Table of Contents

Table of Contents 1
Примеры настройки 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 10
- Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов 14
- Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux 20

Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1)

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

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

Настройка VPN-сервера

Для настройки NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   В разделе **Настройки → Сеть → Зоны** создайте зону WAN и активируйте сервис VPN в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе « Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию на узле зоной VPN for Site-to-Site. Подробнее о создании и настройке зон — в разделе «Настройка зон».

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   В этом примере воспользуемся созданным по умолчанию интерфейсом tunnel3. Подробнее о создании и настройке сетевых интерфейсов — в разделе « Настройка интерфейсов».

4. Настройте параметры аутентификации.

   - Создайте локальную учетную запись, которая будет использоваться для аутентификации узла-инициатора соединения (NGFW2) при установлении L2TP-туннеля. В веб-консоли NGFW1 в разделе **Настройки → Пользователи и устройства → Пользователи** создана локальная учетная запись User for S2S (логин vpn_user_s2s). 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 — в разделе « Пользователи и группы».
   - Создайте профиль аутентификации. Для примера в разделе **Настройки → Пользователи и устройства → Профили аутентификации** создан профиль local user auth profile, на вкладке метода аутентификации выбран **Локальный пользователь**. Подробнее о профилях аутентификации — в разделе « Профили аутентификации».

5. Создайте правило подключения.

   В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол IKE. Укажите следующие ключевые параметры:

   - На вкладке **Общие**:
     - Укажите название правила подключения.
     - Выберите протокол подключения **IKEv1PSK**.
     - Выберите режим IKE: **Основной**.
     - Укажите значение общего ключа для аутентификации удаленного узла при установлении защищенного соединения IPsec.

   - На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
  - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
  - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site → IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите профиль аутентификации удаленного сервера-инициатора соединения, созданный на шаге 4.
  - Выберите тип идентификации узлов (**IPv4**).
  - Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Site-to-Site → IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
    - Укажите название политики VPN-подключения.
    - В блоке **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

- На вкладке **Пользователи** вы можете указать учетные записи или группы, созданные для серверов, которым разрешено подключаться по VPN.
- На вкладке **Подсети для VPN**:
    - Выберите VPN-адаптер, который будет использоваться для установления соединения (tunnel3).
    - Укажите диапазон IP-адресов и маску подсети, которые будут использованы клиентами. Необходимо исключить из диапазона адрес, который назначен VPN-интерфейсу NGFW1 (172.16.0.1), используемому совместно с этой сетью.
    - Оставьте флажок **Использовать системные DNS-серверы** , в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW1.

- На вкладке **Маршруты VPN** вы можете указать маршруты к подсетям за VPN-сервером, передаваемые узлу-инициатору.

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в свойствах виртуального маршрутизатора VPN-сервера (**Настройки → Сеть → Виртуальные маршрутизаторы**), указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1.

Подробнее о создании и настройке правил межсетевого экрана — в разделе « Межсетевой экран».

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN подключений.

В этом примере воспользуемся уже созданной на узле зоной VPN for Site-to-Site.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс tunnel4. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

4. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IPsec/L2TP**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите режим IKE: **Основной**.
  - Укажите значение общего ключа для аутентификации узлов. Ключи на VPN-сервере и узле-инициаторе соединения должны совпадать.
  - Выберите параметр идентификации узлов: **IPv4**.
  - Укажите в качестве значений параметров идентификации IP-адреса интерфейсов NGFW2 и NGFW1 из зоны WAN.
  - Укажите логин и пароль учетной записи, созданной на шаге 4 при настройке NGFW1 для аутентификации NGFW2 в процессе установления L2TP-туннеля.

- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения.
    - Для этого примера настроены параметры работы механизма DPD в режиме **Всегда включено**.
    - Значения параметров криптографии для этого примера оставим заданными по умолчанию.

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала. Для этого примера оставим значения криптографических параметров, заданные по умолчанию.

5. Создайте клиентское правило.

В разделе **Настройки → VPN Site-to-Site клиент → Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (ipsec/l2tp).
- Выберите в качестве туннельного интерфейса интерфейс tunnel4, созданный на шаге 2.
- Укажите IP-адрес VPN-сервера (10.72.0.32).

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

В разделе **Диагностика и мониторинг → Мониторинг → Маршруты** на узле NGFW2 добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс tunnel4.

IP-адреса противоположной стороны туннеля доступны с каждого узла.

Со стороны NGFW1.

Со стороны NGFW2.

Сервер и компьютер в сетях обоих офисов доступны друг для друга.

```
Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c91/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=5.13 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.64 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=3.37 ms
^C
--- 10.6.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.370/4.043/5.126/0.772 ms

Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.29 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.17 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=8.40 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.169/6.952/8.402/1.026 ms
```

Пример настройки site-to-site VPN с L2TP/IPSec (IKEv1) с помощью интерфейса CLI

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.

Настройка VPN-сервера

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

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   Admin@NGFW1# create network zone name WAN enabled-services [VPN]

   Подробнее о командах и параметрах для создания и редактирования зон в CLI — в разделе « Зоны».

2. Создайте зону для VPN-подключений.

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

```
Admin@NGFW1# 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
```

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   Для создания VPN-интерфейса используется команда:

   Admin@ug# create network interface vpn <parameters>

   Подробнее о порядке создания VPN-интерфейса в CLI — в разделе « Интерфейсы».

   На узле изначально уже создан VPN-интерфейс tunnel3, который может быть использован для настройки site-to-site VPN. Установите статический IP-адрес 172.16.0.1 для этого примера.

```
Admin@NGFW1# set network interface vpn tunnel3 ip-addresses [ 172.16.0.1/24 ]
Admin@NGFW1# show network interface vpn tunnel3

type            : vpn
node_name       : cluster
interface-name  : tunnel3
description     : Interface for site-to-site vpn
enabled         : on
netflow-profile  : Undefined
iface-mode      : static
mtu             : 1420
mss             : 0
speed           : 0
zone            : VPN for Site-to-Site
running         : off
master          : off
ip-addresses    : 172.16.0.1/24
```

4. Настройте параметры аутентификации.

   - Создайте локальную учетную запись для аутентификации узла-инициатора соединения при установлении L2TP-туннеля.

     Пример создания учетной записи User for s2s с логином vpn_user_s2s, входящего в группу VPN servers:

     Admin@NGFW1# create users user name "User for s2s" login vpn_user_s2s groups ["VPN servers"] enabled on

     Подробнее о командах и параметрах для создания локальных пользователей в CLI — в разделе « Настройки пользователей».

   - Создайте профиль аутентификации для VPN-пользователей.

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

     Admin@NGFW1# create users auth-profile name "local user auth profile" auth-methods local-user-auth on

Подробнее о порядке создания профилей аутентификации для пользователей в CLI — в разделе « Настройка профилей аутентификации».

5. Создайте правило подключения.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW1# create vpn-server connection-rules ike name ikev1_test_rule protocol ikev1 ike-mode main src-zones [ WAN ] dh-groups [ "Group 2 Prime 1024 bit" "Group 14 Prime 2048 bit" ] security [ SHA1/AES256 SHA256/AES256 ] psk 123
Repeat preshared key:
Admin@NGFW1# show vpn-server connection-rules ike ikev1_test_rule

name                : ikev1_test_rule
type                : ike
protocol            : ikev1
ike-mode            : main
src-zones           : WAN
dh-groups           : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
security            :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

key-lifetime        : 1 h
dpd-state           : off
dpd-interval        : 60
dpd-max-failures    : 5
```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе « Настройка серверных правил VPN».

6. Создайте правило аутентификации.

Пример создания правила аутентификации для протокола l2tp-ipsec:

```
Admin@NGFW1# create vpn-server authentication-rules site-to-site l2tp-ipsec name "s2s ipsec-l2tp auth rule" connection-rules [ "ikev1 conn rule" ] initiator-type ipv4 initiator-value 10.72.0.31 responder-type ipv4 responder-value 10.72.0.32 auth-prc
Admin@NGFW1# show vpn-server authentication-rules site-to-site l2tp-ipsec "s2s ipsec-l2tp auth rule"

name                    : s2s ipsec-l2tp auth rule
connection-rules        : ikev1 conn rule
initiator-type          : ipv4
initiator-value         : 10.72.0.31
responder-type          : ipv4
responder-value         : 10.72.0.32
auth-profile            : local user auth profile
key-lifetime            : 1 h
key-lifesize-enabled    : off
key-lifesize            : 100.0 MB
nat-keepalive           : 0
security                :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256
```

Подробнее о командах и параметрах для создания правила аутентификации в CLI — в разделе « Настройка серверных правил VPN».

7. Создайте политику VPN-подключения.

Политики VPN создаются с помощью синтаксиса языка UASL.

Пример создания правила политики VPN-подключения:

```
Admin@NGFW1# create vpn-server vpn-policy 7 upl-rule \
...OK
...auth_rules("s2s ipsec-l2tp auth rule") \
...vpn_routes(10.75.0.0/16) \
...ip_range("172.16.0.2-172.16.0.254") \
...desc("VPN server policy for S2S IPSec/L2TP connection.") \
...mask(255.255.255.0) \
...use_system_dns(true) \
...enabled(true) \
...type(s2s_l2tp) \
...interface(tunnel3) \
...name("S2S IPSec/L2TP example VPN policy")
```

Подробнее о создании политик VPN в CLI — в разделе « Настройка серверных правил VPN».

Чтобы VPN-сервер (NGFW1) узнал о подсетях за узлом-инициатором соединения, вы можете прописать маршрут к подсетям в виртуальном маршрутизаторе VPN-сервера, указав в качестве адреса назначения адрес VPN-туннеля, используемый на NGFW2.

```
Admin@NGFW1# set network virtual-router default routes new name route1 destination-ip 10.6.0.0/16 gateway 172.16.0.2 enabled on
Admin@NGFW1# show network virtual-router default routes

route1
    name            : route1
    enabled         : on
    destination-ip  : 10.6.0.0/16
    gateway         : 172.16.0.2
    interface       : auto
    metric          : 0
```

8. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1:

```
Admin@NGFW1# create network-policy firewall 8 upl-rule \
...PASS \
...src.zone = (LAN1, "VPN for Site-to-Site") \
...dst.zone = (LAN1, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan1_s2s)
```

Подробнее о порядке настройки правил межсетевого экрана в CLI — в разделе « Настройка правил межсетевого экрана».

Настройка VPN-клиента

Для настройки NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону, которой будет принадлежать интерфейс, используемый для подключения по VPN.

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

```
Admin@NGFW2# 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
```

2. Создайте VPN-интерфейс.

Пример создания VPN-интерфейса tunnel4:

```
Admin@NGFW2# create network interface vpn interface-name 4 iface-mode dynamic zone "VPN for Site-to-Site" enabled on
Admin@NGFW2# show network interface vpn tunnel4

type              : vpn
node_name         : cluster
interface-name    : tunnel4
enabled           : on
netflow-profile   : Undefined
iface-mode        : dynamic
mtu               : 1420
mss               : 0
speed             : 0
zone              : VPN for Site-to-Site
running           : off
master            : off
```

3. Настройте доступ к сетевым ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

```
Admin@NGFW2# create network-policy firewall 8 upl-rule \
...PASS \
...src.zone = (LAN2, "VPN for Site-to-Site") \
...dst.zone = (LAN2, "VPN for Site-to-Site") \
...rule_log(session) \
...enabled(true) \
...name(allow_lan2_s2s)
```

4. Создайте правило подключения к VPN.

Пример создания правила подключения для протокола IKEv1:

```
Admin@NGFW2# create vpn-client connections l2tp-ipsec name ipsec/l2tp ike-mode main authentication-login vpn_user_s2s authentication-password 123456 initiator-type ipv4 initiator-value 10.72.0.31 responder-type ipv4 responder-value 10.72.0
Repeat preshared key:
Admin@NGFW2# show vpn-client connections l2tp-ipsec ipsec/l2tp

name                    : ipsec/l2tp
ike-mode                : main
authentication-login    : vpn_user_s2s
phase1-key-lifetime     : 1 h
phase2-key-lifetime     : 1 h
key-lifesize-enabled    : off
key-lifesize            : 100.0 MB
initiator-type          : ipv4
initiator-value         : 10.72.0.31
responder-type          : ipv4
responder-value         : 10.72.0.32
dpd-state               : off
dpd-interval            : 60
dpd-max-failures        : 5
dh-groups               : Group 2 Prime 1024 bit; Group 14 Prime 2048 bit
phase1-security         :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256

phase2-security         :
    authentication    : SHA1
    encryption        : AES256

    authentication    : SHA256
    encryption        : AES256
```

Подробнее о командах и параметрах для создания правила подключения в CLI — в разделе « Настройка клиентских правил VPN ».

5. Создайте клиентское правило.

Клиентские правила создаются с помощью синтаксиса языка UASL.

Пример создания клиентского правила для протокола l2tp-ipsec:

```
Admin@NGFW2# create vpn-client rules 4 upl-rule \
...OK \
...server_address("10.72.0.32") \
...connection("ipsec/l2tp") \
...interface(tunnel4) \
...enabled(false) \
...name("ipsec/l2tp")
```

Подробнее о командах и параметрах для создания клиентского правила в CLI — в разделе « Настройка клиентских правил VPN ».

Для инициации соединения включите клиентское правило.

```
Admin@NGFW2# set vpn-client rules 4 upl-rule \
...enabled(true)
```

Проверка VPN-соединения

Проверка доступности соседнего узла и маршрута в сеть удаленного офиса.

Со стороны NGFW 1:

```
Admin@NGFW1> 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
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:12:57
K>* 10.6.0.0/16 [0/0] via 172.16.0.2, tunnel3, 00:00:16
C>* 10.72.0.0/16 is directly connected, port1, 00:12:57
C>* 10.75.0.0/16 is directly connected, port2, 00:12:57
C>* 10.153.0.0/16 is directly connected, port3, 00:12:57
C>* 172.16.0.0/24 is directly connected, tunnel3, 00:12:57
C>* 172.26.0.0/16 is directly connected, port0, 00:12:57
C>* 172.30.250.0/24 is directly connected, tunnel1, 00:12:57
C>* 172.30.255.0/24 is directly connected, tunnel2, 00:12:57

Admin@NGFW1> ping host 172.16.0.2

PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_req=1 ttl=64 time=1.32 ms
64 bytes from 172.16.0.2: icmp_req=2 ttl=64 time=3.89 ms
64 bytes from 172.16.0.2: icmp_req=3 ttl=64 time=1.71 ms

--- 172.16.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.327/2.311/3.893/1.129 ms
```

Со стороны NGFW 2:

```
Admin@NGFW2> 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
K>* 0.0.0.0/0 [0/0] via 172.26.0.1, port0, 00:08:41
C>* 10.6.0.0/16 is directly connected, port2, 00:08:41
C>* 10.72.0.0/16 is directly connected, port1, 00:08:41
K>* 10.75.0.0/16 [0/0] via 172.16.0.1, tunnel4, src 172.16.0.2, 00:01:18
K>* 172.16.0.1/32 [0/0] is directly connected, tunnel4, 00:01:23
C>* 172.16.0.2/32 is directly connected, tunnel4, 00:01:23
C>* 172.26.0.0/16 is directly connected, port0, 00:08:41

Admin@NGFW2> ping host 172.16.0.1

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_req=1 ttl=64 time=2.70 ms
64 bytes from 172.16.0.1: icmp_req=2 ttl=64 time=1.76 ms
64 bytes from 172.16.0.1: icmp_req=3 ttl=64 time=3.35 ms

--- 172.16.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.763/2.609/3.359/0.655 ms
```

Проверка установления L2TP-туннеля в журналах узлов.

На NGFW1.

```
Admin@NGFW1> show logs log vpn-server static | grep "LCP connected" -BA 0:23
2026-02-04 13:36:47.063149<0.1074.0> [info][vpn] lcp_fsm:send_connected/1:256 LCP connected
2026-02-04 13:36:47.063159<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:62 PAPResponse with password
2026-02-04 13:36:47.063180<0.1074.0> [info][vpn] lcp_fsm:send_auth_challenge/1:226 PAP protocol selected - wait for client
2026-02-04 13:36:47.064482<0.1074.0> [info][xmlrpc] database:process_server_policy_phase/2:380 server policy "S2S IPSec/L2TP example VPN policy"
2026-02-04 13:36:47.064547<0.1074.0> [warning][xmlrpc] database:login_user_v2/5:449 login user "vpn_user_s2s" ip "10.72.0.31" token
        "35a447c5-a03f-49f4-83d5-3493cd4b983a" guid "c9202ee4-cb35-4d18-91fb-62a67f72aa0e"
2026-02-04 13:36:47.066152<0.1074.0> [info][vpn] lcp_fsm:STATE_OPENED_9/2:984 auth succeed, username <<"vpn_user_s2s">>, guid
        "c9202ee4-cb35-4d18-91fb-62a67f72aa0e", parent pid <0.1073.0>
2026-02-04 13:36:47.066526<0.1074.0> [info][vpn] lcp_fsm:send_auth_response_pap/4:210 send PAP response ID 1 code 2 <<"Willkommen">>
2026-02-04 13:36:47.066581<0.1074.0> [info][vpn] lcp_fsm:send_ccp_configure/2:750 Send CCP configure packet <<1,1,0,6,4,2>>
2026-02-04 13:36:47.066953<0.1074.0> [info][vpn] lcp_fsm:send_ipcp_configure/4:735 Send IPCP configure packet {172,16,0,1}/[{{10,75,0,0},{255,255,0,0}}]
2026-02-04 13:36:47.067352<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,1,[{'IPCPOpt_Address',<<0,0,0,0>>},{'IPCPOpt_PriDNS',<<0,0,0,0>>}]}}
2026-02-04 13:36:47.067440<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',255,3,49185,{'LCPProtocolReject',8,1,257}}
2026-02-04 13:36:47.067498<0.1074.0> [error][vpn] lcp_fsm:STATE_OPENED_9/2:1054 Protocol 257 rejected!
2026-02-04 13:36:47.067821<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',2,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.068119<0.1073.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.068174<0.1074.0> [critical][vpn] lcp_fsm:analyze_ipcp_option/2:785 IPClientSuggested {172,16,0,2} IPClientReqTuple {172,16,0,2}
2026-02-04 13:36:47.068258<0.1074.0> [critical][vpn] lcp_fsm:send_ipcp_response/2:881 IPCP ACK! Great deal
        {'IPCPHeader',1,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}
2026-02-04 13:36:47.069245<0.1073.0> [warning][vpn] l2tp_fsm:handle_info/3:750 NewIPs [{client_ip,{172,16,0,2}},{server_ip,{172,16,0,1}}] Routes
        [{{10,75,0,0},{255,255,0,0}}]
```

На NGFW2.

```
Admin@NGFW2> show logs log vpn-client static | grep "LCP connected" -BA 0:19
2026-02-04 13:36:47.052244<0.1069.0> [info][vpn] lcp_client:send_connected/1:155 LCP connected, send auth
2026-02-04 13:36:47.056257<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,49187,{pap_success,1}}
2026-02-04 13:36:47.056341<0.1069.0> [info][vpn] lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip undefined dns undefined
2026-02-04 13:36:47.056330<0.1066.0> [info][vpn] ppp_protocol:decode_ccp/1:387 {'CCPHeader',1,1,<<4,2>>}
2026-02-04 13:36:47.056408<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP: {'PPPHeader',undefined,undefined,33021,{'CCPHeader',1,1,<<4,2>>}}
2026-02-04 13:36:47.056668<0.1069.0> [info][vpn] lcp_client:encode_protocol_reject/2:125 send LCP reject protocol "010100060402"
2026-02-04 13:36:47.056903<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',1,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.056958<0.1069.0> [critical][vpn] lcp_client:send_ipcp_response/2:628 IPCP ACK! Server ip <<172,16,0,1>>, routes
        [{{10,75,0,0},{255,255,0,0}}]
2026-02-04 13:36:47.057046<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',3,1,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.057072<0.1069.0> [warning][vpn] lcp_client:send_ipcp_response/2:689 Send IPCP answer
        {'IPCPHeader',2,1,[{'IPCPOpt_Routes',[{{10,75,0,0},{255,255,0,0}}]},{'IPCPOpt_Address',<<172,16,0,1>>}]}
2026-02-04 13:36:47.057355<0.1069.0> [info][vpn] lcp_client:send_ipcp_configure/4:580 Send IPCP configure packet ip <<172,16,0,2>> dns <<172,16,0,1>>
2026-02-04 13:36:47.060539<0.1066.0> [info][vpn] ppp_protocol:decode_packet/1:64 PPP:
        {'PPPHeader',undefined,undefined,32801,{'IPCPHeader',2,2,[{'IPCPOpt_Address',<<172,16,0,2>>},{'IPCPOpt_PriDNS',<<172,16,0,1>>}]}}
2026-02-04 13:36:47.060650<0.1069.0> [critical][vpn] lcp_client:send_ipcp_response/2:660 IPCP ACK! Client IP <<172,16,0,2>> dns <<172,16,0,1>>
2026-02-04 13:36:47.061877<0.1069.0> [info][vpn] lcp_client:send_ipcp_response/2:672 AuthToken "a270d112-428f-4d28-8727-354510f99325"
2026-02-04 13:36:47.062790<0.1066.0> [info][vpn] l2tp_client:handle_info/3:729 configure device "tunnel4" static undefined dynamic <<172,16,0,2>>
```

Пример настройки site-to-site VPN с IPSec (IKEv2) и аутентификацией посредством сертификатов

Product: NGFW
Version: 7.x, 7.5.x
Technology: VPN

В качестве примера для создания site-to-site VPN-туннеля будет рассмотрена следующая схема.

Настройка VPN-сервера

Для настройки узла NGFW1 в качестве VPN-сервера (ответчика) выполните следующие шаги:

1. Создайте зону, из которой будет подключаться сервер-инициатор подключения и разрешите сервис VPN для этой зоны.

   В разделе **Настройки → Сеть → Зоны** создайте зону WAN и активируйте сервис VPN в параметрах контроля доступа для этой зоны. Подробнее о создании и настройке зон — в разделе « Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию на узле зоной VPN for Site-to-Site. Подробнее о создании и настройке зон — в разделе «Настройка зон».

3. Создайте VPN-интерфейс, который будет использоваться для установления туннеля.

   В этом примере воспользуемся созданным по умолчанию интерфейсом tunnel2. Подробнее о создании и настройке сетевых интерфейсов — в разделе « Настройка интерфейсов».

4. Настройте параметры аутентификации.

   - Импортируйте созданный заранее сертификат VPN-сервера и корневой сертификат. О примерах создания самоподписанных сертификатов — в Приложении.

     В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импорт.** В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

   - Создайте профиль клиентского сертификата в веб-консоли NGFW1. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите поле **Subject altname IPv4** для получения из сертификата узла-инициатора соединения (NGFW2) его IP-адреса.

5. Создайте правило подключения.

   В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

   - На вкладке **Общие**:
     - Укажите название правила подключения.
     - Выберите протокол подключения **IKEv2**.

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения.
- На вкладке **Фаза 1** укажите время жизни ключей, параметры работы режима DPD и криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Site-to-Site → IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите режим аутентификации посредством сертификатов (**PKI**).
  - Выберите импортированный на шаге 4 сертификат VPN-сервера.
  - Выберите созданный на шаге 4 профиль клиентского сертификата.
  - Выберите тип идентификации узлов (**IPv4**).
  - Укажите значения параметров идентификации узла-инициатора и узла-ответчика. В этом примере в качестве значений параметров идентификации указаны IP-адреса внешних интерфейсов узлов NGFW2 и NGFW1.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Site-to-Site → IPsec**. Укажите следующие ключевые параметры:

- Укажите название правила аутентификации.
- Выберите VPN-адаптер, созданный на шаге 2 (tunnel2).
- В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

8. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной

на шаге 2 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN1.

Подробнее о создании и настройке правил межсетевого экрана — в разделе « Межсетевой экран».

Настройка VPN-клиента

Для настройки узла NGFW2 в качестве узла-инициатора соединения выполните следующие шаги:

1. Создайте зону для VPN-подключений.

В этом примере воспользуемся уже созданной на узле зоной VPN for Site-to-Site.

2. Создайте VPN-интерфейс.

Для этого примера создан VPN-интерфейс tunnel5. Режим получения IP-адреса у этого интерфейса динамический.

3. Настройте параметры аутентификации.

Импортируйте созданный заранее сертификат VPN-клиента.

В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импорт.** В открывшемся окне укажите название сертификата и добавьте сгенерированные файлы сертификата VPN-сервера и его закрытого ключа.

4. Контроль доступа к ресурсам.

Для предоставления доступа пользователям VPN в определенные сегменты сети создайте в разделе **Настройки → Политики сети → Межсетевой экран** правило межсетевого экрана, разрешающее трафик из созданной на шаге 1 зоны в нужные зоны. Чтобы трафик передавался клиенту из разрешенных зон через VPN-туннель, разрешите трафик из нужной зоны источника в зону VPN for Site-to-Site.

Для этого примера создано правило межсетевого экрана, разрешающее трафик между зоной VPN for Site-to-Site и зоной LAN2.

5. Создайте правило подключения к VPN.

В разделе **Настройки → VPN Site-to-Site клиент → Подключение клиента** нажмите **Добавить** и выберите протокол **IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите режим аутентификации с помощью сертификата (**PKI**).
  - Выберите импортированный на шаге 3 сертификат клиента.
  - Выберите параметр идентификации узла (**IPv4**).
  - Укажите в качестве значения параметра идентификации узла IP-адрес интерфейса из зоны WAN (10.72.0.31).

- На вкладке **Фаза 1** укажите параметры фазы 1 для установления защищенного канала IKE SA: Для этого примера оставим значения параметров, заданные по умолчанию

- На вкладке **Фаза 2** укажите параметры второй фазы для установления защищенного канала IPsec SA.
    - Для этого примера оставим значения криптографических параметров, заданные по умолчанию.
    - В разделе **Peer networks** укажите адреса локальных и удаленных подсетей для определения селекторов трафика при организации защищенного канала передачи данных IPsec. В этом примере указываются адреса подсетей LAN2 и LAN1 соответственно

6. Создайте клиентское правило.

В разделе **Настройки → VPN Site-to-Site клиент → Клиентские правила** нажмите **Добавить** и укажите следующие ключевые параметры:

- Укажите название клиентского правила.
- Выберите созданное ранее подключение к VPN (ikev2 pki).
- Выберите в качестве туннельного интерфейса интерфейс tunnel3.
- Укажите адрес VPN-сервера (vpntest.net).

Для инициации соединения включите клиентское правило.

Проверка VPN-соединения

После установлении VPN-туннеля в веб-консоли NGFW 2 в строке клиентского правила появится индикация успешного установления VPN-туннеля.

На узлах NGFW1 и NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → VPN** появится информация о новом туннеле.

На узле NGFW1 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.6.0.0/16 через туннельный интерфейс tunnel2.

На узле NGFW2 в разделе **Диагностика и мониторинг → Мониторинг → Маршруты** добавится маршрут в сеть удаленного офиса 10.75.0.0/16 через туннельный интерфейс tunnel5.

Узлы в сетях обоих офисов доступны друг для друга.

```
Admin@nodename:~$ ip a show ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:91 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.75.0.27/16 brd 10.75.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c91/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.6.1.11
PING 10.6.1.11 (10.6.1.11) 56(84) bytes of data.
64 bytes from 10.6.1.11: icmp_seq=1 ttl=62 time=3.54 ms
64 bytes from 10.6.1.11: icmp_seq=2 ttl=62 time=3.99 ms
64 bytes from 10.6.1.11: icmp_seq=3 ttl=62 time=4.85 ms
^C
--- 10.6.1.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.536/4.124/4.851/0.545 ms

Admin@nodename:~$ ip a show dev ens224
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:54:54:a8:7c:94 brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 10.6.1.11/16 brd 10.6.255.255 scope global ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::254:54ff:fea8:7c94/64 scope link
       valid_lft forever preferred_lft forever
Admin@nodename:~$ ping 10.75.0.27
PING 10.75.0.27 (10.75.0.27) 56(84) bytes of data.
64 bytes from 10.75.0.27: icmp_seq=1 ttl=62 time=6.81 ms
64 bytes from 10.75.0.27: icmp_seq=2 ttl=62 time=6.78 ms
64 bytes from 10.75.0.27: icmp_seq=3 ttl=62 time=4.68 ms
^C
--- 10.75.0.27 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.677/6.089/6.808/0.998 ms
```

Пример настройки удаленного доступа в сеть для конечного устройства на Astra Linux

Product: NGFW, UserGate Client
Version: 7.x, 7.5.x
Technology: VPN

Пример создания VPN-подключения между конечным устройством с операционной системой Astra Linux и UserGate NGFW версии 7.5.0.

В этом примере UserGate NGFW выступает в роли VPN-сервера, а компьютер пользователя на Astra Linux с установленным ПО UserGate Client — в роли конечного устройства. Аутентификация пользователя будет происходить с помощью сертификата X.509. Конечному устройству будет передан маршрут к сети за VPN-сервером.

Сначала настройте VPN-сервер, затем настройте VPN-клиент на конечном устройстве и инициируйте подключение к VPN-серверу.

Настройка VPN-сервера

Для настройки UserGate NGFW в качестве VPN-сервера выполните следующие шаги:

1. Разрешите сервис VPN в контроле доступа зоны, из которой будут подключаться конечные устройства.

   В веб-консоли UserGate NGFW в разделе **Настройки → Сеть → Зоны** создайте зону WAN. В параметрах контроля доступа зоны разрешите сервис VPN. Подробнее о создании и настройке зон — в разделе « Настройка зон».

2. Создайте зону для VPN-подключений.

   В этом примере воспользуемся уже созданной по умолчанию зоной VPN for remote access. Подробнее о создании и настройке параметров зон — в разделе « Настройка зон».

3. Создайте VPN-интерфейс для организации туннеля.

   В этом примере воспользуемся уже созданным по умолчанию на узле VPN-интерфейсом tunnel1, который может быть использован для настройки remote access VPN. Изначально этот интерфейс не активен, его необходимо включить в свойствах интерфейса.

4. Настройте параметры аутентификации:

   - Импортируйте созданные заранее сертификаты: сертификат VPN-сервера и корневой сертификат. Примеры создания самоподписанных сертификатов приведены в Приложении.

     В разделе **Настройки → Консоль администратора → Сертификаты** нажмите **Импортировать.** В открывшемся окне укажите название сертификата и добавьте созданные ранее файлы сертификата VPN-сервера и его закрытого ключа. В этом же разделе импортируйте корневой сертификат без указания закрытого ключа.

   - Создайте профиль клиентского сертификата в веб-консоли UserGate NGFW. Для этого перейдите в раздел **Настройки → Консоль администратора → Профили клиентских сертификатов** и нажмите **Добавить**. В открывшемся окне укажите название профиля, добавьте импортированный на предыдущем шаге корневой сертификат и выберите **Common-name**, **Subject altname email** или **Principal name** для получения имени пользователя.

   - Создайте профиль аутентификации для пользователей VPN. Подробно о профилях аутентификации — в разделе « Профили аутентификации». Для этого примера был создан профиль аутентификации в домене ADTEST1 через LDAP-коннектор ad16:

5. Создайте правило подключения.

В разделе **Настройки → VPN-сервер → Правила подключения** нажмите **Добавить** и выберите протокол **IKE**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила подключения.
  - Выберите протокол подключения **IKEv2**.

- На вкладке **Источник** укажите зону или адреса, с которых разрешено принимать подключения к VPN. В этом примере разрешено запрашивать подключение к VPN из зоны WAN.

- На вкладке **Назначение** вы можете указать списки адресов, на которые будут приходить запросы на VPN-подключения от конечных устройств.
- На вкладке **Фаза 1** укажите криптографические параметры фазы 1 согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

6. Создайте правило аутентификации.

В разделе **Настройки → VPN-сервер → Правила аутентификации** нажмите **Добавить** и выберите **Удаленный доступ → IKEv2**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Укажите название правила аутентификации.
  - Выберите импортированный на шаге 4 сертификат VPN-сервера.
  - Выберите созданный на шаге 4 профиль аутентификации пользователя.
  - Выберите режим аутентификации посредством сертификатов (**PKI**).
  - Выберите созданный на шаге 4 профиль клиентского сертификата.
  - В разделе **Правила подключения** добавьте созданное на предыдущем шаге правило подключения.

- На вкладке **Фаза 2** укажите параметры второй фазы согласования защищенного соединения. Для этого примера оставим значения параметров, заданные по умолчанию.

7. Создайте политику VPN-подключения.

В разделе **Настройки → VPN-сервер → Политики VPN** нажмите **Добавить** и выберите **Удаленный доступ → UserGate Client**. Укажите следующие ключевые параметры:

- На вкладке **Общие**:
  - Поставьте флажок для включения политики VPN.
  - Укажите название правила аутентификации.
  - В разделе **Правила аутентификации** добавьте созданное на предыдущем шаге правило аутентификации.

- На вкладке **Пользователи** вы можете добавить локальную или доменную учетную запись или группу, которые будут использоваться для аутентификации пользователей.
- На вкладке **Подсети для VPN**
  - Укажите VPN-интерфейс tunnel1, который будет использоваться для подключения.
  - Укажите диапазон IP-адресов, которые будут использованы для подключения. Исключите из диапазона адрес, который назначен VPN-интерфейсу UserGate NGFW, используемому совместно с данной сетью.
  - Укажите маску сети VPN.
  - Оставьте флажок **Использовать системные DNS-серверы** для передачи клиенту туннельного адреса UserGate NGFW в качестве DNS-сервера.

- На вкладке **Маршруты для UserGate Client** укажите параметры маршрутов, передаваемых на конечное устройство с помощью функции раздельного туннелирования.
  - В этом примере на конечном устройстве будет добавлен маршрут к тестовому серверу devsite.ext (10.153.0.5).

8. Настройте контроль доступа к ресурсам.
   - Создайте правило NAT, выполняющее трансляцию IP-адресов при поступлении трафика из зоны VPN for remote access в зону LAN. Правило создается в разделе **Политики сети → NAT и маршрутизация**.
   - При необходимости предоставления доступа пользователям VPN в определенные сегменты сети в разделе **Настройки → Политики сети → Межсетевой экран** необходимо создать правило межсетевого экрана, разрешающее трафик из созданной зоны в требуемые зоны. Для этого примера создано правило межсетевого экрана, разрешающее весь трафик из зоны VPN for remote access в зону LAN.

Настройка VPN-клиента

Предполагается, что ПО UserGate Client уже установлено на конечном устройстве. Подробнее об установке ПО — в разделе « Настройка VPN-соединения на конечном устройстве».

Для настройки VPN-клиента необходимо выполнить следующие шаги:

1. Откройте окно настройки приложения UserGate Client и на вкладке VPN-соединения нажмите **Добавить**.

2. Настройте параметры профиля VPN-соединения:

- Укажите название соединения.
- Укажите IP-адрес или доменное имя VPN-сервера. В этом примере указано доменное имя сервера vpntest.net. Адрес должен быть прописан в серверном сертификате, импортированном на шаге 4 настройки VPN-сервера.
- Выберите протокол для установления VPN-соединения. В этом примере используется протокол **IKEv2**.
- Выберите один из способов аутентификации. В этом примере используется аутентификация посредством сертификатов.
- Выберите заранее созданные файл сертификата пользователя ADTEST1\user, закрытый ключ и введите пароль закрытого ключа.

3. Сохраните параметры профиля, нажав **Сохранить**.

Настройка VPN-клиента завершена.

Для установления VPN-соединения в строке состояния в правом нижнем углу нажмите на значок UserGate Client и в появившемся меню выберите профиль соединения **ikev2 pki**.

В случае успешного подключения на значке UserGate Client появится символ установленного соединения.

Проверка подключения

После установлении VPN-соединения в веб-консоли UserGate NGFW на вкладке **Диагностика и мониторинг** в разделе **Мониторинг →VPN** появилась информация о новом VPN-соединении.

В **Журнале событий** на вкладке **Журналы и отчеты** появилась соответствующая запись.

На конечном устройстве в таблице маршрутизации добавился маршрут к серверу devsite.ext (10.153.0.5) через туннельный интерфейс. Сервер доступен с конечного устройства..