

# Построение VPN туннеля между шлюзом безопасности «Bel VPN Gate» и мобильным клиентом «Bel VPN Client 4.5», аутентификация на ТСОК

## Описание стенда

Сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности ПАК «Bel VPN Gate 4.5» (устройство GW1), и клиентом ПП «Bel VPN Client 4.5» (устройство Client1). Для защиты будет построен VPN туннель между устройствами GW1 и Client1. Устройство Client1 сможет общаться по защищенному каналу (VPN) с устройствами из подсети SN1 (в частности с IPHost1). Адрес мобильного клиента неизвестен заранее. В ходе построения защищенного соединения мобильный клиент получает адрес из заранее определенного на шлюзе пула.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты.

Параметры защищенного соединения:

- IKE параметры:
  - Аутентификация – на сертификатах открытого ключа ЭЦП по СТБ 34.101.45-2013;
  - Алгоритм шифрования – СТБ 34.101.31-2020 (7.3);
  - Алгоритм вычисления хеш-функции – СТБ 34.101.31-2020 (7.8);
  - Протокол согласования ключей – протокол Диффи-Хеллмана на эллиптических кривых (СТБ 34.101.66-2014).
- IPsec параметры:
  - Туннельный режим, протокол ESP:
  - Алгоритм шифрования – СТБ 34.101.31-2020 (7.3);
  - Алгоритм контроля целостности – СТБ 34.101.31-2020 (7.5).

Схема стенда (Рисунок 1):

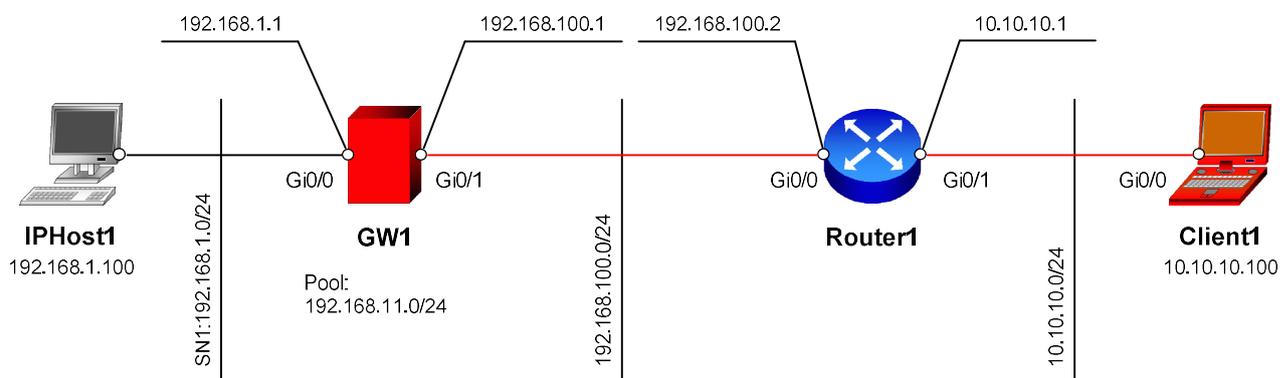


Рисунок 1

# Настройка стенда

## Настройка шлюза безопасности GW1

Настройку начните со шлюза безопасности GW1. Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация шлюза описывается в документации на ПАК «Bel VPN Gate 4.5» – [bel\\_vpn\\_gate\\_45\\_userguides](#) («Руководство пользователя. Настройка», раздел «Инициализация ПАК Bel VPN Gate при первом старте»).

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПАК «Bel VPN Gate 4.5» – [bel\\_vpn\\_gate\\_45\\_cisco-like](#) («Руководство пользователя. Cisco-like команды», раздел «Команды для работы с сертификатами»).

## Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

1. Для входа в консоль запустите `cs_console`:

```
root@belvpngate:~# cs_console
belvpngate>en
Password:
```

Пароль по умолчанию: `csp`.

2. Перейдите в режим настройки:

```
belvpngate#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

3. В настройках интерфейсов задайте IP-адреса:

```
belvpngate(config)#interface GigabitEthernet 0/0
belvpngate(config-if)#ip address 192.168.1.1 255.255.255.0
belvpngate(config-if)#no shutdown
belvpngate(config-if)#exit
belvpngate(config)#interface GigabitEthernet 0/1
belvpngate(config-if)#ip address 192.168.100.1 255.255.255.0
belvpngate(config-if)#no shutdown
belvpngate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию:

```
belvpngate(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

5. Выйдите из cisco-like интерфейса:

```
belvpngate(config)#end
belvpngate#exit
```

## Формирование запроса и регистрация сертификата

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

1. Установите правильное системное время.

```
root@belvpngate:~# date MMDDHHmmYYYY
```

**MM** – месяц;

**DD** – день;  
**HH** – часы;  
**mm** – минуты;  
**YYYY** – год

Пример установки даты:

```
root@belvpngate:~# date 120712152022
Wed Dec 07 12:15:00 UTC 2022
```

Данная запись соответствует 7 апреля 2022 года 12:15.

- Создайте папку /opt/certs:

```
root@belvpngate:~# mkdir /opt/certs
```

- Создайте контейнер на ключевом носителе:

```
root@belvpngate:~#/opt/Avset/bin/cryptocont n -n=контейнер -p=пароль
```

**контейнер** – название создаваемого контейнера, для создания на НКИ (носителе ключевой информации) ДОЛЖНО содержать в начале названия префикс “**av:**”;

**пароль** – пароль (PIN) для доступа к носителю ключевой информации AvPass/AvBign.

Пример создания криптоконтейнера на НКИ:

```
root@belvpngate:~#/opt/Avest/bin/cryptocont n -n=av:container -p=12345678
```

- Сформируйте запрос на сертификат.

```
root@belvpngate:~#/opt/Avset/bin/cryptcont r -n=контейнер -p=пароль -cn=CommonName -c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

**контейнер** – название контейнера, созданного на предыдущем шаге;

**пароль** – пароль (PIN) для доступа к носителю ключевой информации;

**CommonName** – идентификатор устройства;

**OrgName** – наименование организации;

**OrgUnitName** – наименование подразделения;

**путь\_к\_файлу** – путь к файлу с создаваемым запросом, рекомендуется указывать расширение “**.req**”.

Пример создания запроса:

```
root@belvpngate:~#/opt/Avest/bin/cryptocont r -n=av:container -p=12345678 -cn=GW1 -c=BY -o=S-TerraBel -t=Research -f=/opt/certs/GW1.req
```

- Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением **p7b** или **cer**).

Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные сег файлы.

- Доставьте файлы сертификатов на Шлюз безопасности в предварительно созданный на нем каталог /opt/certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp -P 22 исходный_файл root@адрес_шлюза:/путь_к_файлу
```

**исходный файл** – путь к файлу сертификата;

**адрес\_шлюза** – сетевой адрес Шлюза;

**путь\_к\_файлу** – полный путь для сохранения файла на Шлюзе.

Пример передачи файла на Шлюз безопасности:

```
pscp -P 22 D:\ca.cer root@192.168.1.1:/opt/certs
...
```

```
Store key in cache? (y/n)
root@192.168.1.1's password:
```

**Важно:** Среда передачи в этом случае должна быть доверенной. Описание создания доверенной среды через недоверенные каналы связи смотрите в документации на ПАК «Bel VPN Gate 4.5» [bel\\_vpn\\_gate\\_45\\_userguides](#) («Руководство пользователя. Настройка», раздел «Построение VPN туннеля между шлюзом безопасности Bel VPN Gate 4.5 и рабочим местом администратора для удаленной настройки шлюза»).

7. Выполните импорт сертификата УЦ в базу Шлюза используя утилиту `cert_mgr`:

```
root@belvpngate:~# cert_mgr import -f путь_к_файлу -t
```

**путь\_к\_файлу** – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@belvpngate:~# cert_mgr import -f /opt/cert/UC.cer -t
1 OK C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
```

8. Выполните импорт локального (личного) сертификата в базу Шлюза:

```
root@belvpngate:~# cert_mgr import -f путь_к_файлу -kc контейнер -kcp пароль
```

**путь\_к\_файлу** – полный путь к файлу сертификата УЦ;

**контейнер** – название контейнера, созданного ранее. Если контейнер храниться на ключе, введите серийный номер ключа в формате

**av:серийный номер:название контейнера;**

**пароль** – пароль для доступа к ключевому носителю информации.

Пример импорта:

```
root@belvpngate:~#cert_mgr import -f /opt/cert/GW1.cer -
kc av:AVP012345678910:container -kcp 12345678
1 OK CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

9. Выведите список сертификатов, находящихся в базе Шлюза, командой `cert_mgr show` и проверьте наличие записей **trusted** и **local**:

```
root@belvpngate:~# cert_mgr show
```

Пример вывода:

```
root@belvpngate:~# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 Status: local CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

## Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите `cs_console`:

```
root@belvpngate:~# cs_console
belvpngate>en
Password:
```

Пароль по умолчанию: `csp`.

**Важно:** пароль по умолчанию необходимо сменить.

1. Перейдите в режим настройки:

```
belvpngate#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

2. Смените пароль по умолчанию:

```
belvpngate(config)#username cicons password <пароль>
```

3. Смените название шлюза:

```
belvpngate(config)#hostname GW1
```

4. Задайте тип идентификации:

```
GW1(config)#crypto isakmp identity dn
```

5. Задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash belt
GW1(config-isakmp)#encryption belt
GW1(config-isakmp)#authentication belt-sig
GW1(config-isakmp)#group beltdh
GW1(config-isakmp)#exit
```

6. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

7. Задайте пул, из которого будет выдан адрес клиенту:

```
GW1(config)#ip local pool POOL 192.168.11.1 192.168.11.254
```

8. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.11.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

9. Создайте динамическую крипто-карту:

```
GW1(config)#crypto dynamic-map DMAP 1
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs beltdh
GW1(config-crypto-map)#set pool POOL
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

10. Привяжите динамическую карту к статической:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp dynamic DMAP
```

11. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
GW1(config)#interface GigabitEthernet 0/1
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

12. Отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)#revocation-check none
GW1(ca-trustpoint)#exit
```

13. Настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
GW1(config)#end
```

```
GW1#exit
```

14. Убедитесь что все сертификаты активны – статус сертификата должен быть **active**:

```
root@belvpngate:~# cert_mgr check
```

Пример:

```
root@belvpngate:~# cert_mgr check
1 State: Active C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 State: Active CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

В **Приложении** представлен текст [cisco-like конфигурации](#) для шлюза GW1.

## Вариант настройки клиента Client1 без утилиты администратора

Настройка клиента состоит из нескольких этапов:

- установка ПП Bel VPN Client 4.5;
- настройка подключения ПП Bel VPN Client 4.5;
- формирование запроса и получение сертификата.

### Установка ПП Bel VPN Client 4.5

1. Зайдите в папку с программным продуктом Bel VPN Client 4.5;
2. Запустите файл «setup.exe»;
3. Выберите в меню Установщика продукта Bel VPN Client способ «Bel VPN Client 4.5» и нажмите «Далее» (Рисунок 2);

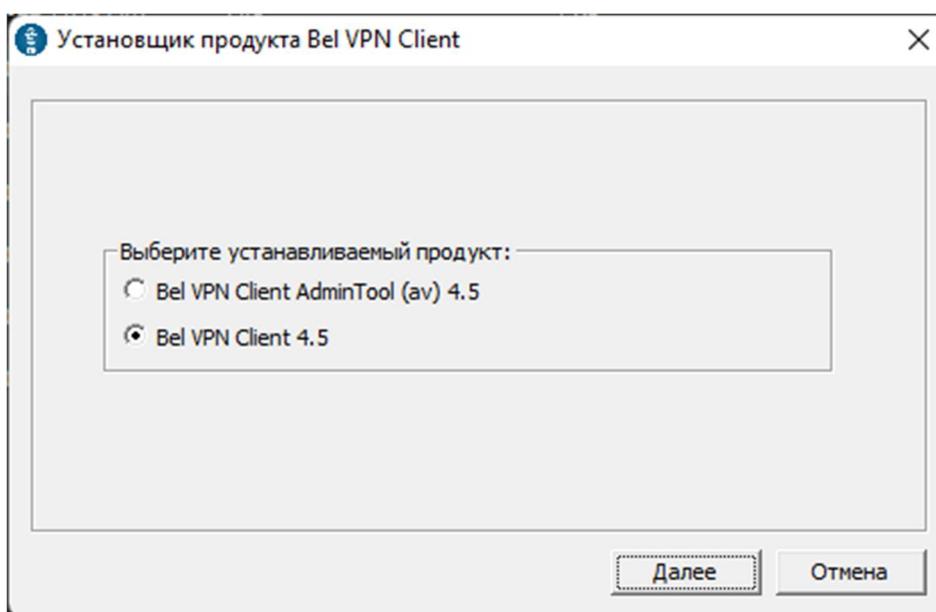


Рисунок 2

4. В новом окне (Рисунок 3) нажмите «Установить»;

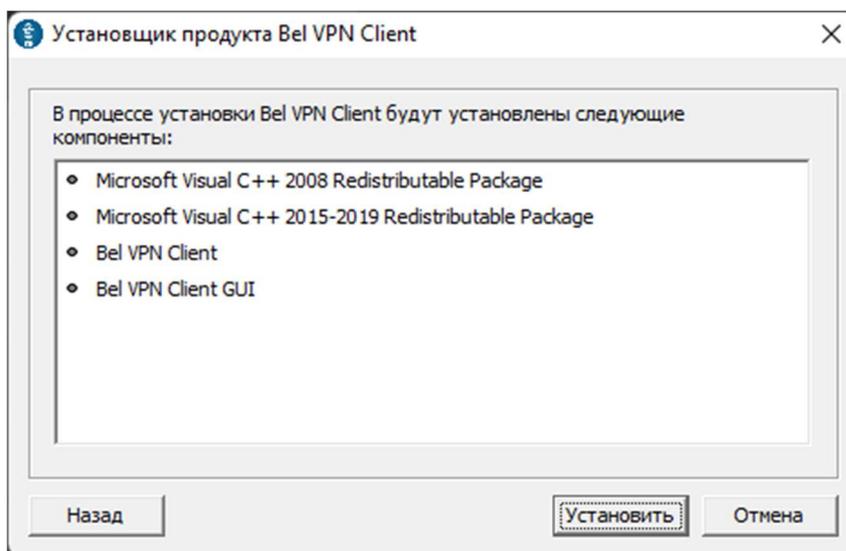


Рисунок 3

5. Нажмите «Next» (Рисунок 4);

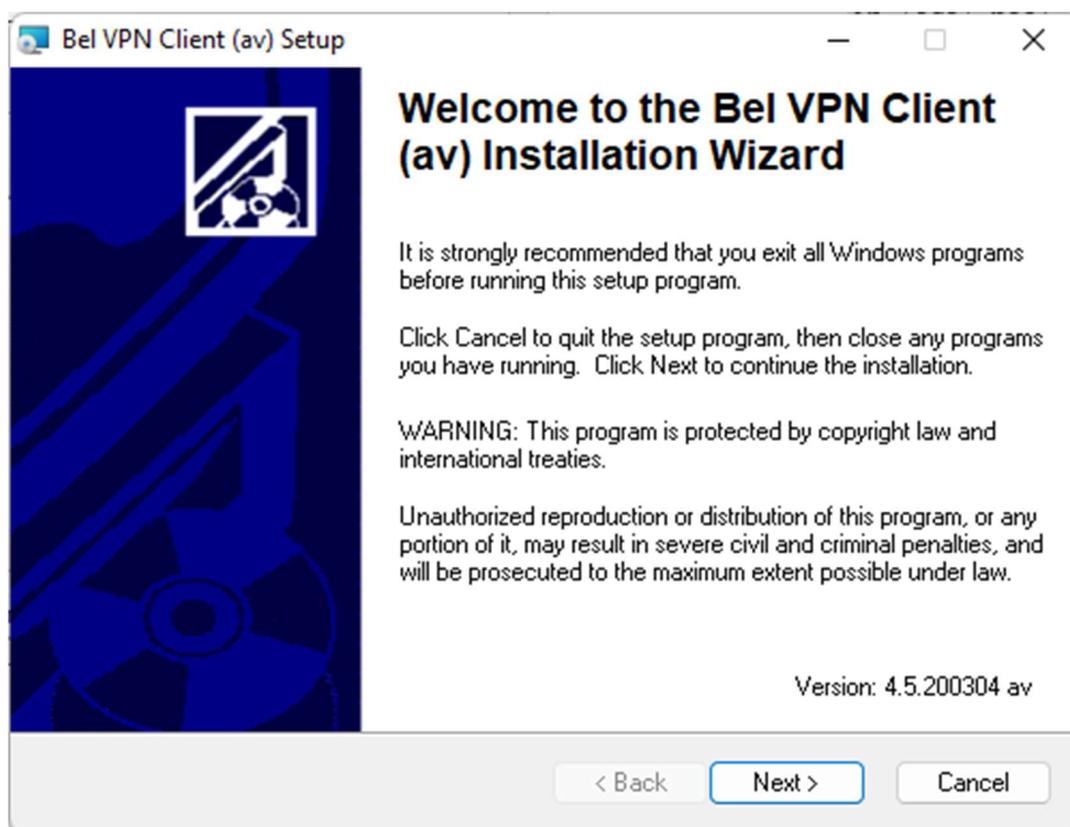


Рисунок 4

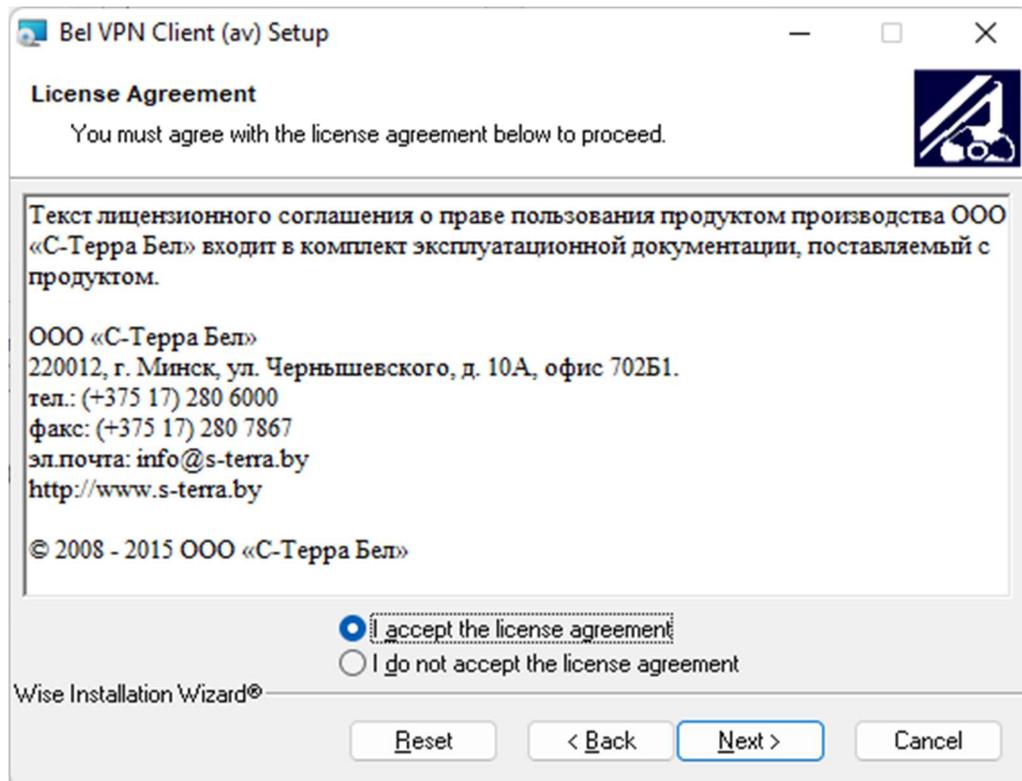


Рисунок 5

6. Подтвердите принятие лицензионного соглашения (Рисунок 5);
7. Выберите папку, в которую будет установлен клиент и нажмите «Next» (Рисунок 6);

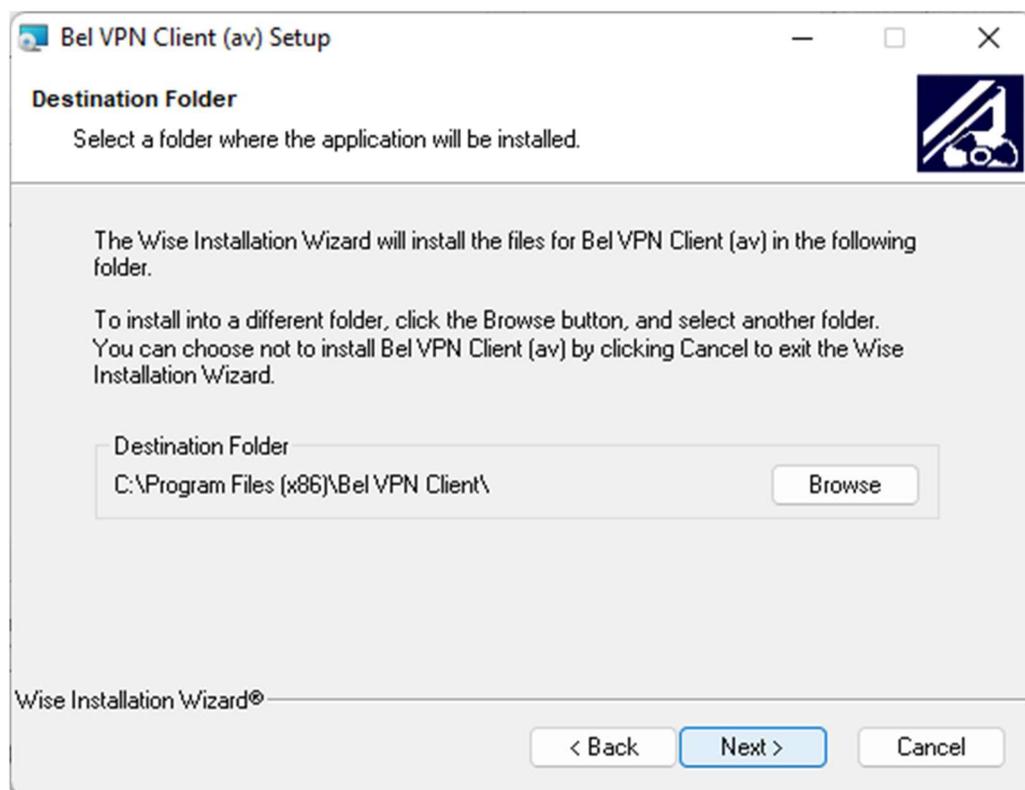


Рисунок 6

8. Выберите способ инициализации, если у вас нет AvPass или AvBign, то просто нажмите «Next» (Рисунок 7);

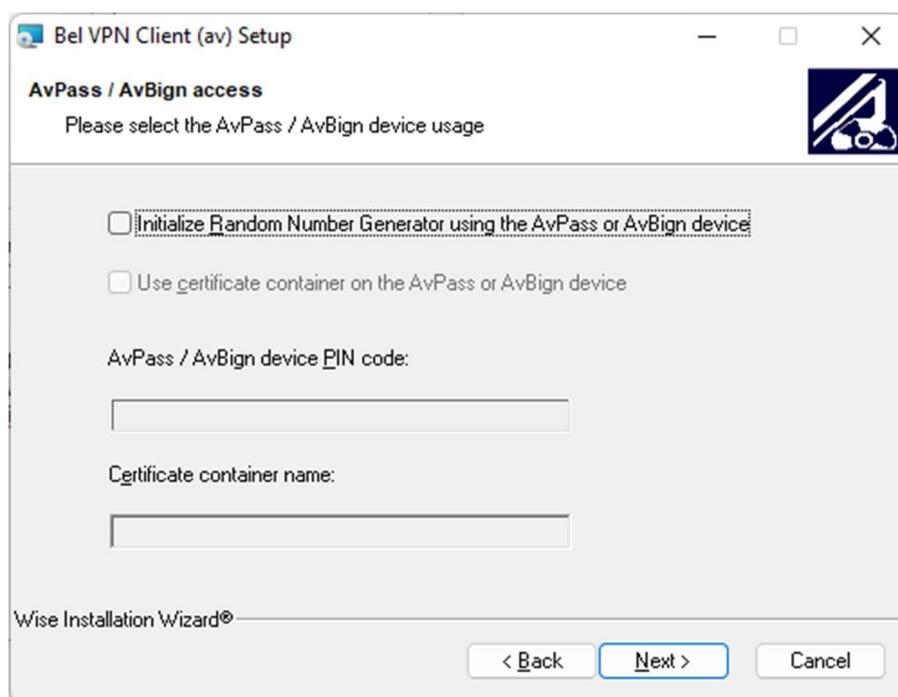


Рисунок 7

9. По умолчанию выбирается биологическая инициализация, нажмите «Next» (Рисунок 8);

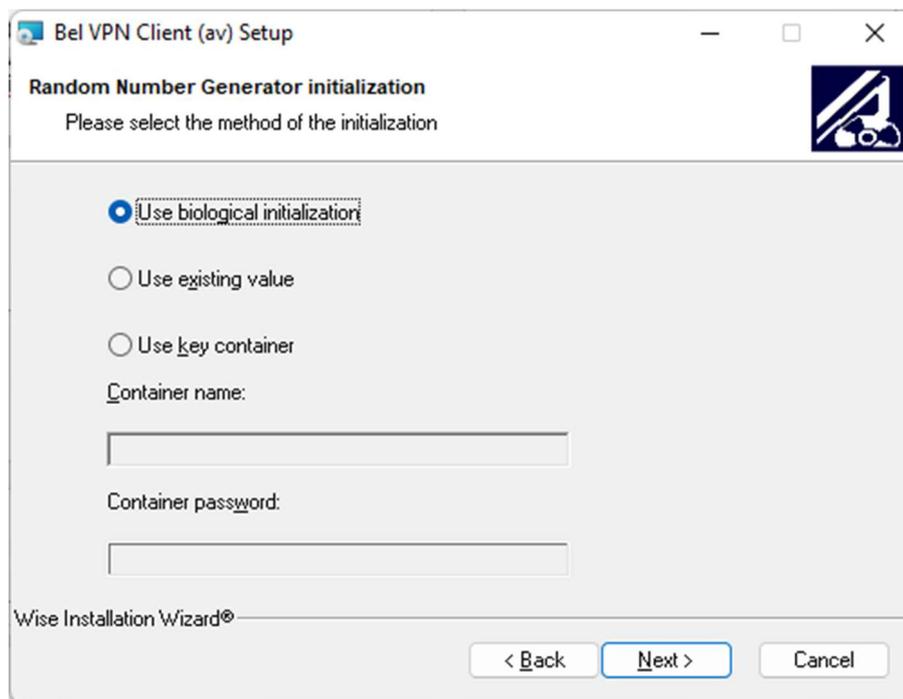


Рисунок 8

10. Нажимайте случайные клавиши, чтобы заполнить строку инициализации (Рисунок 9);

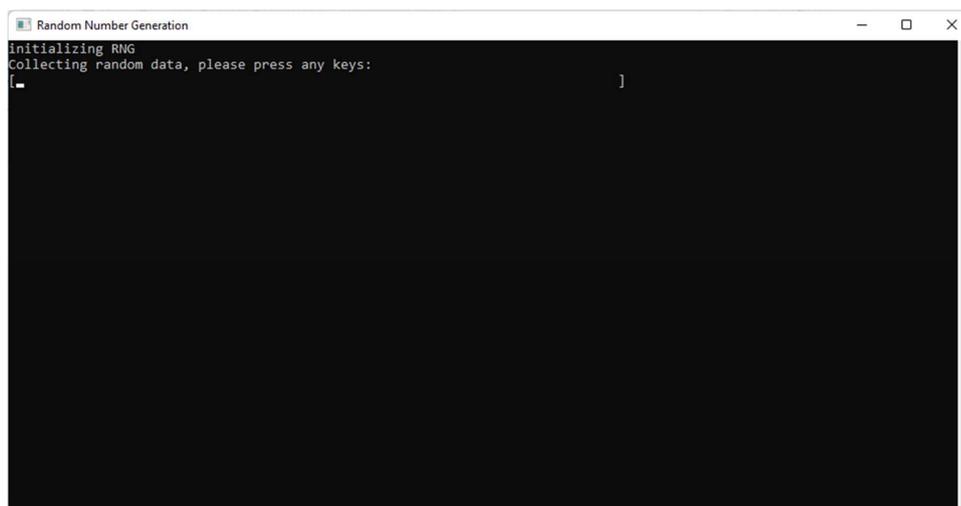


Рисунок 9

11. В следующем окне заполняете данные лицензии и нажимаете «Применить» (Рисунок 10);

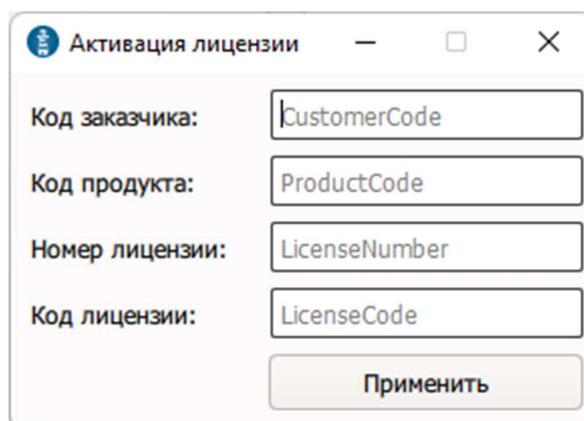


Рисунок 10

12. В окне Входа нажмите «ОК» (Рисунок 11);

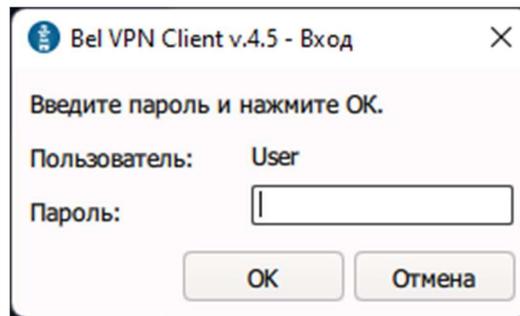


Рисунок 11

## Настройка подключения ПП Bel VPN Client 4.5

13. На вкладке «Настройка соединения» (Рисунок 12), укажите настройки подключения:

**Настройки подключения нужно получить у администратора ИС к которой Вы подключаетесь!**

**Защищённый шлюз** – шлюз, к которому будет идти защищённое подключение;

**Защищаемые подсети** – подсети, к которым вы хотите получить доступ, если их несколько, то их нужно перечислить через запятую;

**Получать IP для туннельного интерфейса от шлюза** – запрос IKECFG адреса от шлюза, выдается автоматически.

При желании Вы можете указать конкретный адрес, а не случайный ( в таком случае его нужно согласовать с администратором ИС);

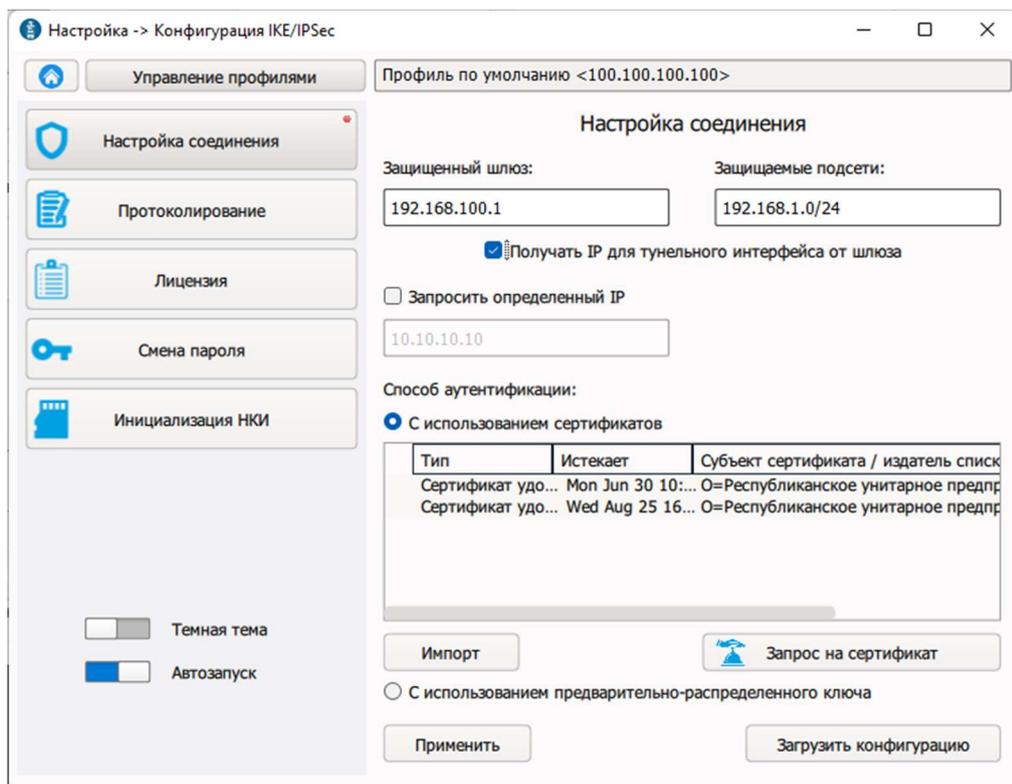


Рисунок 12

## Формирование запроса и получение сертификата

- По умолчанию в качестве способа аутентификации выбрана аутентификация на сертификатах, чтобы создать новый криптоконтейнер и запрос на сертификат необходимо на вкладке «Настройка соединения» (Рисунок 12) нажать на кнопку «Запрос на сертификат»;
- Введите значение атрибутов для нового сертификата;

Поля «С ,О ,CN» являются обязательными. **Необходимо их уточнить у администратора ИС, к которой Вы подключаетесь!**

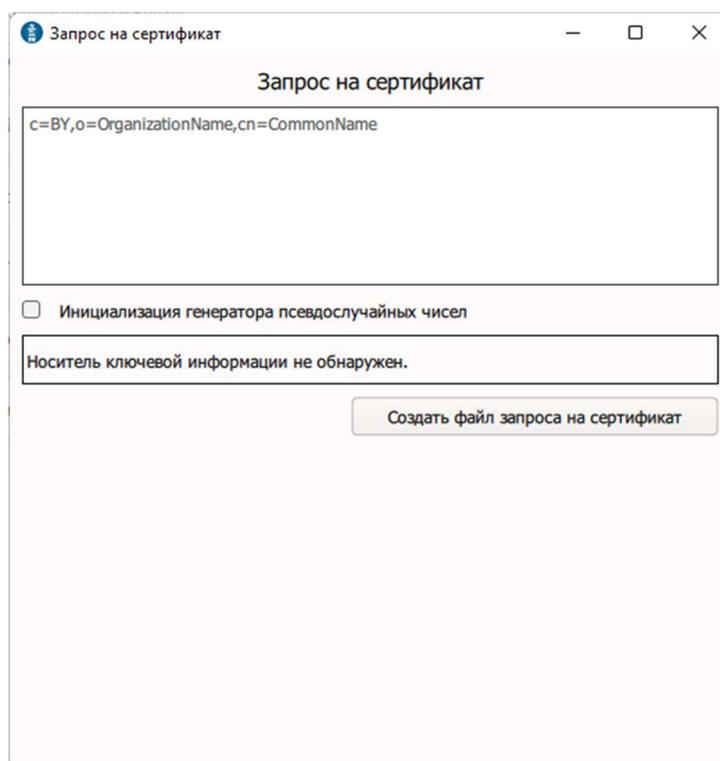


Рисунок 13

- Направьте запрос в удостоверяющий центр (УЦ);
- Импортируйте сертификат который пришел от УЦ. На вкладке «Настройка соединения» (Рисунок 12) нажмите на кнопку «Импорт»;
- Если УЦ прислал Вам сертификат в формате p7b, то необходимо проимпортировать все из них (один из них будет личный и один сертификат УЦ (Рисунок 14) (личный сертификат можно определить по атрибутам, которые Вы указывали при создании запроса на сертификат в п.15);

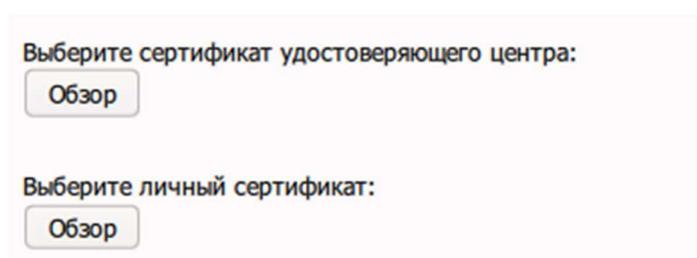
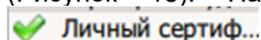


Рисунок 14

- На вкладке «Настройка соединения» (Рисунок 12) в перечне сертификатов нажмите правой кнопкой мыши на личном сертификате и выберите «использовать выбранный сертификат» (Рисунок 15). Напротив данного сертификата должна появиться зелёная галочка.



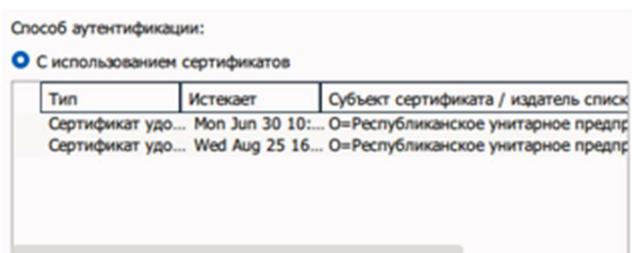


Рисунок 15

20. Установите пароль во вкладке «Смена пароля» (Рисунок 16);

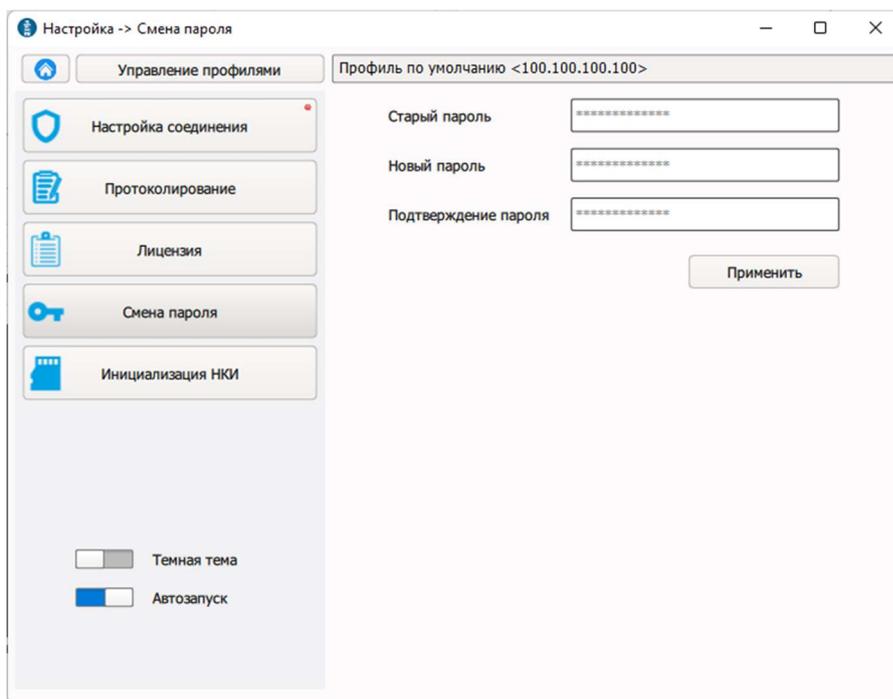


Рисунок 16

## Вариант настройки клиента Client1 утилитой администратора

Настройка клиента состоит из нескольких этапов:

- установка утилиты администратора AdminTool;
- формирование запроса и получение сертификата;
- формирование установочного пакета для целевого клиентского компьютера;
- установка пакета на целевом клиентском компьютере.

### Установка утилиты администратора AdminTool

1. Зайдите в папку с программным продуктом Bel VPN Client 4.5;
2. Запустите файл «setup.exe»;
3. Выберите в меню Установщика продукта Bel VPN Client способ «Bel VPN Client AdminTool (av) 4.5» и нажмите «Далее» (Рисунок 17) и закончите установку;

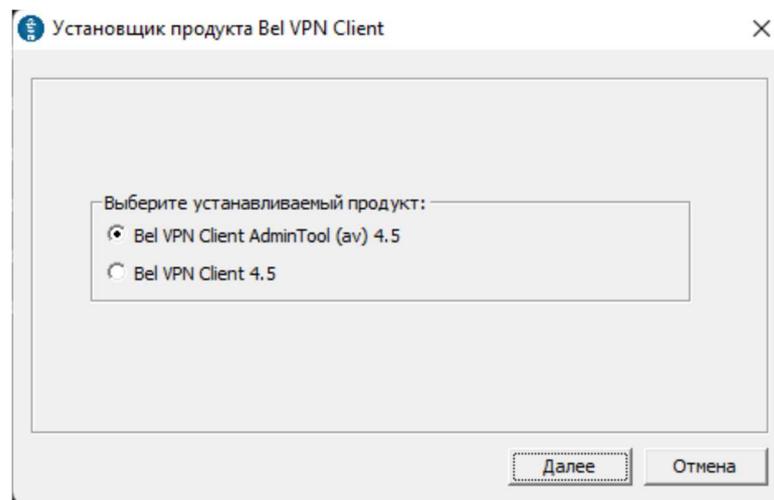


Рисунок 17

### Формирование запроса и получение сертификата AdminTool

Сформируйте запрос на сертификат:

1. Создайте директорию D:\certs:
2. Создайте контейнер на ключевом носителе:

```
C:\Program Files\Bel VPN Client AdminTool av\cryptocont.exe n -n=контейнер -p=пароль
```

**контейнер** – название создаваемого контейнера. Для создания на НКИ (носителе ключевой информации) ДОЛЖНО соответствовать следующему шаблону:

```
av:серийный_номер_НКИ:имя_контейнера
```

**пароль** – пароль (PIN) для доступа к носителю ключевой информации AvPass/AvBign.

Пример создания криптоконтейнера на НКИ:

```
C:\Program Files\Bel VPN Client AdminTool av\cryptocont.exe n  
-n=av:AVP2050050257:client -p=12345678
```

3. Сформируйте запрос на сертификат.

```
C:\Program Files\Bel VPN Client AdminTool av\cryptocont.exe r -n=контейнер -p=пароль  
-cn=CommonName -c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

**контейнер** – название контейнера, созданного на предыдущем шаге;

- пароль** – пароль (PIN) для доступа к носителю ключевой информации;
- CommonName** – идентификатор устройства;
- OrgName** – наименование организации;
- OrgUnitName** – наименование подразделения;
- путь\_к\_файлу** – путь к файлу с создаваемым запросом, рекомендуется указывать расширение **“.req”**.

Пример создания запроса:

```
C:\Program Files\Bel VPN Client AdminTool av\cryptocont.exe r
-n=av:AVP2050050257:client -p=12345678 -cn=client -c=BY -o=S-TerraBel -t=Research
-f=D:\certs\client.req
```

4. Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением **p7b** или **cer**).  
Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные сег файлы.
5. Доставьте файлы сертификатов на рабочее место администратора в предварительно созданную на нем директорию D:\certs.

**Важно:** Среда передачи в этом случае должна быть доверенной.

## Формирование установочного пакета для целевого клиентского компьютера с помощью утилиты AdminTool

Создайте установочный пакет для Client1.

1. На вкладке “Auth” выполните следующие действия (Рисунок 18):
  - в данном сценарии используется метод аутентификации на сертификатах – пункт “Use certificate” выбран по умолчанию;
  - укажите путь к сертификату УЦ и пользовательскому сертификату;
  - отметьте пункт “Check consistency now” и нажмите кнопку “...”;
  - В появившемся окне выберите нужный контейнер (Рисунок 19), а затем введите пароль к созданному контейнеру в графу “password”;
  - Скопируйте имя контейнера из графы “Container name” в графу “User container name”; а затем введите пароль к созданному контейнеру в графу “password”;
  - в графе “User identity type” выберите “DistinguishedName” (выбрано по умолчанию).

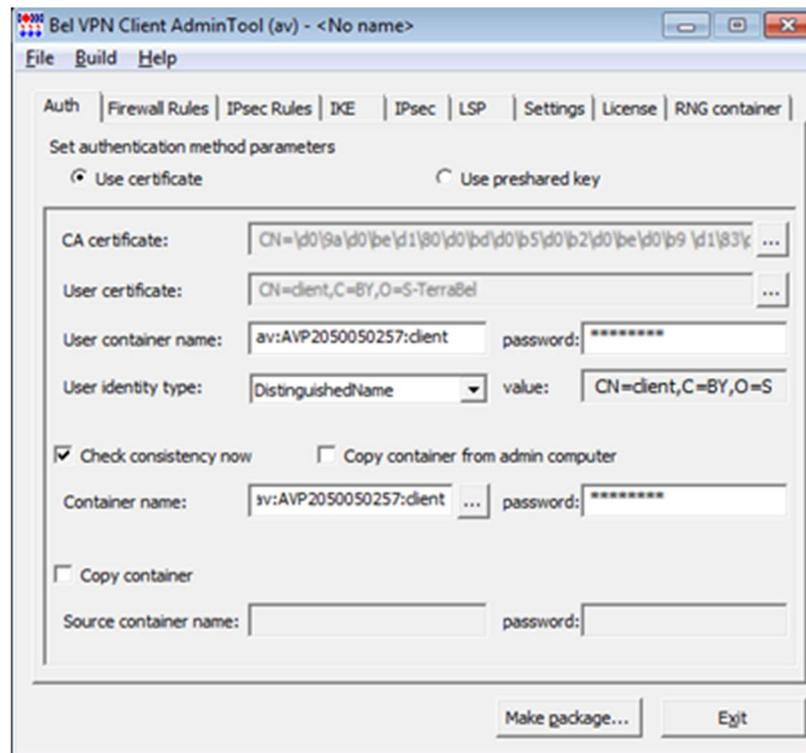


Рисунок 18

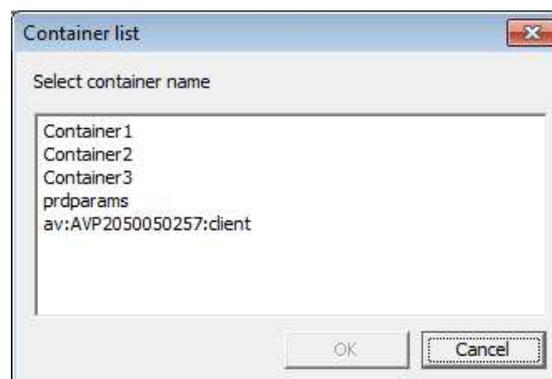


Рисунок 19

2. На вкладке “Firewall Rules” (Рисунок 20) можно настроить правила фильтрации трафика. В данном сценарии оставим настройки по умолчанию – разрешать весь трафик.

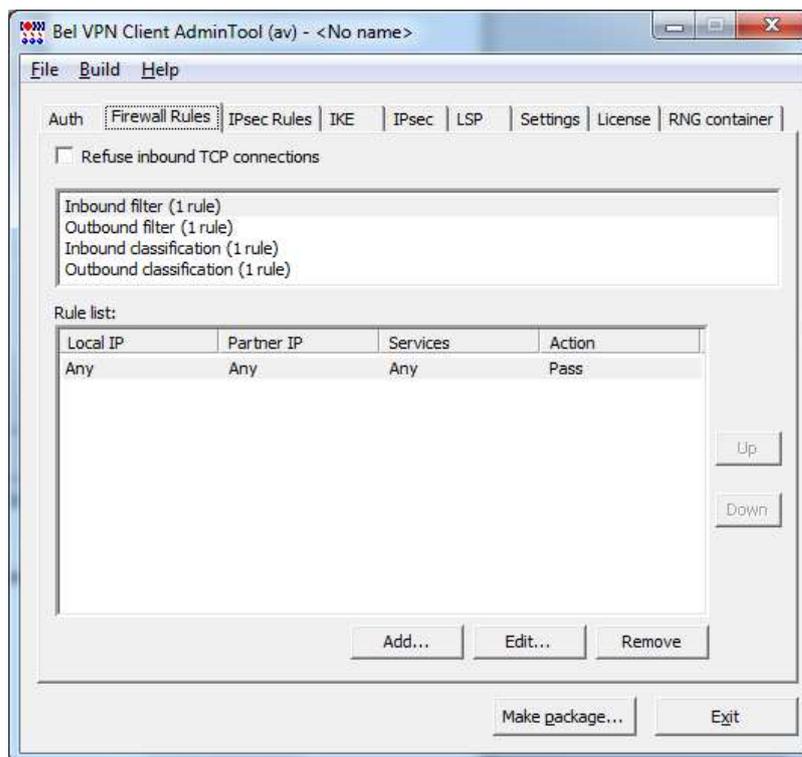


Рисунок 20

3. На вкладке "IPsec Rules" (Рисунок 21) добавьте правило для трафика, подлежащего шифрованию, IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 22). Так же отметьте пункт "Request IKECFG address". Добавленное правило поднимите вверх.

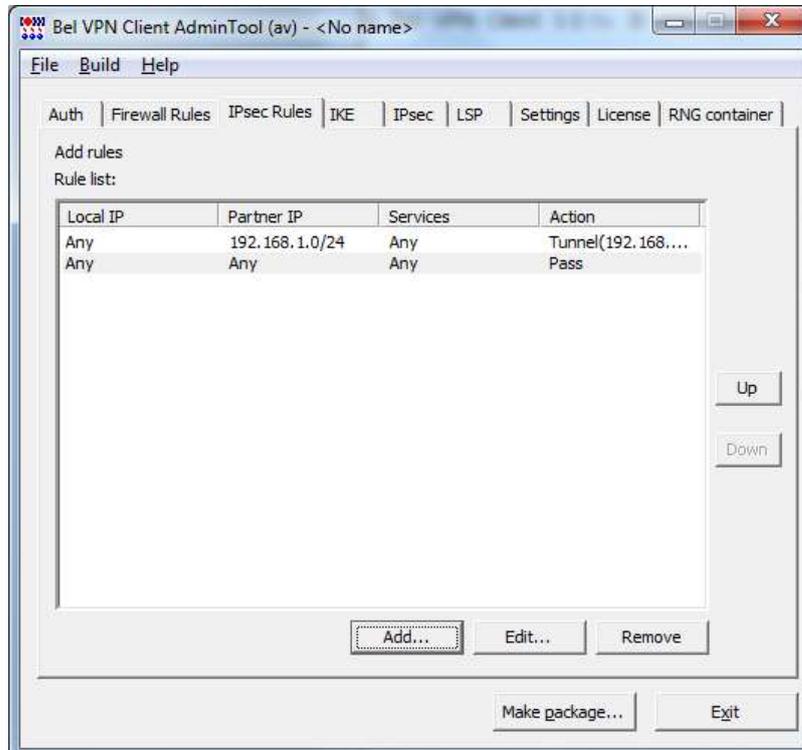


Рисунок 21

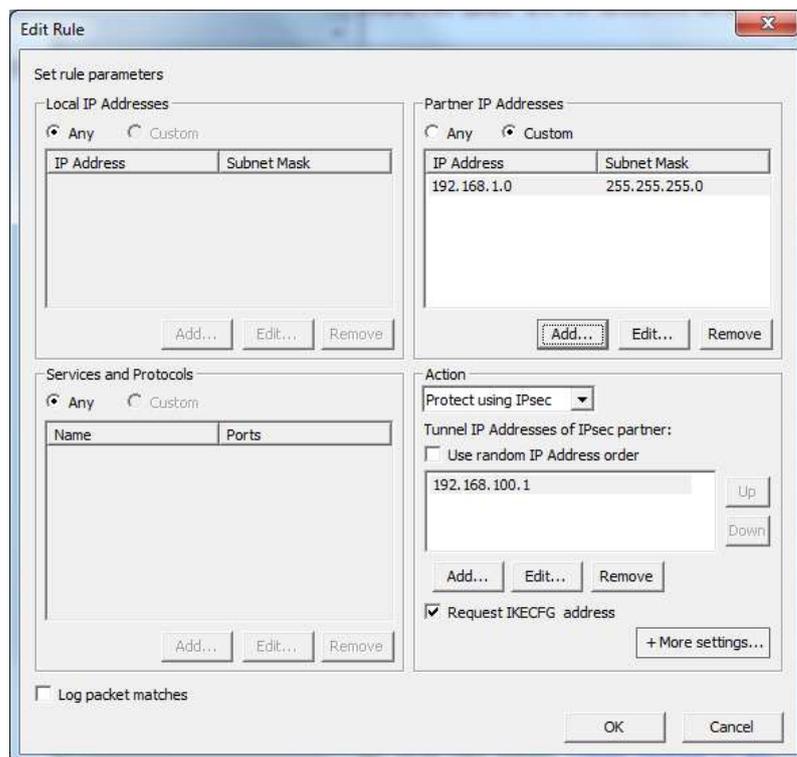


Рисунок 22

4. На вкладке “IPsec” поднимите вверх правило, соответствующее настроенному на шлюзе IPsec Transform Set и выберите “Group” – “BELTDH” (Рисунок 23).

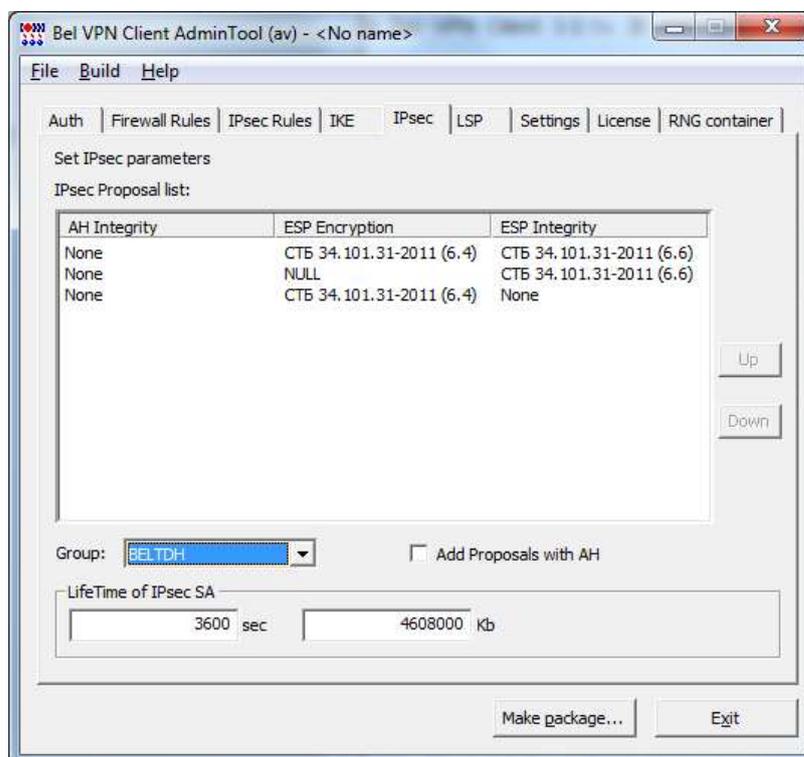


Рисунок 23

5. На вкладке “License” введите лицензию на продукт «Bel VPN Client-P 4.1».
6. Сохраните файл созданного проекта, на тот случай, если захотите в будущем сделать похожий клиентский пакет. Для этого выберите в меню “File” пункт “Save project”.

7. Сгенерируйте клиентский exe-файл, нажав кнопку “Make package...”.
8. Установите на клиентском компьютере полученный exe-файл и перезагрузите компьютер (при использовании НКИ (AvPass, AvBign) , вставьте в клиентский компьютер данный носитель);
9. В системном трее появится иконка «Bel VPN Client 4.5» (Рисунок 24). При нажатии на которую откроется рабочее окно (Рисунок 25). По умолчанию пароль отсутствует, его можно установить, нажав на «шестерёнку» на рабочем окне и выбрать пункт «Смена пароля» (Рисунок 26).



Рисунок 24



Рисунок 25

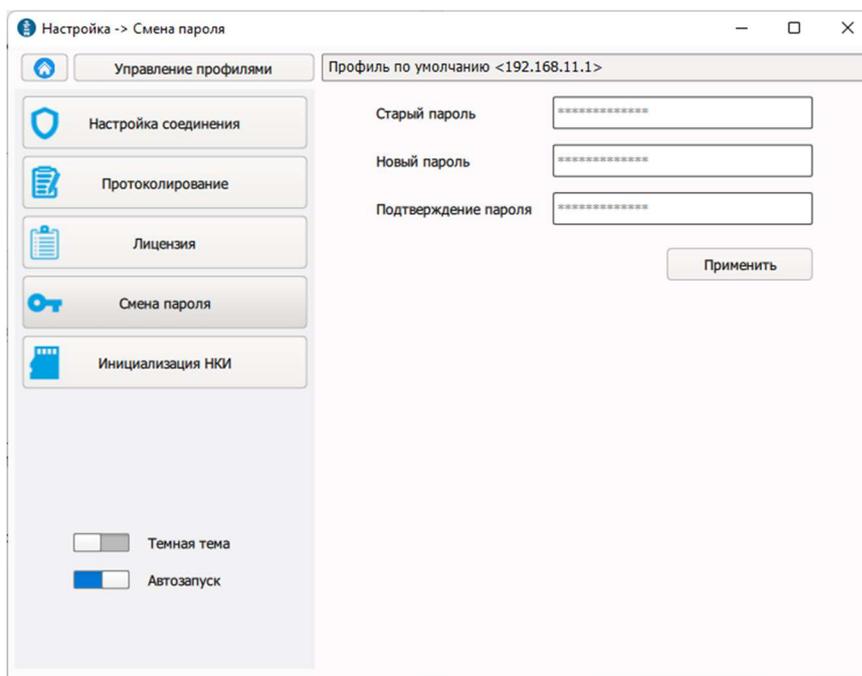


Рисунок 26

## Настройка устройства IPHost1

На устройстве IPHost1 задайте IP-адрес, а в качестве шлюза по умолчанию укажите IP-адрес внутреннего интерфейса шлюза безопасности GW1 – 192.168.1.1.

## Настройка устройства Router1

На устройстве Router1 необходимо настроить IP-адреса.

## Проверка работоспособности стенда

После того, как настройка всех устройств завершена, иницируйте создание защищенного соединения.

На устройстве Client1 выполните команду ping:

```
ping 192.168.1.100
```

```
Обмен пакетами с 192.168.1.100 по с 32 байтами данных:
Ответ от 192.168.1.100: число байт=32 время=1666мс TTL=62
Ответ от 192.168.1.100: число байт=32 время=2мс TTL=62
Ответ от 192.168.1.100: число байт=32 время=3мс TTL=62
Ответ от 192.168.1.100: число байт=32 время=8мс TTL=62

Статистика Ping для 192.168.1.100:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 2мсек, Максимальное = 1666 мсек, Среднее = 419 мсек
```

В результате выполнения этой команды между устройствами Client1 и GW1 будет установлен VPN туннель.

Убедиться в этом можно на устройстве Client1, нажав правой кнопке на трей и выбрать пункт «Сетевая активность»:

Так же в этом можно убедиться на устройстве GW1, выполнив команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (192.168.100.1,500)-(10.10.10.100,500) active 1968 3484

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (192.168.1.0-192.168.1.255,*)-(192.168.11.1,*) * ESP tunn 192 192
```

## Приложение

### Текст cisco-like конфигурации для шлюза GW1

```
!  
version 12.4  
no service password-encryption  
!  
crypto ipsec df-bit copy  
crypto isakmp identity dn  
username ccons privilege 15 password 0 csp  
aaa new-model  
!  
!  
hostname GW1  
enable password csp  
!  
!  
logging trap debugging  
!  
!  
crypto isakmp policy 1  
  encr belt  
  hash belt  
  authentication belt-sig  
  group beltdh  
!  
ip local pool POOL 192.168.11.1 192.168.11.254  
!  
crypto ipsec transform-set TSET esp-belt esp-belt-mac  
!  
ip access-list extended LIST  
  permit ip 192.168.1.0 0.0.0.255 192.168.11.0 0.0.0.255  
!  
!  
crypto dynamic-map DMAP 1  
  match address LIST  
  set transform-set TSET  
  set pfs beltdh  
  set pool POOL  
  reverse-route  
!  
crypto map CMAP 1 ipsec-isakmp dynamic DMAP  
!  
interface GigabitEthernet0/0  
  ip address 192.168.1.1 255.255.255.0  
!  
interface GigabitEthernet0/1  
  ip address 192.168.100.1 255.255.255.0  
  crypto map CMAP  
!  
interface GigabitEthernet0/2  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/3  
  no ip address  
  shutdown  
!
```

```
!  
ip route 0.0.0.0 0.0.0.0 192.168.100.2  
!  
crypto pki trustpoint s-terra_technological_trustpoint  
  revocation-check none  
crypto pki certificate chain s-terra_technological_trustpoint  
certificate 4E4B0B11EFDB389E4E86244CDAA1B275  
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530  
...  
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713  
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F  
quit  
!  
end
```