

Table of Contents

Table of Contents	1
Примеры настройки VPN	2
Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1)	3
Пример настройки Site-to-Site VPN с L2TP/IPSec(IKEv1) с помощью интерфейса CLI	12
Пример настройки Site-to-Site VPN с IPSec(IKEv2)	17
Пример настройки Remote access VPN с L2TP/IPSec(IKEv1)	27
Пример настройки Remote access VPN с IPsec(IKEv2)	37
Пример настройки Remote access VPN с IPsec(IKEv2) с аутентификацией через EAP для OS Linux	49
Пример настройки Remote access VPN с IPsec(IKEv2) с аутентификацией через EAP, PEAP для OS Windows	61

Product: NGFW
Technology: VPN
Version: 7.x

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. **Зададим 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.testd.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
```

Technology: VPN
Version: 7.x
Product: NGFW

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
```

Technology: VPN
Version: 7.x
Product: NGFW

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:

██████████

██████████

██████████

██████████

Version: 7.x
Technology: VPN
Product: NGFW

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, подключающиеся 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:

1

2

3

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:



Technology: VPN
Version: 7.x
Product: NGFW

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 использоваться 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

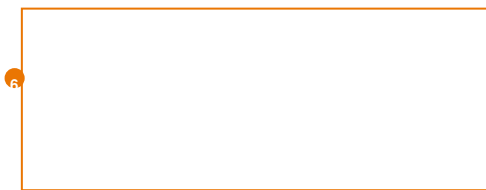
2

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 встроенного 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 [встроенного 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:

Technology: VPN
Version: 7.x
Product: NGFW

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:

Technology: VPN
Version: 7.x
Product: NGFW

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

UserGate NGFW выступает в роли VPN-сервера, а компьютер пользователя с ОС Windows — в роли VPN-клиента.

Будут рассмотрены следующие сценарии аутентификации:

- EAP с аутентификацией по MSCHAPv2 с логином и паролем;
- EAP-TLS с аутентификацией по сертификату пользователя;
- PEAP с аутентификацией по сертификату пользователя;
- PEAP с аутентификацией по MSCHAPv2 с логином и паролем.

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 рассматриваемых сценариях, приведён в [Приложении](#).

Настройка VPN-сервера

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

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

В веб-консоли администратора в разделе **Сеть → Зоны** отредактируйте параметры контроля доступа для зоны Untrusted. Необходимо разрешить сервис VPN в этой зоне. Подробнее о создании и настройках зон — в разделе документации [Настройка зон](#).

Шаг 2. Создайте зону для VPN подключений.

В этом примере используется созданная по умолчанию зона VPN for Remote access. Подробнее о создании и настройках зон — в разделе документации [Настройка зон](#).

Шаг 3. Настройте параметры аутентификации.

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

В разделе **UserGate → Сертификаты** нажмите **Импортировать**. В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его приватного ключа. В этом же разделе импортируйте корневой сертификат без указания приватного ключа:

Создайте профиль аутентификации для пользователей VPN. Подробнее о профилях аутентификации — в разделе руководства [Профили аутентификации](#). Для этого примера был создан профиль, содержащий в качестве методов аутентификации RADIUS-сервер (rad16) и LDAP-коннектор (adtest1):

Настройка LDAP-коннектора:

Настройка RADIUS-сервера:

Шаг 4.Создайте профиль безопасности VPN.

В разделе **VPN → Серверные профили безопасности** создайте профиль безопасности со следующими настройками:

- в качестве протокола для создания защищённого канала укажите IKEv2;
- тип идентификации в рассматриваемом примере можно не указывать;
- укажите сертификат сервера, импортированный ранее на [шаге 3](#);
- в качестве режима аутентификации выберите AAA.

Далее необходимо задать параметры первой и второй фаз согласования защищённого соединения:

Шаг 5. Создайте VPN-интерфейс.

В этом примере используется созданный по умолчанию VPN-интерфейс `tunnel1`. Ключевые параметры этого интерфейса для примера создания защищённого VPN-соединения:

- поставьте флажок включения интерфейса;
- название интерфейса уже задано — `tunnel1`;
- указана зона `VPN for remote access`, к которой будет относиться данный интерфейс; все клиенты, подключившиеся по VPN к NGFW, будут помещены в эту зону;

- при использовании интерфейса для приёма VPN-подключений необходимо использовать статический IP-адрес;
- размер MTU в этом примере оставим по умолчанию;
- статический IP-адрес туннельного интерфейса tunnel1: 172.30.250.1 с маской 255.255.255.0.

Шаг 6. Создайте сеть VPN.

В данном примере используется созданная по умолчанию сеть Remote access VPN network. Ключевые настройки этой сети для примера создания защищённого VPN-соединения:

- 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;
- маска сети VPN.
- оставьте флажок **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW.

В этом примере на вкладке **Маршруты VPN** добавлен список "1", включающий в себя адрес сети (15.0.0.0/24).

Шаг 7. Создайте серверное правило VPN.

Воспользуемся созданным по умолчанию серверным правилом Remote access VPN rule. Ключевые настройки правила для данного примера:

- в качестве профиля безопасности VPN укажите серверный профиль безопасности, созданный ранее на шаге [4](#);
- в качестве сети VPN укажите сеть, созданная ранее на [шаге 6](#);
- в качестве профиля аутентификации указан профиль, созданный ранее (см. [шаг 3](#));
- указан интерфейс VPN, созданный ранее на [шаге 5](#).

Шаг 8. Контроль доступа к ресурсам.

Чтобы трафик мог ходить из созданной на [шаге 2](#) зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Правило создаётся 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.

При необходимости предоставления доступа пользователям VPN в определённые 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 зоны Trusted и Untrusted. Правило выключено по умолчанию, его необходимо включить.

Настройка VPN-клиента

Общие настройки

В этом разделе рассматриваются настройки нативного клиента операционной системы Windows для удалённого VPN-подключения.

Для всех сценариев настроек VPN-клиента в этой статье необходимо импортировать сертификат корневого центра в раздел **Доверенные корневые центры сертификации** компьютера пользователя:

Сценарий настройки VPN-клиента с аутентификацией посредством метода EAP с MSCHAPv2 с логином и паролем

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:

3. В окне **Добавить VPN-подключение** настройте параметры подключения:
 - В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
 - В поле **Имя подключения** укажите имя для этого подключения (EAP LOGIN);
 - В поле **Имя или адрес сервера** укажите адрес NGFW;
 - В поле **Тип VPN** выберите **IKEv2**;

- В поле **Тип данных для входа** выберите **Имя пользователя и пароль**.

4. Нажмите **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 2. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт **Настройки параметров адаптера**:



2. Выберите только что созданное сетевое подключение **EAP LOGIN** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:

В поле **Проверка подлинности** выберите пункт **Microsoft: защищённый пароль (EAP-MSCHAP v2) (шифрование включено)**.

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

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

Уберите флажок в поле **Использовать основной шлюз в удалённой сети** :

4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

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

Проверка подключения

После установления 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 удалённого Windows-компьютера добавится ppp-адаптер EAP LOGIN:

Появился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Шаге 6](#):

IP-адрес в удалённой сети доступен:

Сценарий настройки VPN-клиента с аутентификацией посредством метода EAP-TLS

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Импортируйте ранее созданный пользовательский сертификат в хранилище сертификатов пользователя в личную папку:

Шаг 2. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

- 1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
- 2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



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

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (EAP-TLS);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;
- В поле **Тип данных для входа** выберите **Сертификат**.

4. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 3. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

- 1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт **Настройки параметров адаптера**:



2. Выберите только что созданное сетевое подключение **EAP-TLS** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите во вкладку **Безопасность**:

В поле **Проверка подлинности** должен быть выбран пункт **Microsoft: смарт-карта или иной сертификат (шифрование включено)**.

В свойствах проверки подлинности в разделе **При подключении** должен быть выбран пункт **Использовать сертификат на этом компьютере**:

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

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

Уберите флажок в поле **Использовать основной шлюз в удалённой сети** :

4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

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

При наличии нескольких сертификатов пользователя перед установлением соединения будет предложен выбор нужного сертификата.

Проверка подключения

После установления 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 удалённого Windows-компьютера добавится ppp-адаптер EAP-TLS:

Добавился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [шаге 6](#):

IP-адрес в удалённой сети доступен:

Сценарий настройки VPN-клиента с аутентификацией посредством метода PEAP с сертификатом

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Импортируйте ранее созданный пользовательский сертификат в хранилище сертификатов пользователя в личную папку:

Шаг 2. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
2. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:



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

- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
- В поле **Имя подключения** укажите имя для этого подключения (PEAP CERT);
- В поле **Имя или адрес сервера** укажите адрес NGFW;
- В поле **Тип VPN** выберите **IKEv2**;

4. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.

Шаг 3. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:

1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт: **Настройки параметров адаптера**:



2. Выберите только что созданное сетевое подключение **PEAP CERT** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:

В поле **Проверка подлинности** выберите пункт: **Microsoft: защищенные EAP (PEAP) (шифрование включено)**.

В свойствах проверки подлинности в поле выбора метода проверки необходимо выбрать: **Смарт-карта или иной сертификат**. Флажки **Подтверждать удостоверение сервера с помощью проверки сертификата** и **Включить быстрое переподключение** могут быть установлены опционально:

В настройках метода проверки подлинности должен быть активен пункт: **Использовать сертификат на этом компьютере**.

Опционально может быть активировано поле **Подтверждать удостоверение сервера с помощью проверки сертификата**:

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

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

Уберите флажок в поле **Использовать основной шлюз в удалённой сети** :

4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

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

При наличии нескольких сертификатов пользователя перед установлением соединения будет предложен выбор нужного сертификата:

Проверка подключения

После установления 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 удалённого Windows-компьютера добавится ppp-адаптер PEAP CERT:

Появился маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Шаге 6](#):

IP-адрес в удалённой сети доступен:

Сценарий настройки VPN-клиента с аутентификации посредством PEAP с методом MSCHAPv2 с логином и паролем

Для настройки VPN-клиента необходимо выполнить следующие шаги:

Шаг 1. Добавьте новое VPN-подключение на компьютере пользователя. Для этого:

1. Кликните правой кнопкой мыши по значку сетевого подключения на панели и выберите пункт **Открыть "Параметры сети и Интернет"**.
3. В появившемся окне **Параметры** выберите пункт **VPN**, а затем нажмите на пункт **Добавить VPN-подключение**:

4. В окне **Добавить VPN-подключение** настройте параметры подключения:
- В поле **Поставщик услуг VPN** выберите **Windows (встроенные)**;
 - В поле **Имя подключения** укажите имя для этого подключения (PEAP LOGIN);
 - В поле **Имя или адрес сервера** укажите адрес NGFW;
 - В поле **Тип VPN** выберите **IKEv2**;

5. Нажмите кнопку **Сохранить**, чтобы сохранить настройки VPN-соединения.
- Шаг 2. Настройте параметры созданного VPN-подключения на компьютере пользователя. Для этого:
1. В панели управления перейдите в раздел **Сеть и Интернет** и в дополнительных сетевых параметрах выберите пункт: **Настройки параметров адаптера**:

2. Выберите только что созданное сетевое подключение **PEAP LOGIN** и через меню правой кнопки мыши перейдите в свойства этого подключения. В открывшемся окне перейдите на вкладку **Безопасность**:

В поле **Проверка подлинности** выберите пункт: **Microsoft: защищенные EAP (PEAP) (шифрование включено)** .

В свойствах проверки подлинности в поле выбора метода проверки необходимо выбрать: **Защищенный пароль (EAP-MSCHAP v2)**. В разделе **Доверенные корневые центры сертификации** необходимо указать сертификат корневого центра.

Флажки **Подтверждать удостоверение сервера с помощью проверки сертификата** и **Включить быстрое переподключение** могут быть установлены опционально:

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

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

Уберите флажок в поле **Использовать основной шлюз в удалённой сети** :

4. Сохраните настройки, нажав **ОК**.

Настройка VPN-клиента завершена.

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

Проверка подключения

После установления 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 удалённого Windows-компьютера добавится ppp-адаптер PEAP LOGIN:

Появится маршрут в сеть 15.0.0.0/24, добавленный в настройках VPN-сети на сервере на [Шаге 6](#):

IP-адрес в удалённой сети доступен:

Приложение

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

Настройки политики запросов на подключение

Для работы со сценариями аутентификации с помощью EAP-TLS и EAP MSCHAP v2 необходимы соответствующие типы EAP в настройках методов проверки подлинности сервера:

Необходимо 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.

Для работы со сценариями аутентификации с помощью PEAP необходимо добавить соответствующий тип EAP в настройках методов проверки подлинности сервера:

В настройках добавленного метода укажите сертификат корневого центра и необходимый тип EAP.

Для сценария PEAP с аутентификацией по MSCHAPv2 с логином и паролем:

Для сценария PEAP с аутентификацией по сертификату:

Для сертификата далее нажмите **Edit** и добавьте сертификат корневого центра:

