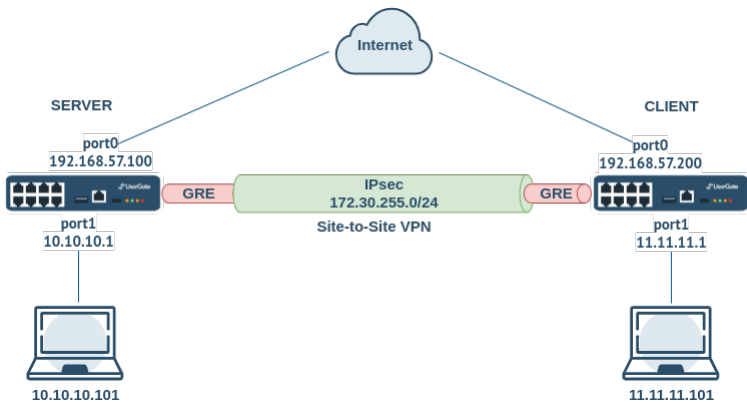
NAT и маршрутизация							
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи							
✓							
#	Тип	Статус журнали...	Название	Зона источника	Адрес источника	Пользователи	Зона назначения
1	NAT		VPN to allowed	VPN for Site-to-Site	Любой	—	Trusted

Примечание Для соединений со стороны кластера VPN-клиента правила NAT избавляют от необходимости создания статических маршрутов. Если требуется устанавливать соединения со стороны VPN-сервера, то для передачи маршрутов от VPN-клиента к VPN-серверу нужно использовать протокол OSPF между интерфейсами tunnel всех узлов обоих кластеров. При работе с кластером отказоустойчивости Актив-Пассив OSPF удваивает стоимости и метрики на пассивном узле. Подробнее о настройке протокола OSPF в UserGate читайте в [Руководстве администратора](#).

Примечание Режимы работы кластера отказоустойчивости (Актив-Актив или Актив-Пассив) относятся только к работе протокола VRRP. VPN-соединение каждый узел кластера, выступающий в роли VPN-клиента, устанавливает независимо.

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

В данной статье рассматривается настройка маршрутизации между двумя сетями по протоколу OSPF с использованием зашифрованного канала связи (IPsec) при помощи GRE-туннеля.



Адресация на UserGate-сервере:

- Выход в интернет настроен через интерфейс port0 с IP-адресом 192.168.57.100.
- Локальная сеть подключена через port1 с IP-адресом 10.10.10.1.
- Туннельному интерфейсу GRE назначен адрес 12.0.0.1.
- IP-адрес VPN-туннеля - 172.30.255.1.

Адресация на UserGate-клиенте:

- Выход в интернет настроен через интерфейс port0 с IP-адресом 192.168.57.200.
- Локальная сеть подключена через port1 с IP-адресом 11.11.11.1.
- Туннельному интерфейсу GRE назначен адрес 12.0.0.2.
- IP-адрес VPN-туннеля - 172.30.255.2.

Как видно из схемы, представленной выше, между 2-мя UserGate настроено Site-to-Site VPN-соединение. Подробнее о настройке Site-to-Site VPN читайте в соответствующем разделе [UserGate 6. Ручководство администратора](#).

Далее будет рассмотрена настройка туннеля GRE и OSPF; считается, что между устройствами настроено Site-to-Site VPN-соединение; заданы правила межсетевого экрана, разрешающие трафик.

Настройка GRE-туннеля.

1. Перейдите в раздел **Сеть → Интерфейсы**, нажмите **Добавить** и выберите **Добавить туннель**.
2. Во вкладке **Общие** укажите:
 - Порядковый номер туннельного интерфейса.
 - **Описание** (опционально).
 - **Зону**, которой будет относиться интерфейс (**VPN for Site-to-Site**).

Настройка туннельного интерфейса

Общие

Сеть

Включено: ☒

Название:

Описание:

Имя узла:

utmcore@ageterithpre

Зона:

VPN for Site-to-Site

Сохранить

Отмена

Перейдите во вкладку **Сеть** и задайте следующие параметры (в качестве локального и удалённого IP-адресов используются IP-адреса VPN-интерфейсов):

- **MTU:** 1400.
- **Локальный IP:** 172.30.255.1.
- **Удалённый IP:** 172.30.255.2.
- **Режим:** GRE.
- **IP-адрес интерфейса и маску :** 12.0.0.1/24.

Настройка туннельного интерфейса

Общие **Сеть**

MTU: 1400

Локальный IP: 172.30.255.1

Удаленный IP: 172.30.255.2

Режим: GRE

VXLAN ID: 0

IP интерфейса

+ Добавить ✎ Редактировать ✖ Удалить

IP интерфейса	Маска
12.0.0.1	255.255.255.0

Сохранить Отмена

На UserGate-клиенте настройка туннельного интерфейса производится аналогично; измените локальный (172.30.255.2) и удаленный (172.30.255.1) IP-адреса и IP-адрес интерфейса (12.0.0.2/24).

Настройка OSPF.

- В разделе **Сеть** → **Зоны** в свойствах зоны, к которой относится VPN-интерфейс, во вкладке **Контроль доступа** разрешите сервис **OSPF** (по умолчанию VPN for Site-to-Site).
- Перейдите в раздел **Сеть** → **Виртуальные маршрутизаторы**. Можно использовать виртуальный маршрутизатор, созданный по умолчанию, или добавить новый маршрутизатор. Далее необходимо настроить OSPF-роутер.

Во вкладке **OSPF-маршрутизатор**:

- Активируйте чекбокс **Включено**.
- Укажите **идентификатор маршрутизатора** - IP-адрес маршрутизатора; должен совпадать с одним из адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору.
- Укажите **Redistribute connected**, т.е. распространять другим OSPF-роутерам маршруты в непосредственно подключенные к UserGate сети.
- Установите метрику распространяемым маршрутам.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор Интерфейсы Области

Включено: ☒

Идентификатор маршрутизатора: 192.168.57.100

Redistribute

☐ connected ☐ kernel

Метрика: 1

☐ Default originate

Сохранить Отмена

Во вкладке **Интерфейсы** укажите интерфейсы, на которых будет работать протокол динамической маршрутизации OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор **Интерфейсы** Области

+ Добавить ✎ Редактировать Включить Отключить ✖ Удалить

Интерфейс	Стоимость	Приоритет	Аутентификация
port1	1	1	Отключено
gre1	1	1	Отключено

Сохранить Отмена

Во вкладке **Области** создайте область OSPF, указав интерфейсы, на которых она будет доступна.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор Интерфейсы **Области**

+ Добавить ✎ Редактировать Включить Отключить ✖ Удалить

Имя	Стоимость	Идентифи...	Тип области	Тип авторизации	Интерфейсы	Виртуальные ...
test_area	1	0	Нормальная	Нет	port1 gre1	Любой

Сохранить Отмена

Проверка. Для проверки анонсов маршрутов перейдите во вкладку **Диагностика и мониторинг** в раздел **Мониторинг** → **Маршруты** веб-интерфейса UserGate. Задайте фильтр, указав просмотр маршрутов **OSPF**.

Маршруты

Узел: utmcore@thethurati Виртуальный маршрутизатор: Виртуальный маршрути Обновить OSPF X

Codes: K - kernel route, C - connected, S - static, R - RIP
 O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP
 T - Table, V - VNC, V - VNC-Direct, A - Babel, D - SHARP
 F - PBR, I - OpenFabric
 > - selected route, * - FIB route, q - queued route, r - rejected route

```

O 10.10.10.0/24 [110/10] is directly connected, port1, weight 1, 00:19:28
O* 11.11.11.0/24 [110/20] via 12.0.0.2, gre1, weight 1, 00:16:22
O 12.0.0.0/24 [110/10] is directly connected, gre1, weight 1, 00:16:52
O 172.30.255.0/24 [110/1] via 12.0.0.2, gre1, weight 1, 00:16:21
  
```

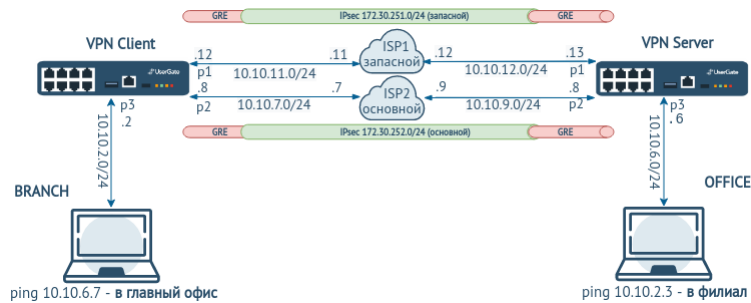
На рисунке ниже представлен анализ трафика, из которого видно, что передача происходит по зашифрованному каналу.

No.	Time	Source	Destination	Protocol	Length	Info
1 0	192.168.57.100	93.91.171.46	SSH	222	Client: Encrypted packet (len=108)	
2 0	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=169 Win=4038 Len=0	
3 0	192.168.57.100	192.168.57.100	ESP	290	ESP (SPI=0xe9dcebab)	
5 0	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
6 0	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=257 Win=4038 Len=0	
8 1	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
9 1	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=345 Win=4038 Len=0	
12 2	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
13 2	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=433 Win=4038 Len=0	
16 3	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
17 3	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=521 Win=4038 Len=0	
18 4	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
19 4	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=609 Win=4038 Len=0	
21 5	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
22 5	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=697 Win=4038 Len=0	
25 6	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
26 7	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=785 Win=4038 Len=0	
28 7	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
29 7	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=873 Win=4038 Len=0	
30 8	192.168.57.100	192.168.57.200	ESP	190	ESP (SPI=0x36458e4b)	
31 8	192.168.57.100	93.91.171.46	SSH	142	Client: Encrypted packet (len=88)	
32 9	93.91.171.46	192.168.57.100	TCP	60	22 - 2638 [ACK] Seq=1 Ack=961 Win=4038 Len=0	
33 9	192.168.57.100	192.168.57.200	ESP	190	ESP (SPI=0x36458e4b)	
34 9	192.168.57.200	192.168.57.100	ESP	190	ESP (SPI=0xe9dcebab)	
35 9	192.168.57.200	192.168.57.100	ESP	190	ESP (SPI=0xe9dcebab)	

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

Подробную инструкцию по настройке VPN-соединений и виртуальных маршрутизаторов читайте в [UserGate 6. Руководство администратора](#).

Рассмотрим создание отказоустойчивого VPN-соединения между двумя UserGate с использованием сетей двух провайдеров.



Исходные данные. Создано соединение между двумя UserGate: UserGate VPN Server - UserGate, за которым подключена локальная сеть офиса с IP-адресом 10.10.6.0/24, и UserGate VPN Client - UserGate, за которым подключена локальная сеть филиала с IP-адресом 10.10.2.0/24.

Между офисом и филиалом подняты VPN-туннели через разных провайдеров с адресами 172.30.251.0/24 и 172.30.252.0/24. На обоих UserGate были произведены сетевые настройки. На каждом UserGate для выхода в сети провайдеров были указаны шлюзы: на UserGate VPN Server - 10.10.9.9 и 10.10.12.12; на UserGate VPN Client - 10.10.7.7 и 10.10.11.11.

Для установки VPN соединения через сети двух провайдеров на UserGate VPN Server были настроены интерфейсы с IP-адресами 172.30.252.1 (для основного подключения) и 172.30.251.1 (для резервного канала); на UserGate VPN Client - 172.30.252.2 (для основного подключения) и 172.30.251.2 (для резервного канала).

На обоих UserGate в разделе **Сеть → Виртуальные маршрутизаторы** были настроены статические маршруты.

Маршруты на UserGate VPN Server.

- Выход в сеть 10.10.11.0/24 через интерфейс с адресом 10.10.12.12.
- Выход в сеть 10.10.7.0/24 через интерфейс с адресом 10.10.9.9.

Маршруты на UserGate VPN Client.

- Выход в сеть 10.10.12.0/24 через интерфейс с адресом 10.10.11.11.
- Выход в сеть 10.10.9.0/24 через интерфейс с адресом 10.10.7.7.

На каждом из UserGate в разделе **Политики сети → NAT** и маршрутизация были настроены правила типа **Policy-based routing**.

Правила Policy-based routing, предназначенные для основного канала связи, сценариев не используют. Правило, настроенное на UserGate VPN Server и предназначенное для резервного канала связи, настроено на негативный сценарий с проверкой связи до внешнего IP-адреса основного канала UserGate VPN Client.

Правило, настроенное на UserGate VPN Client и предназначенное для резервного канала связи, настроено на негативный сценарий с проверкой связи до внешнего IP-адреса основного канала UserGate VPN Server. Т.к. правило основного канала не использует сценариев, то правило, настроенное для резервного канала, необходимо поставить выше.

Сценарии можно добавить и настроить в разделе **Политики безопасности → Сценарии**. Во вкладке **Общие** указать, что сценарий должен применяться для всех пользователей в течение 2 минут. Во вкладке **Условия** выбрать **Проверка состояния** и указать следующие параметры.

- Метод:** ping.
- Адрес:** 10.10.7.8 (при настройке добавлении сценария на UserGate VPN Server) и 10.10.9.8 (при настройке добавлении сценария на UserGate VPN Client).
- Шлюз:** 10.10.9.9 (при настройке добавлении сценария на UserGate VPN Server) и 10.10.7.7 (при настройке добавлении сценария на UserGate VPN Client).
- Результат:** отрицательный.
- Таймаут подключения:** 1 сек.
- Количество срабатываний:** 1.
- За интервал:** 1.

Создание сценария на UserGate VPN Server:

Свойства сценария

Общие Условия

Включено: ☒

Название: ping rule

Описание:

Применить для: всех пользователей

Продолжительность: 2 минут

Сохранить Отмена

Свойства сценария

Общие Условия

Сценарий работает, если выполняются все условия

добавить редактировать удалить

Выберите тип проверки

Метод: ping

Адрес: 10.10.7.8

FQDN запроса:

Шлюз: 10.10.9.9 (utmcore@sticomardsta)

Результат: Отрицательный

Таймаут подключения (сек): 1

Таймаут ответа (сек):

Тип DNS запроса: a

Количество срабатываний: 1

За интервал: 1 интервал времени в минутах

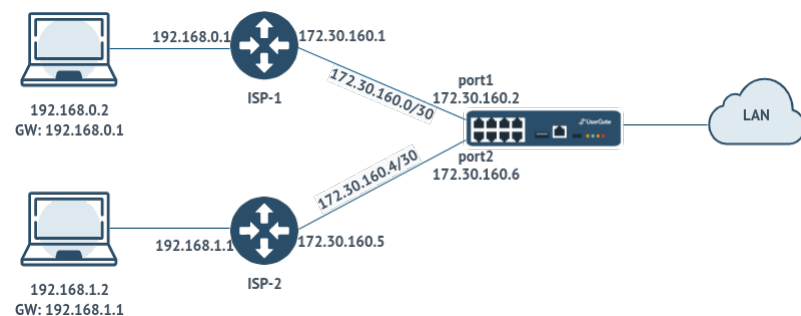
Сохранить Отмена

Переход на резервный канал при разрыве соединения в основном происходит за счёт срабатывания негативного сценария в правиле Policy-based routing резервного канала. Срабатывание сценария произойдет при отрицательном результате ping с UserGate VPN Client до внешнего IP-адреса основного канала UserGate VPN Server или с UserGate VPN Server до внешнего IP-адреса основного канала UserGate VPN Client. Таким образом, в результате выполнения сценария будет добавлен маршрут до сети филиала либо офиса с более высоким приоритетом через шлюз запасного VPN.

После восстановления основного канала связи через 2 минуты сценарий отключается и удаляет созданный ранее маршрут. Запросы начинают проходить через основной канал.

Настройка VPN для удалённого доступа клиентов (Remote access VPN) при использовании двух провайдеров

Product: UserGate NGFW
Version: 6.1.8, 6.1.9



Подробнее о настройке VPN читайте в [UserGate 6. Руководство администратора](#).

Необходимо настроить UserGate для предоставления удалённого доступа клиентам из подсетей 172.30.160.0/30, подключённой к UserGate через **port1** с адресом 172.30.160.2, и 172.30.160.4/30, подключённой к UserGate через **port2** с адресом 172.30.160.6.

В разделе **Сеть** → **Шлюзы** были добавлены шлюзы с IP-адресами 172.30.160.1 и 172.30.160.5. Шлюз с адресом 172.30.160.1 указан как шлюз по умолчанию.

Название	IP шлюза	Вес	Балансировка	Виртуальный ма...	Интерфейс	MAC	Прот...	
Узел кластера: utmcore@ediverheinal (текущий узел)								
ISP-1 (По умолчанию)	172.30.160.1	1	Отключено	Виртуальный м...	Автомат...	00:0c:29:5a:d4:73	static	●
ISP-2	172.30.160.5	1	Отключено	Виртуальный м...	Автомат...	00:0c:29:5a:d4:7d	static	●

- В разделе **Сеть** → **Зоны** создайте зоны, с которых будет разрешено подключение по VPN, например, **ISP-1** - зона для провайдера 1; **ISP-2** - зона для провайдера 2. Для обеих зон во вкладке **Контроль доступа** разрешите сервис **VPN**.

Свойства сетевой зоны

Общие

Контроль доступа

Защита от IP-спуфинга

Разрешённые сервисы	Разрешённые адреса
☒ Ping	Любой
☐ SNMP	Любой
☐ Captive-портал и страница блокировки	Любой
☐ Кластер	Любой
☐ VRRP	Любой
☐ Консоль администрирования	Любой
☐ DNS	Любой
☐ HTTP(S)-прокси	Любой
☐ Агент авторизации	Любой
☐ SMTP(S)-прокси	Любой
☐ POP3(S)-прокси	Любой
☐ CLI по SSH	Любой
☒ VPN	Любой

Сохранить

Отмена

- Перейдите в раздел **Сеть** → **Интерфейсы**, выберите интерфейс **port1** и назначьте ему соответствующую первому провайдеру зону, созданную на шаге 1 (в данном примере: зону **ISP-1**).

Свойства интерфейса

Общие

Сеть

DHCP-релей

Включено:

☒

Название:

port1

Описание:

Тип интерфейса:

Layer 3

Имя узла:

utmcore@nthardspende

Зона:

ISP-1

Профиль netflow:

Не выбран

Сохранить

Отмена

Выберите интерфейс **port2** и назначьте ему соответствующую второму провайдеру зону, созданную на шаге 1 (в данном примере: зону **ISP-2**).

Свойства интерфейса

Общие

Сеть

DHCP-релей

Включено:

☒

Название:

port2

Описание:

Тип интерфейса:

Layer 3

Имя узла:

utmcore@nthardspende

Зона:

ISP-2

Профиль netflow:

Не выбран

Сохранить

Отмена

3. Создайте VPN-интерфейс в разделе **Сеть → Интерфейсы**. Был использован созданный по умолчанию интерфейс **tunnel1**, который рекомендуется использовать для Remote access VPN.
4. Перейдите в раздел **VPN → Сети VPN** и добавьте сеть VPN, указав необходимые параметры. Можно, как в данном примере, использовать сеть **Remote access VPN network**, созданную по умолчанию.
5. Перейдите в раздел **Пользователи → Профили авторизации** и создайте профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP.
6. Создайте профиль безопасности в разделе **VPN → Профили безопасности VPN**. По умолчанию в UserGate создан серверный профиль **Remote access VPN profile**, задающий необходимые настройки. Данный профиль был использован в данном примере.

При использовании данного профиля необходимо изменить общий ключ шифрования.

7. Создайте серверное правило в разделе **VPN → Серверные правила**. Можно, как в данном примере, использовать правило, созданное по умолчанию **Remote access VPN rule**. Во вкладке **Общие** укажите:
 - Отметьте чекбокс **Включено**.
 - **Название** правила.
 - **Описание** (опционально).
 - **Профиль безопасности**, созданный в пункте 6.
 - **Сеть VPN**, созданную в пункте 4.
 - **Профиль авторизации**, созданный в пункте 5.
 - **Интерфейс**, созданный в пункте 3.

Во вкладке **Источник** укажите зоны или адреса, с которых разрешено подключение (в данном случае - это зоны ISP-1 и ISP-2).

Во вкладке **Пользователи** укажите пользователей, которым разрешено подключение по VPN.

Список пользователей, подключённых по VPN, доступен во вкладке **Диагностика и мониторинг** в разделе **Мониторинг → VPN**.

Пользователь	Роль этого сервера	Время сессии	Туннельный IP	IP адрес	GeO IP	Шифрование
vpn1	Сервер	08 апреля 20...	172.30.250.2	192.168.0.2		aes
vpn2	Сервер	08 апреля 20...	172.30.250.3	192.168.1.2		aes

В соответствии с данными настройками, если, запрос на подключение будет приходить на UserGate (**port1** или **port2**), то ответ будет отправлен через порт первого провайдера (**port1**), т.к. первый провайдер указан в качестве шлюза по умолчанию. В таком случае первый провайдер при наличии защиты от антиспуфинга может отбросить пакет, т.к. он ожидает ответ от 172.30.160.2, а получает от 172.30.160.6. Чтобы исключить возникновение такой ситуации, необходимо настроить правила типа **Policy-based routing**. Т.к. в данном примере один из шлюзов указан в качестве шлюза по умолчанию, то достаточно настроить одно правило PBR. Если шлюз по умолчанию не обозначен, то необходимо настроить соответствующее правило и для другого провайдера.

Настройте правило для провайдера 2. Для этого перейдите в раздел **Политики сети → NAT и маршрутизация** и нажмите **Добавить**. Во вкладке **Общие** укажите:

- Отметьте чекбокс **Включено**.
- **Название** правила.
- **Описание** (опционально).
- **Тип**: Policy-based routing.
- **Шлюз**: выберите шлюз провайдера 2 (в примере: ISP-2).

Свойства правила

Общие

Источник

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Включено:

Название:

Описание:

Тип:

Шлюз:

Сценарий:

SNAT IP (внешний адрес):

Журналирование:

Включить лимит журналирования:

Ограничить число событий, записываемых в журнал:

Максимальное количество пакетов, журналируемых на событие:

НAT — Преобразование сетевых адресов. Обычно используется для разрешения доступа из локальной сети в интернет.
DNAT — Перенаправляет трафик на указанный IP-адрес. Обычно используется для публикации внутренних ресурсов в интернет.
Policy-based routing — Позволяет маршрутизировать IP-пакеты на основе расширенной информации, например, сервисов, MAC-адресов или серверов (IP-адресов).
SNAT IP — Адрес, на который будет заменен адрес источника для трафика NAT.
Порт-форвардинг — Так же, как и DNAT, обычно используется для публикации внутренних ресурсов в интернет, но способен изменять номер порта публикуемого сервиса.
Network mapping — Позволяет произвести замену IP-адресов источника или назначения одной сети на другую сеть.

Сохранить

Отмена

Во вкладке **Источник** на панели **Адрес источника** необходимо добавить IP-адрес интерфейса, к которому подключён провайдер 2. IP-адрес интерфейса должен быть добавлен в список IP-адресов, который можно создать в разделе **Библиотеки** → **IP-адреса** или при настройке правила (для этого нажмите **Создать и добавить новый объект** и укажите название списка и адрес).

Свойства правила

Общие

Источник

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Зона источника

Адрес источника

Создать и добавить новый объект

Инвертировать

Создать и добавить новый объект

Инвертировать

Сохранить

Отмена

Проверка. Для проверки использовалась программа-анализатор Wireshark.

Обратный пакет клиент из подсети 192.168.0.0/24 получает от **port1** (172.30.160.2).

1	2022-04-08	12:02:24,999745	192.168.0.2	172.30.160.2	500	500
2	2022-04-08	12:02:25,054988	172.30.160.2	192.168.0.2	500	500
3	2022-04-08	12:02:25,057534	192.168.0.2	172.30.160.2	500	500
4	2022-04-08	12:02:25,062930	172.30.160.2	192.168.0.2	500	500
5	2022-04-08	12:02:25,064217	192.168.0.2	172.30.160.2	500	500
6	2022-04-08	12:02:25,065360	172.30.160.2	192.168.0.2	500	500
7	2022-04-08	12:02:25,066736	192.168.0.2	172.30.160.2	500	500
8	2022-04-08	12:02:25,070959	172.30.160.2	192.168.0.2	500	500
9	2022-04-08	12:02:25,075105	192.168.0.2	172.30.160.2	500	500

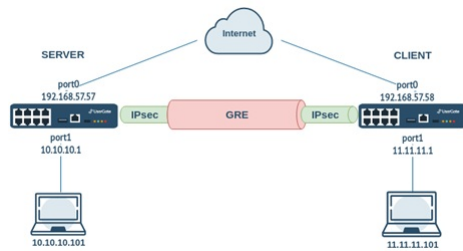
Клиент из подсети 192.168.1.0/24 получает обратный пакет от **port2** с IP-адресом 172.30.160.6.

1	2022-04-08	12:03:30,972277	192.168.1.2	172.30.160.6	500	500
2	2022-04-08	12:03:31,034253	172.30.160.6	192.168.1.2	500	500
3	2022-04-08	12:03:31,052379	192.168.1.2	172.30.160.6	500	500
4	2022-04-08	12:03:31,059912	172.30.160.6	192.168.1.2	500	500
5	2022-04-08	12:03:31,061454	192.168.1.2	172.30.160.6	500	500
6	2022-04-08	12:03:31,062727	172.30.160.6	192.168.1.2	500	500
7	2022-04-08	12:03:31,064501	192.168.1.2	172.30.160.6	500	500
8	2022-04-08	12:03:31,067704	172.30.160.6	192.168.1.2	500	500
9	2022-04-08	12:03:31,069303	192.168.1.2	172.30.160.6	500	500

Настройка IPsec over GRE с OSPF

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

В данной статье рассматривается настройка маршрутизации между двумя сетями по протоколу OSPF с использованием GRE-туннеля, в который будут инкапсулированы зашифрованные пакеты (IPsec).



Адресация на UserGate-сервере:

- Выход в интернет настроен через интерфейс port0 с IP-адресом 192.168.57.57.
- Локальная сеть подключена через port1 с IP-адресом 10.10.10.1.
- Туннельному интерфейсу GRE назначен адрес 12.12.12.1.
- IP-адрес VPN-туннеля - 172.30.255.1.

Адресация на UserGate-клиенте:

- Выход в интернет настроен через интерфейс port0 с IP-адресом 192.168.57.58.
- Локальная сеть подключена через port1 с IP-адресом 11.11.11.1.
- Туннельному интерфейсу GRE назначен адрес 12.12.12.2.
- IP-адрес VPN-туннеля - 172.30.255.2.

Настройка GRE-туннеля.

1. Перейдите в раздел **Сеть → Интерфейсы** нажмите **Добавить** и выберите **Добавить туннель**.
2. Во вкладке **Общие** укажите:
 - Порядковый номер туннельного интерфейса.
 - **Описание** (опционально).
 - **Зону**, которой будет относиться интерфейс (Untrusted).

Перейдите во вкладку **Сеть** и задайте следующие параметры (в качестве локального и удалённого IP-адресов используются IP-адреса внешних интерфейсов UserGate):

- **MTU:** 1500.
- **Локальный IP:** 192.168.57.57.
- **Удалённый IP:** 192.168.57.58.
- **Режим:** GRE.
- **IP-адрес интерфейса и маску:** 12.12.12.1/24.

На UserGate-клиенте настройка туннельного интерфейса производится аналогично; измените локальный (192.168.57.58) и удалённый (192.168.57.57) IP-адреса и IP-адрес интерфейса (12.12.12.24).

Далее необходимо настроить Site-to-Site VPN-соединение между двумя UserGate. Подробнее о настройке читайте в соответствующем разделе [UserGate 6. Руководство администратора](#).

Примечание! При настройке клиентского правила в качестве IP-адреса сервера VPN необходимо указать адрес туннельного интерфейса GRE, заданный на UserGate-сервере.

Настройка OSPF.

1. В разделе **Сеть → Зоны** в свойствах зоны, к которой относится VPN-интерфейс, во вкладке **Контроль доступа** разрешите сервис **OSPF** (по умолчанию VPN for Site-to-Site).
2. Перейдите в раздел **Сеть → Виртуальные маршрутизаторы**. Можно использовать виртуальный маршрутизатор, созданный по умолчанию, или добавить новый маршрутизатор. Далее необходимо настроить OSPF-роутер.

Во вкладке **OSPF-маршрутизатор**:

- Активируйте чекбокс **Включено**.
- Укажите **идентификатор маршрутизатора** - IP-адрес маршрутизатора; должен совпадать с одним из адресов, назначенным сетевым интерфейсам UserGate, относящимся к данному виртуальному маршрутизатору.
- Укажите **Redistribute connected**, т.е. распространять другим OSPF-роутерам маршруты в непосредственно подключённые к UserGate сети (опционально).
- Укажите **Redistribute kernel**, т.е. распространять другим OSPF-роутерам маршруты, которые были автоматически созданы ядром операционной системы (опционально).
- Установите метрику распространяемым маршрутам.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор Интерфейсы Области

Включено: ☒

Идентификатор маршрутизатора: 192.168.57.51

Redistribute

☐ connected ☐ kernel

Метрика: 1

☐ Default originate

Сохранить Отмена

Во вкладке **Интерфейсы** укажите интерфейсы, на которых будет работать протокол динамической маршрутизации OSPF. Интерфейсы должны быть предварительно добавлены в маршрутизатор по умолчанию; интерфейс может принадлежать только одному виртуальному маршрутизатору.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор Интерфейсы Области

Добавить Редактировать Включить Отключить Удалить

Интерфейс	Стоимость	Приоритет	Аутентифика...
port1	1	1	Отключено
tunnel2	1	1	Отключено

Сохранить Отмена

Во вкладке **Области** создайте область OSPF, указав интерфейсы, на которых она будет доступна.

Свойства виртуального маршрутизатора

OSPF

OSPF-маршрутизатор Интерфейсы Области

Добавить Редактировать Включить Отключить Удалить

Имя	Стоимость	Идентифика...	Тип области	Тип аутентификации	Интерфейсы	Виртуальн...
area	1	1	Нормальная	Нет	port1 tunnel2	Любой

Сохранить Отмена

На этом настройка IPsec over GRE с использованием протокола динамической маршрутизации OSPF окончена.

Настройка GRE-туннеля

KnowledgeBase: ☒
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

- 1. Перейдите в раздел **Сеть → Интерфейсы** нажмите **Добавить** и выберите **Добавить туннель**.
- 2. Укажите необходимые данные об интерфейсе.

Во вкладке **Общие** укажите:

- Порядковый номер туннельного интерфейса (будет использоваться в названии интерфейса; после создания интерфейса, изменение номера недоступно).
- **Описание** (опционально).
- **Зону**, которой будет принадлежать интерфейс.

Настройка туннельного интерфейса

Общие

Сеть

Включено: ☒

Название: gre1 1

Описание:

Имя узла: utmcore@einoreheiss

Зона: Зона не установлена

Сохранить

Отмена

Перейдите во вкладку **Сеть** и задайте следующие параметры:

- **MTU**.
- **Локальный IP**: IP-адрес внешнего интерфейса UserGate A, на котором производится настройка GRE-туннеля.
- **Удалённый IP**: IP-адрес внешнего интерфейса UserGate B, до которого создаётся туннель GRE.
- **Режим работы туннеля**: GRE.
- **IP-адрес интерфейса и маску**: туннельный IP-адрес и маска.

Настройка туннельного интерфейса

Общие

Сеть

MTU: 1500

Локальный IP: 172.31.255.1

Удалённый IP: 172.31.255.2

Режим: GRE

VXLAN ID: 0

Добавить

Редактировать

Удалить

IP интерфейса	Маска
12.0.0.1	255.255.255.0

Сохранить

Отмена

Произведите аналогичную зеркальную настройку локального и удалённого IP-адресов на UserGate B, до которого настраивается GRE-туннель. Измените локальный IP-адрес на 172.31.255.2 и удалённый - на 172.31.255.1 IP-адреса, туннельный IP-адрес интерфейса назначьте из подсети 12.0.0.0/24.

Если локальный и удалённый IP-адреса принадлежат разным подсетям, обеспечьте маршрутизацию между ними в разделе **Сеть → Виртуальные маршрутизаторы**.

Во вкладке **Диагностика и мониторинг** в разделе **Сеть → Ping** проверьте сетевую доступность узлов UserGate внутри туннеля.

Ping

Настройка ping

Ping host: 12.0.0.2

TTL: 30

Интерфейс: 12.0.0.1 (gre1)

Старт

Сброс

Счётчик: 6

☐ Показывать временные метки

☐ Не резолвить имена

Вывод ответа

```
PING 12.0.0.2 (12.0.0.2) from 12.0.0.1 : 56(84) bytes of data.  
64 bytes from 12.0.0.2: icmp_seq=1 ttl=64 time=0.626 ms  
64 bytes from 12.0.0.2: icmp_seq=2 ttl=64 time=0.564 ms  
64 bytes from 12.0.0.2: icmp_seq=3 ttl=64 time=19.2 ms  
64 bytes from 12.0.0.2: icmp_seq=4 ttl=64 time=0.331 ms  
64 bytes from 12.0.0.2: icmp_seq=5 ttl=64 time=0.434 ms  
64 bytes from 12.0.0.2: icmp_seq=6 ttl=64 time=0.422 ms  
  
--- 12.0.0.2 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5067ms  
rtt min/avg/max/mdev = 0.331/3.602/19.238/6.993 ms
```

Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:

В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя — в роли VPN-клиента.
Сначала необходимо настроить VPN-сервер, затем произвести настройки VPN-клиента на компьютере пользователя и инициировать подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки узла NGFW в качестве VPN-сервера необходимо выполнить следующие шаги:

- Шаг 1.** Разрешить сервис **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.
- В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы VPN и Подключение конечных устройств в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).
- Шаг 2.** Создать зону для VPN подключений.
- В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).
- Шаг 3.** Настроить параметры аутентификации.
1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.
- В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

Создадим профиль клиентских сертификатов в веб-консоли администратора NGFW, исполняющего роль VPN-сервера. Для этого необходимо перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле **Common-name, Subject altname email** или **Principal name** для получения имени пользователя:

2. Создадим профиль аутентификации для VPN пользователей. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль аутентификации в домене testd.local через LDAP-коннектор:

Шаг 4. Создать профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создадим профиль безопасности, указав в настройках следующие ключевые параметры:

1

2

3

4

5

1. **Протокол.** В данном примере для создания защищенного канала будет использоваться протокол IKEv2.
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере можно не указывать тип идентификации.
3. Указать **сертификат сервера**, импортированный ранее на [Шаге 3](#).
4. В качестве **режима аутентификации** выберем PKI.
5. Выберем профиль клиентского сертификата, созданный ранее на [Шаге 3](#).
- Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле по умолчанию:

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

1

2

3

1. Поставить флажок включения интерфейса.
2. **Название** — название интерфейса уже задано (tunnel1).
3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключающиеся по VPN к NGFW, будут также помещены в эту зону. В данном примере указывается зона VPN for Remote access.

4

5

6

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.250.1, который задается в поле **6**.
5. **MTU** — размер MTU в данном примере оставим по умолчанию.
6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.
- Шаг 6.** Создать сеть VPN.
- В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Remote access VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

3

4

5

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.250.1), используемому совместно с данной сетью.
2. **Маска** сети VPN.
3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

4

4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть офиса 10.10.0.0/24.

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

1

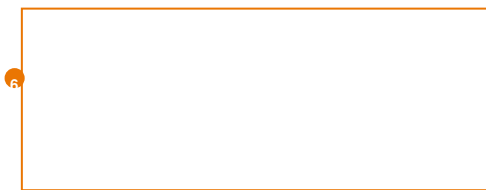
2

3

4

5

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (RA 1).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).



6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. **Пользователи** — доменные пользователи, которым разрешено пользоваться сервисом VPN.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

1. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**. По умолчанию оно не активно. Необходимо его включить.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

В данном примере рассмотрим настройку "нативных" клиентов для операционных систем Windows и Linux для удаленного VPN-подключения.

Встроенный VPN-клиент OS Windows

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Импортировать ранее созданный пользовательский сертификат в хранилище сертификатов компьютера в личную папку:

Сертификат корневого центра импортировать в раздел **Доверенные корневые центры сертификации**:

2. Кликнуть правой кнопкой мыши по значку сетевого подключения в трее и выбрать пункт **Открыть "Параметры сети и Интернет"**.
3. В появившемся окне **Параметры** выбрать пункт **VPN**, а затем нажать на пункт **Добавить VPN-подключение**:



4. В окне Добавить VPN-подключение настроить параметры подключения:
- В поле **Поставщик услуг VPN** выбрать **Windows (встроенные)**;
 - В поле **Имя подключения** указать имя для этого подключения (IKEv2 VPN);
 - В поле **Имя** или **адрес сервера** указать доменное имя NGFW (ug.testd.local);
 - В поле **Тип VPN** выбрать **IKEv2**;
 - В поле **Тип данных для входа** выбрать **Сертификат**;

5. Нажать кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.
6. В панели управления перейти в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выбрать пункт **Настройки параметров адаптера**:



7. Выбрать только что созданное сетевое подключение **IKEv2 VPN** и через меню правой кнопки мыши перейти в свойства этого подключения. В открывшемся окне перейти во вкладку **Безопасность**:



Выбрать пункт **Использовать сертификаты компьютеров**.

Чтобы в туннель заворачивался не весь трафик, на вкладке **Сеть** открыть свойства **IP версии 4 (TCP/IPv4)**:

Нажать **Дополнительно** в настройках общих параметров IP:

Убрать флажок в поле **Использовать основной шлюз в удаленной сети** :

8. Сохранить настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **IKEv2 VPN** и нажмите кнопку **Подключиться**.

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

На стороне удаленного Windows-компьютера добавится rpp-адаптер IKEv2 VPN, хост (10.10.0.100) в сети офиса доступен:

IKEv2 VPN-клиент (strongswan) для OS Linux

Рассмотрим настройку IKEv2 VPN-клиента для Linux на примере OS Ubuntu.

Для начала необходимо установить дополнительные пакеты для работы с IKEv2 VPN:

```
sudo apt update && sudo apt upgrade
```

```
sudo apt install network-manager-strongswan libcharon-extra-plugins
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



2. Выбрать из списка опцию **IPsec/IKEv2 (strongswan)**:

3. В настройках VPN перейти на вкладку **Идентификация**. Указать название соединения, метод аутентификации (Certificate), способ аутентификации (Certificate/private key), указать заранее созданные файлы клиентского сертификата и ключа, параметры соединения:

4. На вкладке IPv4 оставить указанный по умолчанию метод получения адресов по DHCP:

5. В системе должен присутствовать корневой сертификат. При необходимости нужно поместить его в системный раздел /etc/ssl/certs/.

Настройка VPN-клиента завершена.

Для установления VPN-соединения нажать кнопку включения созданного соединения VPN:

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

На стороне удаленного Linux-компьютера добавится виртуальный адаптер, хост (10.10.0.100) в сети офиса доступен:

Для частного случая, когда в среде OS Windows необходимо в явном виде выбирать один из нескольких имеющихся в хранилище пользователя (Current User) сертификатов, подходит следующее решение:

На VPN-сервере

UserGate NGFW начиная с релиза ПО 7.2.0 поддерживает метод аутентификации EAP TLS. Необходимо в настройках профиля безопасности VPN (см. [Шаг 4](#) в настройках VPN-сервера) указать в поле режима аутентификации: **AAA**.

На VPN-клиенте

На [шаге 7](#) настройки встроеного VPN-клиента OS Windows сделать следующую конфигурацию:

- В настройках параметров адаптера через меню правой кнопки мыши перейти в свойства созданного подключения (в данном примере это подключение с названием **IKEv2 VPN**). В открывшемся окне перейти во вкладку **Безопасность**:

В разделе **Проверка подлинности** выбрать **Протокол расширенной проверки подлинности (EAP) → Microsoft смарт-карта или иной сертификат**.

- В свойствах выбранного метода проверки подлинности выбрать опцию **Использовать сертификат на этом компьютере** и поставить флажок **Использовать для подключения другое имя пользователя** :

На контроллере домена

Настроить NPS для новой политики:

Остальные шаги настройки [VPN-сервера](#) и [встроеного VPN-клиента OS Windows](#) аналогичны рассмотренным ранее в этой статье.

При установлении VPN-соединения со стороны клиента кликните по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите сконфигурированное VPN-соединение (в данном примере соединение с названием **IKEv2 VPN**) и нажмите кнопку **Подключиться**:

Появится опция выбора сертификата из хранилища пользователя:

Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:

В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя с OS Linux — в роли VPN-клиента.

Сначала необходимо [настроить VPN-сервер](#), затем произвести [настройку VPN-клиента](#) на компьютере пользователя и инициировать подключение к VPN-серверу.

Пример настройки RADIUS-сервера, используемого в рассматриваемом методе аутентификации, приведен в [Приложении](#).

Настройка VPN-сервера

Для настройки узла **NGFW** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы VPN и Подключение конечных устройств в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

2. Создадим профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль, содержащий в качестве методов аутентификации LDAP-коннектор (ldapcon) и RADIUS-сервер (radiuscon):

Настройка LDAP-коннектора:

Настройка RADIUS-сервера:

Шаг 4. Создать профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создадим профиль безопасности, указав в настройках следующие ключевые параметры:

1. **Протокол.** В данном примере для создания защищенного канала будет использоваться протокол IKEv2.
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере можно не указывать тип идентификации.
3. Указать **сертификат сервера**, импортированный ранее на [Шаге 3](#).
4. В качестве **режима аутентификации** выберем AAA.

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле по умолчанию:

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

1

2

3

1. Поставить флажок включения интерфейса.
2. **Название** — название интерфейса уже задано (tunnel1).
3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключающиеся по VPN к NGFW, будут также помещены в эту зону. В данном примере указывается зона VPN for Remote access.

4

5

6

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.250.1, который задается в поле **6**.
5. **MTU** — размер MTU в данном примере оставим по умолчанию.
6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.
- Шаг 6.** Создать сеть VPN.
- В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Remote access VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

3

4

5

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.250.1), используемому совместно с данной сетью.
2. **Маска** сети VPN.
3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

4

4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть офиса 10.10.0.0/24.

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (RA 2).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).



6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.



7. **Пользователи** — доменные пользователи, которым разрешено пользоваться сервисом VPN.



8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

1. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**. По умолчанию оно не активно. Необходимо его включить.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

В данном примере рассмотрим настройку VPN-клиента strongswan на операционной системе Ubuntu.

Для начала необходимо установить дополнительные пакеты для работы с IKEv2 VPN:

```
sudo apt update && sudo apt upgrade
```

```
sudo apt install network-manager-strongswan libcharon-extra-plugins
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



2. Выбрать из списка опцию **IPsec/IKEv2 (strongswan)**:

3. В настройках VPN перейти на вкладку **Идентификация**. Указать название соединения, имя сервера, метод аутентификации, указать имя пользователя, параметры соединения:

4. На вкладке IPv4 оставить указанный по умолчанию метод получения адресов по DHCP:

5. В системе должен присутствовать корневой сертификат. При необходимости нужно поместить его в системный раздел /etc/ssl/certs/.

6. Так как в данном примере используется аутентификация с методом EAP MSCHAPv2 необходимо проверить настройки в файле /etc/strongswan.conf (должны быть отключены eap-peap, eap-md5, eap-gtc):

```
# strongswan.conf - strongSwan configuration file
#
# Refer to the strongswan.conf(5) manpage for details
#
# Configuration changes should be made in the included files
```

```
charon {
    load_modular = yes
    plugins {
        include strongswan.d/charon/*.conf
    }
}
```

```
charon-nm {
    plugins {
        eap-peap {
            load = no
        }
        eap-md5 {
            load = no
        }
        eap-gtc {
            load = no
        }
    }
}
```

```
include strongswan.d/*.conf
```

Настройка VPN-клиента завершена.

Для установления VPN-соединения нажать кнопку включения созданного соединения VPN:

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

На стороне удаленного Linux-компьютера добавится виртуальный адаптер, хост (10.10.0.100) в сети офиса доступен:

Приложение

Настройка RADIUS-сервера

Рассматривается настройка RADIUS-сервера на примере Windows Server 2019 с настроенной Active Directory.

1. Установить службы политики сети и доступа (Network Policy and Access Services).

В диспетчере серверов добавить роли и компоненты. В окне мастера добавления ролей и компонентов на шаге **Роли сервера** найти в списке и выбрать **Службы политики сети и доступа** :

Далее следовать инструкции мастера для установки компонентов.

2. Зарегистрировать сервер в AD.

В окне диспетчера серверов выбрать **Средства → Сервер политики сети** :

Далее нажать **Действие** → **Зарегистрировать сервер в Active Directory** :

3. Добавить RADIUS-клиента.

Устройства, с которыми RADIUS-сервер будет взаимодействовать (в данном случае это NGFW), необходимо добавить в список RADIUS-клиентов:

Далее заполнить следующие поля (остальные настройки оставить по умолчанию):

- **Понятное имя**;
- **Адрес** устройства (клиента), с которого будут приходить запросы на RADIUS-сервер;
- **Общий секрет** для авторизации устройства на RADIUS-сервер.

Новый RADIUS-клиент X

Параметры Дополнительно

☒ Включить этот RADIUS-клиент

☐ Выберите существующий шаблон:

Имя и адрес:

Полное имя:
UserGate NGFW

Адрес (IP или DNS):
10.10.0.1

Проверить...

Общий секрет

Выберите существующий шаблон общих секретов:
Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

☒ Вручную ☐ Создать

Общий секрет:

Подтверждение общего секрета:

OK Отмена

4. Настроить Сетевую политику.

Добавить политику:

Настроить политику. Указать название политики и условия её применения:

В качестве условия добавить заранее созданную группу пользователей, которой разрешен удаленный доступ:

Указать разрешение доступа — **Доступ разрешен**:

Далее выбрать следующие методы проверки подлинности:

- **Типы EAP** — **Microsoft: защищённый пароль (EAP-MSCHAP v2)**;
- Разрешить пункт **Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2)**;
- Метод PAP (**Проверка открытым тестом (PAP, SPAP)**) рекомендуется разрешить для параллельной работы IKEv1 AAA. Если планируется использовать только IKEv2 AAA, то достаточно включения только EAP-MSCHAP v2.

Рекомендуемые настройки вкладки: **Параметры**:

Настройка завершена:

Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Remote access VPN-туннеля будет рассмотрена следующая схема:

В данном примере NGFW выступает в роли VPN-сервера, а компьютер пользователя — в роли VPN-клиента. При создании VPN с помощью L2TP/IPsec(IKEv1), протокол L2TP создает туннель, в котором передаются пакеты сетевого уровня в кадрах PPP. IPsec обеспечивает шифрование, аутентификацию и проверку целостности передаваемых данных.

Сначала необходимо настроить VPN-сервер, затем произвести настройки VPN-клиента на компьютере пользователя и инициировать подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки NGFW в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервисы **VPN** и **Подключение конечных устройств** в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервисы VPN и Подключение конечных устройств в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for remote access**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 3. Настроить параметры аутентификации.

Для примера в разделе **Пользователи и устройства → Профили аутентификации** создадим профиль ldap_con для аутентификации пользователей VPN через имеющийся сервер AD. На вкладке **Методы аутентификации** выберем ранее настроенный в системе сервер аутентификации LDAP/Active Directory. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#).

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Remote access VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для данного примера:

1

2

3

4

1. **Версия** протокола **IKE** (Internet Key Exchange). В рассматриваемом примере для создания защищенного канала будет использоваться протокол IKEv1.
2. **Режим** работы **IKE**. В рассматриваемом примере используется Основной режим работы IKEv1.
3. **Тип идентификации** (параметр IKE local ID). Опциональный параметр. В рассматриваемом примере указывать не требуется.
4. **Общий ключ** (Pre-shared key) для аутентификации удаленных компьютеров пользователей. Ключ должен совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения.

Шаг 5. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel1**, который может быть использован для настройки Remote access VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера:

1. Поставить флажок включения интерфейса.

2. **Название** — название интерфейса уже задано (tunnel1).

3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. В этом примере указывается зона **VPN for remote access**, созданная на [шаге 2](#).

- 4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес.
- 5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.
- 6. Добавим статический IP-адрес туннельного интерфейса tunnel1 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

Для примера на узле создана сеть **Remote access VPN network** с настройками по умолчанию. Рассмотрим ключевые настройки этой сети для данного примера:

1

2

3

- 1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW (172.30.250.1), используемому совместно с данной сетью.
- 2. **Маска** сети VPN.
- 3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

4

- 4. На вкладке **Маршруты VPN** настраиваются маршруты, передаваемые клиенту при установлении соединения. В данном примере добавлен список *Local net*, включающий в себя подсеть офиса 192.168.1.0/24.

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Remote access VPN rule**, в котором указаны необходимые настройки для Remote access VPN. Рассмотрим ключевые настройки этого правила для данного примера:

1

2

3

4

5

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (Remote access VPN profile).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Remote access VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel1).

6

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.

7

7. **Пользователи** — доменные пользователи, которым разрешено пользоваться сервисом VPN.

8.

8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW — 203.0.113.1.

Шаг 8. Контроль доступа к ресурсам.

1. Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создается в разделе **Политики сети → NAT и маршрутизация**.

Для примера в веб-консоли администратора уже создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее подмену IP-адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**.

2. При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны.

Для примера в консоли администратора создано правило межсетевого экрана **VPN for Remote Access to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Remote Access** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

В данном примере рассмотрим настройку "нативных" клиентов для операционных систем Windows и Linux для удаленного VPN-подключения.

Встроенный VPN-клиент OS Windows

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Кликнуть правой кнопкой мыши по значку сетевого подключения в трее и выбрать пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выбрать пункт **VPN**, а затем нажать на пункт **Добавить VPN-подключение**:

3. В окне **Добавить VPN-подключение** настроить параметры подключения:

- В поле **Поставщик услуг VPN** выбрать **Windows (встроенные)**;
- В поле **Имя подключения** указать имя для этого подключения;
- В поле **Имя или адрес сервера** указать IP-адрес внешнего интерфейса NGFW, к которому будут подключаться клиенты(203.0.113.1);
- В поле **Тип VPN** выбрать **L2TP/IPsec с общим ключом**;
- В поле **Общий ключ** указать тот же ключ, что был указан на [шаге 4](#) настройки VPN-сервера;
- В поле **Тип данных для входа** выбрать **Имя пользователя и пароль**;
- В поле **Имя пользователя** указать имя доменного пользователя, в данном примере: user2@testd.local;
- В поле **Пароль** указать пароль пользователя.

4. Нажать кнопку Сохранить, чтобы сохранить настройки VPN-соединения.

5. В панели управления перейти в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выбрать пункт **Настройки параметров адаптера**:



6. Выбрать только что созданное сетевое подключение **L2TP** и через меню правой кнопки мыши перейти в свойства этого подключения. В открывшемся окне перейти во вкладку **Безопасность**:



Выбрать пункт **Разрешить следующие протоколы** и далее выбрать **PAP**.

7. Сохранить настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения клиньте по значку сетевого соединения в трее левой кнопкой мыши. Далее выберите соединение **L2TP** и нажмите кнопку **Подключиться**.

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

На стороне удаленного Windows-компьютера добавится ppp-адаптер L2TP, появятся маршруты в сеть виртуального адаптера и сеть удаленного офиса. Хост (10.10.0.100) в сети офиса доступен:

L2TP VPN-клиент для OS Linux

Рассмотрим настройку L2TP VPN-клиента для Linux на примере OS Ubuntu.

Для начала необходимо установить L2TP-плагин для приложения Network Manager:

```
sudo apt update  
sudo apt install -y network-manager-l2tp network-manager-l2tp-gnome
```

Далее для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Открыть окно **Настройки** и зайти в раздел **Сеть**. В разделе **VPN** нажать **+** для настройки нового VPN-соединения:



2. Выбрать из списка опцию **Туннельный протокол второго уровня (L2TP)** :

3. В настройках L2TP VPN перейти на вкладку **Идентификация**. Указать название соединения, адрес VPN-сервера, параметры аутентификации пользователя:

4. Перейти к настройкам протокола IPsec, нажав внизу окна настроек VPN кнопку **Параметры IPsec**. В открывшемся окне настроек поставить флажок для активации настроек IPsec туннеля к L2TP хосту, указать общий ключ и параметры первой и второй фаз согласования защищенного соединения:

Нажать **Применить** для сохранения настроек IPsec.

5. Перейти к настройкам протокола PPP, нажав внизу окна настроек VPN кнопку **Параметры PPP**. В открывшемся окне настроек поставить флажок, разрешая в качестве метода аутентификации PAP. Остальные методы отключить:

Нажать **Apply** для сохранения настроек PPP.

6. В окне настроек VPN нажать Применить для сохранения настроек соединения:

Настройка VPN-клиента завершена.

Для установления VPN-соединения нажмите кнопку включения созданного соединения VPN:

Проверка подключения

После установлении VPN-соединения в веб-консоли администратора NGFW на вкладке **Диагностика и мониторинг** в разделе **VPN** появится индикация нового VPN-соединения:

В **Журнале событий** на вкладке **Журналы и отчеты** отобразится соответствующая запись:

На стороне удаленного Linux-компьютера добавится rrr-адаптер, появятся маршрут в сеть виртуального адаптера. Хост (10.10.0.100) в сети офиса доступен:



Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:

Настройка VPN-сервера

Для настройки узла **NGFW 1** в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной по умолчанию на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 3. Настроить параметры аутентификации.

1. Примеры создания самоподписанных сертификатов приведены в [Приложении](#). Импортируем созданные сертификаты VPN-сервера и корневой сертификат.

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируем корневой сертификат без указания приватного ключа.

Создадим профиль клиентских сертификатов в веб-консоли администратора NGFW 1, исполняющего роль VPN-сервера. Для этого необходимо перейти в раздел **UserGate → Профили клиентских сертификатов** и нажать кнопку **Добавить**. В открывшемся окне указать название профиля, добавить импортированный на предыдущем шаге корневой сертификат и выбрать поле **Common-name, Subject altname email** или **Principal name** для получения имени пользователя:

2. Создадим профиль аутентификации для VPN пользователей. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#). Для данного примера был создан профиль аутентификации в домене testd.local через LDAP-коннектор:

Шаг 4. Создать профиль безопасности VPN.

В данном примере воспользуемся уже созданным по умолчанию на узле профилем безопасности **Site-to-Site VPN profile**, задающим необходимые настройки. Рассмотрим ключевые настройки этого профиля для примера создания защищенного VPN-соединения в этой статье:

1

2

3

4

5

1. **Версия протокола IKE** (Internet Key Exchange). В данном примере для создания защищенного канала будет использоваться протокол IKEv2.
2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.
3. Указать **сертификат сервера**, импортированный ранее на [Шаге 3](#).
4. В качестве **режима аутентификации** выберем PKI.
5. Выберем профиль клиентского сертификата, созданный ранее на [Шаге 3](#).
- Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:

Шаг 5. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые параметры этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

1

2

3

1. Поставить флажок включения интерфейса.
2. **Название** — название интерфейса уже задано (tunnel2).
3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW 1, будут также помещены в эту зону. В данном примере указывается зона VPN for Site-to-Site.

4

5

6

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес. В данном примере используется статический IP-адрес 172.30.255.1, который задается в поле **6**.

5. **MTU** — размер MTU в данном примере оставим по умолчанию.

6. Добавим статический IP-адрес туннельного интерфейса tunnel2 172.30.255.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

В данном примере воспользуемся уже созданной по умолчанию на узле сетью **Site-to-Site VPN network**. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

1

1

3

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.255.1), используемому совместно с данной сетью.

2. **Маска** сети VPN.

3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

4

4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

Чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте.

В разделе **Журналы и отчеты** → **Мониторинг** → **Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:

Шаг 7. Создать серверное правило VPN.

В данном примере воспользуемся уже созданным по умолчанию на узле серверным правилом **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для примера создания защищенного VPN-соединения в этой статье:

1

2

3

4

5

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (Site-to-Site VPN profile).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Site-toSite VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel2).

6

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.

7

7. **Пользователи** — в данном примере указывается имя пользователя домена user1 (testd.local\user1), на которого был выписан сертификат, с которым аутентифицируется VPN-клиент NGFW 2 при установлении защищенного соединения.

8

8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1

Шаг 8. Контроль доступа к ресурсам.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети** → **Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной на [Шаге 2](#) зоны в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в статье [Межсетевой экран](#).

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить.

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Настройка VPN-клиента

Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать VPN-интерфейс.

В данном примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для примера создания защищенного VPN-соединения в этой статье:

1

2

3

1. Поставить флажок включения интерфейса.
2. **Название** — название интерфейса уже задано (tunnel3).
3. **Зона**, к которой будет относиться данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на [Шаге 1](#).

4

5

4. **Режим**. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, созданной на [Шаге 6](#) настроек VPN-сервера.
5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

Шаг 3. Настроить параметры аутентификации.

Импортируем созданный ранее сертификат VPN-клиента. Примеры создания самоподписанных сертификатов приведены в [Приложении](#).

В разделе **UserGate → Сертификаты** нажать кнопку **Импортировать**. В открывшемся окне указать название сертификата и добавить сгенерированные файлы сертификата VPN-клиента и приватного ключа.

Шаг 4. Контроль доступа к ресурсам.

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site**, **Trusted** и **Untrusted**.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, создадим разрешающее правило межсетевого экрана, указав нужную зону источника (**Trusted** и **Untrusted**) и зону назначения **VPN for Site-to-Site**.

Шаг 5. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для рассматриваемого примера создания защищенного VPN-соединения.

1

2

3

1. **Протокол.** В рассматриваемом примере для создания защищенного канала будет использоваться **IKEv2 с сертификатом**.

2. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.

3. Выберем сертификат клиента, импортированный ранее на [Шаге 3](#).

Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:

Шаг 6. Создать клиентское правило VPN.

Для примера на узле создано клиентское правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения.

1

2

3

4

1. **Включено** — включить правило.
2. **Профиль безопасности VPN** — созданный на [Шаге 5](#) клиентский профиль безопасности VPN.
3. **Интерфейс** — созданный на [Шаге 2](#) VPN-интерфейс.
4. **Адрес сервера**. В рассматриваемом примере это доменное имя NGFW 1 (ug.testd.local), выполняющего роль VPN-сервера.

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узлах NGFW 1 и NGFW 2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

На NGFW 1:

На NGFW 2:

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW 2 добавится маршрут в сеть удаленного офиса 192.168.1.0/24 через туннельный интерфейс tunnel3:

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW 1:

Со стороны NGFW 2:

Хосты в сетях обоих офисов доступны друг для друга:

██████████

██████████

██████████

██████████

Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:

Настройка VPN-сервера

Для настройки узла NGFW 1 в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Контроль доступа зоны.

Разрешим сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

Для редактирования параметров зоны используется следующая команда:

```
Admin@ug# set network zone <parameters>
```

Подробнее о командах и параметрах для создания/редактирования зон в CLI смотрите в статье [Зоны](#).

Пример редактирования зоны **Untrusted** с целью разрешить сервис VPN в этой зоне:

```
Admin@ug# set network zone Untrusted enabled-services [ VPN ]
```

Шаг 2. Создание зоны для VPN подключений.

Для создания зон используется следующая команда:

```
Admin@ug# create network zone <parameters>
```

Подробнее о командах и параметрах для создания/редактирования зон в CLI смотрите в статье [Зоны](#).

На узле уже создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@ug# show network zone
+ <Enter>          Finish input
+ (                Start complex filter
+ Cluster
+ DMZ
+ Management
+ Trusted
+ "Tunnel inspection zone"
+ Untrusted
+ "VPN for remote access"
+ "VPN for Site-to-Site"
```

```
Admin@ug# show network zone "VPN for Site-to-Site"
```

```
name          : VPN for Site-to-Site
antispoof-enable      : off
antispoof-negate      : off
dos-protection-syn    :
  enabled        : on
  aggregate      : off
  alert-threshold  : 3000
  drop-threshold   : 6000
dos-protection-udp    :
  enabled        : on
  aggregate      : off
  alert-threshold  : 3000
  drop-threshold   : 6000
dos-protection-icmp   :
  enabled        : on
  aggregate      : off
  alert-threshold  : 100
  drop-threshold   : 200
services-access       :
  service         : Any ICMP
  allowed-addresses : Any
  enabled         : on

  service         : reponse_pages
  allowed-addresses : Any
  enabled         : on

  service         : DNS
  allowed-addresses : Any
  enabled         : on

  service         : HTTP Proxy
  allowed-addresses : Any
  enabled         : on

  service         : Endpoint connect
  allowed-addresses : Any
  enabled         : on

sessions-limit-enabled : off
sessions-limit-threshold : 0
```

Шаг 3. Настройка параметров аутентификации.

1. Создадим локальную учетную запись для аутентификации сервера, выступающего в роли VPN-клиента.

Для этого используется следующая команда:

```
Admin@ug# create users user <parameters>
```

Подробнее о командах и параметрах для создания локальных пользователей в CLI смотрите в статье [Настройки пользователей](#).

Пример создания учетной записи vpn client 1 с логином **vpncint1**, входящего в группу **VPN servers**:

```
Admin@ug# create users user name "vpn client 1" login vpncint1 groups [ "VPN servers" ] enabled on
```

2. Создадим профиль аутентификации для VPN пользователей.

Для этого используется следующая команда:

```
Admin@ug# create users auth-profile <parameter>
```

Подробнее о порядке создания профилей аутентификации для пользователей в CLI смотрите в статье [Настройка профилей аутентификации](#).

Пример создания профиля аутентификации local с аутентификацией по базе данных локально заведенных пользователей:

```
Admin@ug# create users auth-profile name local auth-methods local-user-auth on
```

Шаг 4. Создание профиля безопасности VPN-сервера.

Для создания профиля безопасности VPN-сервера используется следующая команда:

```
Admin@ug# create vpn server-security-profiles <parameters>
```

Подробнее о порядке создания профилей безопасности VPN в CLI смотрите в статье [Настройка профилей безопасности VPN](#).

Изначально для примера на узле уже создан профиль безопасности **Site-to-Site VPN profile**, задающий необходимые настройки:

```
Admin@ug# show vpn server-security-profiles
```

```
Site-to-Site VPN profile
name          : Site-to-Site VPN profile
description   : Example VPN security profile for Site-to-Site VPN. Preshared key is "examplepresharedkey" - it must be changed! This profile can be changed or deleted if necessary.
ike-version   : 1
ike-mode      : main
local-id-type : none
certificate   : no certificate
authentication-mode : any
dh-groups     : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
dpd-state     : off
dpd-interval  : 60
dpd-max-failures : 5
phase1-security :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256

phase1-key-lifetime : 1 d
phase2-key-lifetime : 12 h
key-lifetime-enabled : off
key-lifetime-size : 4 GB
phase2-security :
  authentication : SHA1
  encryption     : AES256

  authentication : SHA256
  encryption     : AES256

nat-keepalive : 0
Admin@ug# set vpn server-security-profiles "Site-to-Site VPN profile" ike-version 1 psk 123456
```

Шаг 5. Создание VPN-интерфейса.

Для создания VPN-интерфейса используется следующая команда:

```
Admin@ug# create network interface vpn <parameters>
```

Подробнее о порядке создания VPN-интерфейса в CLI смотрите в статье [Интерфейсы](#).

Для примера на узле уже создан VPN-интерфейс **tunnel2**, который может быть использован для настройки Site-to-Site VPN:

```
Admin@ug# show network interface vpn tunnel2
```

```
type          : vpn
node_name     : cluster
name          : tunnel2
description   : Example VPN interface to be used in Site-to-Site VPN server rule. This is an example VPN interface which
               can be changed or deleted if necessary.
enabled       : on
netflow-profile : Undefined
iface-mode    : manual
mtu           : 1420
speed         : 0
zone          : VPN for Site-to-Site
running       : off
master        : off
Admin@ug# set network interface vpn tunnel2 ip-addresses [ 172.30.255.1/24 ]
Admin@ug# show network interface vpn tunnel2
```

```
type          : vpn
node_name     : cluster
name          : tunnel2
description   : Example VPN interface to be used in Site-to-Site VPN server rule. This is an example VPN interface which
               can be changed or deleted if necessary.
enabled       : on
netflow-profile : Undefined
iface-mode    : static
mtu           : 1420
speed         : 0
zone          : VPN for Site-to-Site
running       : off
master        : off
ip-addresses  : 172.30.255.1/24
```

Шаг 6. Создание сети VPN.

Для создания сети VPN используется следующая команда:

```
Admin@ug# create vpn networks <parameters>
```

Подробнее о порядке создания сети VPN в CLI смотрите в статье [Настройка сетей VPN](#).

Для примера на узле уже создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Скорректируем в ней диапазон IP-адресов для установления VPN с NGFW 2:

```
Admin@ug# show vpn networks
```

```
Site-to-Site VPN network
name          : Site-to-Site VPN network
description   : Example VPN network for Site-to-Site VPN. It can be changed or deleted if necessary.
mask          : 255.255.255.0
use-system-dns : on
ip-range      : 172.30.255.2-172.30.255.254
all-routes    : off
restrict-lan-access : off
Admin@ug# set vpn networks "Site-to-Site VPN network" ip-range 172.30.255.2-172.30.255.2
Admin@ug# show vpn networks
```

```
Site-to-Site VPN network
name          : Site-to-Site VPN network
description   : Example VPN network for Site-to-Site VPN. It can be changed or deleted if necessary.
mask          : 255.255.255.0
use-system-dns : on
ip-range      : 172.30.255.2-172.30.255.2
all-routes    : off
restrict-lan-access : off
```

В качестве маршрута, передаваемого VPN-клиенту, добавим в настройки этой сети заранее созданный список Local network, включающий в себя подсеть 192.168.1.0/24:

```
Admin@ug# set vpn networks "Site-to-Site VPN network routes-ip-list [ "Local network" ]
Admin@ug# show vpn networks
```

```
Site-to-Site VPN network
name          : Site-to-Site VPN network
description   : Example VPN network for Site-to-Site VPN. It can be changed or deleted if necessary.
mask          : 255.255.255.0
use-system-dns : on
```

```
routes-ip-list      : Local network
ip-range           : 172.30.255.2-172.30.255.2
all-routes         : off
restrict-lan-access : off
```

Шаг 7. Создание серверного правила VPN.

Правила для VPN-сервера создаются с помощью синтаксиса UPL командой:

```
Admin@ug# create vpn server-rules <position> upl-rule <commands>
```

Подробнее о порядке настройки серверных правил VPN в CLI смотрите в статье [Настройка серверных правил](#).

Для примера на узле создано серверное правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группы **VPN servers**:

```
Admin@ug# show vpn server-rules
```

```
% ----- 1 -----
OK \
  user = "CN=VPN servers,DC=LOCAL" \
  src.zone = Untrusted \
  profile("Site-to-Site VPN profile") \
  auth_profile(local) \
  vpn_network("Site-to-Site VPN network") \
  interface(tunnel2) \
  desc("Example VPN server rule which allows access for Site-to-Site VPN clients connections from Untrusted zone and places them to VPN for Site-to-Site zone (zone assigned to VPN interface). This rule can be changed or deleted if necessary.");
  enabled(false) \
  name("Site-to-Site VPN rule")
```

В качестве адреса назначения добавим в правило заранее созданный список Ext. address, в который входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1, и включим это правило:

```
Admin@ug# set vpn server-rules 1 upl-rule OK \
...dst.ip = lib.network("Ext. address") \
...enabled(true)
Admin@ug# show vpn server-rules

% ----- 1 -----
OK \
  user = "CN=VPN servers,DC=LOCAL" \
  src.zone = Untrusted \
  dst.ip = lib.network("Ext. address") \
  profile("Site-to-Site VPN profile") \
  auth_profile(local) \
  vpn_network("Site-to-Site VPN network") \
  interface(tunnel2) \
  desc("Example VPN server rule which allows access for Site-to-Site VPN clients connections from Untrusted zone and places them to VPN for Site-to-Site zone (zone assigned to VPN interface). This rule can be changed or deleted if necessary.");
  enabled(true) \
  name("Site-to-Site VPN rule")
```

Шаг 8. Контроль доступа к ресурсам.

Правила межсетевого экрана создаются с помощью синтаксиса UPL командой:

```
Admin@ug# create network-policy firewall <position> upl-rule <commands>
```

Подробнее о порядке настройки правил межсетевого экрана в CLI смотрите в статье [Настройка правил межсетевого экрана](#).

Изначально для примера на узле уже создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить:

```
Admin@ug# show network-policy firewall
```

```
% ----- 1 -----
PASS \
  src.zone = Trusted \
  dst.zone = Untrusted \
  desc("Firewall rule which allows traffic from Trusted zone to Untrusted zone. This is an example rule which can be changed or deleted if necessary.");
  rule_log(session) \
  enabled(false) \
  name("Allow trusted to untrusted")
% ----- 2 -----
PASS \
  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.");
  rule_log(session) \
  enabled(false) \
  name("VPN for Site-to-Site to Trusted and Untrusted")
Admin@ug# set network-policy firewall 2 upl-rule PASS \
...enabled(true)
Admin@ug# show network-policy firewall 2

% ----- 2 -----
PASS \
  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.");
  rule_log(session) \
  enabled(true) \
  name("VPN for Site-to-Site to Trusted and Untrusted")
```

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Пример создания правила межсетевого экрана для разрешения трафика из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**:

```
Admin@ug# create network-policy firewall 3 upl-rule PASS \
...src.zone = "VPN for Site-to-Site" \
...dst.zone = (Trusted, Untrusted) \
...rule_log(session) \
...name("VPN for Site-to-Site to Trusted and Untrusted") \
...enabled(true)
```

Настройка VPN-клиента

Для настройки NGFW 2 в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создание зоны, в которую будут помещен интерфейс, используемый для подключения по VPN.

На узле уже создана зона **VPN for Site-to-Site**. Воспользуемся этой зоной для рассматриваемого примера:

```
Admin@ug2# show network zone "VPN for Site-to-Site"
```

```
name           : VPN for Site-to-Site
antispoof-enable : off
antispoof-negate : off
dos-protection-syn :
  enabled      : on
  aggregate    : off
  alert-threshold : 3000
  drop-threshold : 6000
dos-protection-udp :
  enabled      : on
  aggregate    : off
  alert-threshold : 3000
  drop-threshold : 6000
dos-protection-icmp :
  enabled      : on
  aggregate    : off
  alert-threshold : 100
  drop-threshold : 200
services-access :
  service      : Any ICMP
  allowed-addresses : Any
  enabled      : on
```

```
service      : reponse_pages
allowed-addresses : Any
enabled      : on

service      : DNS
allowed-addresses : Any
enabled      : on

service      : HTTP Proxy
allowed-addresses : Any
enabled      : on

service      : Endpoint connect
allowed-addresses : Any
enabled      : on

sessions-limit-enabled : off
sessions-limit-threshold : 0
```

Шаг 2. Создать VPN-интерфейс.

Для примера на узле уже создан VPN-интерфейс **tunnel3**, который может быть использован для настройки Site-to-Site VPN.

Admin@ug2# show network interface vpn tunnel3

```
type      : vpn
node_name  : cluster
name       : tunnel3
description : Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN interface which
can be changed or deleted if necessary.
enabled    : off
netflow-profile : Undefined
iface-mode : dynamic
mtu        : 1420
speed      : 0
zone       : VPN for Site-to-Site
running    : off
master     : off
Admin@ug2# set network interface vpn tunnel3 enabled on
Admin@ug2# show network interface vpn tunnel3
```

```
type      : vpn
node_name  : cluster
name       : tunnel3
description : Example VPN interface to be used in Site-to-Site VPN client rule. This is an example VPN
interface which can be changed or deleted if necessary.
enabled    : on
netflow-profile : Undefined
iface-mode : dynamic
mtu        : 1420
speed      : 0
zone       : VPN for Site-to-Site
running    : off
master     : off
```

Шаг 3. Контроль доступа к ресурсам.

Настройки в CLI аналогичны настройкам на NGFW 1 (См. [Шаг 8](#) настройки NGFW 1 в cli).

Шаг 4. Создать профиль безопасности VPN-клиента.

Для создания профиля безопасности VPN-клиента используется следующая команда:

Admin@ug2# create vpn client-security-profiles <parameters>

Подробнее о порядке создания профилей безопасности VPN в CLI смотрите в статье [Настройка профилей безопасности VPN](#).

Для примера на узле уже создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Добавим в профиль общий ключ, аналогичный заданному в настройках VPN-сервера на [Шаге 4](#), и логин/пароль созданной на [Шаге 3](#) учетной записи для аутентификации VPN-клиента при установлении L2TP туннеля.

Admin@ug2# show vpn client-security-profiles

```
Client VPN profile
name      : Client VPN profile
description : Example VPN security profile for client VPN rule. Preshared key is
"examplepresharedkey" - it must be changed! This profile can be changed or deleted if
necessary.
protocol  : ipsec2
ike-mode  : main
local-id-type : none
certificate : no certificate
dh-groups  : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
dpd-state  : off
dpd-interval : 60
dpd-max-failures : 5
phase1-security :
authentication : SHA1
encryption     : AES256

authentication : SHA256
encryption     : AES256

phase1-key-lifetime : 1 d
phase2-key-lifetime : 12 h
key-lifetime-enabled : off
key-lifetime-size : 4 GB
phase2-security :
authentication : SHA1
encryption     : AES256

authentication : SHA256
encryption     : AES256

nat-keepalive : 0
Admin@ug2# set vpn client-security-profiles "Client VPN profile" protocol ipsec2 psk 123456 authentication-login vpnclnt1 authentication-password 123123
```

Шаг 5. Создать клиентское правило VPN.

Правила для VPN-клиента создаются с помощью синтаксиса UPL командой:

Admin@ug2# create vpn client-rules <position> upl-rule <commands>

Подробнее о порядке настройки клиентских правил VPN в CLI смотрите в статье [Настройка клиентских правил](#).

Для примера на узле уже создано серверное правило **Client VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Необходимо добавить в это правило IP-адрес VPN-сервера, куда подключается данный VPN-клиент. В рассматриваемом примере это IP-адрес интерфейса в зоне **Untrusted** на NGFW 1 — 203.0.113.1.

```
Admin@ug2# set vpn client-rules 1 upl-rule OK \
...server_address("203.0.113.1") \
...enabled(true)
Admin@ug2# show vpn client-rules
```

```
% ----- 1 -----
OK \
server_address("203.0.113.1") \
last_error(Disabled) \
status(disconnected) \
connection_time(0) \
profile("Client VPN profile") \
interface(tunnel3) \
desc("Example VPN client rule which connect UserGate server as client to another UserGate server acting as VPN server. This rule can be changed or deleted if necessary.") \
enabled(true) \
name("Client VPN rule")
```

После завершения настройки VPN-сервера и VPN-клиента и активации правил VPN клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

Проверка доступности соседнего узла и маршрута в сеть удаленного офиса.

Со стороны NGFW 1:

```
Admin@ug> show network route
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
        O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
        > - selected route, * - FIB route, q - queued, r - rejected, b - backup
        t - trapped, o - offload failure
C>* 203.0.113.0/24 is directly connected, port2, 04:20:11
K>* 100.100.0.0/24 [0/0] via 172.30.255.2, tunnel2, 04:19:43
C>* 172.30.255.0/24 is directly connected, tunnel2, 04:20:11
C>* 192.168.1.0/24 is directly connected, port1, 04:20:11
C>* 192.168.56.0/24 is directly connected, port0, 04:20:11
```

```
Admin@ug> ping host 172.30.255.2
```

```
PING 172.30.255.2 (172.30.255.2) 56(84) bytes of data.
64 bytes from 172.30.255.2: icmp_req=1 ttl=64 time=3.34 ms
64 bytes from 172.30.255.2: icmp_req=2 ttl=64 time=2.49 ms
64 bytes from 172.30.255.2: icmp_req=3 ttl=64 time=1.04 ms
^C
--- 172.30.255.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.041/2.292/3.347/0.953 ms
```

Со стороны NGFW 2:

```
Admin@ug2> show network route
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
        O - OSPF, B - BGP, T - Table, v - VNC, V - VNC-Direct,
        > - selected route, * - FIB route, q - queued, r - rejected, b - backup
        t - trapped, o - offload failure
C>* 198.51.100.0/24 is directly connected, port2, 04:18:41
C>* 100.100.0.0/24 is directly connected, port1, 04:18:41
C>* 172.30.255.0/24 is directly connected, tunnel3, 00:08:00
C>* 192.168.56.0/24 is directly connected, port0, 04:18:41
```

```
Admin@ug2> ping host 172.30.255.1
```

```
PING 172.30.255.1 (172.30.255.1) 56(84) bytes of data.
64 bytes from 172.30.255.1: icmp_req=1 ttl=64 time=2.92 ms
64 bytes from 172.30.255.1: icmp_req=2 ttl=64 time=2.04 ms
64 bytes from 172.30.255.1: icmp_req=3 ttl=64 time=1.13 ms
^C
--- 172.30.255.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 1.138/2.032/2.920/0.729 ms
```

Product: NGFW
Version: 7.x
Technology: VPN

В качестве примера для создания Site-to-Site VPN-туннеля будет рассмотрена следующая схема:

Настройка VPN-сервера

Для настройки узла NGFW 1 в качестве VPN-сервера необходимо выполнить следующие шаги:

Шаг 1. Разрешить сервис VPN в контроле доступа зоны, с которой будут подключаться VPN-клиенты.

В разделе **Сеть → Зоны** отредактируем параметры контроля доступа для зоны **Untrusted**. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Зоны				
Добавить Редактировать Копировать Удалить				
Зона	Защита от DoS включена для	Исключения ...	Защита от спуфинга	Контроль доступа
Cluster	Ничего		Отключено	Ping, Кластер, Консоль администрирования
DMZ	SYN, UDP, ICMP		Отключено	Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management	SYN, UDP, ICMP		Отключено	Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
Trusted	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-пр
Tunnel inspection zone	Ничего		Отключено	Всё отключено
Untrusted	SYN, UDP, ICMP		Отключено	Ping, SMTP(S)-прокси, POP3(S)-прокси, VPN
VPN for remote access	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств
VPN for Site-to-Site	SYN, UDP, ICMP		Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси, Подключение конечных устройств

Шаг 3. Настроить параметры аутентификации.

1. Создадим локальную учетную запись, которая будет использоваться для аутентификации узла, выступающего в роли VPN-клиента при установлении L2TP туннеля. В веб-консоли NGFW 1 в разделе **Пользователи и устройства → Пользователи** создадим локальную учетную запись *vpn client 1* (логин: *vpncnt1*) для удаленного узла VPN-клиента NGFW 2. Для удобства использования все созданные подобные учетные записи могут быть помещены в имеющуюся группу **VPN servers**, которой будет дан доступ для подключения по VPN. Подробнее о создании учетных записей пользователей и групп смотрите в статье [Пользователи и группы](#).
2. Создадим профиль аутентификации для VPN пользователей. Для примера в разделе **Пользователи и устройства → Профили аутентификации** создадим профиль *local*, во вкладке метода аутентификации выберем **Локальный пользователь**. Подробно о профилях аутентификации смотрите в разделе данного руководства [Профили аутентификации](#).

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Site-to-Site VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для примера создания защищенного VPN-соединения в этой статье:

1

2

3

4

1. **Версия протокола IKE** (Internet Key Exchange). В рассматриваемом примере для создания защищенного канала будет использоваться протокол IKEv1.
2. **Режим работы IKE**. В рассматриваемом примере используется Основной режим работы IKEv1.
3. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.
4. **Задать значение общего ключа** (Pre-shared key) для аутентификации удаленного узла. Ключ должен совпадать на VPN-сервере и VPN-клиенте для успешного подключения.
- Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Site-to-Site VPN profile** по умолчанию:

Шаг 5. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel2**, который может быть использован для настройки Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера.

1

2

3

- 1. Поставить флажок включения интерфейса.
- 2. **Название** — название интерфейса уже задано (tunnel2).
- 3. **Зона**, к которой будет относиться данный интерфейс. Все клиенты, подключающиеся по VPN к NGFW 1, будут также помещены в эту зону. В этом примере указывается зона VPN for Site-to-Site.

4

5

6

4. **Режим** — тип присвоения IP-адреса. При использовании интерфейса для приема VPN-подключений необходимо использовать статический IP-адрес.
5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.
6. Добавим статический IP-адрес туннельного интерфейса tunnel2 172.30.255.1 с маской 255.255.255.0.

Шаг 6. Создать сеть VPN.

Для примера на узле создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Рассмотрим ключевые настройки этой сети для примера создания защищенного VPN-соединения в этой статье:

1

1

3

1. **Диапазон IP-адресов**, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW 1 (172.30.255.1), используемому совместно с данной сетью. Соединение будет устанавливаться с одним NGFW, выполняющим роль VPN-клиента, в таком случае диапазон IP-адресов в данном поле будет следующим: 172.30.255.2-172.30.255.2.
2. **Маска** сети VPN.
3. Оставим флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

4

4. **Маршруты VPN** — в данном примере добавлен список Local network, включающий в себя подсеть 192.168.1.0/24.

Чтобы VPN-сервер узнал о подсетях клиента, необходимо в свойствах виртуального маршрутизатора (**Сеть → Виртуальные маршрутизаторы**) сервера прописать статический маршрут, указав в качестве адреса назначения адрес VPN-туннеля, используемый на VPN-клиенте.

В разделе **Журналы и отчеты** → **Мониторинг** → **Маршруты** можно увидеть, что добавился маршрут в сеть 100.100.0.0/24 через туннельный интерфейс tunnel2:

Шаг 7. Создать серверное правило VPN.

Для примера на узле создано серверное правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группы **VPN servers**. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения:

1

2

3

4

5

1. **Включено** — включить правило VPN.
2. **Профиль безопасности VPN** — серверный профиль безопасности VPN, созданный ранее на [Шаге 4](#) (Site-to-Site VPN profile).
3. **Сеть VPN** — сеть VPN, созданная ранее на [Шаге 6](#) (Site-to-Site VPN network).
4. **Профиль аутентификации** — профиль аутентификации для пользователей VPN, созданный ранее (см. [Шаг 3](#)).
5. **Интерфейс** — созданный ранее на [Шаге 5](#) интерфейс VPN (tunnel2).

6

6. **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. В данном примере укажем зону **Untrusted**.

7

7. **Пользователи** — в данном примере группа **VPN servers** включает в себя созданную на [Шаге 3](#) учетную запись *vpn client 1*.

8

8. **Назначение** — в данном случае в список **Ext. address** входит внешний IP-адрес VPN-сервера NGFW 1 — 203.0.113.1.

Шаг 8. Контроль доступа к ресурсам.

При необходимости предоставления доступа пользователям VPN в определенные сегменты сети, или, например, для предоставления доступа в интернет в разделе **Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной на Шаге 3 зоны в требуемые зоны. Подробнее о создании и настройке правил межсетевого экрана смотрите в статье [Межсетевой экран](#).

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик из зоны **VPN for Site-to-Site** в зоны **Trusted** и **Untrusted**. Правило выключено по умолчанию, необходимо его включить.

Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения, например, **VPN for Site-to-Site**.

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

Сбросить счётчики

Все

Принудительно применить

✓

#	Статус журн...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис
1		Allow trusted to untrusted	✓ Разрешить	Trusted	Любой	Untrusted	Любой	Любой	Любой
2		VPN for Site-to-Site to Trusted and Untrusted	✓ Разрешить	VPN for Site-to-Site	Любой	Untrusted Trusted	Любой	Любой	Любой
3		Trusted and Untrusted to VPN for Site-to-Site	✓ Разрешить	Untrusted Trusted	Любой	VPN for Site-to-Site	Любой	Любой	Любой
4	(...)	Default block	⊘ Запретить	Любая	Любой	Любая	Любой	Любой	Любой

Настройка VPN-клиента

Для настройки узла **NGFW 2** в качестве VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Создать зону для VPN подключений.

В данном примере воспользуемся уже созданной на узле зоной **VPN for Site-to-Site**. Подробнее о создании и настройках зон смотрите в статье [Настройка зон](#).

Шаг 2. Создать VPN-интерфейс.

Для примера на узле создан VPN-интерфейс **tunnel3**, который может быть использован для клиентского подключения Site-to-Site VPN. Рассмотрим ключевые настройки этого интерфейса для рассматриваемого примера создания защищенного VPN-соединения:

1

2

3

- 1. Поставить флажок включения интерфейса.
- 2. **Название** — название интерфейса уже задано (tunnel3).
- 3. **Зона**, к которой будет относиться данный интерфейс. В этом примере указывается зона VPN for Site-to-Site, созданная на [Шаге 1](#).

4

5

- 4. **Режим**. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. При установлении соединения интерфейсу будет присвоен IP-адрес из диапазона сети VPN, созданной на [Шаге 6](#) настроек VPN-сервера.
- 5. **MTU** — размер MTU в рассматриваемом примере оставим по умолчанию.

Шаг 3. Контроль доступа к ресурсам.

Для примера на узле создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site**, **Trusted** и **Untrusted**.

Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, создадим разрешающее правило межсетевого экрана, указав нужную зону источника (**Trusted** и **Untrusted**) и зону назначения **VPN for Site-to-Site**.

Шаг 4. Создать профиль безопасности VPN.

Для примера на узле создан профиль безопасности **Client VPN profile**, задающий необходимые настройки. Рассмотрим ключевые настройки этого профиля для рассматриваемого примера создания защищенного VPN-соединения:

1

→

2

3

4

5

1. **Протокол.** В рассматриваемом примере для создания защищенного канала будет использоваться **IPsec L2TP**.
 2. **Режим работы IKE.** В рассматриваемом примере используется **Основной** режим работы IKEv1.
 3. **Тип идентификации** (параметр IKE local ID). В рассматриваемом примере VPN-соединение устанавливается между узлами UserGate, указывать тип идентификации не требуется.
 4. Зададим значение общего ключа (Pre-shared key) для аутентификации удаленного узла. Ключ должен совпадать с ключом, заданным на VPN-сервере на [Шаге 4](#).
 5. **Аутентификация** — логин и пароль учетной записи, созданной на [Шаге 3](#) при настройке VPN-сервера для аутентификации узла, выступающего в роли VPN-клиента при установлении L2TP туннеля (vpncint1).
- Далее необходимо задать параметры первой и второй фаз согласования защищенного соединения. Для рассматриваемого примера оставим эти параметры, как они созданы в профиле **Client VPN profile** по умолчанию:

Шаг 5. Создать клиентское правило VPN.

Для примера на узле создано клиентское правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN. Рассмотрим ключевые настройки этого правила для рассматриваемого примера создания защищенного VPN-соединения:

1

2

3

4

1. **Включено** — включить правило.
2. **Профиль безопасности VPN** — созданный на [Шаге 4](#) клиентский профиль безопасности VPN.
3. **Интерфейс** — созданный на [Шаге 2](#) VPN-интерфейс.
4. **Адрес сервера**. В рассматриваемом примере это доменный адрес NGFW 1, выполняющего роль VPN-сервера (ug.testid.local).

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение в сторону сервера, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное (на сервере) правило VPN.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли администратора на узле NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля:

На узлах NGFW 1 и NGFW 2 в разделе **Диагностика и мониторинг** → **Мониторинг** → **VPN** появится информация о новом туннеле.

На NGFW 1:

На NGFW 2:

В разделе **Диагностика и мониторинг** → **Мониторинг** → **Маршруты** на узле NGFW 2 добавится маршрут в сеть удаленного офиса 192.168.1.0/24 через туннельный интерфейс tunnel3:

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW 1:

Со стороны NGFW 2:

Хосты в сетях обоих офисов доступны друг для друга:

```
~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:60:bc:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
~# ping 100.100.0.2
PING 100.100.0.2 (100.100.0.2) 56(84) bytes of data.
64 bytes from 100.100.0.2: icmp_seq=1 ttl=62 time=3.89 ms
64 bytes from 100.100.0.2: icmp_seq=2 ttl=62 time=4.39 ms
64 bytes from 100.100.0.2: icmp_seq=3 ttl=62 time=4.21 ms
64 bytes from 100.100.0.2: icmp_seq=4 ttl=62 time=1.72 ms
64 bytes from 100.100.0.2: icmp_seq=5 ttl=62 time=2.74 ms
^C
--- 100.100.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4020ms
rtt min/avg/max/mdev = 1.721/3.388/4.390/1.012 ms
```

```
~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:64:97:19 brd ff:ff:ff:ff:ff:ff
    inet 100.100.0.2/24 brd 100.100.0.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::9879:e61f:8ac5:b117/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
~# ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=62 time=5.97 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=62 time=4.27 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=62 time=8.62 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=62 time=7.34 ms
64 bytes from 192.168.1.102: icmp_seq=5 ttl=62 time=2.01 ms
64 bytes from 192.168.1.102: icmp_seq=6 ttl=62 time=1.97 ms
^C
--- 192.168.1.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.969/5.030/8.621/2.522 ms
```

KnowledgeBase: ☒
Product: UserGate NGFW

Далее представлены настройки для организации удалённого подключения устройств, работающих на macOS, к UserGate по протоколу L2TP. На UserGate перейдите в раздел **VPN → Профили безопасности VPN** и произведите настройку профилей безопасности:

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

8

часов

Интервал проверки dead peer detection:

60

(в секундах)

Неудачных попыток:

5

Diffie-Hellman группы

Добавить

Удалить

Группа 14 Prime 2048 бит

Группа 2 Prime 1024 бит

Безопасность

Добавить

Редактировать

Удалить

Выше

Ниже

Авторизация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

Свойства профиля безопасности VPN

Общие

Фаза 1

Фаза 2

Время жизни ключа:

8

часов

Максимальный размер данных, шифруемых одним ключом:

Отключено

1000

КБ

Безопасность

Добавить

Редактировать

Удалить

Выше

Ниже

Авторизация	Шифрование
SHA1	AES128
SHA1	3DES
MD5	AES128
MD5	3DES

Поддерживаемые алгоритмы авторизации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх или вниз

Сохранить

Отмена

В общем случае устройства с операционной системой macOS не требуют дополнительной настройки. В случае, если не удалось установить соединение, необходимо выбрать протокол PAP для аутентификации. Для этого выполните в терминале следующие команды:

```
echo refuse-chap > ~/.ppprc
echo refuse-mschap >> ~/.ppprc
echo refuse-mschap-v2 >> ~/.ppprc
```

Результатом выполнения команд является создание файла ~/.ppprc со следующим содержимым:

```
refuse-chap
refuse-mschap
refuse-mschap-v2
```

