Построение VPN туннеля между шлюзом безопасности «Bel VPN Gate» и мобильным клиентом «Bel VPN Client-P» с выдачей адреса из пула и аутентификацией на pre-shared key

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и мобильным клиентом «Bel VPN Client-P» (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 общий ключ.

Параметры защищенного соединения:

- IKE параметры:
  - Аутентификация – общий ключ;
  - 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):

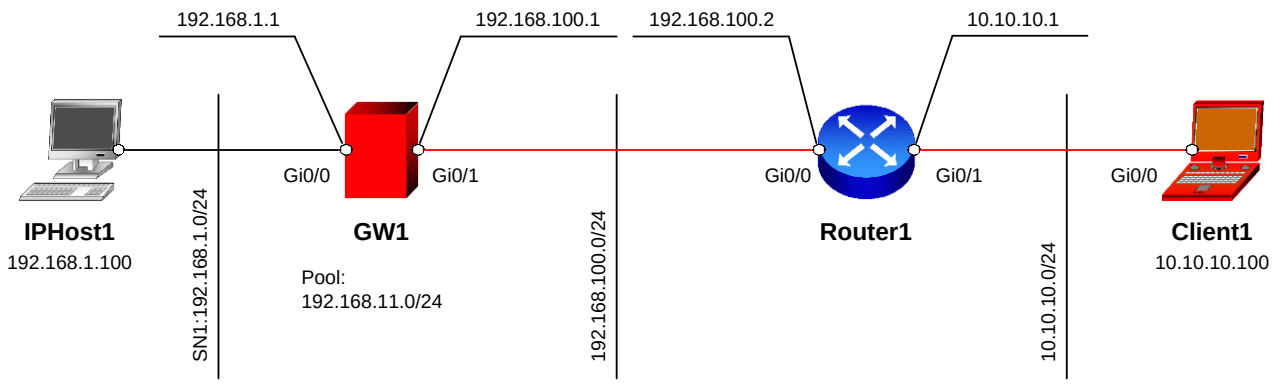

Рисунок 1

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 4.5» – bel_vpn_gate_45_userguides («Руководство пользователя. Настройка», раздел «Инициализация ПАК Bel VPN Gate при первом старте»).

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
```

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 cscons password <пароль>
```

3. Смените название шлюза:

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

4. Задайте тип идентификации:

```
GW1(config)#crypto isakmp identity address
GW1(config)#crypto isakmp key qw34rt67 address 0.0.0.0 0.0.0.0
```

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 pre-share
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. 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 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.

Установка продукта Bel VPN Client AdminTool описывается в документации на ПА «Bel VPN Client-P 4.1» – Bel_VPN_Client-P_41_Admin_Guide («Руководство администратора. Общее руководство», раздел «Подготовка рабочего места администратора безопасности»).

Формирование установочного пакета для целевого клиентского компьютера

Запустите Package Maker (Bel VPN Client AdminTool) и создайте установочный пакет для Client1.

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

- в данном сценарии используется метод аутентификации на предопределенных ключах – выберете пункт “Use preshared key”;
- задайте наименование ключа в поле “Key name”: *key*;
- задайте значение предопределенного ключа в поле “Key body”, пункт “From keyboard” выбран по умолчанию.
- измените “User identity type” на “IPV4Addr” и установите значение поля “value”: *10.0.0.1.*

Важно: IP-адрес 10.0.0.1 используется исключительно для идентификации клиента и должен быть уникальным среди всех клиентов, подключенных к шлюзу, при использовании для идентификации локального IP-адреса возможны совпадения, что приведет к невозможности одновременной работы клиентов. В случае использования для идентификации “Key ID” необходимо в конфигурации шлюза задавать pre-share key для каждого клиента отдельно.

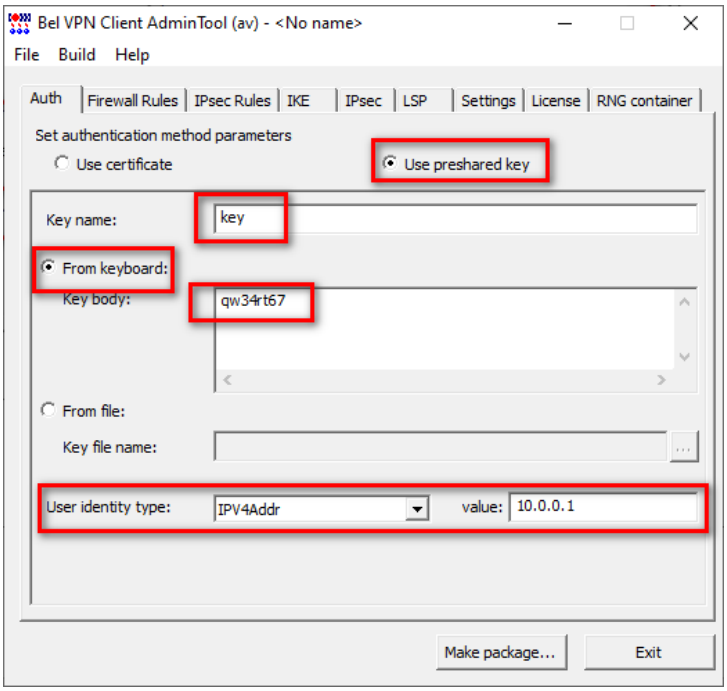

Рисунок 2

2. На вкладке “Firewall Rules” (Рисунок 3) можно настроить правила фильтрации трафика. В данном сценарии оставим настройки по умолчанию – разрешать весь трафик.

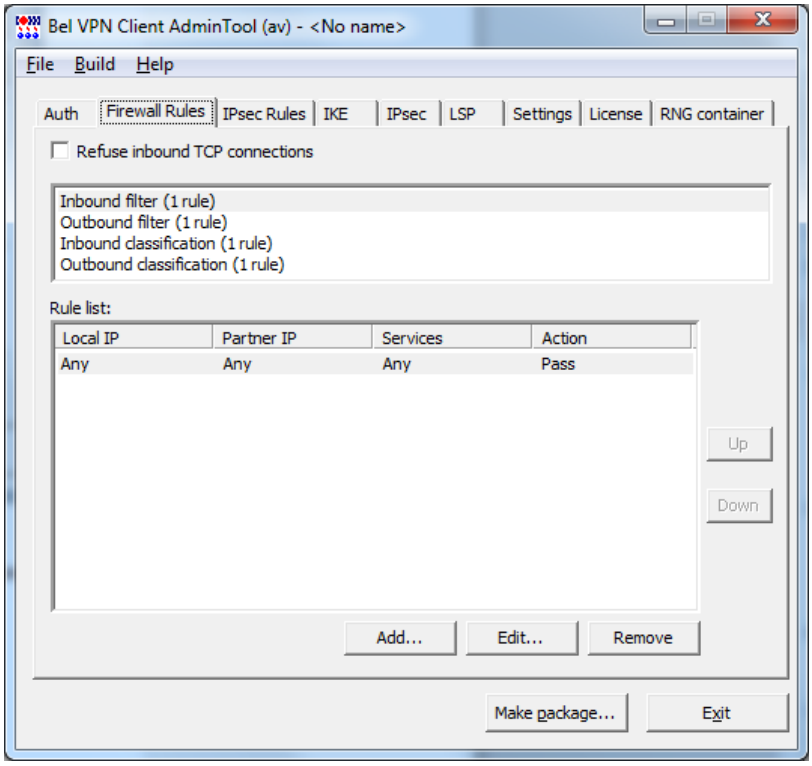

Рисунок 3

3. На вкладке “IPsec Rules” (Рисунок 4) добавьте правило для трафика, подлежащего шифрованию, IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 5). Так же отметьте пункт “Request IKECFG address”. Добавленное правило поднимите вверх.

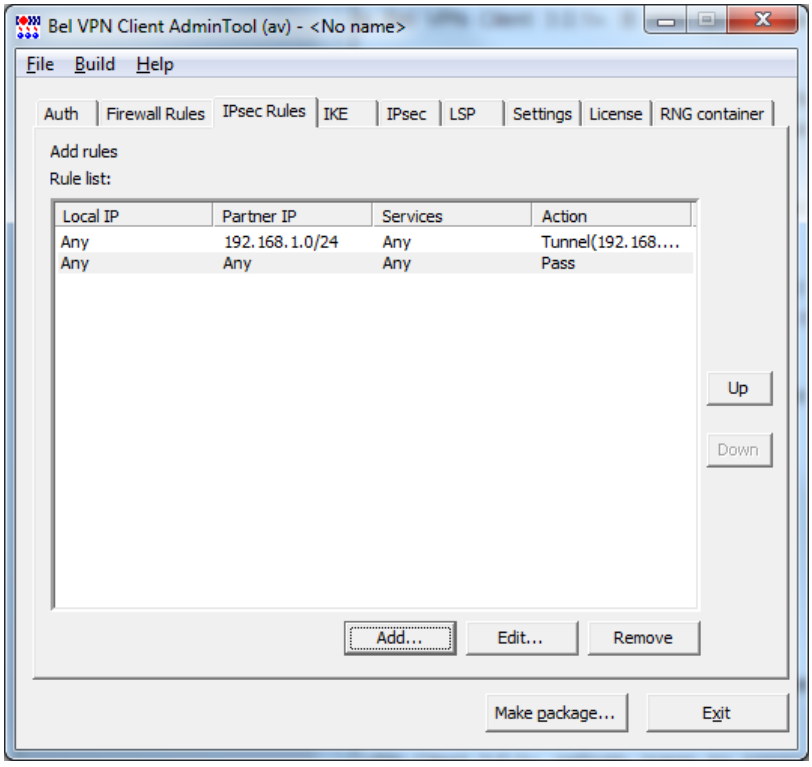

Рисунок 4

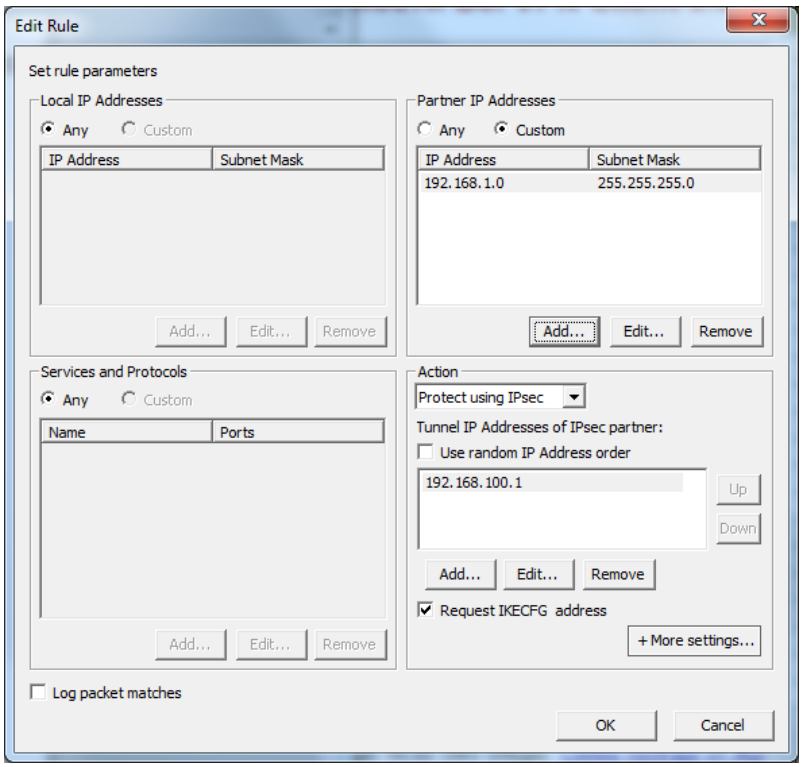

Рисунок 5

4. На вкладке “IPsec” поднимите вверх правило, соответственно настроенному на шлюзе IPsec Transform Set и выберете “Group” – “BELTDH” (Рисунок 6).

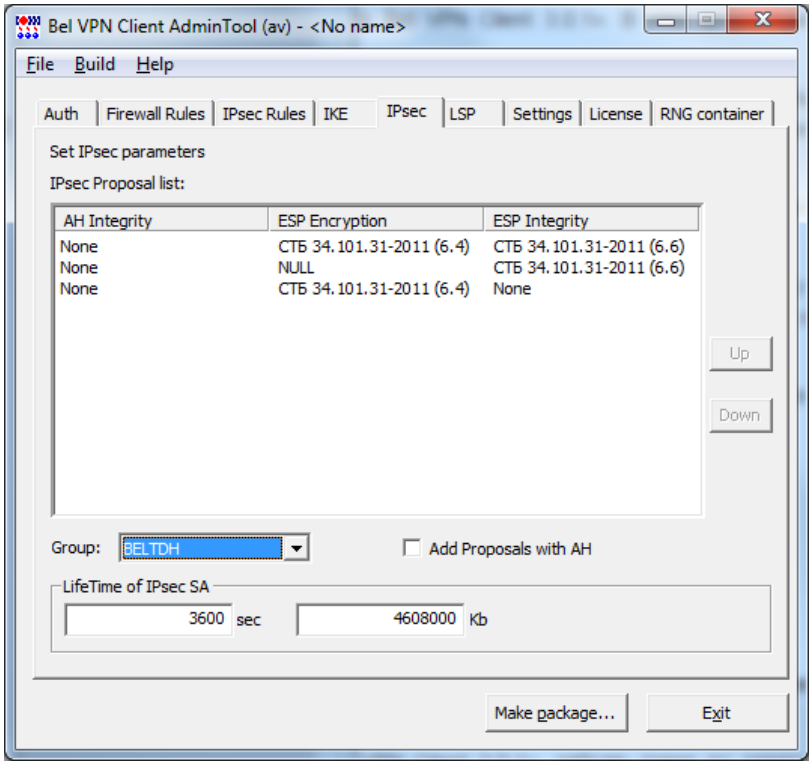

Рисунок 6

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. 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-P» (Рисунок 7). Для начала работы необходимо залогинится (Рисунок 8). По умолчанию пароль отсутствует, в дальнейшем его можно установить.

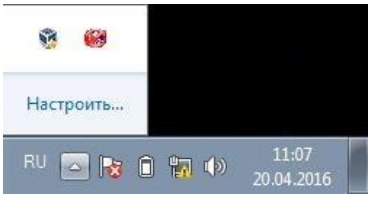

Рисунок 7

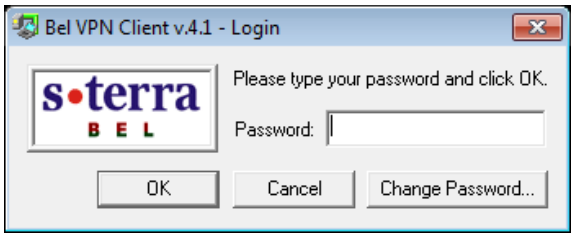

Рисунок 8

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, 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:

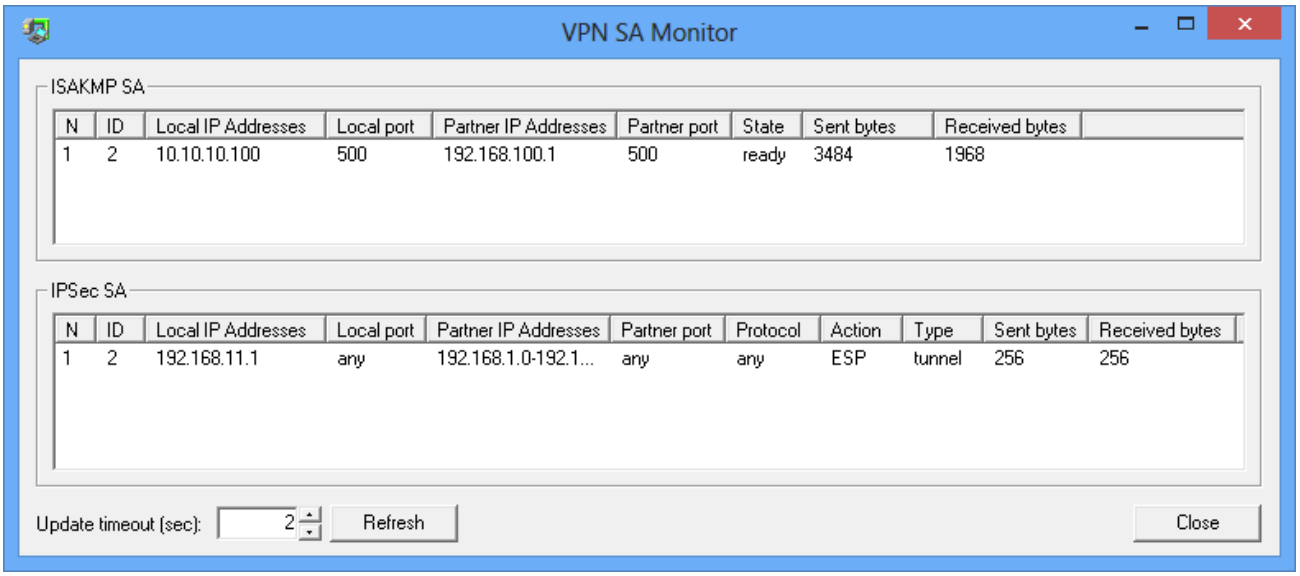

Рисунок 9

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 address
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 pre-share
 group beltdh
!
crypto isakmp key qw34rt67 address 0.0.0.0 0.0.0.0
!
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
!
end
```