

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):

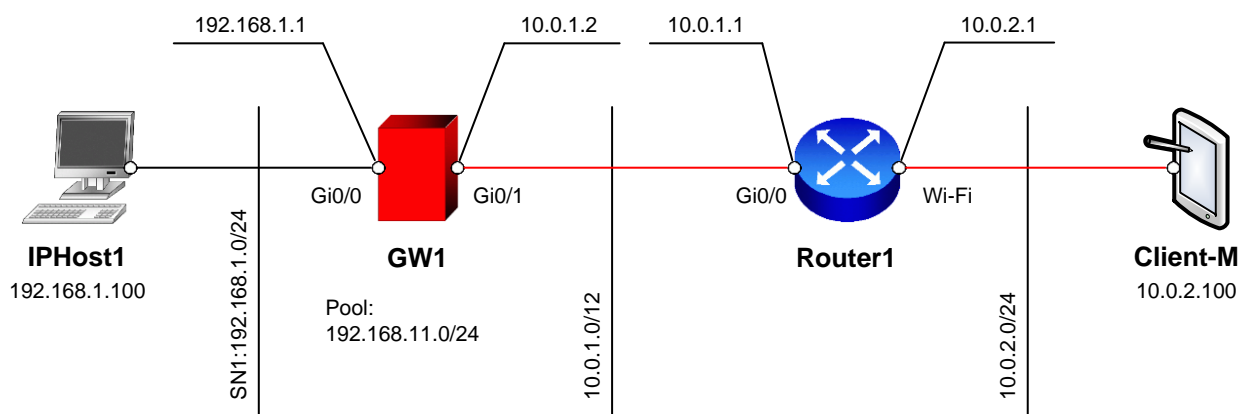


Рисунок 1

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 4.5» – [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 10.0.1.2 255.255.255.0
belvpngate(config-if)#no shutdown
belvpngate(config-if)#exit
```

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

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

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 042013152016
Wed Apr 20 13:15:00 UTC 2016
```

Данная запись соответствует 20 апреля 2016 года 13:15.

2. Создайте папку /opt/certs:

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

3. 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
```

4. Сформируйте запрос на сертификат.

```
root@belvpngate:~#/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@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
```

5. Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением **r7b** или **cer**).

Если вы получили файл сертификата в формате r7b, 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 -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= RootCA
```

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= RootCA
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 cscons 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 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
```

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=RootCA
2 State: Active CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

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

Настройка мобильного клиента Client-M

Инициализация шлюза описывается в документации на ПК «Bel VPN Client-M 4.5» – [belvpn_client-m_4-5_user_guide](#) («Руководство пользователя», раздел «Установка и инициализация продукта»).

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 “Открыть” (Рисунок 3).

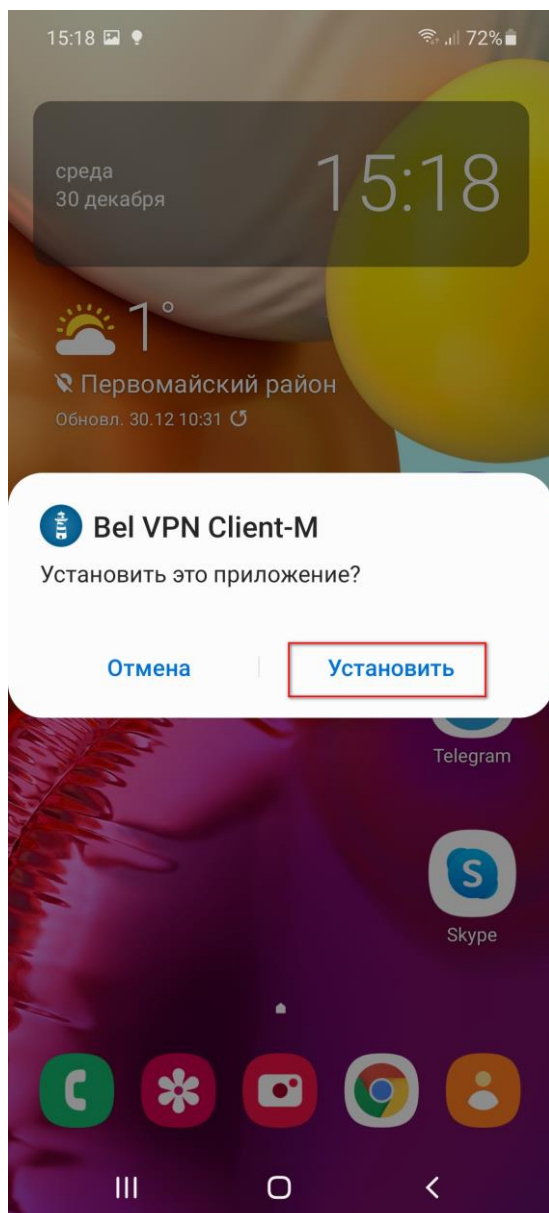


Рисунок 2

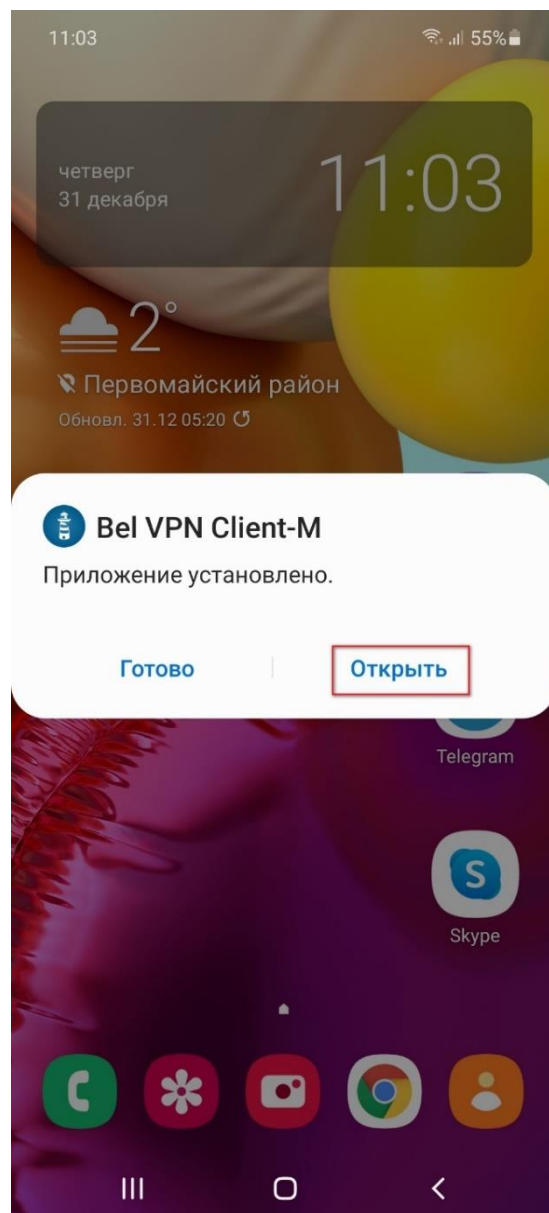


Рисунок 3

3. Запустится приложение. Предоставьте доступ к данным на внутреннем накопителе на устройстве нажав кнопку “Разрешить” (Рисунок 4). Ознакомьтесь с текстом лицензионного соглашения и нажмите кнопку “Принять” (Рисунок 5).

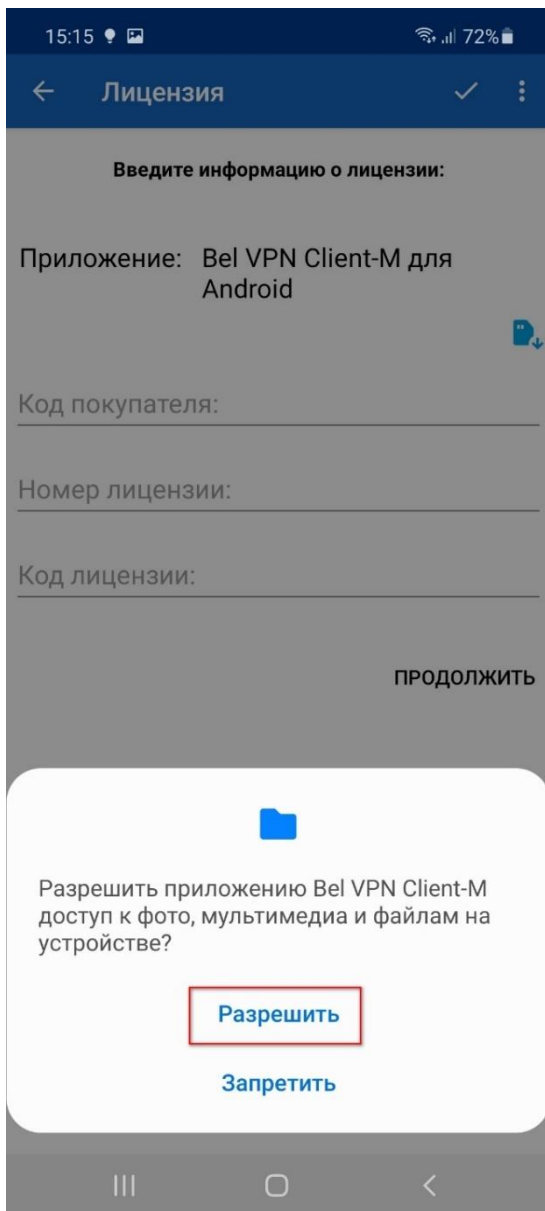


Рисунок 4



Рисунок 5

4. В следующем окне введите информацию о лицензии и нажмите кнопку “Продолжить” (Рисунок 6).
5. Далее инициализируется генератор случайных чисел. Выберите способ генерации случайных чисел и изменяйте положение телефона в пространстве или производите нажатия в разных частях экрана телефона пока идет сбор данных, в зависимости от выбранного варианта, пока индикатор не заполнится на 100% (Рисунок 7Рисунок 7).
6. По завершению процесса инициализации откроется главный экран Bel VPN Client-M (Рисунок 8Рисунок 8). Для начала работы запустите службы IKE/IPsec нажав кнопку “ СТАРТ”.
7. После успешного старта служб IKE/IPsec выдается окно логина пользователя (Рисунок 9). В данном меню введите имя пользователя “user” с пустым паролем и нажмите кнопку “Продолжить”.

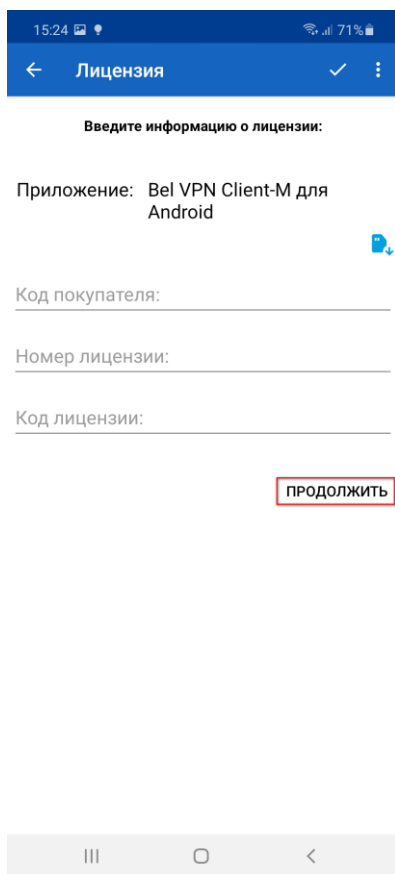


Рисунок 6



Рисунок 8

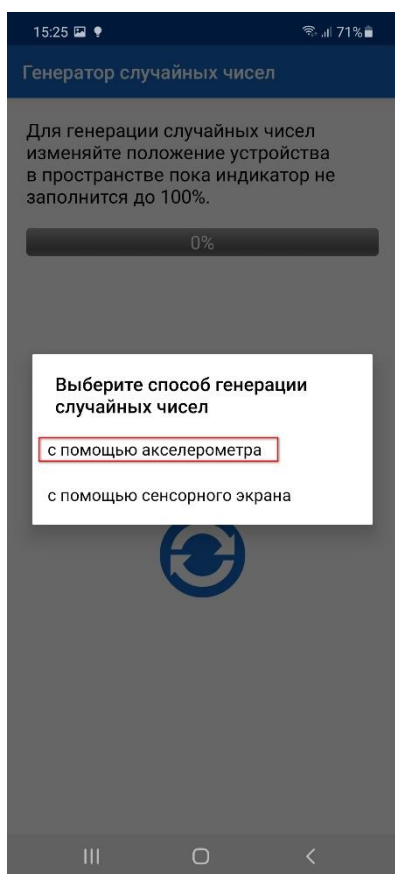


Рисунок 7

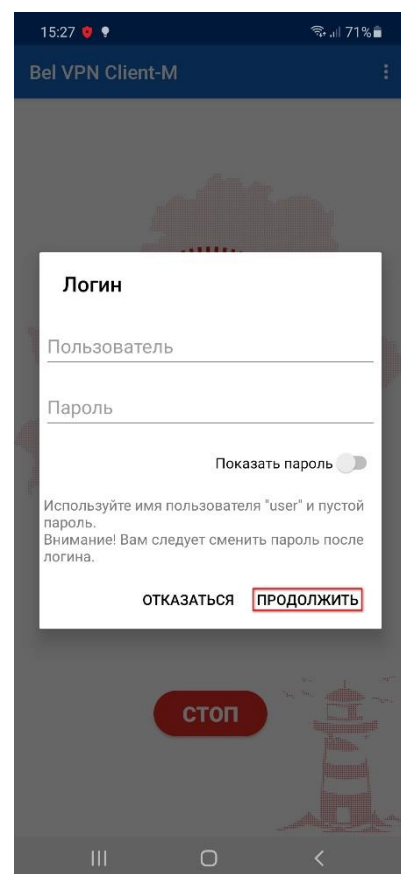


Рисунок 9

Важно: после логина необходимо сменить пароль.

- Для смены пароля откройте меню в правом верхнем углу и выберите пункт “Сменить пароль” (Рисунок 10).
- В окне смены пароля заполните необходимые поля и нажмите кнопку “Продолжить” (Рисунок 11).



Рисунок 10

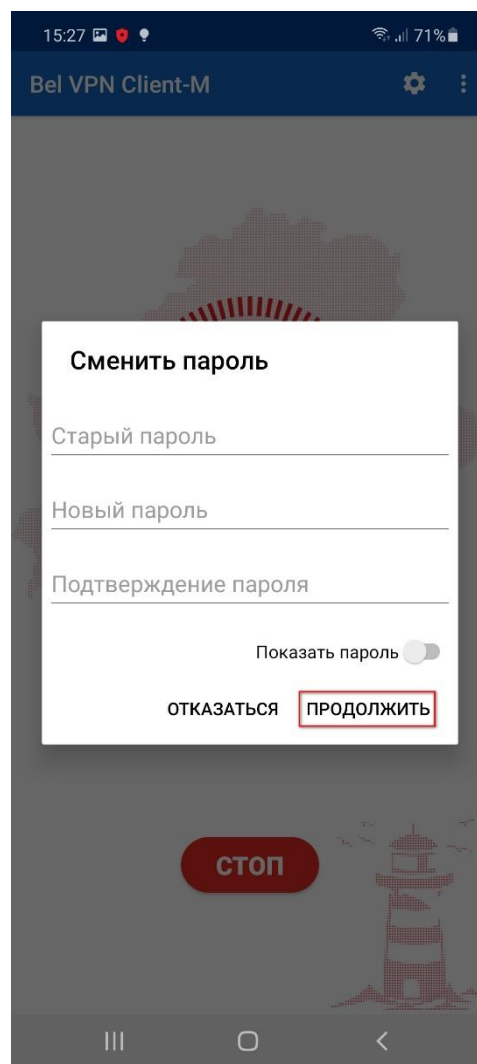


Рисунок 11

Формирование запроса на сертификат

- Для создания запроса на сертификат откройте меню в правом верхнем углу и выберите пункт “Настройки” (Рисунок 12).
- Выберите раздел “Сертификаты” (Рисунок 14), а затем “Запрос на сертификат” (Рисунок 13).
- В появившемся окне заполните поле “Subject DN для сертификата” и нажмите кнопку “Продолжить” (Рисунок 15). Например:

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

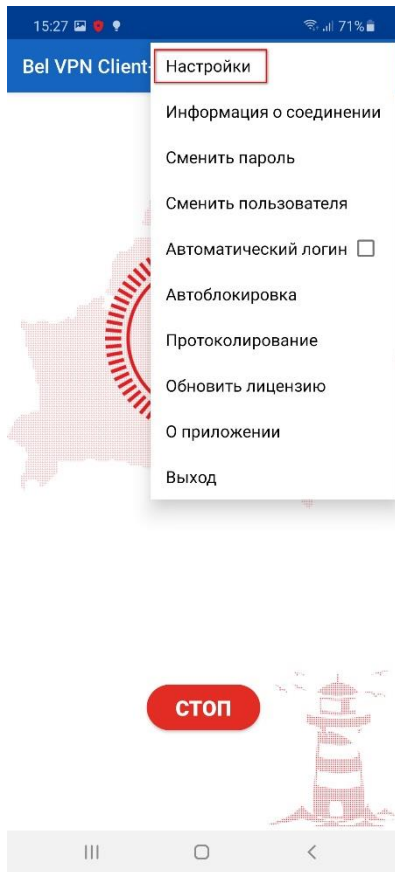


Рисунок 12

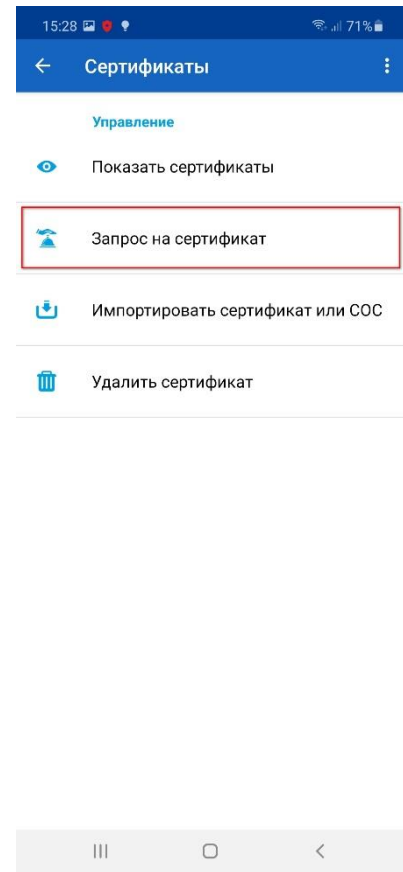


Рисунок 14

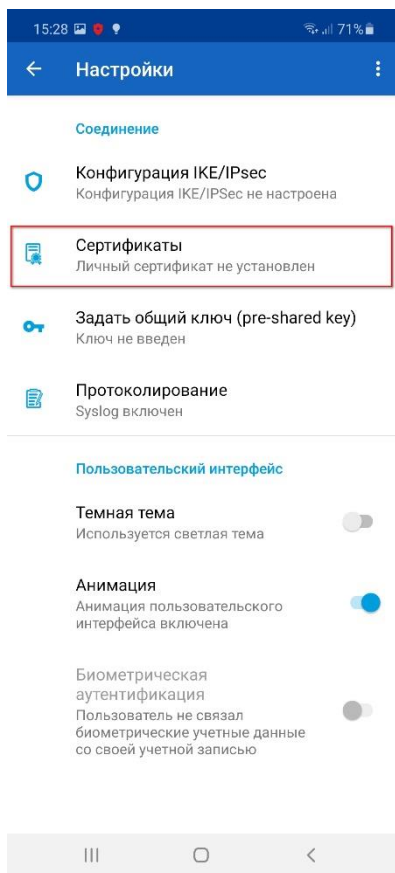


Рисунок 13

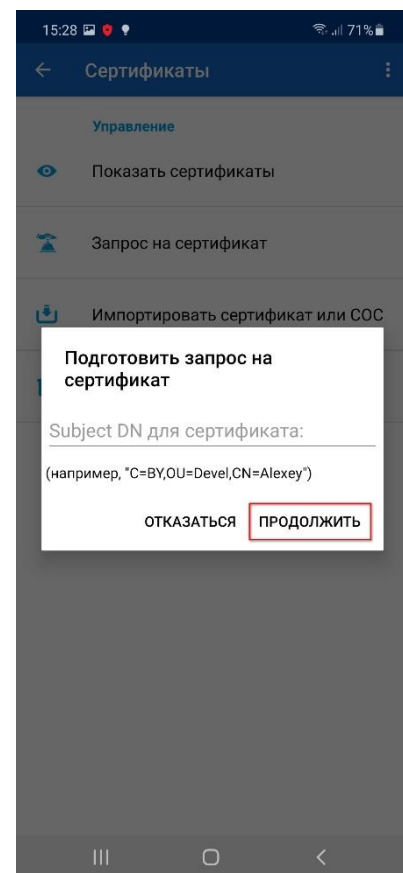


Рисунок 15

13. Далее инициализируется генератор случайных чисел. В случае отсутствия в мобильном устройстве акселерометра для сбора входных данных генератора случайных чисел выберите сенсорный экран.
14. Запрос сертификата сохраните в файл, дважды нажав кнопку “Продолжить” (Рисунок 16).
15. Далее необходимо доставить сохраненный файл запроса в УЦ.

Важно: Среда передачи в этом случае должна быть доверенной.

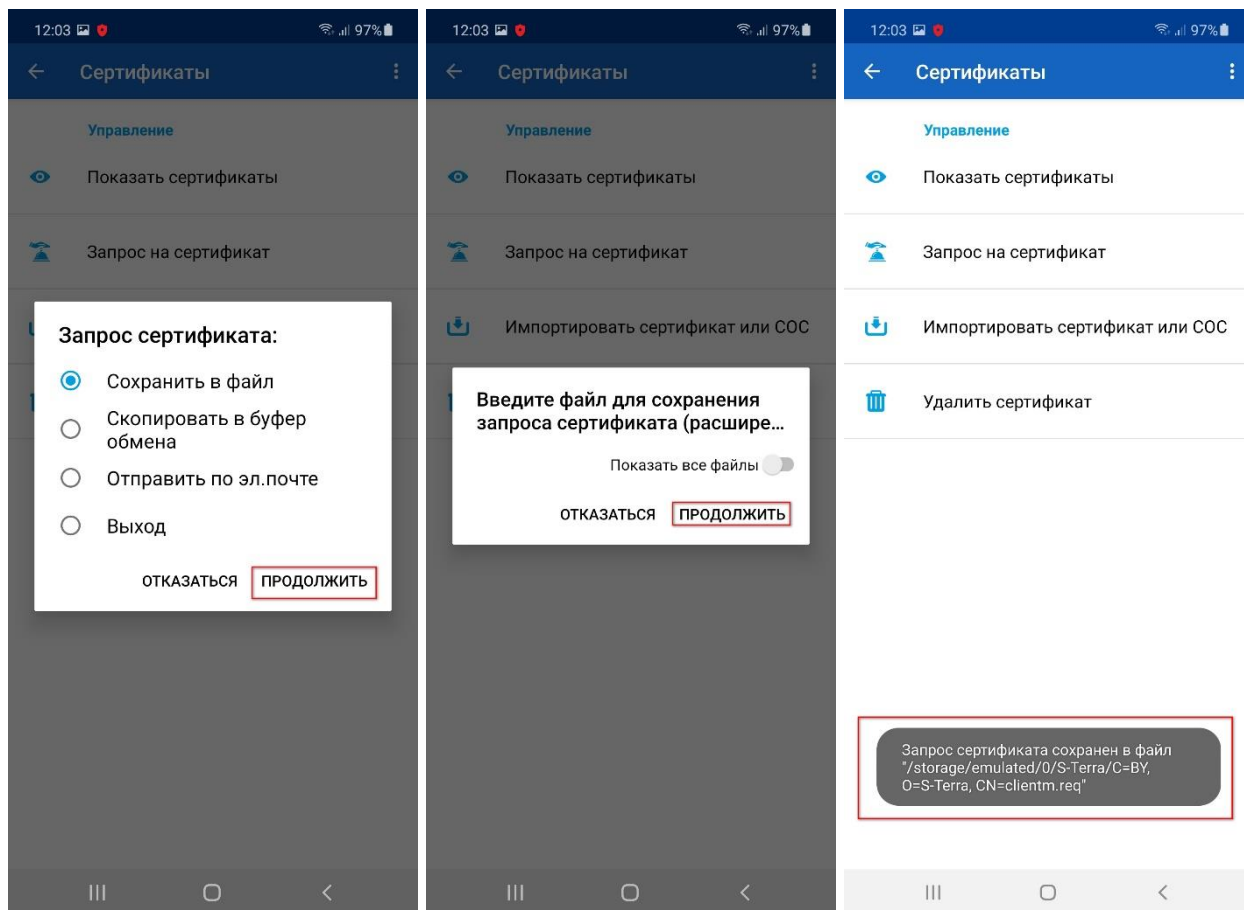


Рисунок 16

Регистрация сертификата УЦ

1. Скопируйте полученный сертификат в папку /Память устройства/S-Terra.
2. Для импорта сертификата удостоверяющего центра выберите в меню “Настройки” пункт “Сертификаты”, далее пункт “Импортировать сертификат или СОС”, а затем пункт “Сертификат открытого ключа УЦ” (Рисунок 17).
3. В появившемся меню выберите пункт “Добавить из файла”, далее в появившемся меню включите переключатель “Показать все файлы” и выберите сертификат, который ранее скопировали в папку /Память устройства/S-Terra и нажмите кнопку “Продолжить”, затем в появившемся меню выберите сертификат УЦ (Рисунок 18).

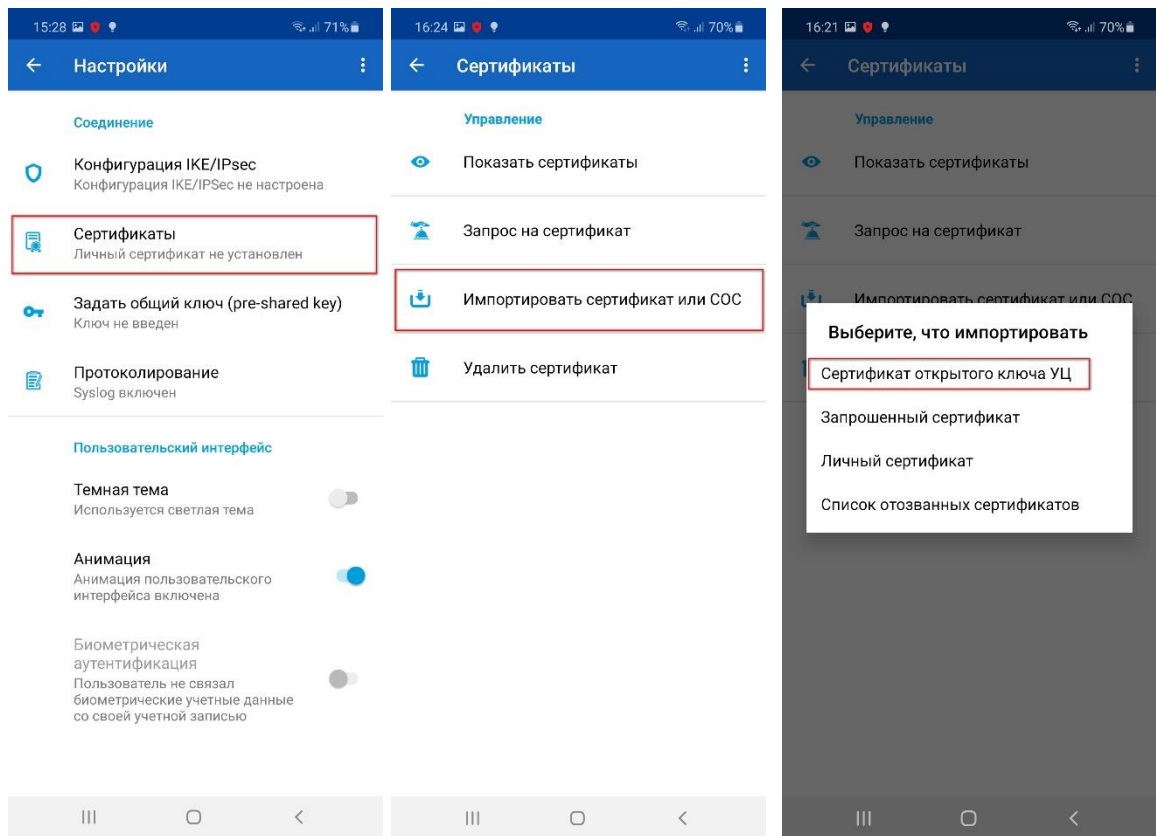


Рисунок 17

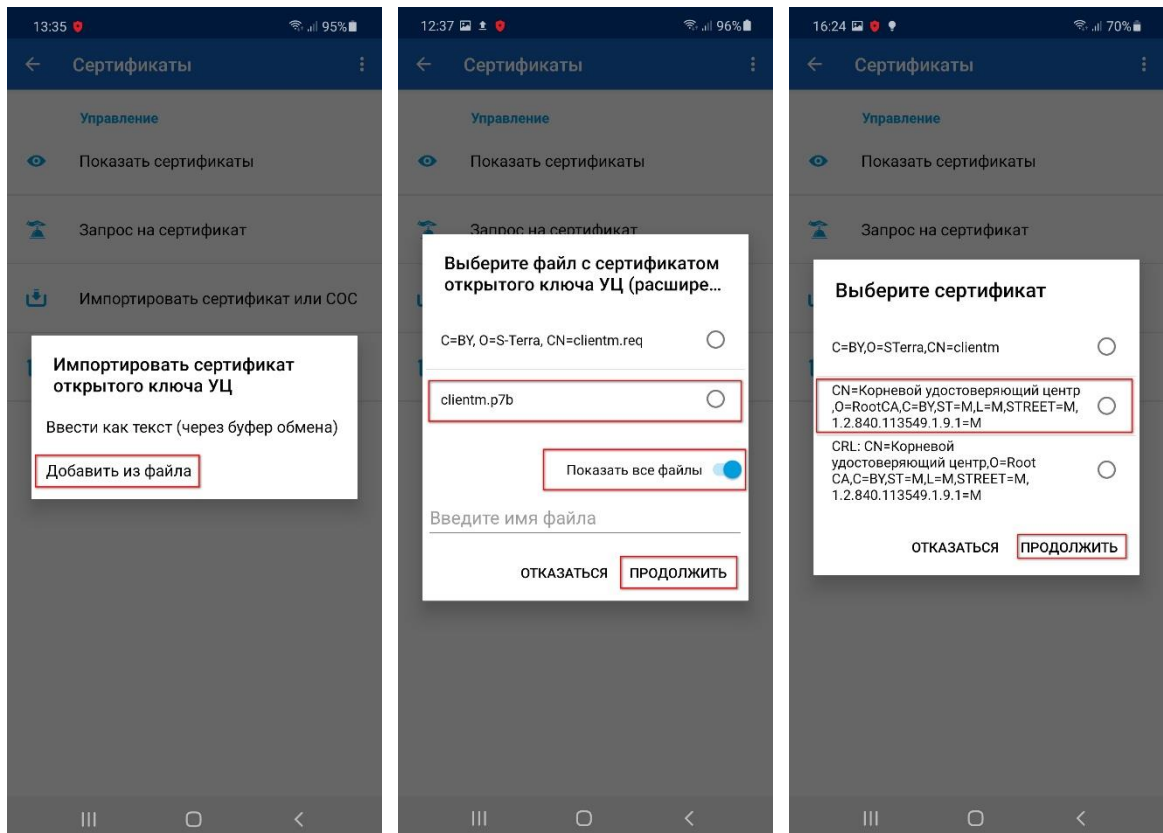


Рисунок 18

Регистрация локального сертификата

1. Для импорта локального сертификата выберите в меню “Настройки” пункт “Сертификаты”, далее пункт “Импортировать сертификат или СОС”, а затем пункт “Личный сертификат” (Рисунок 19).
2. В появившемся меню выберите пункт “Установить из файла”, далее в появившемся меню включите переключатель “Показать все файлы” и выберите сертификат, который ранее скопировали в папку /Память устройства/S-Terra и нажмите кнопку “Продолжить”, затем в появившемся меню выберите полученный сертификат (Рисунок 20).

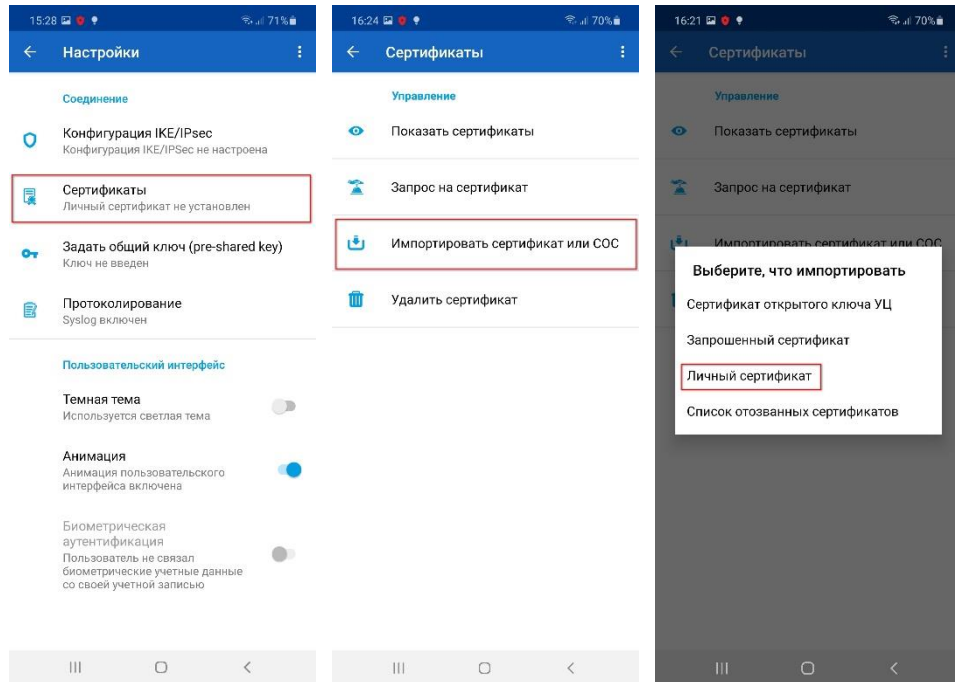


Рисунок 19

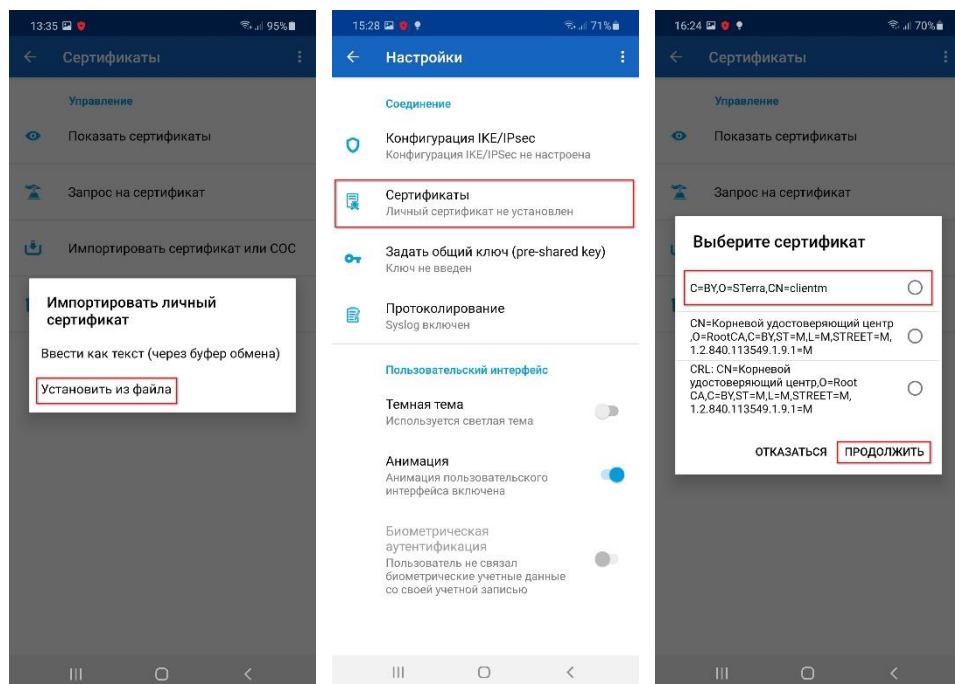


Рисунок 20

Создание политики безопасности

1. После регистрации сертификатов настройте политику безопасности. В меню “Настройки” выберите пункт “Конфигурация IKE/IPsec”, далее “Настроить конфигурацию”, после чего в поле “Защищенный шлюз” введите IP-адрес устройства GW1 (10.0.1.2), а в поле “Защищаемые подсети” введите адрес подсети SN1 (192.168.1.0/24) и нажмите кнопку “Применить конфигурацию” (Рисунок 21).

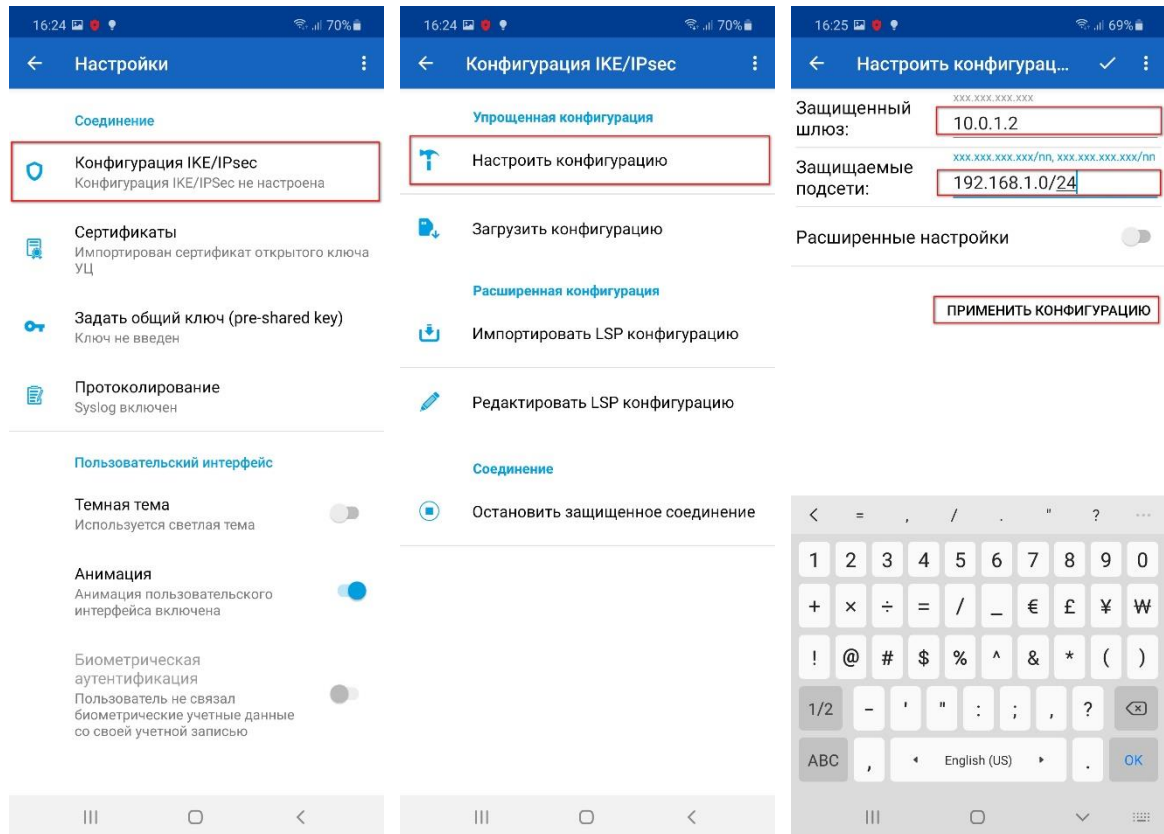


Рисунок 21

2. Настройка устройства Client-M завершена.

- В пункте “Редактировать LSP конфигурацию” можно внести изменения в конфигурацию, а также сохранить ее в файл.
- Для загрузки из файла выберите пункт “Импортировать LSP конфигурацию 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, иницируйте 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
```


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
```