

Построение VPN туннеля между двумя подсетями, защищаемыми шлюзами безопасности «С-Терра Шлюз», с использованием сертификатов, выпущенных разными УЦ

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между двумя подсетями SN1 и SN2, которые защищаются шлюзами безопасности «С-Терра Шлюз». Для защиты будет построен VPN туннель между устройствами GW1 и GW2. Устройства IPHost1 и IPHost2 смогут общаться между собой по защищенному каналу (VPN). Все остальные соединения разрешены, но защищаться не будут.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты, выпущенные разными УЦ. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6 (R4). Шлюзы безопасности «С-Терра Шлюз 4.1».

Параметры защищенного соединения:

- IKE параметры:
 - Аутентификация на сертификатах – GOST R 34.10-2001 Signature;
 - Алгоритм шифрования – GOST 28147-89 Encryption;
 - Алгоритм вычисления хеш-функции – GOST R 34.11-94 Hash;
 - Группа Диффи-Хеллмана – VKO GOST R 34.10-2001;
- IPsec параметры:
 - ESP алгоритм шифрования – ESP_GOST-4M-IMIT cipher.

Схема стенда (Рисунок 1):

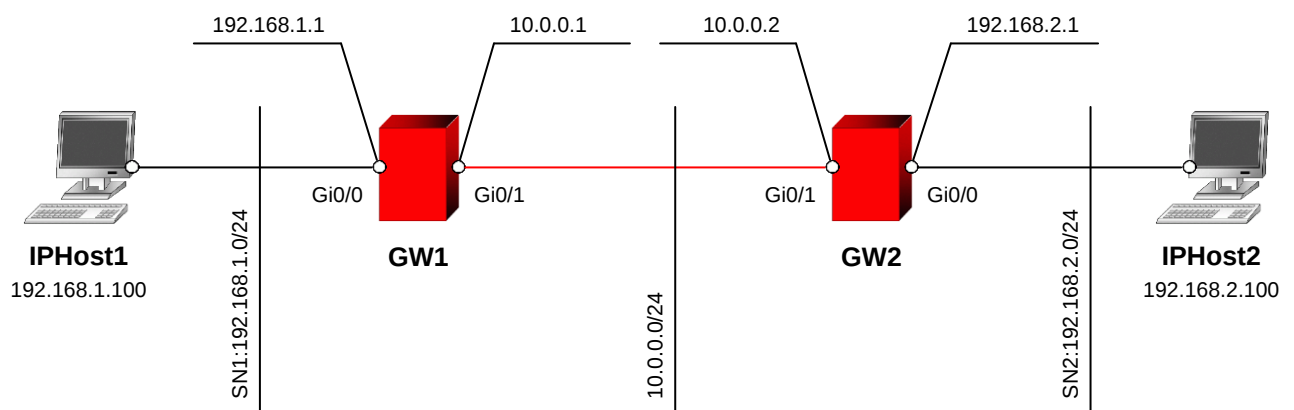


Рисунок 1

Варианты использования сертификатов

Три варианта использования сертификатов, выпущенными разными УЦ:

- [Два независимых корневых УЦ.](#)
- [Цепочка сертификатов: корневой и подчиненный регистрируются как доверенные.](#)
- [Цепочка сертификатов: корневой регистрируется как доверенный, а подчиненный – как удаленный.](#)

Настройка стенда

Вариант 1. Два независимых корневых УЦ

Схема подчинения сертификатов (Рисунок 2):

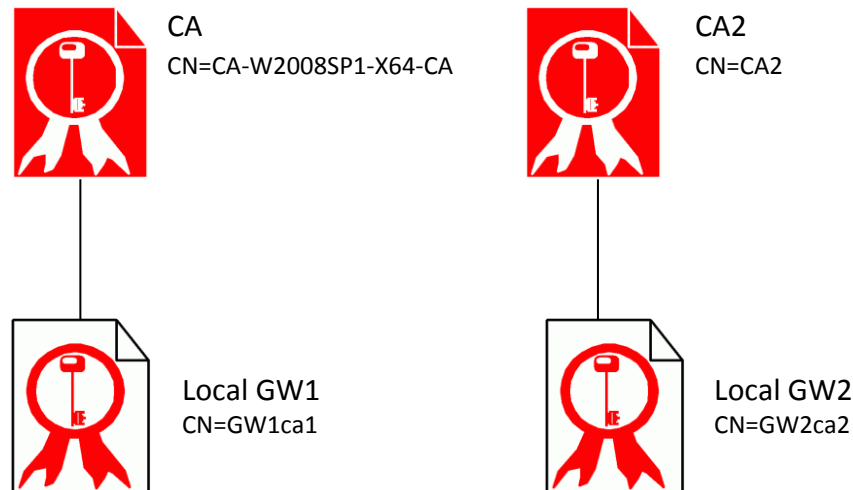


Рисунок 2

В данном варианте у каждого шлюза зарегистрированы оба корневых сертификата УЦ (CA-W2008SP1-X64-CA и CA2) как доверенные (trusted, регистрируются с ключом -t).

У шлюза GW1 зарегистрирован локальный сертификат от первого УЦ (GW1ca1).

У шлюза GW2 зарегистрирован локальный сертификат от второго УЦ (GW2ca2).

Шлюз GW1

Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация шлюза описывается в документации на ПК «С-Терра Шлюз 4.1» ([«Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64»](#), раздел «Инициализация S-Terra Gate при первом старте»).

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПК «С-Терра Шлюз 4.1» ([«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 10.0.0.1 255.255.255.0
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 10.0.0.3
```

5. Выйдите из cisco-like интерфейса:

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

Регистрация СА сертификатов (сертификатов УЦ)

Для регистрации СА сертификатов (сертификатов УЦ) необходимо выполнить следующие действия:

1. Установите правильное системное время.

Например:

```
root@sterragate:~# date 041013152013
Wed Apr 10 13:15:00 UTC 2013
```

Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку /certs:

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

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

```
pscp <CA file path>/<CA file name> root@<gate address>:/<path>
```

Например:

```
pscp D:\ca1.cer root@192.168.1.1:/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 ПК «С-Терра Шлюз 4.1» ([«Инициализация и настройка шлюза»](#), раздел «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза»).

4. С помощью утилиты cert_mgr зарегистрируйте оба сертификата в базе продукта:

```
root@sterragate:~# cert_mgr import -f /certs/ca1.cer -t
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
root@sterragate:~# cert_mgr import -f /certs/ca2.cer -t
1 OK C=RU,L=Moscow,O=Company,OU=IT,CN=CA2
```

Параметр `-t` в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните нижеописанные действия.

1. Сформируйте запрос на сертификат при помощи утилиты `cert_mgr`:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1cal" -GOST_R3410EL
Press keys...
[.....]
-----BEGIN CERTIFICATE REQUEST-----
MIIBDTCBuwIBADAxMQswCQYDVQQGEwJSVTERMA8GA1UECzMlUmVzZWZyY2gx
...
jGLc
-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на ПК «С-Терра Шлюз 4.1» ([«Приложение»](#), раздел «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP»»).
3. Перенесите полученный файл на шлюз безопасности (параметры `rsr` описаны выше).
4. Зарегистрируйте локальный сертификат в базе продукта, применив утилиту `cert_mgr`:

```
root@sterragate:~# cert_mgr import -f /certs/gw1cal.cer
1 OK C=RU,OU=Research,CN=GW1cal
```

5. Убедитесь, что сертификаты импортированы успешно:

```
root@sterragate:~# cert_mgr show
Found 3 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
2 Status: trusted C=RU,L=Moscow,O=Company,OU=IT,CN=CA2
3 Status: local C=RU,OU=Research,CN=GW1cal
```

Регистрация сертификатов на шлюзе GW1 закончена.

Создание политики безопасности шлюза 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 gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication gost-sig
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit
```

6. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-imit
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

7. 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 0.0.0.255 192.168.2.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

8. Создайте крипто-карту:

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

```
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

```
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set peer 10.0.0.3
GW1(config-crypto-map)#exit
```

9. 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
```

10. 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
```

11. 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](#) и текст [LSP конфигурации](#) для шлюза GW1.

Шлюз GW2

Настройка и регистрация сертификатов на шлюзе GW2 происходит аналогично настройке шлюза GW1.

Вывод команды `cert_mgr show` будет выглядеть следующим образом:

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

```
Found 3 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
2 Status: trusted C=RU,L=Moscow,O=Company,OU=IT,CN=CA2
3 Status: local C=RU,OU=IT,CN=GW2ca2
```

В Приложении представлен текст [cisco-like конфигурации](#) и текст [LSP конфигурации](#) для шлюза GW2.

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 IPHost2

На устройстве IPHost2 задайте IP-адрес, а в качестве шлюза по умолчанию укажите IP-адрес внутреннего интерфейса шлюза безопасности GW2 – 192.168.2.1.

Вариант 2. Цепочка сертификатов: корневой и подчиненный регистрируются как доверенные

Схема подчинения сертификатов (Рисунок 3):

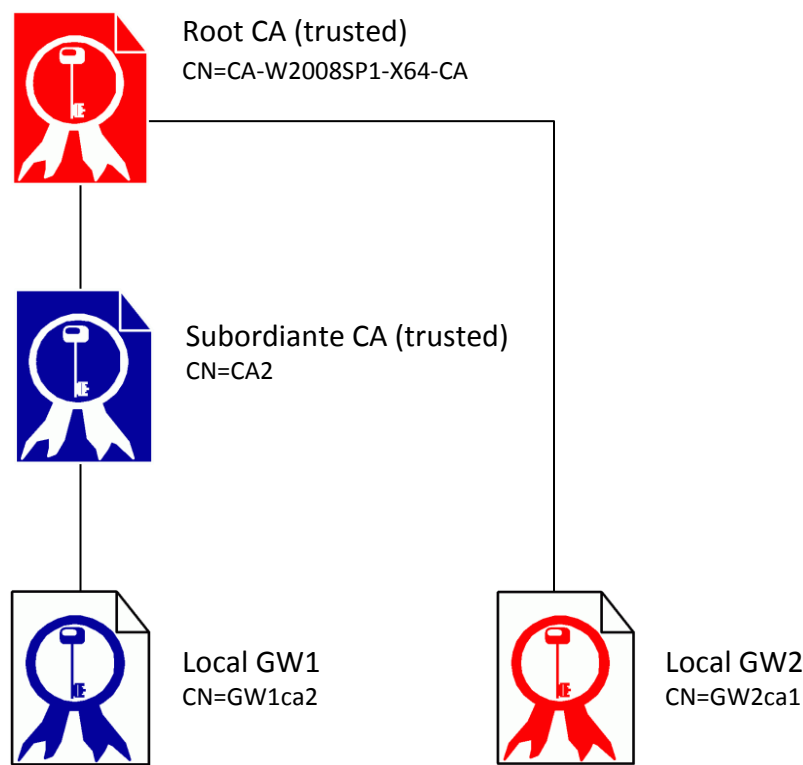


Рисунок 3

В данном варианте рассматривается случай, когда на GW1 регистрируется корневой и подчиненный сертификаты CA (УЦ) как доверенные (trusted, регистрируются с ключом -t). Локальный сертификат шлюза GW1 подписывается сертификатом подчиненного CA (УЦ).

На шлюзе GW2 регистрируется корневой сертификат и локальный сертификат, подписанный сертификатом корневого CA (УЦ).

Шлюз GW1

Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация шлюза описывается в документации на ПК «С-Терра Шлюз 4.1» ([«Инициализация и настройка шлюза»](#), раздел «Инициализация S-Terra Gate при первом старте»).

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПК «С-Терра Шлюз 4.1» ([«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 10.0.0.1 255.255.255.0
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 10.0.0.3
```

5. Выйдите из cisco-like интерфейса:

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

Регистрация СА сертификатов (сертификатов УЦ)

Для регистрации СА сертификатов (сертификатов УЦ) необходимо выполнить следующие действия:

1. Установите правильное системное время.

Например:

```
root@sterragate:~# date 041013152013
```

```
Wed Apr 10 13:15:00 UTC 2013
```

Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку /certs:

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

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

```
pscp <CA file path>/<CA file name> root@<gate address>:/<path>
```

Например:

```
pscp D:\rootca.cer root@192.168.1.1:/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 ПК «С-Терра Шлюз 4.1» ([«Инициализация и настройка шлюза»](#), раздел «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза»).

4. С помощью утилиты cert_mgr зарегистрируйте оба сертификата в базе продукта:

```
root@sterragate:~# cert_mgr import -f /certs/rootca.cer -t
```

```
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA
```

```
root@sterragate:~# cert_mgr import -f /certs/subca.cer -t
```

```
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=SubCA
```

Параметр `-t` в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните нижеописанные действия.

1. Сформируйте запрос на сертификат при помощи утилиты `cert_mgr`:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1ca1" -GOST_R3410EL
```

```
Press keys...
[.....]
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBuAIBADAuMQswCQYDVQGEwJSVTERMA8GA1UECxMIUmVzZWZyY2gx
...
Y5NkR8A9igWP+uk+r8AJkZzHbGZxhUVjoB4wHAYJKoZIhvcNAQkOMQ8wDTAL
-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на ПК «С-Терра Шлюз 4.1» ([«Приложение»](#), раздел «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP»»).
3. Перенесите полученный файл на шлюз безопасности (параметры `pscp` описаны выше).
4. Зарегистрируйте локальный сертификат в базе продукта, применив утилиту `cert_mgr`:

```
root@sterragate:~# cert_mgr import -f /certs/gw1.cer
```

```
1 OK C=RU,OU=Research,CN=GW1
```

5. Убедитесь, что сертификаты импортированы успешно:

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

```
Found 3 certificates. No CRLs found.
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA
2 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=SubCA
3 Status: local C=RU,OU=Research,CN=GW1
```

Регистрация сертификатов на шлюзе GW1 закончена.

Создание политики безопасности шлюза 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 gost
GW1(config-isakmp)#encryption gost
GW1(config-isakmp)#authentication sign
GW1(config-isakmp)#group vko
GW1(config-isakmp)#exit
```

Важно: Параметр **authentication sign** в отличие от **gost-sig** будет запрашивать цепочку сертификатов.

6. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-gost28147-4m-imit
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

7. 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 0.0.0.255 192.168.2.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

8. Создайте крипто-карту:

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

```
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
```

```
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs vko
GW1(config-crypto-map)#set peer 10.0.0.3
GW1(config-crypto-map)#exit
```

9. 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
```

10. 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
```

11. 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](#) и текст [LSP конфигурации](#) для шлюза GW1.

Шлюз GW2

Настройка и регистрация сертификатов на шлюзе GW2 происходит аналогично настройке шлюза GW1.

На шлюзе GW2 зарегистрируйте сертификат от корневого CA (УЦ), а так же локальный сертификат, подписанный сертификатом корневого CA (УЦ).

Вывод команды `cert_mgr show` будет выглядеть следующим образом:

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

```
Found 2 certificates. No CRLs found.
```

```
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA
```

```
2 Status: local   C=RU,OU=IT,CN=GW2
```

В Приложении представлен текст [cisco-like конфигурации](#) и текст [LSP конфигурации](#) для шлюза GW2.

Вариант 3. Цепочка сертификатов: корневой регистрируется как доверенный, а подчиненный - как удаленный (remote)

Схема подчинения сертификатов (Рисунок 4):

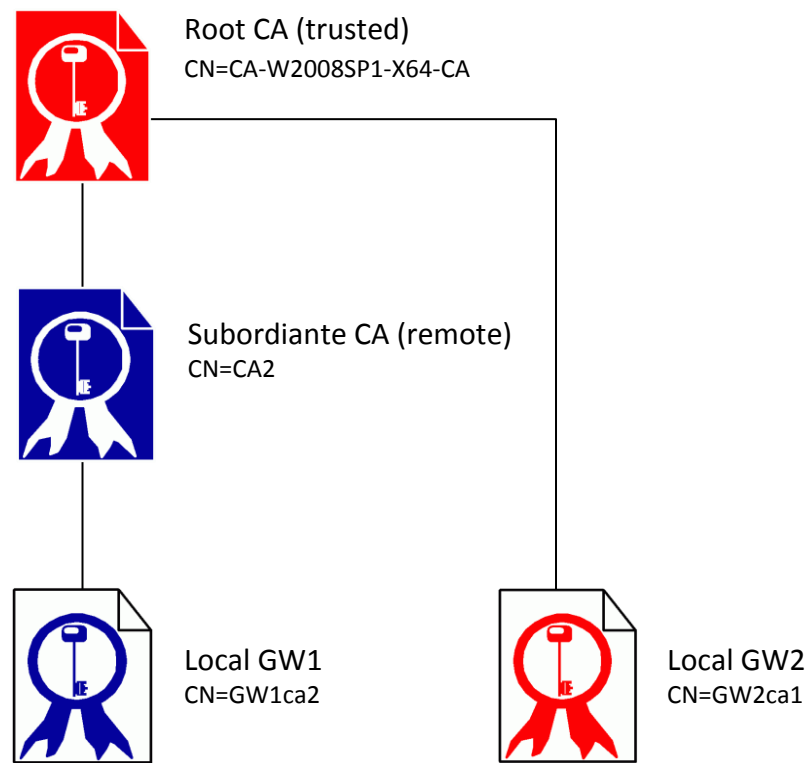


Рисунок 4

В данном варианте рассматривается случай, когда на GW1 регистрируется корневой сертификат CA (УЦ) как доверенный (trusted, регистрируется с ключом `-t`), а подчиненный сертификат CA (УЦ) как удаленный (remote, регистрируется без ключа `-t`). Также регистрируется локальный сертификат, подписанный сертификатом подчиненного CA (УЦ).

На шлюзе GW2 регистрируется корневой сертификат и локальный сертификат, подписанный сертификатом корневого CA (УЦ)

Шлюз 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 ПК «С-Терра Шлюз 4.1» ([«Инициализация и настройка шлюза»](#), раздел «Инициализация S-Terra Gate при первом старте»).

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПК «С-Терра Шлюз 4.1» ([«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 10.0.0.1 255.255.255.0
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 10.0.0.3
```

5. Выйдите из cisco-like интерфейса:

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

Регистрация CA сертификатов (сертификатов УЦ)

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

1. Установите правильное системное время.

Например:

```
root@sterragate:~# date 041013152013
```

```
Wed Apr 10 13:15:00 UTC 2013
```

Данная запись соответствует 10 апреля 2013 года 13:15.

2. Создайте папку /certs:

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

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

```
pscp <CA file path>/<CA file name> root@<gate address>:/<path>
```

Например:

```
pscp D:\cal.cer root@192.168.1.1:/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 ПК «С-Терра Шлюз 4.1» ([«Инициализация и настройка шлюза»](#), раздел «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза»).

4. С помощью утилиты cert_mgr зарегистрируйте оба сертификата в базе продукта:

```
root@sterragate:~# cert_mgr import -f /certs/cal.cer -t
```

```
1 OK C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=CA-W2008SP1-X64-CA
```

```
root@sterragate:~# cert_mgr import -f /certs/ca2.cer -t
```

```
1 OK C=RU,L=Moscow,O=Company,OU=IT,CN=CA2
```

Параметр `-t` в данной команде указывает на то, что импортируемый сертификат – корневой (сертификат УЦ).

Регистрация локального сертификата

Для регистрации локального сертификата в базе продукта выполните нижеописанные действия.

1. Сформируйте запрос на сертификат при помощи утилиты `cert_mgr`:

```
root@sterragate:~# cert_mgr create -subj "C=RU,OU=Research,CN=GW1ca1" -GOST_R3410EL
```

```
Press keys...
```

```
[.....]
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBDTCBuwIBADAxMQswCQYDVQQGEwJSVTERMA8GA1UECxMIUmVzZWZyY2gx
DzANBgNVBAMTBkdXMWNhMTBjMBwGBiqFAwICEzASBgqhQMCAiMBBgqhQMC
Ah4BA0MABECBiqi3k3v5gLnu3iedowPCjzG03qCaUy8WKEVWwW0V280MVGXv
KYKBWmr5grB+BoZFIF9iA1TeyZJlec5+gKswB4wHAYJKoZIhvcNAQkOMQ8w
rKfpzmbbn1DqpceL3zQzImgvUxSaei6tOAQj888uIUYzaJ25XqRZzc+KsOH
jGLc
```

```
-----END CERTIFICATE REQUEST-----
```

2. Передайте полученный запрос сертификата на УЦ. Процедура выдачи сертификата на УЦ по запросу описана в документации на ПК «С-Терра Шлюз 4.1» ([«Приложение»](#), раздел «Создание локального сертификата с использованием СКЗИ «КриптоПро CSP»»).
3. Перенесите полученный файл на шлюз безопасности (параметры `pscp` описаны выше).
4. Зарегистрируйте локальный сертификат в базе продукта, применив утилиту `cert_mgr`:

```
root@sterragate:~# cert_mgr import -f /certs/gw1ca1.cer
```

```
1 OK C=RU,OU=Research,CN=GW1ca1
```

5. Убедитесь, что сертификаты импортированы успешно:

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

```
Found 3 certificates. No CRLs found.
```

```
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA
```

```
2 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=SubCA
```

```
3 Status: local C=RU,OU=Research,CN=GW1
```

Регистрация сертификатов на шлюзе GW1 закончена.

Создание политики безопасности шлюза GW1 описывается происходит аналогично [варианту 2](#).

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

Шлюз GW2

Настройка и регистрация сертификатов на шлюзе GW2 происходит аналогично настройке шлюза GW1.

Вывод команды `cert_mgr show` будет выглядеть следующим образом:

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

```
Found 2 certificates. No CRLs found.
```

```
1 Status: trusted C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA
```

```
2 Status: local C=RU,OU=IT,CN=GW2
```

В [Приложении](#) представлен текст [cisco-like конфигурации](#) и текст [LSP конфигурации](#) для шлюза GW2.

Проверка работоспособности стенда

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

На устройстве IPHost1 выполните команду ping:

```
ping 192.168.2.100
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.  
64 bytes from 192.168.2.100: icmp_req=1 ttl=62 time=1359 ms  
64 bytes from 192.168.2.100: icmp_req=2 ttl=62 time=356 ms  
64 bytes from 192.168.2.100: icmp_req=3 ttl=62 time=4.37 ms  
64 bytes from 192.168.2.100: icmp_req=4 ttl=62 time=5.52 ms  
64 bytes from 192.168.2.100: icmp_req=5 ttl=62 time=7.11 ms  
^C  
--- 192.168.2.100 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 4.372/346.586/1359.566/524.385 ms, pipe 2
```

В результате выполнения этой команды между устройствами GW1 и GW2 будет установлен VPN туннель.

Убедиться в этом можно, выполнив на устройстве GW1 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 3 (192.168.100.1,4500)-(10.10.10.3,4500) active 1976 1904  
  
IPsec connections:  
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd  
1 2 (192.168.1.0-192.168.1.255,*)-(192.168.2.0-192.168.2.255,*) * ESP nat-t-tunn 440  
440
```

Согласно созданной политике безопасности весь трафик между сетями SN1 и SN2 будет зашифрован. Прохождение остального трафика будет разрешено, но не будет защищаться шифрованием.

Приложение

Вариант 1

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 gost  
  hash gost  
  authentication gost-sig  
  group vko  
!  
crypto ipsec transform-set TSET esp-gost4mimit  
!  
ip access-list extended LIST  
  permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255  
!  
!  
crypto map CMAP 1 ipsec-isakmp  
  match address LIST  
  set transform-set TSET  
  set pfs vko  
  set peer 10.0.0.3  
!  
interface GigabitEthernet0/0  
  ip address 192.168.1.1 255.255.255.0  
!  
interface GigabitEthernet0/1  
  ip address 10.0.0.1 255.255.255.0  
  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 10.0.0.3
```

```
!  
crypto pki trustpoint s-terra_technological_trustpoint  
  revocation-check none  
crypto pki certificate chain s-terra_technological_trustpoint  
certificate 4E4B0B11EFDB389E4E86244CDAA1B275  
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530  
...  
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713  
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F  
  
quit  
certificate 02A03970421DD6894F13B0315EFBC818  
308201E430820193A003020102021002A03970421DD6894F13B0315EFBC81830  
...  
F5B786894A1F63E8D823CBB0989339C2160E13DE27A9BD61BE5A1C28E4894D20  
A5521AFB0BCF89AB  
  
quit  
!  
end
```

Текст cisco-like конфигурации для шлюза GW2

```
!  
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 GW2  
enable password csp  
!  
!  
!  
logging trap debugging  
!  
!  
crypto isakmp policy 1  
  encr gost  
  hash gost  
  authentication gost-sig  
  group vko  
!  
crypto ipsec transform-set TSET esp-gost4mimit  
!  
ip access-list extended LIST  
  permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255  
!  
!  
crypto map CMAP 1 ipsec-isakmp  
  match address LIST  
  set transform-set TSET  
  set pfs vko  
  set peer 10.0.0.1  
!  
interface GigabitEthernet0/0  
  ip address 192.168.2.1 255.255.255.0
```

```
!  
interface GigabitEthernet0/1  
  ip address 10.0.0.3 255.255.255.0  
  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 10.0.0.1  
!  
crypto pki trustpoint s-terra_technological_trustpoint  
  revocation-check none  
crypto pki certificate chain s-terra_technological_trustpoint  
certificate 4E4B0B11EFDB389E4E86244CDAA1B275  
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530  
...  
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713  
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F  
  
quit  
certificate 02A03970421DD6894F13B0315EFBC818  
308201E430820193A003020102021002A03970421DD6894F13B0315EFBC81830  
...  
F5B786894A1F63E8D823CBB0989339C2160E13DE27A9BD61BE5A1C28E4894D20  
A5521AFB0BCF89AB  
  
quit  
!  
end
```

Текст LSP конфигурации для шлюза GW1

```
# This is automatically generated LSP  
#  
# Conversion Date/Time: Wed May 29 14:11:00 2013  
  
GlobalParameters(  
  Title = "This LSP was automatically generated by CSP  
Converter at Wed May 29 14:11:00 2013"  
  Version = LSP_4_1  
  CRLHandlingMode = OPTIONAL  
  PreserveIPsecSA = FALSE  
)  
  
IKEParameters(  
  FragmentSize = 0  
)  
  
RoutingTable(  
  Routes =  
    Route(  
      Destination = 0.0.0.0/0  
      Gateway = 10.0.0.3  
    )  
  )  
)
```

```
FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg = "G2814789CPR01-K256-CBC-65534"
    HashAlg = "GR341194CPR01-65534"
    GroupID = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg* = "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID = IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode = ALWAYS
    SendCertMode = ALWAYS
)

IKERule IKERule:CMAP:1
(
    IKEPeerIPFilter = 10.0.0.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod = GOST:Sign
    MainModeAuthMethod = GOST:Sign
    DoNotUseDPD = TRUE
    Priority = 10
)

IPsecAction IPsecAction:CMAP:1
(
    TunnelingParameters = TunnelEntry(
        PeerIPAddress = 10.0.0.3
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1
)
```

```
FilterChain IPsecPolicy:CMAp (
  Filters = Filter (
    ProtocolID = 17
    SourcePort = 500, 4500
    Action = PASS
    PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
  ),
  Filter (
    SourceIP = 192.168.1.0/24
    DestinationIP = 192.168.2.0/24
    Action = PASS
    ExtendedAction = ipsec< sa = IPsecAction:CMAp:1 >
    LogEventID = "IPsec:Protect:CMAp:1:LIST"
  )
)

NetworkInterface (
  LogicalName = "GigabitEthernet0/1"
  IPsecPolicy = IPsecPolicy:CMAp
)
```

Текст LSP конфигурации для шлюза GW2

```
# This is automatically generated LSP
#
# Conversion Date/Time: Wed May 29 14:41:44 2013

GlobalParameters(
  Title = "This LSP was automatically generated by CSP
Converter at Wed May 29 14:41:44 2013"
  Version = LSP_4_1
  CRLHandlingMode = OPTIONAL
  PreserveIPsecSA = FALSE
)

IKEParameters(
  FragmentSize = 0
)

RoutingTable(
  Routes =
    Route(
      Destination = 0.0.0.0/0
      Gateway = 10.0.0.1
    )
)

FirewallParameters(
  TCPSynSentTimeout = 30
  TCPFinTimeout = 5
  TCPClosedTimeout = 30
  TCPSynRcvdTimeout = 30
  TCPEstablishedTimeout = 3600
  TCPHalfOpenLow = 400
  TCPHalfOpenMax = 500
  TCPSessionRateLow = 400
  TCPSessionRateMax = 500
)

IKETransform crypto:isakmp:policy:1
(
```

```
CipherAlg      = "G2814789CPR01-K256-CBC-65534"
HashAlg        = "GR341194CPR01-65534"
GroupID        = VKO_1B
RestrictAuthenticationTo = GOST_SIGN
LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*      = "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID          = IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode   = ALWAYS
    SendCertMode      = ALWAYS
)

IKERule IKERule:CMAP:1
(
    IKEPeerIPFilter = 10.0.0.1
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod = GOST:Sign
    MainModeAuthMethod = GOST:Sign
    DoNotUseDPD         = TRUE
    Priority             = 10
)

IPsecAction IPsecAction:CMAP:1
(
    TunnelingParameters = TunnelEntry(
        PeerIPAddress = 10.0.0.1
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.2.0/24
        DestinationIP = 192.168.1.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)
```

```
NetworkInterface (  
    LogicalName = "GigabitEthernet0/1"  
    IPsecPolicy = IPsecPolicy:CMAP  
)
```

Вариант 2 и 3

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 gost  
    hash gost  
    authentication sign  
    group vko  
!  
crypto ipsec transform-set TSET esp-gost4mimit  
!  
ip access-list extended LIST  
    permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255  
!  
!  
crypto map CMAP 1 ipsec-isakmp  
    match address LIST  
    set transform-set TSET  
    set pfs vko  
    set peer 10.0.0.3  
!  
interface GigabitEthernet0/0  
    ip address 192.168.1.1 255.255.255.0  
!  
interface GigabitEthernet0/1  
    ip address 10.0.0.1 255.255.255.0  
    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 10.0.0.3  
!  
crypto pki trustpoint s-terra_technological_trustpoint  
  revocation-check none  
crypto pki certificate chain s-terra_technological_trustpoint  
certificate 229FD2C02A1856894A9A524AD49553D4  
308201F2308201A1A0030201020210229FD2C02A1856894A9A524AD49553D430  
...  
68570883F6C6984D11A50B894EBA50BB44B6EBEF4A3013ED969A465DFC8A84E2  
E47F48CE536A0A441A6716E15787BA2AEAE025DAC319  
  
quit  
certificate 613B4E3000000000000002  
308202FA308202A9A003020102020A613B4E300000000000002300806062A8503  
...  
AB2B5291D7E89FC875C2C6E01ACB4D7010404CC1CBDF45546D624F93956D0E33  
D2AC7B93CA35A5D5A59A2714BE41A4BB0B2355FE1F2E9603055248CA7B77  
  
quit  
!  
end
```

Текст cisco-like конфигурации для шлюза GW2

```
!  
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 GW2  
enable password csp  
!  
!  
!  
logging trap debugging  
!  
!  
crypto isakmp policy 1  
  encr gost  
  hash gost  
  authentication sign  
  group vko  
!  
crypto ipsec transform-set TSET esp-gost4mimit  
!  
ip access-list extended LIST  
  permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255  
!  
!  
crypto map CMAP 1 ipsec-isakmp  
  match address LIST  
  set transform-set TSET  
  set pfs vko  
  set peer 10.0.0.1
```

```
!  
interface GigabitEthernet0/0  
  ip address 192.168.2.1 255.255.255.0  
!  
interface GigabitEthernet0/1  
  ip address 10.0.0.3 255.255.255.0  
  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 10.0.0.1  
!  
crypto pki trustpoint s-terra_technological_trustpoint  
  revocation-check none  
crypto pki certificate chain s-terra_technological_trustpoint  
certificate 229FD2C02A1856894A9A524AD49553D4  
308201F2308201A1A0030201020210229FD2C02A1856894A9A524AD49553D430  
...  
68570883F6C6984D11A50B894EBA50BB44B6EBEF4A3013ED969A465DFC8A84E2  
E47F48CE536A0A441A6716E15787BA2AEAE025DAC319  
  
quit  
!  
end
```

Текст LSP конфигурации для шлюза GW1

```
# This is automatically generated LSP  
#  
# Conversion Date/Time: Thu May 30 15:28:14 2013  
  
GlobalParameters(  
  Title = "This LSP was automatically generated by CSP  
Converter at Thu May 30 15:28:14 2013"  
  Version = LSP_4_1  
  CRLHandlingMode = OPTIONAL  
  PreserveIPsecSA = FALSE  
)  
  
IKEParameters(  
  FragmentSize = 0  
)  
  
RoutingTable(  
  Routes =  
    Route(  
      Destination = 0.0.0.0/0  
      Gateway = 10.0.0.3  
    )  
)  
  
FirewallParameters(  
  TCPSynSentTimeout = 30  
  TCPFinTimeout = 5
```

```

    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
)

CertDescription CA:GOST
(
    Issuer          = "C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA"
    SerialNumber    = "229fd2c02a1856894a9a524ad49553d4"
    Subject         = "C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA"
)

CertDescription CA:GOST$$1
(
    Issuer          = "C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA"
    SerialNumber    = "613b4e3000000000000002"
    Subject         = "C=RU,L=Moscow,O=S-Terra CSP,OU=Research,CN=SubCA"
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg       = "G2814789CPR01-K256-CBC-65534"
    HashAlg         = "GR341194CPR01-65534"
    GroupID         = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*       = "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds  = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID         = IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    AcceptCredentialFrom = CA:GOST, CA:GOST$$1
    SendRequestMode  = ALWAYS
    SendCertMode     = ALWAYS
)

IKERule IKERule:CMAF:1
(
    IKEPeerIPFilter = 10.0.0.3
    Transform       = crypto:isakmp:policy:1
    AggrModeAuthMethod = GOST:Sign
    MainModeAuthMethod = GOST:Sign
    DoNotUseDPD      = TRUE
    Priority         = 10
)

IPsecAction IPsecAction:CMAF:1

```

```
(
    TunnelingParameters = TunnelEntry(
        PeerIPAddress = 10.0.0.3
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
    GroupID = VKO_1B
    IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.1.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
        LogEventID = "IPsec:Protect:CMAP:1:LIST"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    IPsecPolicy = IPsecPolicy:CMAP
)
```

Текст LSP конфигурации для шлюза GW2

```
# This is automatically generated LSP
#
# Conversion Date/Time: Thu May 30 15:32:48 2013

GlobalParameters(
    Title = "This LSP was automatically generated by CSP
Converter at Thu May 30 15:32:48 2013"
    Version = LSP_4_1
    CRLHandlingMode = OPTIONAL
    PreserveIPsecSA = FALSE
)

IKEParameters(
    FragmentSize = 0
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 10.0.0.1
        )
)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
)
```

```
TCPClosedTimeout = 30
TCPSynRcvdTimeout = 30
TCPEstablishedTimeout = 3600
TCPHalfOpenLow = 400
TCPHalfOpenMax = 500
TCPSessionRateLow = 400
TCPSessionRateMax = 500
)

CertDescription CA:GOST
(
    Issuer          = "C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA"
    SerialNumber    = "229fd2c02a1856894a9a524ad49553d4"
    Subject         = "C=RU,L=Moscow,O=S-Terra CSP,OU=IT,CN=RootCA"
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg       = "G2814789CPR01-K256-CBC-65534"
    HashAlg         = "GR341194CPR01-65534"
    GroupID         = VKO_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal TSET:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*       = "G2814789CPR01-K288-CNTMAC-253"
        LifetimeSeconds   = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodGOSTSign GOST:Sign
(
    LocalID          = IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    AcceptCredentialFrom = CA:GOST, CA:GOST$$1
    SendRequestMode   = ALWAYS
    SendCertMode      = ALWAYS
)

IKERule IKERule:CMAp:1
(
    IKEPeerIPFilter = 10.0.0.1
    Transform       = crypto:isakmp:policy:1
    AggrModeAuthMethod = GOST:Sign
    MainModeAuthMethod = GOST:Sign
    DoNotUseDPD      = TRUE
    Priority         = 10
)

IPsecAction IPsecAction:CMAp:1
(
    TunnelingParameters = TunnelEntry(
        PeerIPAddress = 10.0.0.1
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( TSET:ESP )
)
```

```
GroupID = VKO_1B
IKERule = IKERule:CMAP:1
)

FilterChain IPsecPolicy:CMAP (
  Filters = Filter (
    ProtocolID = 17
    SourcePort = 500, 4500
    Action = PASS
    PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
  ),
  Filter (
    SourceIP = 192.168.2.0/24
    DestinationIP = 192.168.1.0/24
    Action = PASS
    ExtendedAction = ipsec< sa = IPsecAction:CMAP:1 >
    LogEventID = "IPsec:Protect:CMAP:1:LIST"
  )
)

NetworkInterface (
  LogicalName = "GigabitEthernet0/1"
  IPsecPolicy = IPsecPolicy:CMAP
)
```