Построение VPN туннеля между шлюзом безопасности «Bel VPN Gate» и мобильным клиентом «Bel VPN Client», находящимся за динамическим NAT-ом, с выдачей адреса из пула

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и мобильным клиентом «Bel VPN Client» (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 – клиент находится за динамическим NAT-ом. 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 34.101.31-2011 (раздел 6.4);
  - Алгоритм вычисления хеш-функции – СТБ 34.101.31-2011 (раздел 6.9);
  - Протокол согласования ключей – протокол Диффи-Хеллмана на эллиптических кривых (СТБ 34.101.66.2-2014).
- IPsec параметры:
  - Туннельный режим, протокол ESP:
    - Алгоритм шифрования – СТБ 34.101.31-2011 (раздел 6.4);
    - Алгоритм контроля целостности – СТБ 34.101.31-2011 (раздел 6.6).

Схема стенда (Рисунок 1):

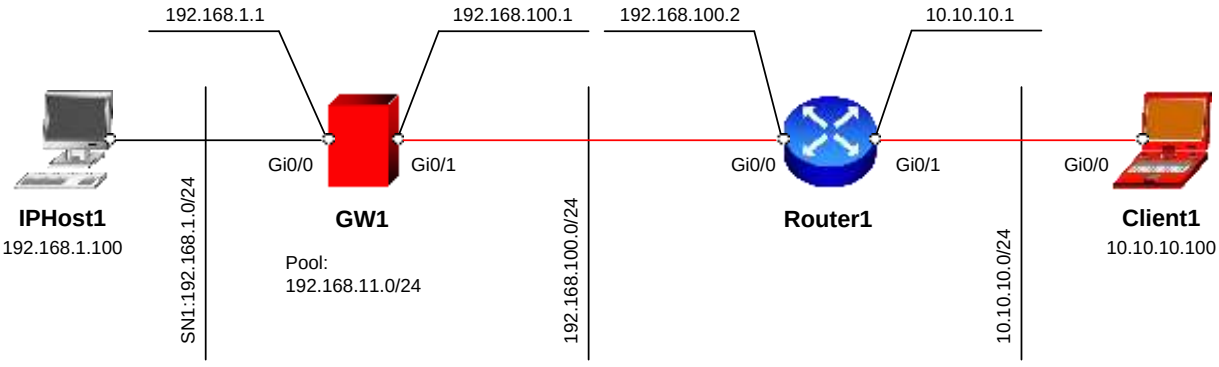

Рисунок 1

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 4.1» – Initialization_gate_Gate_41 («Инициализация», раздел «Инициализация шлюза безопасности Bel VPN Gate 4.1 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 4.1» – Console_command_reference_Gate_41 («Руководство администратора. 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@sterragate:~# cs_console
sterragate>en
Password:
```

   Пароль по умолчанию: csp.
2. Перейдите в режим настройки:

```
sterragate#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

3. В настройках интерфейсов задайте IP-адреса:

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

4. Задайте адрес шлюза по умолчанию:

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

5. Выйдите из cisco-like интерфейса:

```
sterragate(config)#end
sterragate#exit
```

Формирование запроса и регистрация сертификата

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

1. Установите правильное системное время.

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

   MM – месяц;

DD – день;

HH – часы;

mm – минуты;

YYYY – год

Пример установки даты:

```
root@sterragate:~# date 042013152016
Wed Apr 20 13:15:00 UTC 2016
```

Данная запись соответствует 20 апреля 2016 года 13:15.

2. Создайте папку /opt/certs:

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

3. Создайте контейнер на ключевом носителе:

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

4. Сформируйте запрос на сертификат:

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

5. 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 cer файлы.
6. 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 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 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.

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

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

путь_к_файлу – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@sterragate:~# 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@sterragate:~# 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;

пароль – пароль для доступа к ключевому носителю информации.

Пример импорта:

```
root@sterragate:~#cert_mgr import -f /opt/cert/GW1.cer -kc av: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@sterragate:~# cert_mgr show
```

Пример вывода:

```
root@sterragate:~# 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
```

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

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

Пример:

```
root@sterragate:~# 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
```

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@sterragate:~# cs_console
sterragate>en
Password:
```

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

1. Перейдите в режим настройки:


```
sterragate#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Смените пароль по умолчанию:

```
sterragate(config)#username cscons password <пароль>
```

3. Смените название шлюза:

```
sterragate(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
```

В **Приложении** представлен текст cisco-like конфигурации для шлюза GW1.

Настройка мобильного клиента Client1

Настройка мобильного клиента состоит из нескольких этапов:

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

Создавать установочный пакет можно как на целевом клиентском компьютере, так и на компьютере администратора.

Формирование запроса и получение сертификата

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 содержать в начале названия префикс ***“av:”***;

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: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:client -p=12345678 -cn=client -c=BY -o=S-TerraBel -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 cer 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

Создайте установочный пакет для Client1.

1. На вкладке “Auth” выполните следующие действия (Рисунок 2):

- 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 3), 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).

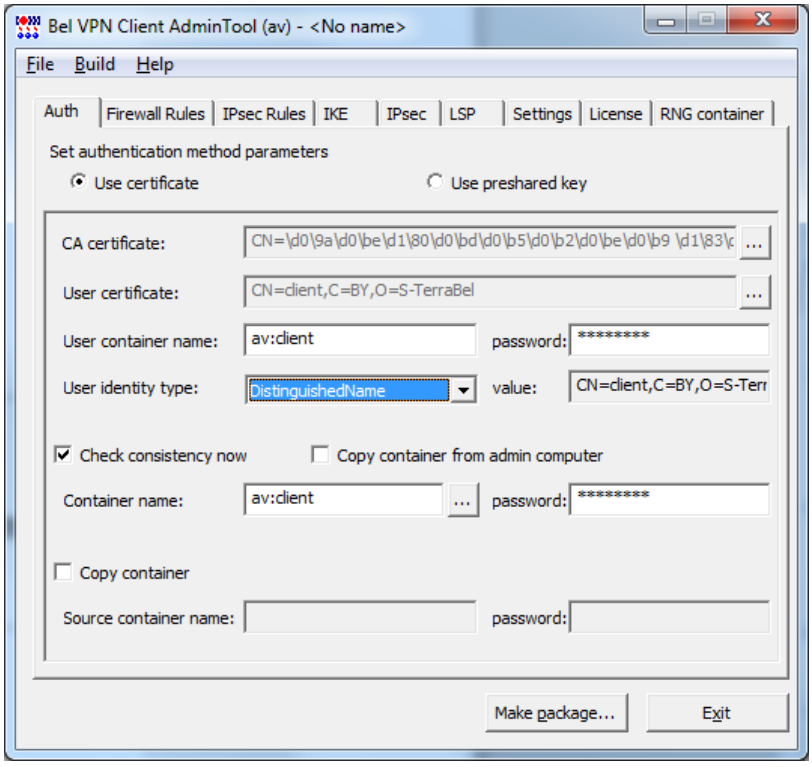

Рисунок 2

Рисунок 3

2. На вкладке “Firewall Rules” (Рисунок 4) можно настроить правила фильтрации трафика. В данном сценарии оставим настройки по умолчанию – разрешать весь трафик.

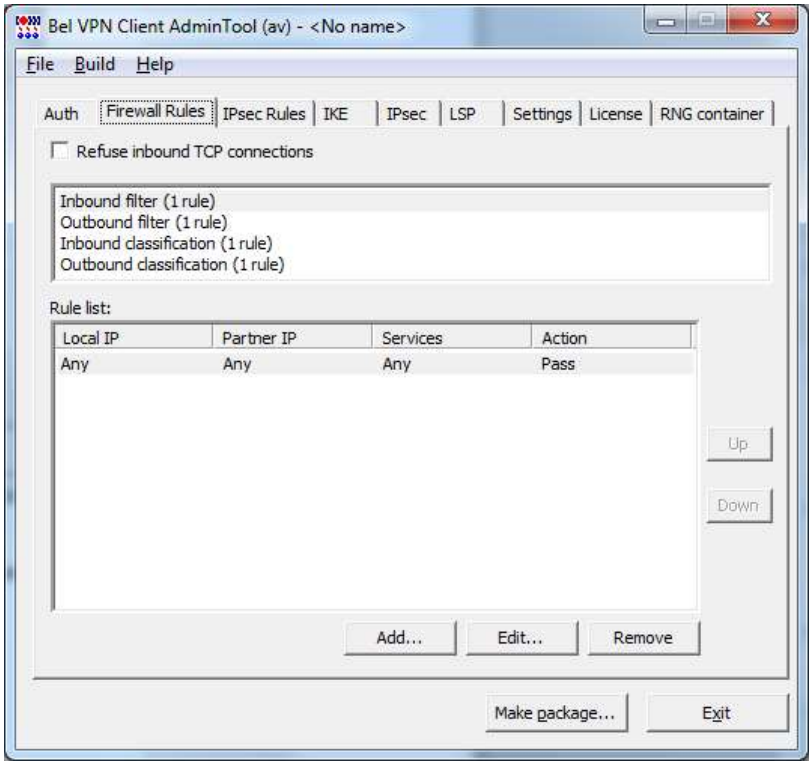

Рисунок 4

3. На вкладке “IPsec Rules” (Рисунок 5) добавьте правило для трафика, подлежащего шифрованию, IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 6). Так же отметьте пункт “Request IKECFG address”. Добавленное правило поднимите вверх.

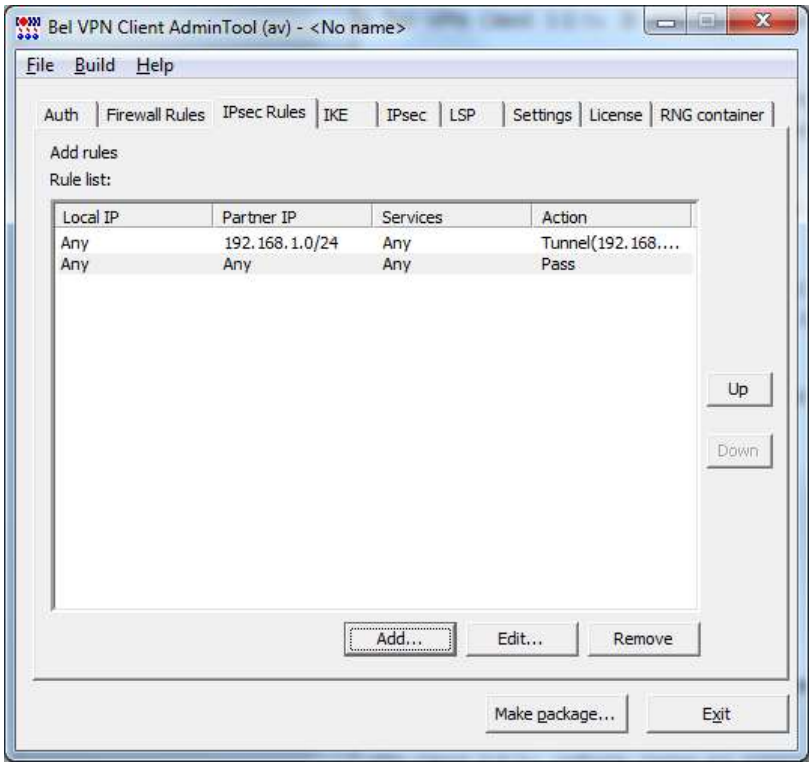

Рисунок 5

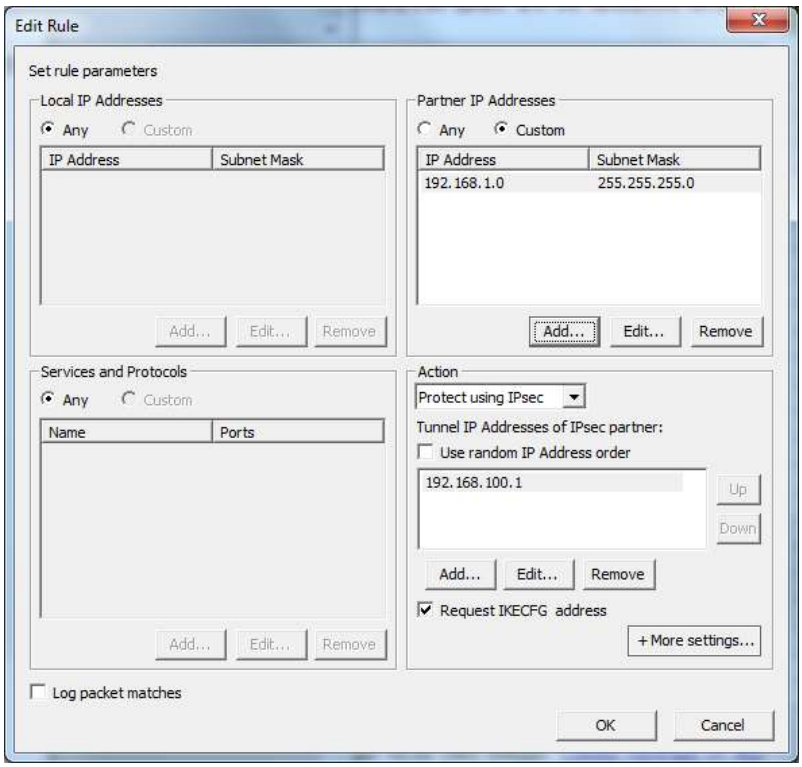

Рисунок 6

4. На вкладке “IPsec” поднимите вверх правило, соответственно настроенному на шлюзе IPsec Transform Set и выберете “Group” – “BELTDH” (Рисунок 7).

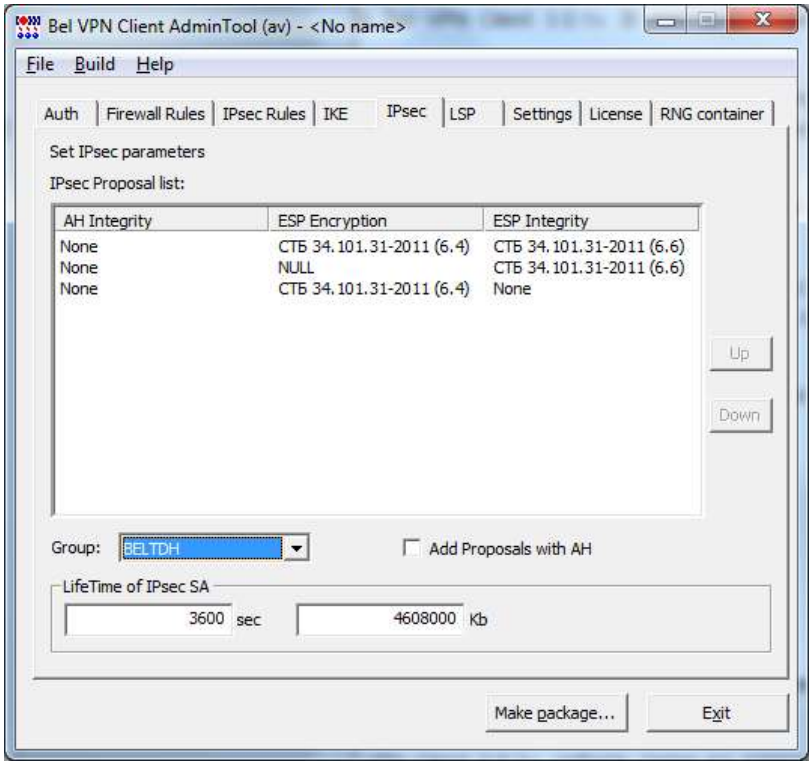

Рисунок 7

5. На вкладке “License” введите лицензию на продукт «Bel VPN Client 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. Вставьте в клиентский компьютер носитель с секретными ключами. Установите на клиентском компьютере полученный exe-файл и перегрузите компьютер (на операционных системах Windows 7 и Windows 8 перезагрузка не требуется).
9. В трее появится иконка «Bel VPN Client» (Рисунок 8). Для начала работы необходимо залогинится (Рисунок 9). По умолчанию пароль отсутствует, в дальнейшем его можно установить.

Рисунок 8

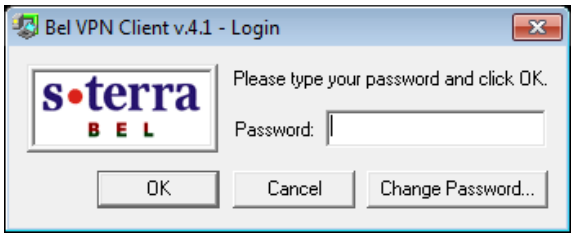

Рисунок 9

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 динамический NAT, который будет преобразовывать адреса из подсети 10.10.10.0/24 во внешний адрес 192.168.100.2 и наоборот.

Проверка работоспособности стенда

После того, как настройка всех устройств завершена, инициируйте 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 в программе VPN SA Monitor:

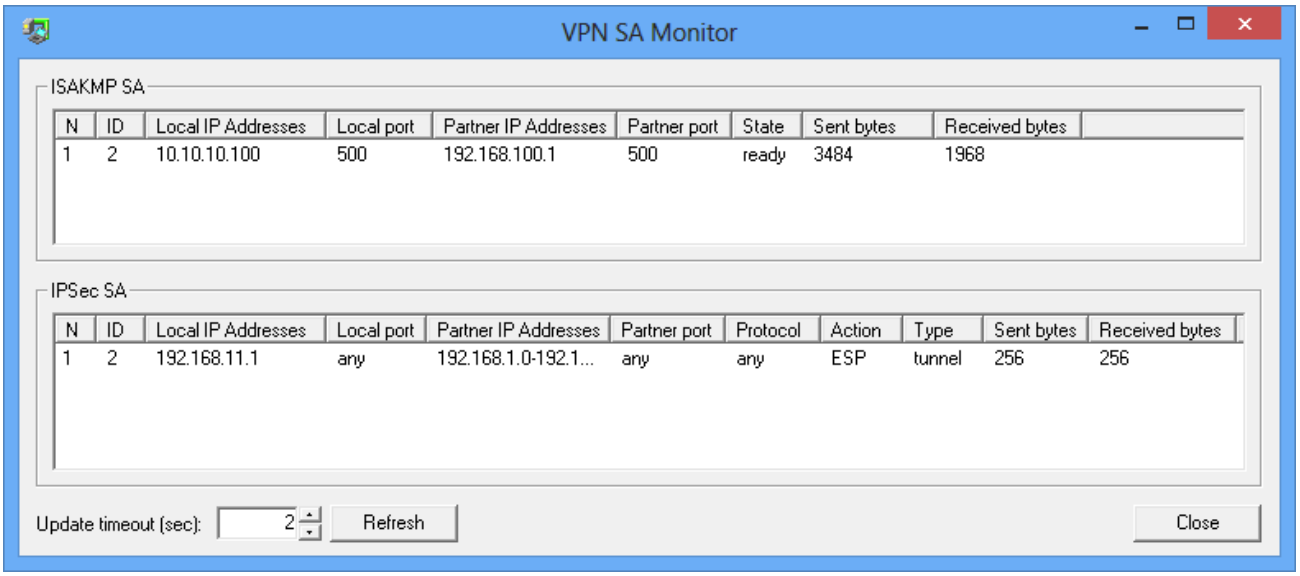

Рисунок 10

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 cscons 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
```