Построение VPN туннеля между шлюзом безопасности «Bel VPN Gate» и мобильным клиентом «Bel VPN Client-M» на базе Android

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и мобильным клиентом «Bel VPN Client-M» (на базе Android). Для защиты будет построен VPN туннель между устройствами GW1 и Client-M. Адрес мобильного клиента неизвестен заранее – клиент находится за динамическим NAT-ом.

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):

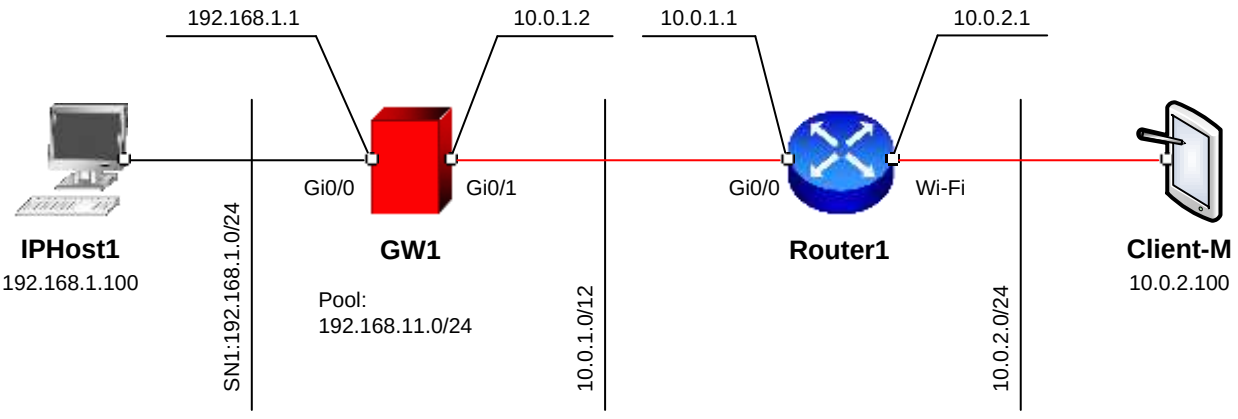

Рисунок 1

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 10.0.1.2 255.255.255.0
sterragate(config-if)#no shutdown
sterragate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию (интерфейс Gi0/0 устройства Router1):

```
sterragate(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.1
```

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/Avest/bin/cryptocont 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” для файлов с запросом на сертификат.

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= RootCA
```

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= RootCA
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=RootCA
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 pool POOL
GW1(config-crypto-map)#set pfs beltdh
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 Client-M

Начальная настройка

1. Загрузите установочный пакет «Bel VPN Client-M» на мобильное устройство.
2. Выберите иконку установочного файла и нажмите кнопку “Установить” (Рисунок 2). Дождитесь окончания установки и нажмите кнопку “Готово”.

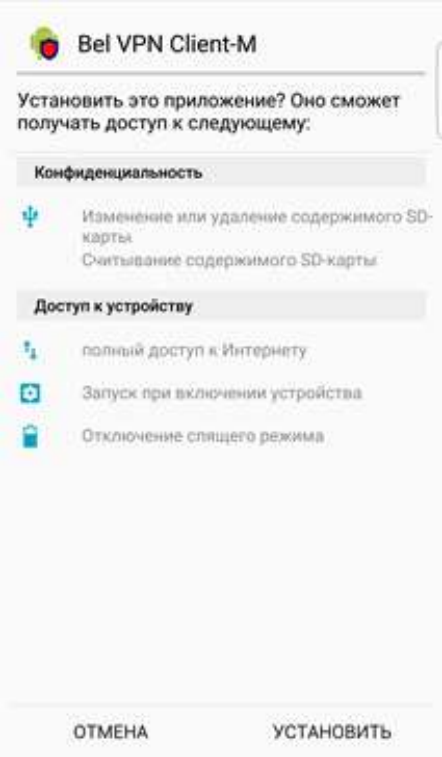

Рисунок 2

3. Запустите приложение. Ознакомьтесь с текстом лицензионного соглашения и нажмите кнопку “Принять”.
4. В следующем окне введите информацию о лицензии и нажмите кнопку “Продолжить” (Рисунок 4).

Рисунок 3

5. Запустится генератор случайных чисел. Изменяйте положение телефона в пространстве, пока индикатор не заполнится на 100% (Рисунок 3).

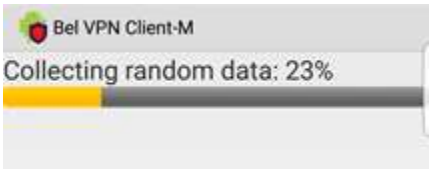

Рисунок 4

6. Откроется основное меню. Отметьте пункт “Службы IKE/IPsec” (Рисунок 5). При этом появится меню ввода пароля (Рисунок 6). В данном меню введите имя пользователя “user” с пустым паролем и нажмите кнопку “Продолжить”.

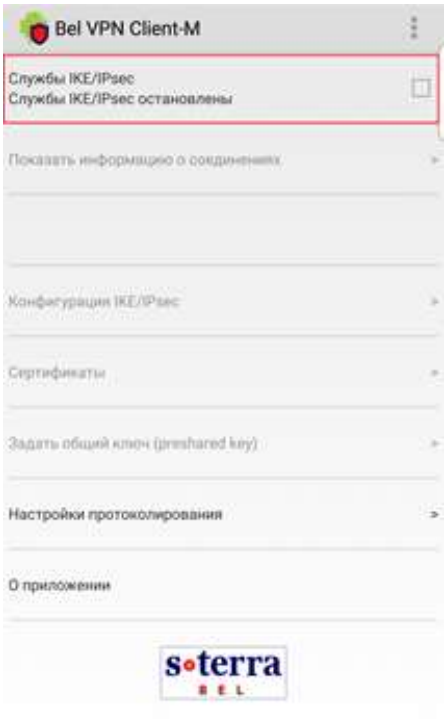

Рисунок 5

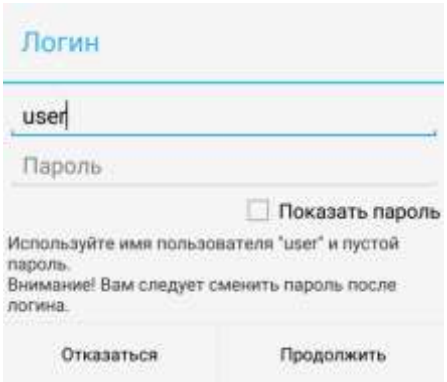

Рисунок 6

Важно: после логина необходимо сменить пароль.

7. Для смены пароля откройте меню в правом верхнем углу и выберите пункт “Сменить пароль” (Рисунок 7).

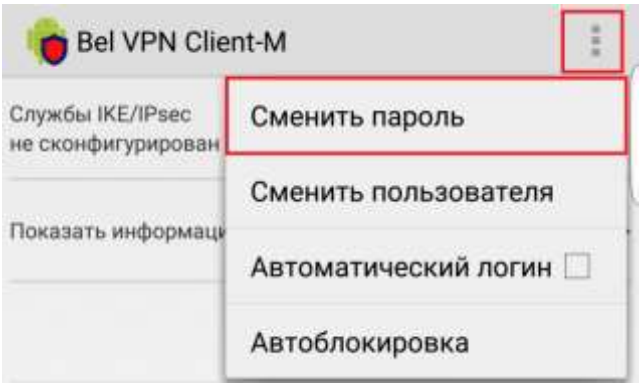

Рисунок 7

8. В окне смены пароля заполните необходимые поля и нажмите кнопку “Продолжить” (Рисунок 8).

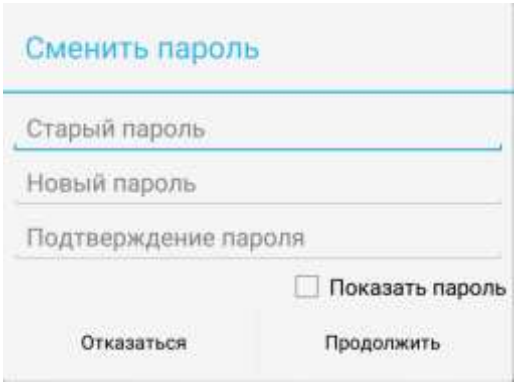

Рисунок 8

Формирование запроса на сертификат

1. Создайте запрос на клиентский сертификат. В меню “Сертификаты” выберите пункт “Подготовить запрос на сертификат bign” (Рисунок 9).

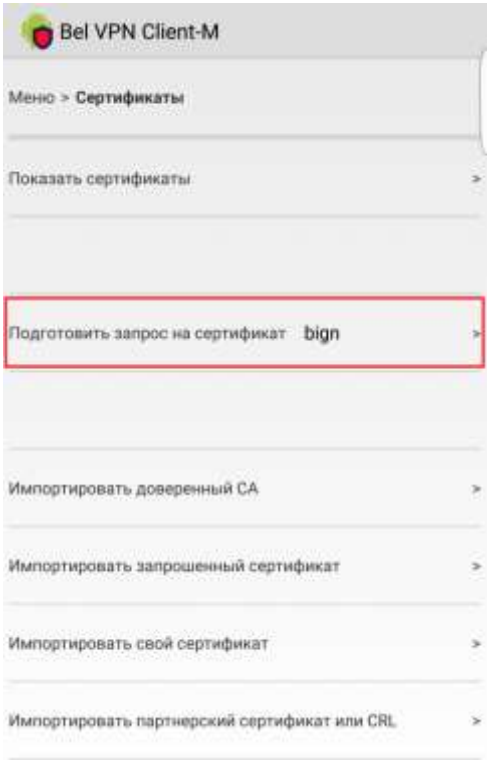

Рисунок 9

2. В появившемся окне заполните поле “Subject DN для сертификата” и нажмите кнопку “Продолжить”. Например:

```
C=BY, O=S-TerraBel, CN=clientm
```

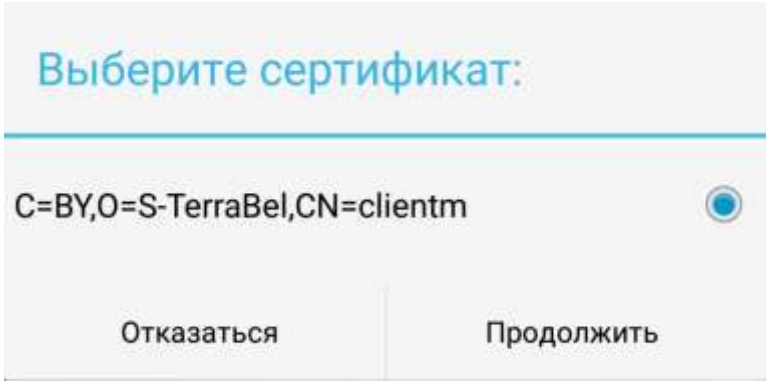

Рисунок 10

3. Запустится генератор случайных чисел. Изменяйте положение телефона в пространстве, пока индикатор не заполнится на 100%.
4. Запрос сертификата сохраните в файл (Рисунок 11). Введите название файла запроса на сертикат нажмите кнопку “Продолжить” (Рисунок 12).

Рекомендуется указывать расширение “.req” для файлов с запросом на сертификат.

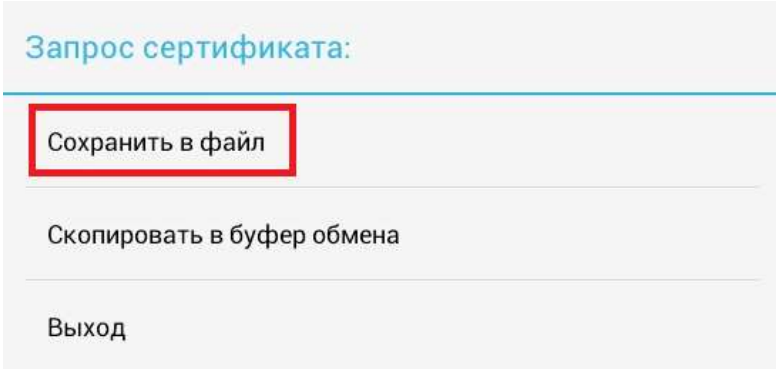

Рисунок 11

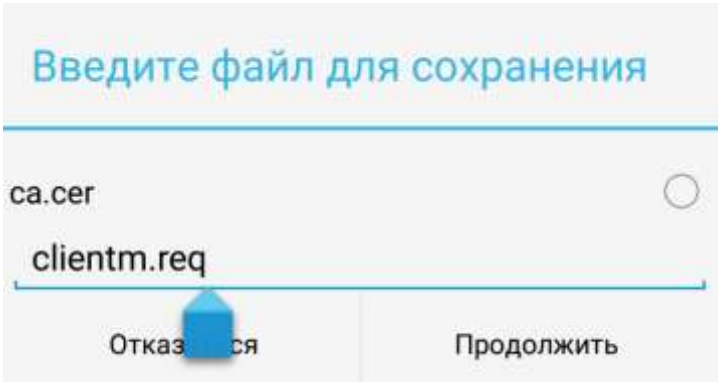

Рисунок 12

5. Далее необходимо доставить сохраненный файл запроса в УЦ.

Важно: Среда передачи в этом случае должна быть доверенной.

Регистрация сертификата УЦ

1. Скопируйте сертификат УЦ в папку /Память устройства/S-Terra.
2. В основном меню выберите пункт “Сертификаты”. В меню настройки сертификатов выберите пункт “Импортировать доверенный CA” (Рисунок 13).

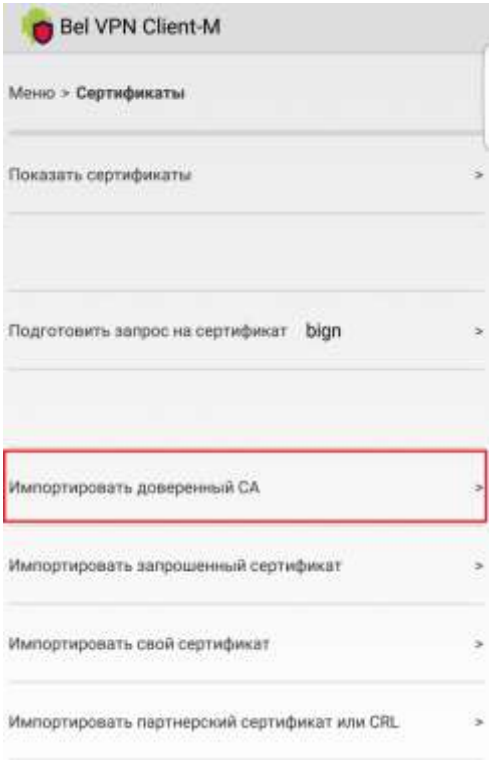

Рисунок 13

3. В появившемся меню выберите пункт “Добавить доверенный CA из файла” (Рисунок 14).

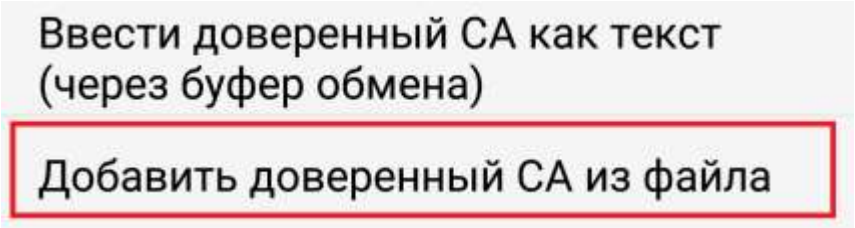

Рисунок 14

4. В появившемся меню выберите сертификат УЦ, который ранее скопировали в папку /Память устройства/S-Terra и нажмите кнопку “Продолжить” (Рисунок 15).

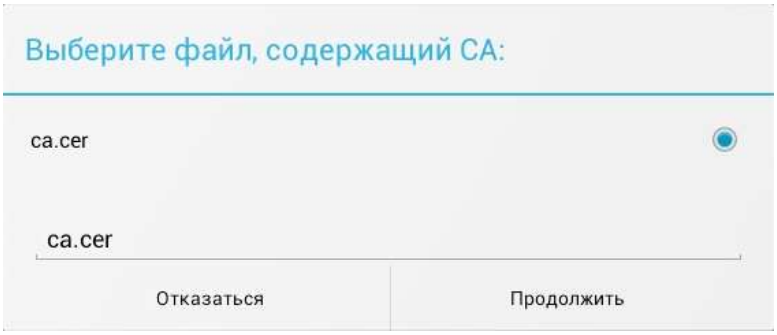

Рисунок 15

5. В окне с описанием полей сертификата нажмите кнопку “Продолжить” (Рисунок 16).

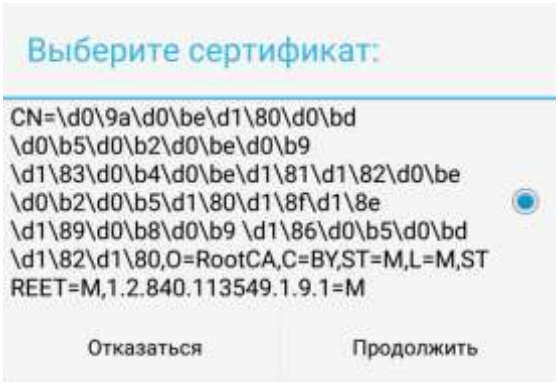

Рисунок 16

Регистрация локального сертификата

1. Скопируйте локальный сертификат в папку /Память устройства/S-Terra.
2. В меню “Сертификаты” выберите пункт “Импортировать запрошенный сертификат” (Рисунок 17).

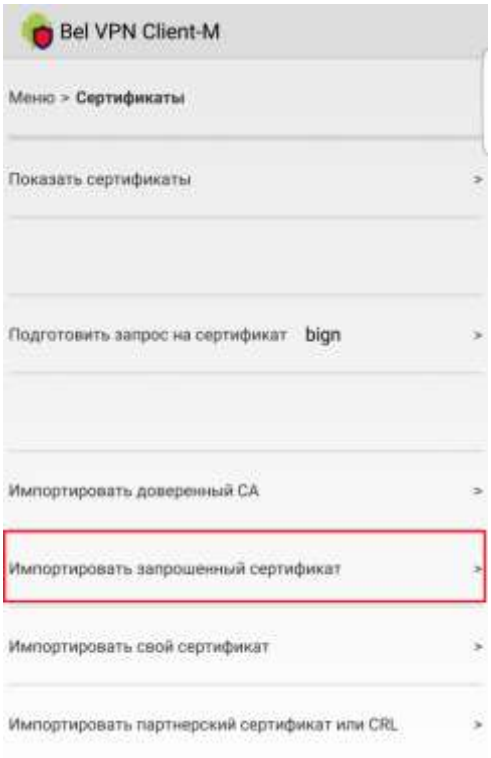

Рисунок 17

3. В появившемся окне выберите пункт “Установить свой сертификат из файла” (Рисунок 18).

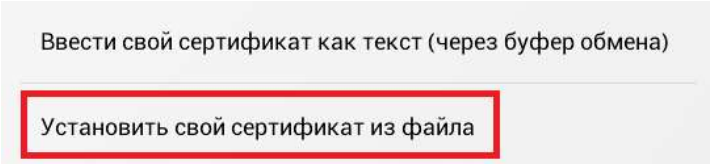

Рисунок 18

4. Выберите необходимый файл сертификата (Рисунок 19) и нажмите кнопку “Продолжить”.

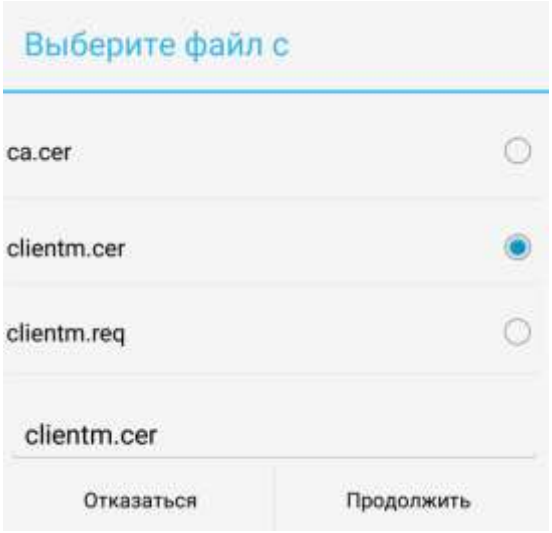

Рисунок 19

5. Подтвердите выбранный сертификат (Рисунок 20).

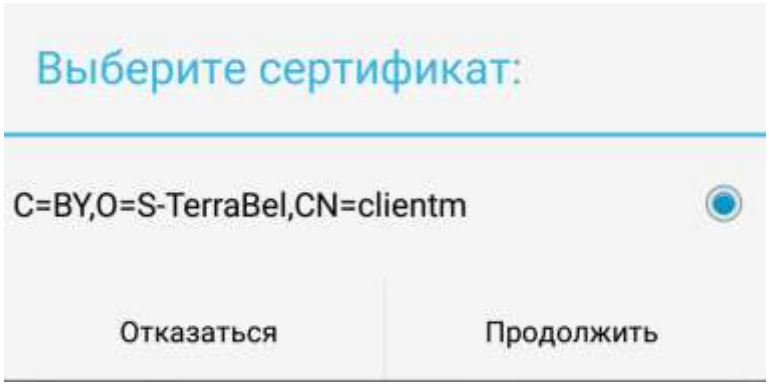

Рисунок 20

Создание политики безопасности

1. После регистрации сертификатов настройте политику безопасности. В основном меню «Bel VPN Client-M» выберите пункт “Конфигурация IKE/IPsec” (Рисунок 21).

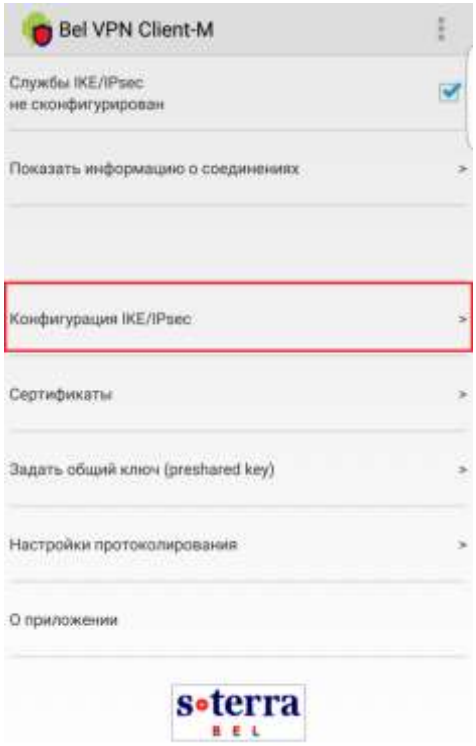

Рисунок 21

2. Выберите пункт “Создать конфигурацию” (Рисунок 22).

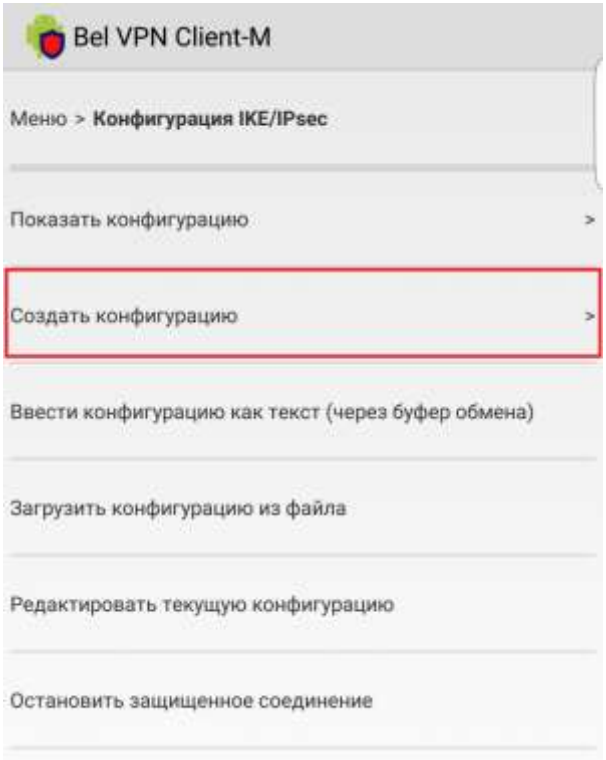

Рисунок 22

3. В поле “Защищенный шлюз” введите IP-адрес устройства GW1 (10.0.1.2). В поле “Защищаемые подсети” введите адрес подсети SN1 (192.168.1.0/24) (Рисунок 23).

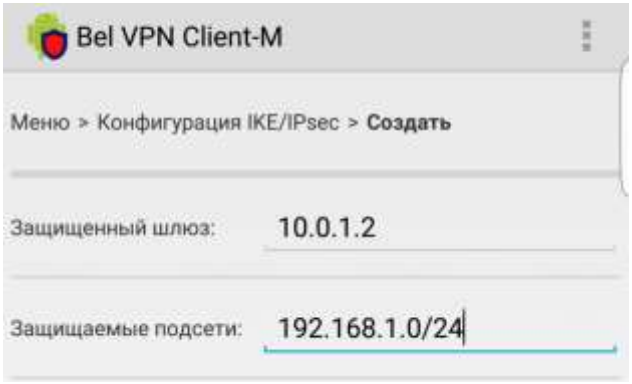

Рисунок 23

4. Раздел “Параметры IKE phase1” оставьте без изменений (Рисунок 24).

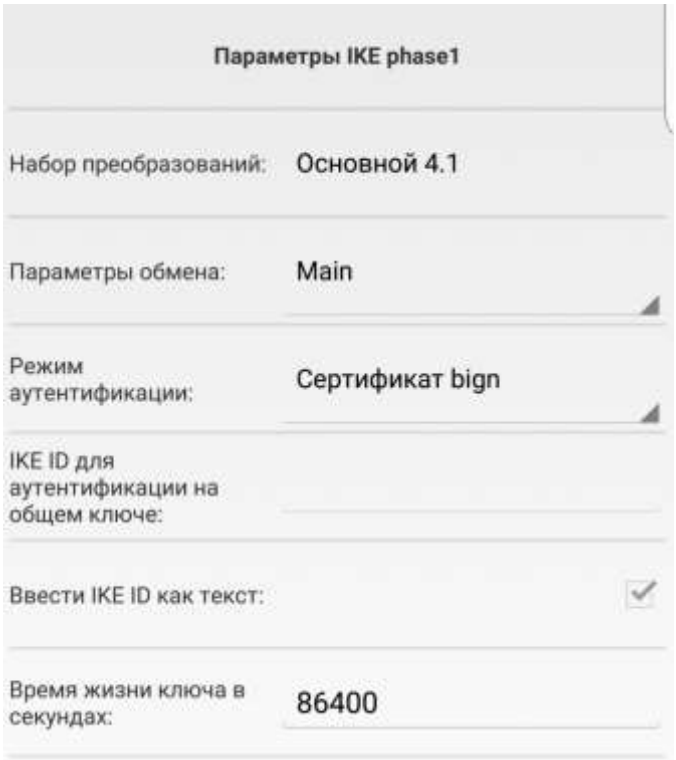

Рисунок 24

5. В разделе “Параметры IKE phase2 / IPsec” установите параметр “Группа PFS” в значение “СТБ 34.101.66-2013”, а параметр “Набор преобразований” в значение “СТБ 34.101.31-2011 (6.4+6.6)” (Рисунок 25).

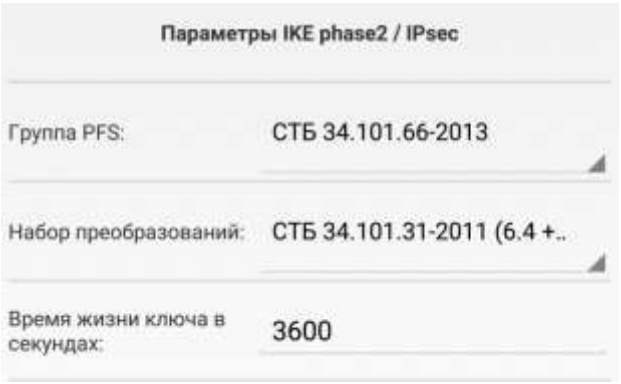

Рисунок 25

6. Раздел “Разное” оставьте без изменений и нажмите кнопку “Применить конфигурацию” (Рисунок 26).

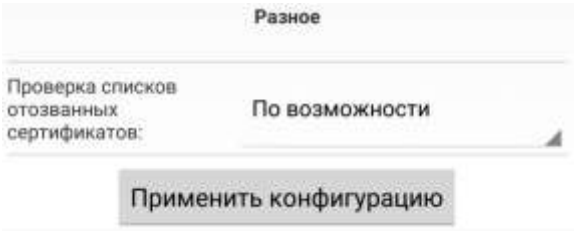

Рисунок 26

7. Настройка устройства Client-M завершена.
   - В пункте “Показать конфигурацию” можно увидеть настроенную конфигурацию.
   - В пункте “Редактировать текущую конфигурацию” можно внести изменения в конфигурацию, а так же сохранить ее в файл.
   - Для загрузки из файла выберите пункт “Загрузить конфигурацию из файла”.

Настройка устройства IPHost1

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

Настройка устройства Router1

На устройстве Router1 настройте соответствующие IP-адреса и динамический NAT.

Проверка работоспособности стенда

После того, как настройка устройств завершена, инициируйте создание защищенного соединения.

На мобильном клиенте откройте браузер и перейдите по веб адресу, находящемуся в защищаемой сети.

После загрузки сайта между шлюзом GW1 и мобильным клиентом Client-M будет установлен VPN туннель.

Убедиться в этом можно выполнив команду на шлюзе безопасности:

```
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 (10.0.1.2,4500)-(10.0.1.1,51156) active 1084 988

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 nat-t-tunn 0 0
```

На устройстве Client-M можно увидеть информацию о соединениях (в основном меню выбрать пункт “Показать информацию о соединениях”) (Рисунок 27).

Рисунок 27

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
```