Организация защищенного взаимодействия между подсетями при одновременном использовании нескольких УЦ (миграция УЦ)

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов. Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Введение

Данный сценарий описывает настройку безопасного взаимодействия между центральным офисом, двумя филиалами и удаленными VPN клиентами в случае, когда партнеры по IPsec используют локальные сертификаты, подписанные двумя разными удостоверяющими центрами. Сценарий также служит примером настройки для выполнения плавной миграции между используемыми УЦ.

Защищаемые подсети в LAN сегменте и недоверенные подсети в WAN сегменте – IPv4. Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec.

Партнеры по IPsec, в настоящем документе – криптошлюзы и удаленные VPN клиенты, для аутентификации будут использовать сертификаты в формате x509. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Шлюзы безопасности (или криптошлюзы) – «С-Терра Шлюз» версий 5.0 и 4.3, удаленные VPN клиенты – «С-Терра Клиент» версий 5.0 и 4.3.

На криптошлюзах версии 5.0 будет настроено межсетевое экранирование с применением статических списков доступа (ACL) и пакетной фильтрации с контролем состояния сессий (stateful, аналог CBAC в Cisco IOS) для протоколов TCP и UDP.

Предварительные требования

Требования к материально-техническому обеспечению

Для переноса запросов и сертификатов между криптошлюзами и центром выпуска сертификатов требуется USB Flash накопитель.

Требования к квалификации администратора

Администратор должен обладать обширными знаниями в области сетевой информационной безопасности, иметь опыт работы с аналогичным оборудованием/программным обеспечением, знать и понимать следующие технологии и протоколы: PKI, IPsec, NAT, Firewall, routing.

Администратор должен быть ознакомлен со сценарием «Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (протокол IPv4)». Далее по тексту он будет называться базовым сценарием.

Требования к инфраструктуре

1. Требования к устройствам.
   1.1. «С-Терра Шлюз».
      1.1.1. Устройства «С-Терра Шлюз» должны быть инициализированы (подробнее на https://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз <версия> -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).
   1.2. Центры выпуска сертификатов.
      1.2.1. Должны быть настроены два центра выпуска сертификатов (удостоверяющий центр, далее УЦ) для IPsec. Устройства с именами CA_old и CA_new на схеме.
      1.2.2. Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2016 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 5.0 (или новее).
      1.2.3. Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp).

      Категорически запрещено использование тестового УЦ от «КриптоПро» в производственной (боевой) эксплуатации, так как в данном случае отсутствует возможность контролировать процесс выпуска сертификатов и, соответственно, процедуру аутентификации.

   1.3. HTTP сервер для распространения списков отозванных сертификатов.
      1.3.1. Функционирующий HTTP сервер для распространения списков отозванных сертификатов (СОС) обоих удостоверяющих центров. Устройство с именем CRL_distribution_point на схеме. Если по объективным причинам использование СОС не представляется возможным или не требуется, то проверку СОС можно отключить в CLI «С-Терра Шлюз» (при соблюдении правил пользования).

      Доставка нового списка отозванных сертификатов с удостоверяющего центра на HTTP сервер должна происходить заблаговременно, до истечения срока действия предыдущего списка.

2. Требования к сетевому взаимодействию.
   2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

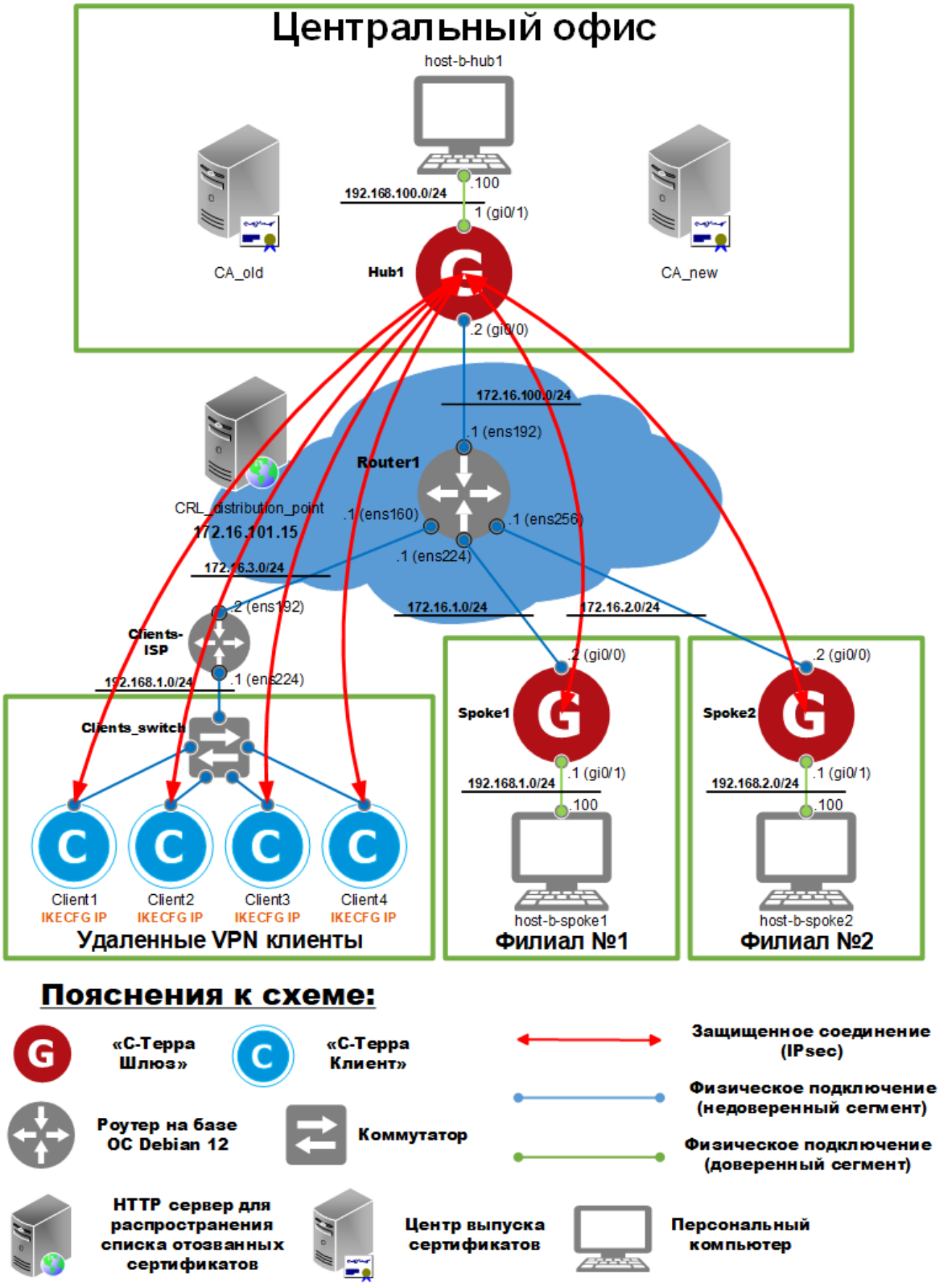


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центры выпуска сертификатов (CA_old и CA_new), криптошлюз «С-Терра Шлюз» (Hub1) и персональный компьютер (Host-b-hub1).

   1.2. В филиале №1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) и персональный компьютер (Host-b-spoke1).

   1.3. В филиале №2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2) и персональный компьютер (Host-b-spoke2).

   1.4. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списков отозванных сертификатов (CRL_distribution_point), маршрутизаторы (Router1 и Clients-ISP) и персональные компьютеры (Client1, Client2, Client3 и Client4).

2. Подключение к сети Интернет.

   В данном сценарии для эмуляции сети Интернет используются маршрутизатор Router1.

   Подключение к сети Интернет на устройствах «С-Терра Шлюз» будет считаться успешным, если по протоколу ICMP (или «ping») будет доступен HTTP сервер для распространения списков отозванных сертификатов (устройство CRL_distribution_point на схеме).

   2.1. Криптошлюзы Hub1, Spoke1 и Spoke2 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   2.2. Адресные пространства подсети Филиала №1 и подсети, в которой размещены VPN-клиенты пересекаются, но использование IKECFG адресов полностью исключает связанные с этим проблемы при одновременном доступе VPN-клиентов и рабочих станций Филиала №1 в подсеть Центрального офиса.

3. Использование нескольких УЦ.

   В данном сценарии используется два удостоверяющих центра. Центральный шлюз имеет два локальных сертификата, каждый из которых выпущен соответствующим УЦ. На центральном шлюзе также должны присутствовать сертификаты обоих удостоверяющих центров (CA_old и CA_new).

   Для криптошлюза Spoke1 локальный сертификат выпущен на УЦ CA_old, для криптошлюза Spoke2 локальный сертификат выпущен на УЦ CA_new.

   Локальные сертификаты удаленных VPN клиентов Client1 и Client4 выданы на УЦ CA_old, Client2 и Client3 – на УЦ CA_new.

   В данном сценарии DN сертификатов УЦ выглядят следующим образом:

   - CA_old: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
   - CA_new: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA

   На основе содержимого атрибута CN поля Issuer в присланном сертификате партнера по IPsec будет выполняться выбор (на центральном криптошлюзе) подходящего локального сертификата.

   DN сертификатов удостоверяющих центров должны различаться между собой.

4. ISAKMP профили.

   В данном сценарии на центральном шлюзе настраиваются ISAKMP профили, которые позволяют шлюзу выбирать правильный локальный сертификат при построении защищенного соединения с партнерами в зависимости от локального сертификата партнера. ISAKMP профили также содержат несколько IKE политик, позволяя использовать новые алгоритмы шифрования, если они поддерживаются партнерами.

5. Параметры шифрования IPsec.

Весь трафик между подсетями центрального офиса (192.168.100.0/24), филиалов (192.168.1.0/24, 192.168.2.0/24) и удаленными VPN клиентами защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном IPv4 режиме.

Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke1 может трафик из подсети филиала №1 (192.168.1.0/24) в подсеть центра (192.168.100.0/24) и наоборот из центра в филиал.

Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke2 может трафик из подсети филиала №2 (192.168.2.0/24) в подсеть центра (192.168.100.0/24) и наоборот из центра в филиал.

Инициировать защищенное соединение между подсетью центрального офиса и удаленными VPN клиентами может только трафик от VPN клиентов в центр.

5.1. Параметры протокола IKE

5.1.1. Параметры протокола IKE для версии 5.0:

- Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
- Алгоритм шифрования – ГОСТ Р 34.12-2015 Магма (ключ 256 бит);
- Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 Стрибог (ключ 256 бит);
- Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

5.1.2. Параметры протокола IKE для совместимости с версией 4.3:

- Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
- Алгоритм шифрования – ГОСТ 28147-89 (ключ 256 бит);
- Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 (ключ 256 бит);
- Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

5.2. Параметры протокола ESP

5.2.1. Параметры протокола ESP для версии 5.0:

- Комбинированный алгоритм шифрования и имитозащиты (контроль целостности) – ГОСТ Р 34.12-2015 Магма в режиме MGM (ключ 256 бит).

5.2.2. Параметры протокола ESP для совместимости с версией 4.3:

- Комбинированный алгоритм шифрования и имитозащиты (контроль целостности) – ESP_GOST-4M-IMIT (ключ 256 бит).

Настройка стенда

Настройка устройства Router1

1. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Настройте IP адрес – 172.16.2.1 и маску – 255.255.255.0 на сетевом интерфейсе ens256.
4. Настройте IP адрес – 172.16.3.1 и маску – 255.255.255.0 на сетевом интерфейсе ens160.
5. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Clients-ISP

1. Настройте IP адрес – 172.16.3.2 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 192.168.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.

3. Задайте маршрут по умолчанию через 172.16.3.1.
4. Настройте выдачу IP адресов по DHCP на интерфейсе ens224 из незанятого диапазона подсети 192.168.1.0/24.
5. Настройте Source NAT на сетевом интерфейсе ens192, транслирующий трафик из подсети 192.168.1.0/24 в адрес 172.16.3.2.
6. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Host-b-hub1

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke1

1. Настройте IP адрес – 192.168.1.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.1.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke2

1. Настройте IP адрес – 192.168.2.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.2.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройств Client1, Client2, Client3 и Client4

1. Настройте получение IP адреса по DHCP на сетевом интерфейсе.
2. Разрешите прием и отправку IP пакетов.

Настройка криптошлюза Hub1

Настройка будет происходить локально при помощи консольного подключения.

Настройка может осуществляться и удаленно (по SSH), но исключительно по доверенному каналу связи. Доверенным каналом связи может считаться канал в пределах контролируемой зоны в случае отсутствия в нем нарушителя. Доверенным каналом связи также считается канал, защищенный при помощи протокола IPsec.

Начальные настройки

Дата и время на всех криптошлюзах и УЦ должны быть одинаковы, так как для аутентификации используются цифровые сертификаты, в которых зафиксированы дата и время начала их действия и окончания. Также одинаковые дата и время на всей инфраструктуре облегчают поиск неисправностей по лог-файлам.

Войдите в CLI разграничения доступа (пользователь и пароль по умолчанию: `administrator`, `s-terra`) установите правильный тип терминала и требуемую ширину, смените пароль для пользователя `administrator`.

Перейдите в linux bash консоль, установите пароль для пользователя `root`, правильное время и временную зону.

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройки PKI (запросы и сертификаты)

Продукт не поддерживает разностные (delta) списки отзыва сертификатов, только базовые. Учитывайте это при выборе или развертывании УЦ.

Для аутентификации партнеров по IPsec можно использовать цифровые сертификаты, выпущенные при помощи сертифицированного СКЗИ, или предварительно распределенные ключи, созданные и введённые в соответствии с правилами пользования СКЗИ (появились в версии 5.0).

Сгенерируйте запрос на первый сертификат криптошлюза и сохраните этот запрос в файл на USB Flash накопителе. Доставьте файл с запросом на УЦ CA_old и выпустите по нему сертификат. Сертификат криптошлюза вместе с сертификатом УЦ доставьте на шлюз и импортируйте их в базу С-Терра Шлюз.

Аналогичным образом получите второй сертификат криптошлюза, подписанный на УЦ CA_new, и импортируйте его в базу С-Терра Шлюз вместе с сертификатом УЦ CA_new.

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка паролей доступа к консоли cisco-like

Войдите в cisco-like консоль и смените пароль для пользователя `cscons` (пароль по умолчанию: csp) и пароль на enable (пароль по умолчанию: csp).

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка сетевых параметров

1. Задайте имя устройства:

```
sterragate(config)#hostname Hub1
```

2. Включите внешний (`GigabitEthernet0/0`) и внутренний (`GigabitEthernet0/1`) интерфейсы:

```
Hub1(config)#interface range GigabitEthernet 0/0 - 1
Hub1(config-if-range)#no shutdown
Hub1(config-if-range)#exit
```

3. Убедитесь, что интерфейсы административно включены и line protocol (способность интерфейса передавать пакеты в данный момент) находится в состоянии up:

```
Hub1(config)#do show interfaces
```

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 0050.569e.94c4
  MTU 1500 bytes
GigabitEthernet0/1 is up, line protocol is up
  Hardware address is 0050.569e.7f79
  MTU 1500 bytes
...
```

Если line protocol находится в состоянии down, то проверьте подключение сетевого интерфейса криптошлюза к коммутационному или прочему оборудованию.

4. Настройте IP адреса на внешнем и внутренних интерфейсах в соответствии со схемой стенда:

```
Hub1(config)#interface GigabitEthernet 0/0
Hub1(config-if)#ip address 172.16.100.2 255.255.255.0
Hub1(config-if)#exit
Hub1(config)#interface GigabitEthernet 0/1
Hub1(config-if)#ip address 192.168.100.1 255.255.255.0
Hub1(config-if)#exit
```

5. Задайте маршрут по умолчанию через устройство Router1:

```
Hub1(config)#ip route 0.0.0.0 0.0.0.0 172.16.100.1
```

6. Проверьте доступность устройства Router1:

```
Hub1(config)#do ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=0.503 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.340 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.512 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.449 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.414 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4074ms
rtt min/avg/max/mdev = 0.340/0.443/0.512/0.063 ms
```

Настройка шифрования

1. Создайте IKECFG пул адресов, из которого будут назначаться IKECFG адреса для удаленных VPN клиентов:

```
Hub1(config)#ip local pool IKECFG_POOL 192.168.255.1 192.168.255.254
```

2. Настройте параметры IKE.

   2.1. Задайте общие параметры IKE:

```
Hub1(config)#crypto isakmp identity dn
Hub1(config)#crypto isakmp keepalive 3 2
Hub1(config)#crypto isakmp keepalive retry-count 5
Hub1(config)#crypto isakmp fragmentation
Hub1(config)#crypto isakmp security-association lifetime delta 50
Hub1(config)#crypto isakmp initiator-sessions-max 100
Hub1(config)#crypto isakmp responder-sessions-max 100
```

   2.2. Создайте две IKE политики:

      2.2.1 Создайте первую политику, описывающую параметры IKE туннеля при взаимодействии с партнерами (шлюзами и клиентами) версии 5.0, с использованием алгоритма шифрования GOST R 34.12-2015 Magma:

```
Hub1(config)#crypto isakmp policy 1
Hub1(config-isakmp)#encryption magma
Hub1(config-isakmp)#hash stribog-256
Hub1(config-isakmp)#authentication gost-sig
Hub1(config-isakmp)#group vko2
Hub1(config-isakmp)#exit
```

      2.2.2 Создайте вторую политику, описывающую параметры IKE туннеля при взаимодействии с партнерами (шлюзами и клиентами) версии 4.3, с использованием алгоритма шифрования GOST 28147-89:

```
Hub1(config)#crypto isakmp policy 2
Hub1(config-isakmp)#encryption gost
Hub1(config-isakmp)#hash stribog-256
Hub1(config-isakmp)#authentication gost-sig
Hub1(config-isakmp)#group vko2
Hub1(config-isakmp)#exit
```

   2.3. Создайте два раздела с описанием сертификатов:

      2.3.1 Создайте раздел с именем `OLD_CA`, который будет содержать описание сертификатов, выпущенных на УЦ CA_old (в данном случае выбираться будут сертификаты, у которых в поле Issuer содержится строка “CN=Old Root CA”):

```
Hub1(config)#crypto pki certificate map OLD_CA 1
Hub1(ca-certificate-map)#issuer-name co CN=Old Root CA
Hub1(ca-certificate-map)#exit
```

2.3.2 Создайте раздел с именем NEW_CA, который будет содержать описание сертификатов, выпущенных на УЦ CA_new (в данном случае выбираться будут сертификаты, у которых в поле Issuer содержится строка “CN=New Root CA”):

```
Hub1(config)#crypto pki certificate map NEW_CA 1
Hub1(ca-certificate-map)#issuer-name co CN=New Root CA
Hub1(ca-certificate-map)#exit
```

2.4. Создайте два ISAKMP профиля, которые позволят шлюзу выбирать правильный локальный сертификат на основе сертификата партнера и подходящую IKE политику при построении IKE SA:

2.4.1 Создайте ISAKMP профиль с именем OLD_CA_PROFILE:

```
Hub1(config)#crypto isakmp profile OLD_CA_PROFILE
```

2.4.2 Задайте фильтр по сертификату партнера на основе созданного ранее описания OLD_CA:

```
Hub1(conf-isa-prof)#match certificate OLD_CA
```

2.4.3 Укажите использование локального сертификата на основе созданного ранее описания OLD_CA:

```
Hub1(conf-isa-prof)#self-certificate OLD_CA
```

2.4.4 Задайте IKE политики, при этом первой (самой приоритетной) укажите политику 1, затем политику 2:

```
Hub1(conf-isa-prof)#set policy 1
Hub1(conf-isa-prof)#set policy 2
Hub1(conf-isa-prof)#exit
```

2.5. Создайте ISAKMP профиль с именем NEW_CA_PROFILE:

```
Hub1(config)#crypto isakmp profile NEW_CA_PROFILE
```

2.5.1 Задайте фильтр по сертификату партнера на основе созданного ранее описания NEW_CA:

```
Hub1(conf-isa-prof)#match certificate NEW_CA
```

2.5.2 Укажите использование локального сертификата на основе созданного ранее описания NEW_CA:

```
Hub1(conf-isa-prof)#self-certificate NEW_CA
```

2.5.3 Задайте IKE политики, при этом первой (самой приоритетной) укажите политику 1, затем политику 2:

```
Hub1(conf-isa-prof)#set policy 1
Hub1(conf-isa-prof)#set policy 2
Hub1(conf-isa-prof)#exit
```

3. **Альтернативный вариант** настройки для случая, когда DN сертификатов двух удостоверяющих центров полностью совпадают и, соответственно, нет возможности разделять сертификаты на основе содержимого полей в DN. В таком случае можно использовать серийные номера сертификатов.

Серийные номера сертификатов можно посмотреть в выводе команды run cert_mgr show -i N, где N – порядковый номер сертификата в локальной базе криптошлюза.

3.1. Создайте раздел с описанием сертификата, в котором укажите серийный номер сертификата УЦ Old_CA:

```
Hub1(config)#crypto pki certificate map TRUSTED_CERT_NUM_OLD_CA 1
Hub1(ca-certificate-map)#serial-number eq 7a61d9f11fcc1fb64dc52516f3a49437
Hub1(ca-certificate-map)#exit
```

3.2. Создайте раздел с описанием сертификата, в котором укажите серийный номер сертификата УЦ New_CA:

```
Hub1(config)#crypto pki certificate map TRUSTED_CERT_NUM_NEW_CA 1
Hub1(ca-certificate-map)#serial-number eq 16a86c112f82928244e9884260c0f61c
Hub1(ca-certificate-map)#exit
```

3.3. Создайте раздел с описанием сертификата, в котором укажите серийный номер локального сертификата криптошлюза Hub1, выпущенный на УЦ Old_CA:

```
Hub1(config)#crypto pki certificate map LOCAL_CERT_NUM_OLD_CA 1
Hub1(ca-certificate-map)#serial-number eq 5a000000061aab72369dd00171000000000006
Hub1(ca-certificate-map)#exit
```

3.4. Создайте раздел с описанием сертификата, в котором укажите серийный номер локального сертификата криптошлюза Hub1, выпущенный на УЦ New_CA:

```
Hub1(config)#crypto pki certificate map LOCAL_CERT_NUM_NEW_CA 1
Hub1(ca-certificate-map)#serial-number eq 4a000000065edda9c56b7eea68000000000006
Hub1(ca-certificate-map)#exit
```

3.5. Создайте ISAKMP профиль, который будет использоваться при построении IKE сессии с партнерами с использованием сертификатов, выпущенных на УЦ Old_CA:

```
Hub1(config)#crypto isakmp profile OLD_CA_PROFILE
Hub1(conf-isa-prof)#match identity dn
Hub1(conf-isa-prof)#ca trust-point TRUSTED_CERT_NUM_OLD_CA
Hub1(conf-isa-prof)#self-certificate LOCAL_CERT_NUM_OLD_CA
Hub1(conf-isa-prof)#set policy 1
Hub1(conf-isa-prof)#set policy 2
Hub1(conf-isa-prof)#exit
```

3.6. Создайте ISAKMP профиль, который будет использоваться при построении IKE сессии с партнерами с использованием сертификатов, выпущенных на УЦ New_CA:

```
Hub1(config)#crypto isakmp profile NEW_CA_PROFILE
Hub1(conf-isa-prof)#match identity dn
Hub1(conf-isa-prof)#ca trust-point TRUSTED_CERT_NUM_NEW_CA
Hub1(conf-isa-prof)#self-certificate LOCAL_CERT_NUM_NEW_CA
Hub1(conf-isa-prof)#set policy 1
Hub1(conf-isa-prof)#set policy 2
Hub1(conf-isa-prof)#exit
```

На этом альтернативный вариант настройки завершен.

4. Настройте параметры IPsec.

4.1. Отключите обновление ключа IPsec SA по достижению определенного объема переданного трафика:

```
Hub1(config)#crypto ipsec security-association lifetime kilobytes unlimited
```

4.2. Создайте IPsec трансформ, задающий комбинированный алгоритм шифрования и имитозащиты ГОСТ 34.12-2015 Магма в режиме MGM для трафика (для версий 5.0):

```
Hub1(config)#crypto ipsec transform-set MAGMA_ENCRYPT_AND_INTEGRITY esp-magma-mgm
Hub1(cfg-crypto-trans)#exit
```

4.3. Создайте IPsec трансформ, задающий комбинированный алгоритм шифрования и имитозащиты на базе ГОСТ 28147-89 для трафика (для версий 4.3):

```
Hub1(config)# crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-
imit
Hub1(cfg-crypto-trans)#exit
```

4.4. Создайте список доступа (ACL) для трафика, который нужно защищать между центральным офисом и филиалом №1:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_SPOKE1
Hub1(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
Hub1(config-ext-nacl)#exit
```

4.5. Создайте список доступа (ACL) для трафика, который нужно защищать между центральным офисом и филиалом №2:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_SPOKE2
Hub1(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 192.168.2.0 0.0.0.255
Hub1(config-ext-nacl)#exit
```

4.6. Создайте список доступа (ACL) для трафика, который нужно защищать между центральным офисом и удаленными VPN клиентами:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_CLIENTS
Hub1(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
Hub1(config-ext-nacl)#exit
```

4.7. Создайте крипто-карту (имя VPN, раздел 1. Данный раздел будет содержать параметры защищенного соединения с партнером Spoke1, с использованием сертификатов, выпущенных на УЦ CA_old):

```
Hub1(config)#crypto map VPN 1 ipsec-isakmp
```

4.7.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_SPOKE1
```

4.7.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

```
Hub1(config-crypto-map)#set transform-set GOST_ENCRYPT_AND_INTEGRITY
```

4.7.3 Укажите IP адрес партнера по IPsec, в данном сценарии это внешний IP адрес устройства Spoke1:

```
Hub1(config-crypto-map)#set peer 172.16.1.2
```

4.7.4 Укажите ISAKMP профиль `OLD_CA_PROFILE`:

```
Hub1(config-crypto-map)#set isakmp-profile OLD_CA_PROFILE
```

4.7.5 Обязательно отключите историю удаленных туннелей (если не отключить, то могут быть проблемы с построением IPsec туннелей с устройствами, которые находятся за NAT):

```
Hub1(config-crypto-map)# set dead-connection history off
Hub1(config-crypto-map)#exit
```

4.8. Создайте крипто-карту (имя VPN, раздел 2. Данный раздел будет содержать параметры защищенного соединения с партнером Spoke2, с использованием сертификатов, выпущенных на УЦ CA_new):

```
Hub1(config)#crypto map VPN 2 ipsec-isakmp
```

4.8.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_SPOKE2
```

4.8.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

```
Hub1(config-crypto-map)#set transform-set MAGMA_ENCRYPT_AND_INTEGRITY
```

4.8.3 Укажите IP адрес партнера по IPsec, в данном сценарии это внешний IP адрес устройства Spoke2:

```
Hub1(config-crypto-map)#set peer 172.16.2.2
```

4.8.4 Укажите ISAKMP профиль `NEW_CA_PROFILE`:

```
Hub1(config-crypto-map)#set isakmp-profile NEW_CA_PROFILE
```

4.8.5 Обязательно отключите историю удаленных туннелей (если не отключить, то могут быть проблемы с построением IPsec туннелей с устройствами, которые находятся за NAT):

```
Hub1(config-crypto-map)# set dead-connection history off
Hub1(config-crypto-map)#exit
```

4.9. Создайте динамическую крипто-карту (имя DMAP, раздел 1. Данный раздел будет содержать параметры защищенного соединения с удаленными VPN клиентами с использованием сертификатов, выпущенных на УЦ CA_old):

```
Hub1(config)#crypto dynamic-map DMAP 1
```

4.9.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_CLIENTS
```

4.9.2 Укажите два набора алгоритмов для защиты трафика, первым указав `MAGMA_ENCRYPT_AND_INTEGRITY`, вторым (через пробел) `GOST_ENCRYPT_AND_INTEGRITY`:

```
Hub1(config-crypto-map)#set transform-set MAGMA_ENCRYPT_AND_INTEGRITY
GOST_ENCRYPT_AND_INTEGRITY
```

4.9.3 Укажите IKECFG пул:

```
Hub1(config-crypto-map)#set pool IKECFG_POOL
```

4.9.4 Укажите ISAKMP профиль `OLD_CA_PROFILE`:

```
Hub1(config-crypto-map)#set isakmp-profile OLD_CA_PROFILE
```

4.9.5 Обязательно отключите историю удаленных туннелей (если не отключить, то могут быть проблемы с построением IPsec туннелей с устройствами, которые находятся за NAT):

```
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

4.10. Создайте динамическую крипто-карту (имя DMAP, раздел 2. Данный раздел будет содержать параметры защищенного соединения с удаленными VPN клиентами с использованием сертификатов, выпущенных на УЦ CA_new):

```
Hub1(config)#crypto dynamic-map DMAP 2
```

4.10.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_CLIENTS
```

4.10.2 Укажите два набора алгоритмов для защиты трафика, первым указав `MAGMA_ENCRYPT_AND_INTEGRITY`, вторым (через пробел) `GOST_ENCRYPT_AND_INTEGRITY`:

```
Hub1(config-crypto-map)#set transform-set MAGMA_ENCRYPT_AND_INTEGRITY
GOST_ENCRYPT_AND_INTEGRITY
```

4.10.3 Укажите IKECFG пул:

```
Hub1(config-crypto-map)#set pool IKECFG_POOL
```

4.10.4 Укажите ISAKMP профиль `NEW_CA_PROFILE`:

```
Hub1(config-crypto-map)#set isakmp-profile NEW_CA_PROFILE
```

4.10.5 Обязательно отключите историю удаленных туннелей (если не отключить, то могут быть проблемы с построением IPsec туннелей с устройствами, которые находятся за NAT):

```
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

4.11. Добавьте динамическую крипто-карту DMAP в третий раздел криптокарты VPN:

```
Hub1(config)#crypto map VPN 3 ipsec-isakmp dynamic DMAP
Hub1(config-crypto-map)#exit
```

4.12. Прикрепите крипто-карту `VPN` к внешнему интерфейсу `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#crypto map VPN
Hub1(config-if)#exit
```

4.13. Примените настройки:

```
Hub1(config)#end
```

Настройка политики обработки COC (CRL)

В целях безопасности настоятельно рекомендуется включать проверку списков отзыва сертификатов. Разностные списки отозванных сертификатов (delta CRL) не поддерживаются.

Включите проверку COC и настройте автоматическую загрузку и импорт в базу Продукта списков отозванных сертификатов обоих УЦ. Загрузка будет выполняться с HTTP сервера CRL_distribution_point.

Поддерживается возможность указания нескольких URL для загрузки COC, например:

```
Hub1(ca-trustpoint)#crl download group NEW_CA_CRL http://172.16.101.15/NEW_CA.crl
Hub1(ca-trustpoint)#crl download group OLD_CA_CRL http://172.16.101.15/OLD_CA.crl
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка межсетевого экрана

1. Создайте сетевой `object-group` с именем `SELF` для хранения в нем WAN адресов криптошлюза:

```
Hub1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hub1(config)#object-group network SELF
Hub1(config-network-group)#remark WAN IP
Hub1(config-network-group)#host 172.16.100.2
Hub1(config-network-group)#exit
```

2. Создайте ACL с именем `FW_INPUT_WAN` для входящего на WAN интерфейс трафика:

```
Hub1(config)#ip access-list extended FW_INPUT_WAN
Hub1(config-ext-nacl)#permit udp any object-group SELF eq isakmp
Hub1(config-ext-nacl)#permit udp any object-group SELF eq non500-isakmp
Hub1(config-ext-nacl)#permit icmp any object-group SELF
Hub1(config-ext-nacl)#permit esp any object-group SELF
Hub1(config-ext-nacl)#exit
```

3. Создайте правила инспектирования всего TCP и UDP трафика и задайте необходимое максимальное количество сессий:

```
Hub1(config)#ip inspect name INSPECT tcp
Hub1(config)#ip inspect name INSPECT udp
Hub1(config)#ip inspect tcp sessions-max 256000
Hub1(config)#ip inspect udp sessions-max 65536
```

4. Прикрепите правила межсетевого экранирования на WAN интерфейс `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#ip access-group FW_INPUT_WAN in
Hub1(config-if)#ip inspect INSPECT out
Hub1(config-if)#exit
```

5. Примените настройки:

```
Hub1(config)#end
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke1

Настройка криптошлюза происходит аналогично настройке Hub1. ISAKMP профили отсутствуют, используется только одна политика для IKE.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP;

Настройка криптошлюза Spoke2

Настройка криптошлюза происходит аналогично настройке Hub1. Используется один ISAKMP профиль и одна IKE политика.

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP;

Настройка удаленных VPN клиентов

Развертывание VPN клиентов «С-Терра Клиент» выполняется с помощью «С-Терра ГСУ» 5.0 или «С-Терра AdminTool» 5.0. Подробная настройка приводится в соответствующем сценарии.

Примечание: при формировании политики безопасности для «С-Терра Клиент 5.0» следует убедиться в том, что новые алгоритмы шифрования в IKE и ESP являются более приоритетными, чем старые алгоритмы, используемые в версии 4.3.

В Приложении представлен текст конфигурации для Client1, Client2, Client3 и Client4:

- текст LSP

Проверка работоспособности стенда

Проверка IP связности

6. Проверьте, что с криптошлюзов Hub1, Spoke1 и Spoke2 доступен маршрутизатор Router1. Для этого выполните команду ping из cisco-like консоли криптошлюзов (пример вывода для Hub1):

```
Hub1#ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=0.290 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.433 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.404 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.616 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.501 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4076ms
rtt min/avg/max/mdev = 0.290/0.448/0.616/0.107 ms
```

7. Проверьте, что со всех защищаемых устройств доступен их соответствующий шлюз по умолчанию. Для этого выполните команду ping из консоли защищаемых устройств (пример вывода для host1-behind-hub1):

```
root@Host-b-hub1:~# ping 192.168.100.1 -c 4
```

```
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.118 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.337 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.238 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.268 ms

--- 192.168.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.118/0.240/0.337/0.079 ms
```

Проверка PKI

1. Проверьте, что на всех криптошлюзах присутствуют локальный и доверенный сертификаты, а также CRL (если загрузка списка отозванных сертификатов была настроена). Для этого выполните следующие команды из cisco-like консоли криптошлюзов:

```
Hub1#run cert_mgr show
```

```
Found 4 certificates. Found 2 CRLs.
1 Status: trusted OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
3 Status: trusted OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
4 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
5 CRL: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
6 CRL: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
```

```
Hub1#run cert_mgr check
```

```
1 State: Active   OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
3 State: Active   OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
```

```
Spoke1#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1
2 Status: trusted OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
3 CRL: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
```

```
Spoke1#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1
2 State: Active   OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=Old Root CA
```

```
Spoke2#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2
2 Status: trusted OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
3 CRL: OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
```

```
Spoke2#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2
2 State: Active   OU=RnD,O=S-Terra CSP,L=Zelenograd,C=RU,CN=New Root CA
```

Проверка построения защищенного соединения

1. Инициируйте построение защищенного соединения между криптошлюзами Hub1 и Spoke1 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke1 на Host-b-hub1 (или в обратную сторону).
2. Инициируйте построение защищенного соединения между криптошлюзами Hub1 и Spoke2 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke2 на Host-b-hub1 (или в обратную сторону).
3. Инициируйте построение защищенного соединения между удаленными VPN клиентами и криптошлюзом Hub1. Для этого следует пройти аутентификацию в окне аутентификации ПО «С-Терра Клиент» на устройствах Client1, Client2, Client3 и Client4, и отправить ICMP запросы на устройство Host-b-hub1.
4. Убедитесь, что на криптошлюзе Hub1 установлены защищенные соединения. Для этого выполните команду `run sa_mgr show` в cisco-like консоли криптошлюза:

```
Hub1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 20 (172.16.100.2,500)-(172.16.1.2,500) active 2028 2012
2 21 (172.16.100.2,500)-(172.16.2.2,500) active 2048 2080
3 22 (172.16.100.2,4500)-(172.16.3.2,4500) active 2128 2536
4 23 (172.16.100.2,4500)-(172.16.3.2,57535) active 2128 2480
5 24 (172.16.100.2,4500)-(172.16.3.2,60024) active 2128 2536
6 25 (172.16.100.2,4500)-(172.16.3.2,62289) active 2128 2480

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 17 (192.168.100.0-192.168.100.255,*)-(192.168.1.0-192.168.1.255,*) * ESP tunn 264
264
2 18 (192.168.100.0-192.168.100.255,*)-(192.168.2.0-192.168.2.255,*) * ESP tunn 176
176
3 19 (192.168.100.0-192.168.100.255,*)-(192.168.255.2,*) * ESP nat-t-tunn 264 264
4 20 (192.168.100.0-192.168.100.255,*)-(192.168.255.1,*) * ESP nat-t3-tunn 264 264
5 21 (192.168.100.0-192.168.100.255,*)-(192.168.255.4,*) * ESP nat-t-tunn 264 264
6 22 (192.168.100.0-192.168.100.255,*)-(192.168.255.3,*) * ESP nat-t3-tunn 264 264
```

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
```

```
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$y$j9T$qQiNawK8p8oXCUsxE287z1$HLiG4hhXSBcVWxOEo1CRTX/wj1Yb0zKepZxbYxo6MS8
aaa new-model
!
!
hostname Hub1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
crypto pki certificate map OLD_CA 1
 issuer-name co CN=Old Root CA
crypto pki certificate map NEW_CA 1
 issuer-name co CN=New Root CA
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp policy 2
 encr gost
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile OLD_CA_PROFILE
 match certificate OLD_CA
 self-certificate OLD_CA
 set identity mapping
 set policy 1
 set policy 2
!
crypto isakmp profile NEW_CA_PROFILE
 match certificate NEW_CA
 self-certificate NEW_CA
 set identity mapping
 set policy 1
 set policy 2
!
ip local pool IKECFG_POOL 192.168.255.1 192.168.255.254
!
crypto ipsec transform-set MAGMA_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
!
ip access-list extended IPSEC_ACL_HUB1_SPOKE1
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
```

```
!
ip access-list extended IPSEC_ACL_HUB1_SPOKE2
 permit ip 192.168.100.0 0.0.0.255 192.168.2.0 0.0.0.255
!
ip access-list extended IPSEC_ACL_HUB1_CLIENTS
 permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_ACL_HUB1_CLIENTS
 set transform-set MAGMA_ENCRYPT_AND_INTEGRITY GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_CA_PROFILE
 set pool IKECFG_POOL
 set pre-fragmentation
 set dead-connection history off
crypto dynamic-map DMAP 2
 match address IPSEC_ACL_HUB1_CLIENTS
 set transform-set MAGMA_ENCRYPT_AND_INTEGRITY GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile OLD_CA_PROFILE
 set pool IKECFG_POOL
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_SPOKE1
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile OLD_CA_PROFILE
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 2 ipsec-isakmp
 match address IPSEC_ACL_HUB1_SPOKE2
 set transform-set MAGMA_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_CA_PROFILE
 set peer 172.16.2.2
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 3 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 172.16.100.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
```

```
 revocation-check crl
 crl download group NEW_CA_CRL http://172.16.101.15/NEW_CA.crl
 crl download group OLD_CA_CRL http://172.16.101.15/OLD_CA.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 15B67BF70980C7AD4B97B3A516758E76
...
4436194085

quit
certificate 1C2F1E21A226ADBF4355135842D25DC8
...
F39223341C

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Mar 20 16:23:27 2024

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Wed Mar 20 16:23:27 2024 (user: root)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.100.1
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

CertDescription OLD_CA:1
(
    Issuer             = TEMPLATE, "CN=Old Root CA"
)

CertDescription NEW_CA:1
```

```
(
    Issuer             = TEMPLATE, "CN=New Root CA"
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

IKETransform crypto:isakmp:policy:2
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO2-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
    )
)

ESPProposal MAGMA_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
```

```
        DestinationIP = 172.16.100.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Local:Cert:OLD_CA_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_CA_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

AddressPool IKECFG_POOL
(
    IPAddresses = 192.168.255.1..192.168.255.254
)

FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
```

```
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:OLD_CA_PROFILE
(
    LocalID              = Local:Cert:OLD_CA_PROFILE
    LocalCredential      = OLD_CA:1
    RemoteCredential     = OLD_CA:1
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

AuthMethodGOSTSign GOST:Sign:NEW_CA_PROFILE
(
    LocalID              = Local:Cert:NEW_CA_PROFILE
    LocalCredential      = NEW_CA:1
    RemoteCredential     = NEW_CA:1
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.1.2
    Transform = crypto:isakmp:policy:1, crypto:isakmp:policy:2
    AggrModeAuthMethod  = GOST:Sign:OLD_CA_PROFILE
    MainModeAuthMethod  = GOST:Sign:OLD_CA_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:VPN:2
(
    IKEPeerIPFilter = 172.16.2.2
    Transform = crypto:isakmp:policy:1, crypto:isakmp:policy:2
    AggrModeAuthMethod  = GOST:Sign:NEW_CA_PROFILE
    MainModeAuthMethod  = GOST:Sign:NEW_CA_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 20
)

IKERule IKERule:VPN:3:DMAP:1
(
    Transform = crypto:isakmp:policy:1, crypto:isakmp:policy:2
    AggrModeAuthMethod  = GOST:Sign:NEW_CA_PROFILE
    MainModeAuthMethod  = GOST:Sign:NEW_CA_PROFILE
    IKECFGPool          = IKECFG_POOL
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

IKERule IKERule:VPN:3:DMAP:2
(
```

```
    Transform = crypto:isakmp:policy:1, crypto:isakmp:policy:2
    AggrModeAuthMethod  = GOST:Sign:OLD_CA_PROFILE
    MainModeAuthMethod  = GOST:Sign:OLD_CA_PROFILE
    IKECFGPool          = IKECFG_POOL
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 110
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.1.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

IPsecAction IPsecAction:VPN:2
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.2.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:2
)

IPsecAction IPsecAction:VPN:3:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals     =     (     MAGMA_ENCRYPT_AND_INTEGRITY:ESP     ),     (
GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:3:DMAP:1
)

IPsecAction IPsecAction:VPN:3:DMAP:2
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals     =     (     MAGMA_ENCRYPT_AND_INTEGRITY:ESP     ),     (
GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:3:DMAP:2
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
```

```
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.1.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_HUB1_SPOKE1"
    ),
    Filter (
        Label = "VPN:2:IPSEC_ACL_HUB1_SPOKE2"
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:2 >
        LogEventID = "IPsec:Protect:VPN:2:IPSEC_ACL_HUB1_SPOKE2"
    ),
    Filter (
        Label = "VPN:3:DMAP:1:IPSEC_ACL_HUB1_CLIENTS"
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.255.0/24
        Action = PASS
        ExtendedAction     =     ipsec<     sa     =     IPsecAction:VPN:3:DMAP:1,
IPsecAction:VPN:3:DMAP:2 >
        LogEventID                                                              =
"IPsec:Protect:VPN:3:DMAP:1:IPSEC_ACL_HUB1_CLIENTS$VPN:3:DMAP:2:IPSEC_ACL_HUB1_CLIENT
S"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes 4294967295
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$y$j9T$qQiNawK8p8oXCUsxE287z1$HLiG4hhXSBcVWxOEo1CRTX/wj1Yb0zKepZxbYxo6MS8
```

```
aaa new-model
!
!
hostname Spoke1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
ip access-list extended IPSEC_ACL_SPOKE1_HUB1
 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
!
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_SPOKE1_HUB1
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 set peer 172.16.100.2
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 crypto map VPN
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group OLD_CA_CRL http://172.16.101.15/OLD_CA.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 15B67BF70980C7AD4B97B3A516758E76
...
4436194085

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Mar 20 16:25:06 2024

GlobalParameters(
    Title                           = "This LSP was automatically generated by CSP
Converter at Wed Mar 20 16:25:06 2024 (user: root)"
    Version                     = LSP_4_3
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
```

```
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.1.1
        )
)

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   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "G2814789CPRO2-K288-CNTMAC-253"
        LifetimeSeconds     = 3600
        LifetimeKilobytes   = 4294967295
    )
)

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

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

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
```

```
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.2
        DFHandling=COPY
        Assemble=TRUE
    )
    ContainedProposals = ( GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    IKERule = IKERule:VPN:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.1.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_SPOKE1_HUB1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    IPsecPolicy = IPsecPolicy:VPN
)
```

Конфигурации криптошлюза Spoke2

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$y$j9T$qQiNawK8p8oXCUsxE287z1$HLiG4hhXSBcVWxOEo1CRTX/wj1Yb0zKepZxbYxo6MS8
aaa new-model
!
!
hostname Spoke2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
```

```
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.2.2
!
ip access-list extended IPSEC_ACL_SPOKE2_HUB1
 permit ip 192.168.2.0 0.0.0.255 192.168.100.0 0.0.0.255
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACL_SPOKE2_HUB1
 set transform-set MAGMA_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.2.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group NEW_CA_CRL http://172.16.101.15/NEW_CA.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 1C2F1E21A226ADBF4355135842D25DC8
...
F39223341C
```

```
quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Sat Apr 27 12:28:28 2024

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Sat Apr 27 12:28:28 2024 (user: root)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.2.1
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
    TCPFinTimeout = 5
    TCPClosedTimeout = 30
    TCPSynRcvdTimeout = 30
    TCPEstablishedTimeout = 3600
    TCPHalfOpenLow = 400
    TCPHalfOpenMax = 500
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

IKETransform crypto:isakmp:policy:1
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

ESPProposal MAGMA_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
```

```
    Filters = Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain InspectChain:INSPECT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)
```

```
IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain IPv6Default (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

AuthMethodGOSTSign GOST:Sign:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
```

```
        SourceIP = 192.168.2.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACL_SPOKE2_HUB1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурация VPN клиентов Client1 и Client3 (версия 4.3)

1. Конфигурация LSP:

```
GlobalParameters (
    Title = "Client 4.3 LSP"
    Version = LSP_4_3
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
AuthMethodGOSTSign auth_method_01(
    LocalID =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode = ALWAYS
    SendCertMode = ALWAYS
)
IKEParameters (
    DefaultPort = 500
    SendRetries = 5
    RetryTimeBase = 1
    RetryTimeMax = 30
    SessionTimeMax = 60
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    BlacklogRelaxTime = 120
    IKECFGPreferDefaultAddress = FALSE
)
IKETransform ike_trf_01(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341112_256TC26-65128"
    GroupID *= VKO2_1B
)
IKETransform ike_trf_02(
    LifetimeSeconds = 28800
```

```
    CipherAlg  *= "GR341215K-K256-CFB-65528"
    HashAlg *= "GR341112_256TC26-65128"
    GroupID *= VKO2_1B
)
IKETransform ike_trf_03(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= VKO_1B
)
IKETransform ike_trf_04(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= MODP_1536
)
ESPTransform esp_trf_01(
    CipherAlg *= "G2814789CPRO2-K288-CNTMAC-253"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
    Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
    CipherAlg *= "GR341215K-K352-MGM-251"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
    Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
    Transform *=esp_trf_03
)
IKERule ike_rule_with_ikecfg_01(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    IKECFGRequestAddress = TRUE
)
IPsecAction ipsec_action_01(
    PersistentConnection = TRUE
    TunnelingParameters *=
        TunnelEntry(
            PeerAddress = 172.16.100.2
            Assemble = TRUE
            ReRoute = FALSE
            TCPEncapsulation = FALSE
        )
    ContainedProposals *= (esp_proposal_01),(esp_proposal_02),(esp_proposal_03)
    IKERule = ike_rule_with_ikecfg_01
)
```

```
FilterChain filter_chain_input(
    Filters *= Filter(
        ProtocolID *= 17
        DestinationPort *= 500
        Action = PASS
        LogEventID = "pass_action_02_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        DestinationPort *= 4500
        Action = PASS
        LogEventID = "pass_action_02_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        SourceIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_03_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        SourceIP *= 172.16.100.2
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_03_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_04"
    )
)
FilterChain filter_chain_output(
    Filters *= Filter(
        ProtocolID *= 17
        SourcePort *= 500
        Action = PASS
        LogEventID = "pass_action_05_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500
        Action = PASS
        LogEventID = "pass_action_05_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_06_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_06_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_07"
    )
)
FilterChain filter_chain_classification_input(
    Filters *= Filter(
```

```
        Action = PASS
        LogEventID = "pass_action_08"
    )
)
FilterChain filter_chain_classification_output(
    Filters *= Filter(
        Action = PASS
        LogEventID = "pass_action_09"
    )
)
FilterChain filter_chain_ipsec(
    Filters *= Filter(
        ProtocolID *= 17
        SourcePort *= 500
        Action = PASS
        LogEventID = "pass_action_10_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500
        Action = PASS
        LogEventID = "pass_action_10_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_11_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_11_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 192.168.100.0/24
        Action = PASS
        ExtendedAction *= ipsec<sa=ipsec_action_01>
        LogEventID = "ipsec_action_01"
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_12"
    )
)
NetworkInterface(
    InputFilter = filter_chain_input
    OutputFilter = filter_chain_output
    InputClassification = filter_chain_classification_input
    OutputClassification = filter_chain_classification_output
    IPsecPolicy = filter_chain_ipsec
)
```

Конфигурация VPN клиентов Client2 и Client4 (версия 5.0)

1. Конфигурация LSP:

```
GlobalParameters (
    Title = "Client 5.0 LSP"
    Version = LSP_5_0
    CRLHandlingMode = BEST_EFFORT
)
```

```
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
AuthMethodGOSTSign auth_method_01(
    LocalID =  IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA )
    SendRequestMode = ALWAYS
    SendCertMode = ALWAYS
)
IKEParameters (
    DefaultPort = 500
    SendRetries = 5
    RetryTimeBase = 1
    RetryTimeMax = 30
    SessionTimeMax = 60
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    BlacklogRelaxTime = 120
    IKECFGPreferDefaultAddress = FALSE
)
IKETransform ike_trf_01(
    LifetimeSeconds = 28800
    CipherAlg  *= "GR341215M-K256-CFB-65526"
    HashAlg *= "GR341112_256TC26-65128"
    GroupID *= VKO2_1B
)
IKETransform ike_trf_02(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341112_256TC26-65128"
    GroupID *= VKO2_1B
)
IKETransform ike_trf_03(
    LifetimeSeconds = 28800
    CipherAlg  *= "GR341215K-K256-CFB-65528"
    HashAlg *= "GR341112_256TC26-65128"
    GroupID *= VKO2_1B
)
IKETransform ike_trf_04(
    LifetimeSeconds = 28800
    CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
    HashAlg *= "GR341194CPRO1-65534"
    GroupID *= VKO_1B
)
ESPTransform esp_trf_01(
    CipherAlg *= "GR341215M-K288-MGM-33"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
    Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
    CipherAlg *= "G2814789CPRO2-K288-CNTMAC-253"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
```

```
    Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
    CipherAlg *= "GR341215K-K352-MGM-251"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
    Transform *=esp_trf_03
)
ESPTransform esp_trf_04(
    CipherAlg *= "G2814789CPRO1-K256-CBC-254"
    IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_04(
    Transform *=esp_trf_04
)
IKERule ike_rule_with_ikecfg_01(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    IKECFGRequestAddress = TRUE
)
IPsecAction ipsec_action_01(
    PersistentConnection = TRUE
    TunnelingParameters *=
        TunnelEntry(
            PeerAddress = 172.16.100.2
            Assemble = TRUE
            ReRoute = FALSE
            TCPEncapsulation = FALSE
        )
    ContainedProposals                                                    *=
(esp_proposal_01),(esp_proposal_02),(esp_proposal_03),(esp_proposal_04)
    IKERule = ike_rule_with_ikecfg_01
)
FilterChain filter_chain_input(
    Filters *= Filter(
        ProtocolID *= 17
        DestinationPort *= 500
        Action = PASS
        LogEventID = "pass_action_02_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        DestinationPort *= 4500
        Action = PASS
        LogEventID = "pass_action_02_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        SourceIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_03_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        SourceIP *= 172.16.100.2
```

```
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_03_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_04"
    )
)
FilterChain filter_chain_output(
    Filters *= Filter(
        ProtocolID *= 17
        SourcePort *= 500
        Action = PASS
        LogEventID = "pass_action_05_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500
        Action = PASS
        LogEventID = "pass_action_05_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_06_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_06_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_07"
    )
)
FilterChain filter_chain_classification_input(
    Filters *= Filter(
        Action = PASS
        LogEventID = "pass_action_08"
    )
)
FilterChain filter_chain_classification_output(
    Filters *= Filter(
        Action = PASS
        LogEventID = "pass_action_09"
    )
)
FilterChain filter_chain_ipsec(
    Filters *= Filter(
        ProtocolID *= 17
        SourcePort *= 500
        Action = PASS
        LogEventID = "pass_action_10_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        ProtocolID *= 17
        SourcePort *= 4500
        Action = PASS
```

```
        LogEventID = "pass_action_10_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_11_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.2
        ProtocolID *= 51
        Action = PASS
        LogEventID = "pass_action_11_02"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 192.168.100.0/24
        Action = PASS
        ExtendedAction *= ipsec<sa=ipsec_action_01>
        LogEventID = "ipsec_action_01"
    ),Filter(
        Action = PASS
        LogEventID = "pass_action_12"
    )
)
NetworkInterface(
    InputFilter = filter_chain_input
    OutputFilter = filter_chain_output
    InputClassification = filter_chain_classification_input
    OutputClassification = filter_chain_classification_output
    IPsecPolicy = filter_chain_ipsec
)
```