Построение отказоустойчивого решения с применением технологии RRI (reverse route injection)

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 удаленным VPN клиентом с применением технологии RRI и отказоустойчивостью криптошлюзов в центральном офисе.

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 для аутентификации будут использовать сертификаты в формате x509. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Криптошлюзы в центральном офисе и филиале № 1 версии 5.0, в филиале № 2 версии 4.3. Удаленный VPN клиент – «С-Терра Клиент» версии 5.0.

Для «С-Терра Шлюз» 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, switching.

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.

Перед развертыванием удаленного VPN клиента «С-Терра Клиент» следует ознакомиться со сценарием «Организация защищенного взаимодействия между криптошлюзом «С-Терра Шлюз» и удаленным VPN клиентом «С-Терра Клиент».

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»).

      В «С-Терра Шлюз» версии 5.0 появилась возможность пройти инициализацию через интерфейс управления (management) по SSH, данная процедура и ее ограничения описаны в документации и на портале https://doc.s-terra.ru.

   1.2. Центр выпуска сертификатов.

      1.2.1. Должен быть настроен центр выпуска сертификатов (удостоверяющий центр, далее УЦ) для IPsec. Устройство с именем Certification_authority 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 списка отозванных сертификатов.

      1.3.1. Функционирующий HTTP сервер для распространения списка отозванных сертификатов (COC). Устройство с именем CRL_distribution_point на схеме. Если по объективным причинам использование COC не представляется возможным или не требуется, то проверку COC 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 криптошлюзами должна быть обеспечена IP связность.

Схема взаимодействия

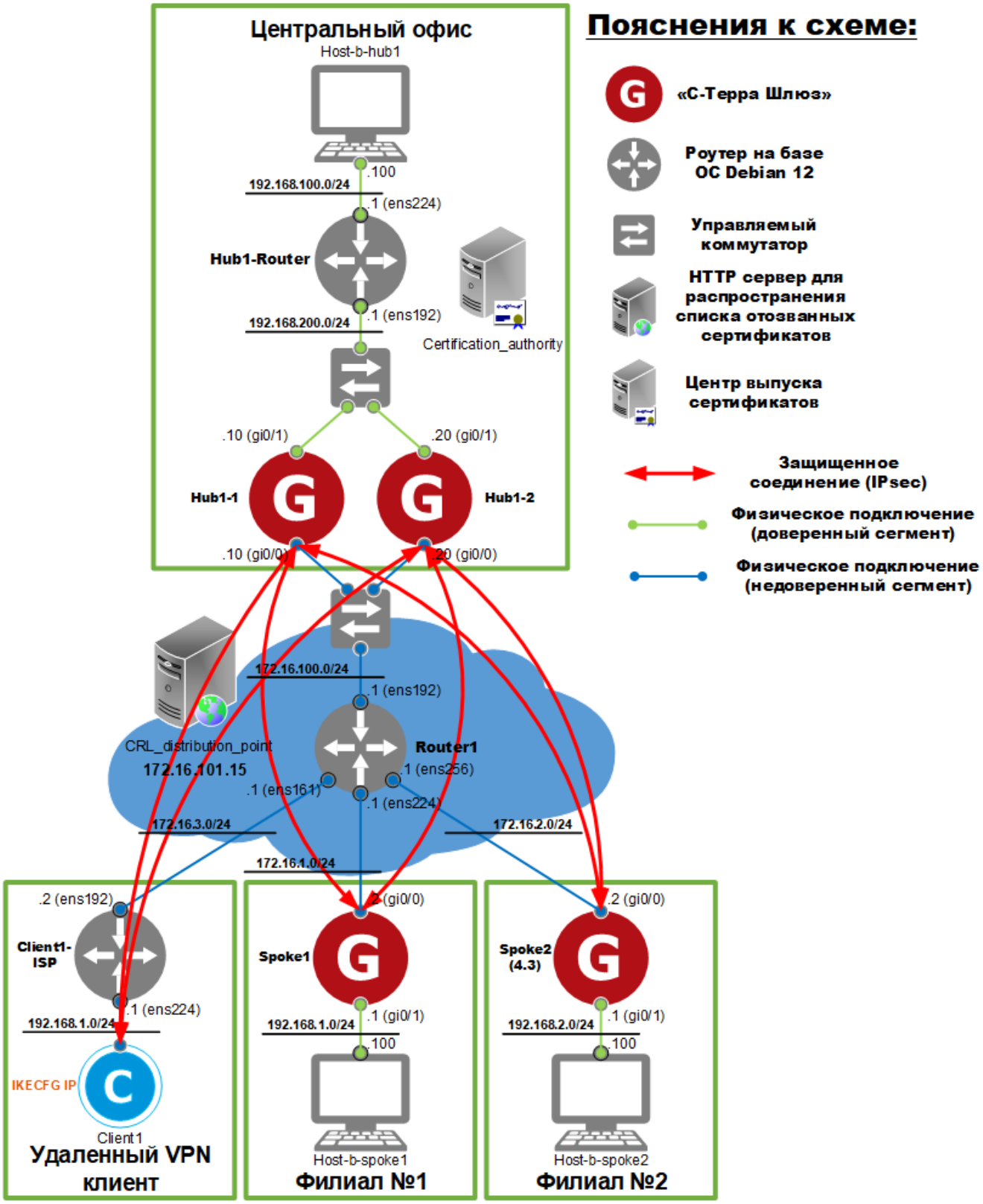


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюзы «С-Терра Шлюз» (Hub1-1 и Hub1-2), маршрутизатор (Hub1-Router) 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 списка отозванных сертификатов (CRL_distribution_point), маршрутизаторы (Router1 и Client1-ISP) и персональный компьютер (Client1).

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 списка отозванных сертификатов (устройство CRL_distribution_point на схеме).

   2.1. Криптошлюз Hub1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   2.2. Криптошлюз Spoke1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   2.3. Криптошлюз Spoke2 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

3. Логика работы RRI.

   В данном сценарии на криптошлюзах центрального офиса используется функционал Reverse Route Injection (RRI). При построении защищенного соединения с партнерами по IPsec на центральных криптошлюзах в таблицу маршрутизации будут добавляться маршруты до защищаемых подсетей партнеров.

   RRI маршрут вычисляется следующим образом:

   - Адрес и маска подсети для RRI маршрута формируются на основе destination части списка доступа для трафика, подлежащего шифрованию. В случае построения защищенного соединения с удаленным VPN клиентом в качестве адреса в RRI маршруте будет использоваться выданный клиенту IKECFG адрес с 32 маской.
   - Next-hop для RRI маршрута формируется посредством поиска маршрута до туннельного адреса партнера в системной таблице маршрутизации. Если маршрут до туннельного адреса партнера доступен через какой-либо next-hop адрес, то этот адрес будет использоваться в качестве next-hop в RRI маршруте. Если туннельный адрес партнера доступен напрямую, то в качестве next-hop в RRI маршруте будет использоваться туннельный адрес партнера.

   RRI маршруты автоматически удаляются из системы при удалении соответствующих IPsec SA.

   Подробнее про RRI на https://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз <версия> -> Создание конфигурационного файла -> Структура конфигурации -> ReverseRoute.

4. Динамическая маршрутизация.

   В центральном офисе на криптошлюзах Hub1-1, Hub1-2 и на маршрутизаторе Hub1-Router настраивается динамическая маршрутизация с использованием протокола BGP. Криптошлюзы Hub1-1 и Hub1-2 анонсируют RRI маршруты на устройство Hub1-Router.

Адресные пространства IKECFG пулов задаваемых на криптошлюзах Hub1-1 и Hub1-2 не пересекаются между собой, чтобы избежать ситуации, в которой два одинаковых RRI маршрута анонсируются с криптошлюзов на Hub1-Router.

5. Отказоустойчивость центральных шлюзов.

Филиальные криптошлюзы и удаленный VPN клиент могут строить защищенные соединения как с центральным криптошлюзом Hub1-1, так и с Hub1-2. При выходе из строя WAN интерфейса на одном из центральных криптошлюзов (или самого криптошлюза целиком), все защищенные соединения с ним со стороны партнеров по IPsec будут разорваны (по таймеру Dead Peer Detection) и построены с другим центральным криптошлюзом. Отказоустойчивость не распространяется на LAN интерфейсы центральных криптошлюзов.

6. Параметры шифрования IPsec.

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

Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke1 может только трафик из подсети филиала (192.168.1.0/24) в подсеть центра (192.168.100.0/24).

Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke2 может только трафик из подсети филиала (192.168.2.0/24) в подсеть центра (192.168.100.0/24).

Инициировать защищенное соединение между криптошлюзами Hub1 и Client1 может только трафик от устройства Client1 в подсеть центра (192.168.100.0/24).

6.1. Параметры протокола IKE

6.1.1. 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).

6.1.2. 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).

6.2. Параметры протокола ESP

6.2.1. 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).

6.2.2. Параметры протокола ESP для совместимости с версией 4.3:

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

7. Параметры межсетевого экранирования.

Для пакетов, которые не защищаются IPsec применяются следующие правила фильтрации:

7.1. Для «С-Терра Шлюз» версии 5.0:

7.1.1. На LAN интерфейсах IPv4 трафик не контролируется.

7.1.2. На LAN интерфейсах IPv6 трафик заблокирован.

7.1.3. На WAN интерфейсах разрешен входящий IPv4 трафик:

7.1.3.1. Протокол UDP порты 500 и 4500 – для IKE и NAT-Traversal (ESP in UDP).

7.1.3.2. Протокол ICMP – для проверки доступности криптошлюза и работы механизма PathMTUd.

7.1.3.3. Протокол ESP (номер 50) – для работы IPsec.

7.1.3.4. Весь TCP и UDP трафик, для которого есть исходящее соединение (это динамические правила, которые создаются при помощи stateful фильтрации).

7.1.4. На WAN интерфейсах IPv6 трафик заблокирован.

7.1.5. На WAN интерфейсах инспектируются все исходящие локальные и транзитные IPv4 соединения для протоколов TCP и UDP. На основе результатов инспектирования осуществляется фильтрация входящего трафика с учетом состояния сессии (stateful).

7.2. Для «С-Терра Шлюз» версии 4.3:

Использование stateful фильтрации для версии 4.3 нежелательно, рекомендуется использовать статические правила (ACL).

7.2.1. На LAN и WAN интерфейсах IPv4 трафик не контролируется.

7.2.2. На LAN и WAN интерфейсах IPv6 трафик заблокирован (протокол IPv6 отключен в ядре операционной системы).

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 ens161.
5. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Client1-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 для устройств из подсети 192.168.1.0/24 на интерфейсе ens224.
5. Настройте Source NAT на сетевом интерфейсе ens192 для трафика из подсети 192.168.1.0/24.
6. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Hub1-Router

1. Настройте IP адрес – 192.168.200.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 192.168.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Настройте динамическую маршрутизацию с использованием протокола динамической маршрутизации BGP, в качестве BGP neighbors укажите адреса LAN интерфейсов криптошлюзов Hub1-1 и Hub1-2. Пример конфигурации (при использовании пакета FRR):

```
frr version 8.4.4
frr defaults traditional
```

```
hostname Hub1-Router
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 192.168.200.1
 neighbor 192.168.200.10 remote-as 65000
 neighbor 192.168.200.20 remote-as 65000
exit
!
```

4. 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 криптошлюза Hub1-1

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 (в нашем примере это подсети 192.168.100.0/24, 192.168.1.0/24, 192.168.2.0/24. 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 сертификат криптошлюза и сохраните этот запрос в файл на USB Flash накопителе. Доставьте файл с запросом на УЦ и выпустите по нему сертификат. Сертификат криптошлюза вместе с сертификатом УЦ доставьте на криптошлюз и импортируйте их в базу Продукта.

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

Изменение состояния интерфейсов и назначение IP адресов в cisco-like консоли применяются сразу после ввода соответствующих команд. Политика безопасности применяются после выхода из режима конфигурирования.

1. Задайте имя устройства:

```
sterragate(config)#hostname Hub1-1
```

2. Включите WAN и LAN интерфейсы и настройте IP адреса в соответствии со схемой стенда:

```
Hub1-1(config)#interface GigabitEthernet 0/0
Hub1-1(config-if)#ip address 172.16.100.10 255.255.255.0
Hub1-1(config-if)#no shutdown
Hub1-1(config-if)#exit
Hub1-1(config)#interface GigabitEthernet 0/1
Hub1-1(config-if)#ip address 192.168.200.10 255.255.255.0
Hub1-1(config-if)#no shutdown
Hub1-1(config-if)#exit
```

3. Задайте маршрут до подсети 192.168.100.0/24 через устройство Hub1-Router:

```
Hub1-1(config)#ip route 192.168.100.0 255.255.255.0 192.168.200.1
```

4. Задайте маршрут по умолчанию через устройство Router1:

```
Hub1-1(config)#ip route 0.0.0.0 0.0.0.0 172.16.100.1
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка шифрования

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

```
Hub1-1(config)#ip local pool IKECFG_POOL 192.168.255.1 192.168.255.127
```

2. Параметры IKE.

   2.1. Задайте общие параметры IKE:

```
Hub1-1(config)#crypto isakmp identity dn
Hub1-1(config)#crypto isakmp keepalive 3 2
Hub1-1(config)#crypto isakmp keepalive retry-count 5
Hub1-1(config)#crypto isakmp fragmentation
```

```
Hub1-1(config)#crypto isakmp security-association lifetime delta 50
Hub1-1(config)#crypto isakmp initiator-sessions-max 100
Hub1-1(config)#crypto isakmp responder-sessions-max 100
```

3. Создайте две IKE политики:

   3.1. Создайте политику 1, описывающую алгоритмы IKE туннеля для совместимости с версией 5.0:

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

   3.2. Создайте политику **2**, описывающую алгоритмы IKE туннеля для совместимости с версией 4.3:

```
Hub1-1(config)#crypto isakmp policy 2
Hub1-1(config-isakmp)#encryption gost
Hub1-1(config-isakmp)#hash gost341112-256-tc26
Hub1-1(config-isakmp)#authentication gost-sig
Hub1-1(config-isakmp)#group vko2
Hub1-1(config-isakmp)#exit
```

   3.3. Создайте профиль настроек ISAKMP под именем `NEW_ALGS` для совместимости с версией 5.0:

```
Hub1-1(config)#crypto isakmp profile NEW_ALGS
Hub1-1(conf-isa-prof)#match identity dn
Hub1-1(conf-isa-prof)#set identity mapping
Hub1-1(conf-isa-prof)#set policy 1
Hub1-1(conf-isa-prof)#exit
```

   3.4. Создайте профиль настроек ISAKMP под именем `OLD_ALGS` для совместимости с версией 4.3:

```
Hub1-1(config)#crypto isakmp profile OLD_ALGS
Hub1-1(conf-isa-prof)#match identity dn
Hub1-1(conf-isa-prof)#set identity mapping
Hub1-1(conf-isa-prof)#set policy 2
Hub1-1(conf-isa-prof)#exit
```

4. Параметры IPsec.

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

```
Hub1-1(config)#crypto ipsec security-association lifetime kilobytes unlimited
```

   4.2. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика (для версии 5.0):

```
Hub1-1(config)#crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-
mgm
Hub1-1(cfg-crypto-trans)#exit
```

   4.3. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика (для версии 4.3):

```
Hub1-1(config)#crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-
imit
Hub1-1(cfg-crypto-trans)#exit
```

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

```
Hub1-1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
Hub1-1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
Hub1-1(config-ext-nacl)#exit
```

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

```
Hub1-1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE2
```

```
Hub1-1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.2.0 0.0.0.255
Hub1-1(config-ext-nacl)#exit
```

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

```
Hub1-1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_CLIENTS
Hub1-1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
Hub1-1(config-ext-nacl)#exit
```

4.7. Создайте крипто-карту (имя VPN, раздел 1) для построения IPsec туннеля между центральным офисом и филиалом №1 (включение RRI выполняется командой `reverse-route`):

```
Hub1-1(config)#crypto map VPN 1 ipsec-isakmp
Hub1-1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKE1
Hub1-1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1-1(config-crypto-map)#set peer 172.16.1.2
Hub1-1(config-crypto-map)#reverse-route
Hub1-1(config-crypto-map)#set isakmp-profile NEW_ALGS
Hub1-1(config-crypto-map)#set security-association mss-fix out
Hub1-1(config-crypto-map)#set pre-fragmentation
Hub1-1(config-crypto-map)#set dead-connection history off
Hub1-1(config-crypto-map)#exit
```

4.8. Создайте крипто-карту (имя VPN, раздел 2) для построения IPsec туннеля между центральным офисом и филиалом №2:

```
Hub1-1(config)#crypto map VPN 2 ipsec-isakmp
Hub1-1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKE2
Hub1-1(config-crypto-map)#set transform-set GOST_ENCRYPT_AND_INTEGRITY
Hub1-1(config-crypto-map)#set peer 172.16.2.2
Hub1-1(config-crypto-map)#reverse-route
Hub1-1(config-crypto-map)#set isakmp-profile OLD_ALGS
Hub1-1(config-crypto-map)#set security-association mss-fix out
Hub1-1(config-crypto-map)#set pre-fragmentation
Hub1-1(config-crypto-map)#set dead-connection history off
Hub1-1(config-crypto-map)#exit
```

4.9. Создайте динамическую криптокарту (имя DMAP, раздел 1) для построения IPsec туннеля между центральным офисом и удаленными VPN клиентами:

```
Hub1-1(config)#crypto dynamic-map DMAP 1
Hub1-1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_CLIENTS
Hub1-1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1-1(config-crypto-map)#set pool IKECFG_POOL
Hub1-1(config-crypto-map)#reverse-route
Hub1-1(config-crypto-map)#set isakmp-profile NEW_ALGS
Hub1-1(config-crypto-map)#set security-association mss-fix out
Hub1-1(config-crypto-map)#set pre-fragmentation
Hub1-1(config-crypto-map)#set dead-connection history off
Hub1-1(config-crypto-map)#exit
```

4.10. Добавьте созданную динамическую криптокарту DMAP в третий раздел криптокарты VPN:

```
Hub1-1(config)#crypto map VPN 3 ipsec-isakmp dynamic DMAP
Hub1-1(config-crypto-map)#exit
```

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

```
Hub1-1(config)#interface GigabitEthernet0/0
Hub1-1(config-if)# crypto map VPN
```

5. Примените настройки:

```
Hub1-1(config-if)#end
```

Подробная настройка с описанием команд приведена в базовом сценарии.

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 импортирование в базу Продукта списка отозванных сертификатов с HTTP сервера CRL_distribution_point.

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.
Hub1-1(config)#object-group network SELF
Hub1-1(config-network-group)#remark WAN IP
Hub1-1(config-network-group)#host 172.16.100.10
Hub1-1(config-network-group)#exit
```

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

```
Hub1-1(config)#ip access-list extended FW_INPUT_WAN
Hub1-1(config-ext-nacl)#permit udp any object-group SELF eq isakmp
Hub1-1(config-ext-nacl)#permit udp any object-group SELF eq non500-isakmp
Hub1-1(config-ext-nacl)#permit icmp any object-group SELF
Hub1-1(config-ext-nacl)#permit esp any object-group SELF
Hub1-1(config-ext-nacl)#exit
```

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

```
Hub1-1(config)#ip inspect name INSPECT tcp
Hub1-1(config)#ip inspect name INSPECT udp
Hub1-1(config)#ip inspect tcp sessions-max 256000
Hub1-1(config)#ip inspect udp sessions-max 65536
```

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

```
Hub1-1(config)#interface GigabitEthernet0/0
Hub1-1(config-if)#ip access-group FW_INPUT_WAN in
Hub1-1(config-if)#ip inspect INSPECT out
Hub1-1(config-if)#exit
```

5. Примените настройки:

```
Hub1-1(config)#end
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка динамической маршрутизации

Настройка динамической маршрутизации выполняется средствами ОС Linux с использованием пакета FRR. В качестве протокола динамической маршрутизации используется BGP.

1. В linux bash консоли включите сервис FRR и добавьте его в автозапуск:

```
root@Hub1-1:~# systemctl start frr.service
root@Hub1-1:~# systemctl enable frr
Synchronizing state of frr.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable frr
```

2. Перейдите в консоль FRR:

```
root@Hub1-1:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
Hub1-1#
```

3. Перейдите в режим конфигурирования:

```
Hub1-1# configure terminal
```

4. Настройте фильтрацию анонсируемых маршрутов с помощью ACL:

```
Hub1-1(config)# access-list BGP_ROUTE_FILTER_OUT seq 5 permit 192.168.1.0/24
Hub1-1(config)# access-list BGP_ROUTE_FILTER_OUT seq 10 permit 192.168.2.0/24
Hub1-1(config)# access-list BGP_ROUTE_FILTER_OUT seq 15 permit 192.168.255.0/24
```

5. Настройте BGP:

```
Hub1-1# configure terminal
Hub1-1(config)# router bgp 65000
Hub1-1(config)# bgp router-id 192.168.200.10
Hub1-1(config)# neighbor 192.168.200.1 remote-as 65000
Hub1-1(config-router)# address-family ipv4 unicast
Hub1-1(config-router-af)# redistribute kernel
Hub1-1(config-router-af)# neighbor 192.168.200.1 next-hop-self
Hub1-1(config-router-af)# neighbor 192.168.200.1 distribute-list BGP_ROUTE_FILTER_OUT
out
Hub1-1(config-router-af)# exit
Hub1-1(config-router)# exit
```

6. Примените настройки и сохраните конфигурацию:

```
Hub1-1(config)# end
Hub1-1# write
```

```
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
```

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP;
- конфигурация FRR

Настройка криптошлюза Hub1-2

Настройка криптошлюза Hub1-2 происходит аналогично настройке Hub1-1. Диапазон адресов IKECFG пула на криптошлюзе Hub1-2 не должен пересекаться с IKECFG пулом, настроенным на криптошлюзе Hub1-1.

В Приложении представлены тексты конфигураций для криптошлюза Hub1-2:

- текст консоли cisco-like;
- текст LSP;
- конфигурация FRR.

Настройка криптошлюза Spoke1

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 сертификат криптошлюза и сохраните этот запрос в файл на USB Flash накопителе. Доставьте файл с запросом на УЦ и выпустите по нему сертификат. Сертификат криптошлюза вместе с сертификатом УЦ доставьте на криптошлюз и импортируйте их в базу Продукта.

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

Изменение состояния интерфейсов и назначение IP адресов в cisco-like консоли применяются сразу после ввода соответствующих команд. Политика безопасности применяются после выхода из режима конфигурирования.

1. Задайте имя устройства:

```
sterragate(config)#hostname Spoke1
```

2. Включите WAN и LAN интерфейсы и настройте IP адреса в соответствии со схемой стенда:

```
Spoke1(config)#interface GigabitEthernet 0/0
Spoke1(config-if)#ip address 172.16.1.2 255.255.255.0
Spoke1(config-if)#no shutdown
Spoke1(config-if)#exit
Spoke1(config)#interface GigabitEthernet 0/1
Spoke1(config-if)#ip address 192.168.1.1 255.255.255.0
Spoke1(config-if)#no shutdown
Spoke1(config-if)#exit
```

3. Задайте маршрут по умолчанию через устройство Router1:

```
Spoke1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка шифрования

1. Настройте параметры IKE.

   1.1. Задайте общие параметры IKE:

```
Spoke1(config)#crypto isakmp identity dn
Spoke1(config)#crypto isakmp keepalive 2 1
Spoke1(config)#crypto isakmp keepalive retry-count 3
Spoke1(config)#crypto isakmp fragmentation
Spoke1(config)#crypto isakmp security-association lifetime delta 50
Spoke1(config)#crypto isakmp initiator-sessions-max 100
Spoke1(config)#crypto isakmp responder-sessions-max 100
```

   1.2. Создайте политику, описывающую параметры IKE туннеля:

```
Spoke1(config)#crypto isakmp policy 1
Spoke1(config-isakmp)#encryption magma
Spoke1(config-isakmp)#hash stribog-256
Spoke1(config-isakmp)#authentication gost-sig
Spoke1(config-isakmp)#group vko2
Spoke1(config-isakmp)#exit
```

   1.3. Создайте профиль настроек ISAKMP (алгоритм IKE) под именем `NEW_ALGS`, чтобы далее его прикрепить к криптокарте:

```
Spoke1(config)#crypto isakmp profile NEW_ALGS
Spoke1(conf-isa-prof)#match identity dn
Spoke1(conf-isa-prof)#set identity mapping
Spoke1(conf-isa-prof)#set policy 1
```

2. Настройте параметры IPsec.

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

```
Spoke1(config)#crypto ipsec security-association lifetime kilobytes unlimited
```

   2.2. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика:

```
Spoke1(config)# crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-
mgm
Spoke1(cfg-crypto-trans)#exit
```

   2.3. Создайте список доступа (ACL) для трафика, который нужно защищать между шлюзом Spoke1 и центральным шлюзом:

```
Spoke1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
Spoke1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
Spoke1(config-ext-nacl)#exit
```

   2.4. Создайте крипто-карту (имя VPN, раздел 1):

```
Spoke1(config)#crypto map VPN 1 ipsec-isakmp
```

2.4.1. Укажите список доступа для защищаемого трафика:

```
Spoke1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKE1
```

2.4.2. Укажите при помощи какого набора алгоритмов нужно защищать трафик:

```
Spoke1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
```

2.4.3. Укажите IP адреса партнеров по IPsec, в данном сценарии это внешние IP адреса криптошлюзов центрального офиса:

```
Spoke1(config-crypto-map)#set peer 172.16.100.10
Spoke1(config-crypto-map)#set peer 172.16.100.20
```

2.4.4. Включите случайный выбор партнера по IPsec:

```
Spoke1(config-crypto-map)#set peer shuffle
```

2.4.5. Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

```
Spoke1(config-crypto-map)#set isakmp-profile NEW_ALGS
```

2.4.6. Включите префрагментацию:

```
Spoke1(config-crypto-map)#set pre-fragmentation
```

2.4.7. Включите автоматическую и интеллектуальную корректировку значения MSS:

```
Spoke1(config-crypto-map)#set security-association mss-fix out
```

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

```
Spoke1(config-crypto-map)#set dead-connection history off
Spoke1(config-crypto-map)#exit
```

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

```
Spoke1(config)#interface GigabitEthernet0/0
Spoke1(config-if)#crypto map VPN
Spoke1(config-if)#exit
```

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 импортирование в базу Продукта списка отозванных сертификатов с HTTP сервера CRL_distribution_point.

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 с целью дальнейшего его использования в ACL:

```
Spoke1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Spoke1(config)#object-group network SELF
Spoke1(config-network-group)#remark WAN IP
Spoke1(config-network-group)#host 172.16.1.2
Spoke1(config-network-group)#exit
```

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

```
Spoke1(config)#ip access-list extended FW_INPUT_WAN
Spoke1(config-ext-nacl)#permit udp any object-group SELF eq 500
Spoke1(config-ext-nacl)#permit udp any object-group SELF eq 4500
Spoke1(config-ext-nacl)#permit icmp any object-group SELF
Spoke1(config-ext-nacl)#permit esp any object-group SELF
```

```
Spoke1(config-ext-nacl)#exit
```

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

```
Spoke1(config)#ip inspect name INSPECT tcp
Spoke1(config)#ip inspect name INSPECT udp
Spoke1(config)#ip inspect tcp sessions-max 256000
Spoke1(config)#ip inspect udp sessions-max 65536
```

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

```
Spoke1(config)#interface GigabitEthernet0/0
Spoke1(config-if)#ip access-group FW_INPUT_WAN in
Spoke1(config-if)#ip inspect INSPECT out
Spoke1(config-if)#exit
```

5. Примените настройки:

```
Spoke1(config)#end
```

Настройка криптошлюза Spoke1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke2

Настройка криптошлюза Spoke2 происходит в соответствии с базовым сценарием. В криптокарте на WAN интерфейсе задаются два партнера по IPsec. RRI на криптошлюзе не используется.

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP.

Настройка устройства Client1

1. Настройте получение IP адреса по DHCP на сетевом интерфейсе.
2. Разрешите прием и отправку IP пакетов.
3. Развертывание VPN клиента «С-Терра Клиент» выполняется с помощью «С-Терра ГСУ» 5.0 или «С-Терра AdminTool» 5.0. Подробная настройка приводится в сценарии «Организация защищенного взаимодействия между криптошлюзом «С-Терра Шлюз» и удаленным VPN клиентом «С-Терра Клиент».

   При формировании политики безопасности Client1 в качестве партнеров по IPsec следует указывать адреса WAN интерфейсов криптошлюзов Hub1-1 и Hub1-2, а также установить галочку для “Use random address order” (см. Рисунок 2).

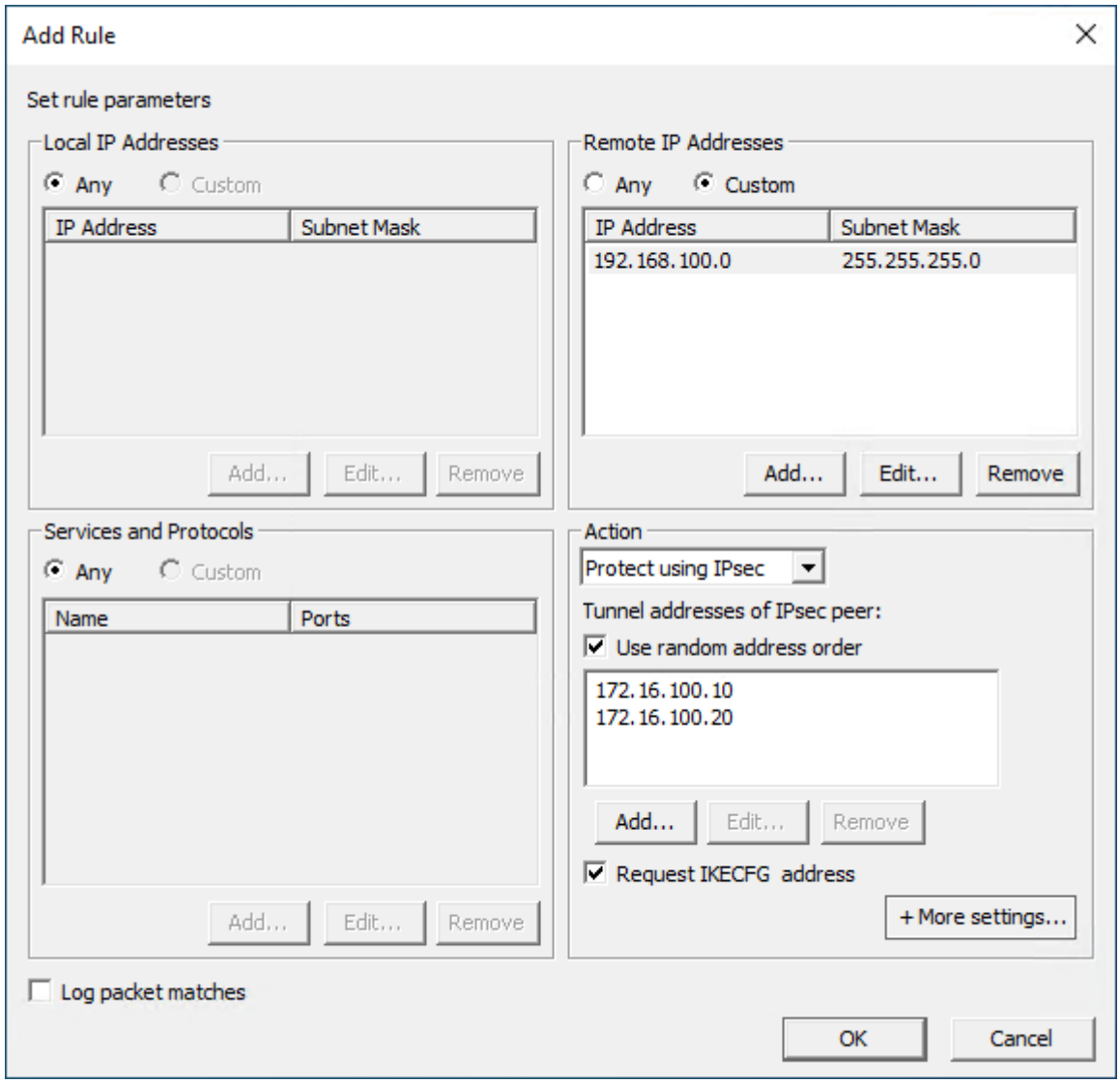


Рисунок 2

Во вкладке “LSP” следует нажать на кнопку «Advanced» и в разделе IKE settings для параметра “Prefer IKECFG address” установить значение “No preferred address” (см. Рисунок 3).

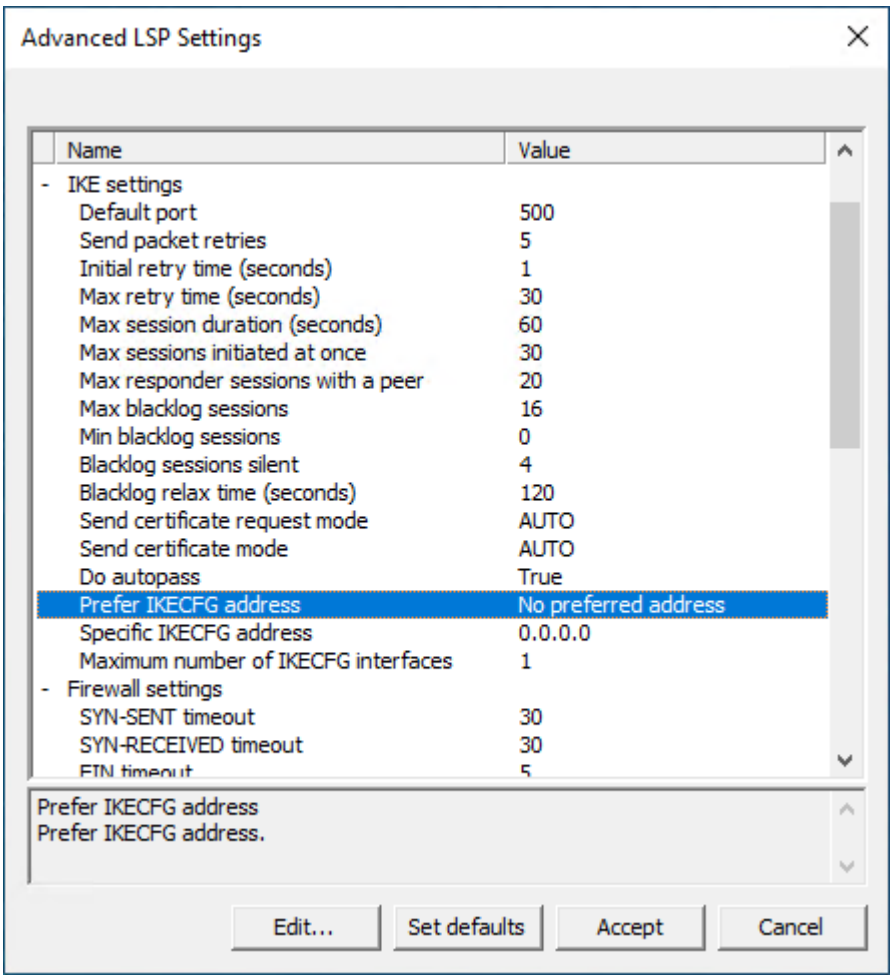


Рисунок 3

Для увеличения скорости перестроения защищенного соединения на VPN клиенте Client1 с одного крпитошлюза центрального офиса на другой в случае отказа в процессе работы рекомендуется отредактировать параметры DPD (Dead Peer Detection). Для этого следует в разделе DPD settings отредактировать значения следующих параметров (см. Рисунок 4):

- `Idle duration` – допустимый период времени (в секундах) отсутствия входящего трафика от партнера в IPsec туннеле при наличии исходящего трафика. По истечению этого периода запускается механизм DPD. Имя параметра в LSP – `DPDIdleDuration`;
- `Response duration` – время (в секундах) ожидания ответа от партнера на DPD запрос. Имя параметра в LSP – `DPDResponseDuration`;
- `Retries` – количество DPD запросов. Имя параметра в LSP – `DPDRetries`.

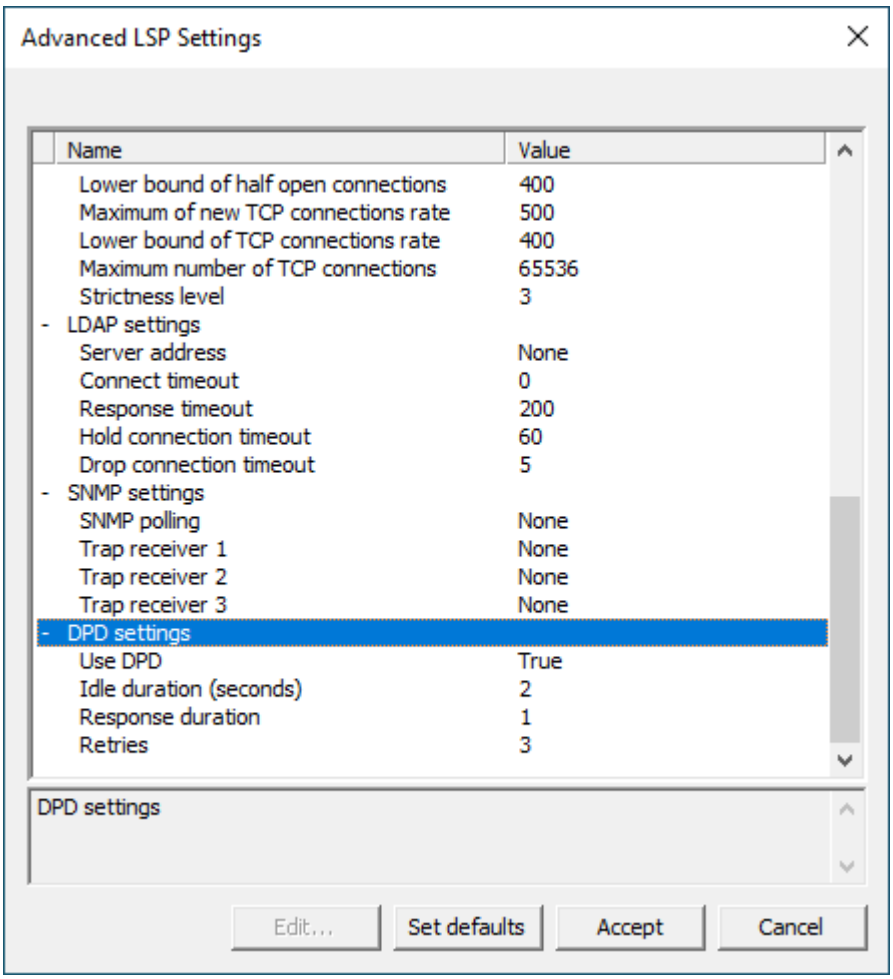


Рисунок 4

Для увеличения скорости построения защищенного соединения в случае, когда попытка построения соединения выполняется на IP адрес неработающего криптошлюза, можно использовать параметр `ResponseTimeMax`. Этот параметр задает время (в секундах) ожидания первого ответного IKE пакета от партнера при построении новой ISAKMP сессии. По истечении этого времени будет выполнена попытка построения сессии с другим партнером.

Для задания этого параметра установите галочку “Use custom LSP” и в тексте LSP в разделе IKEParameters добавьте параметр `ResponseTimeMax` с желаемым значением (значение по умолчанию – 10 сек, минимальное значение – 0, максимальное – 300. Если значение равно 0, то ограничение на время ожидания первого ответного IKE пакета в режиме инициатора приравнивается к значению параметра `SessionTimeMax`) (см. Рисунок 5).

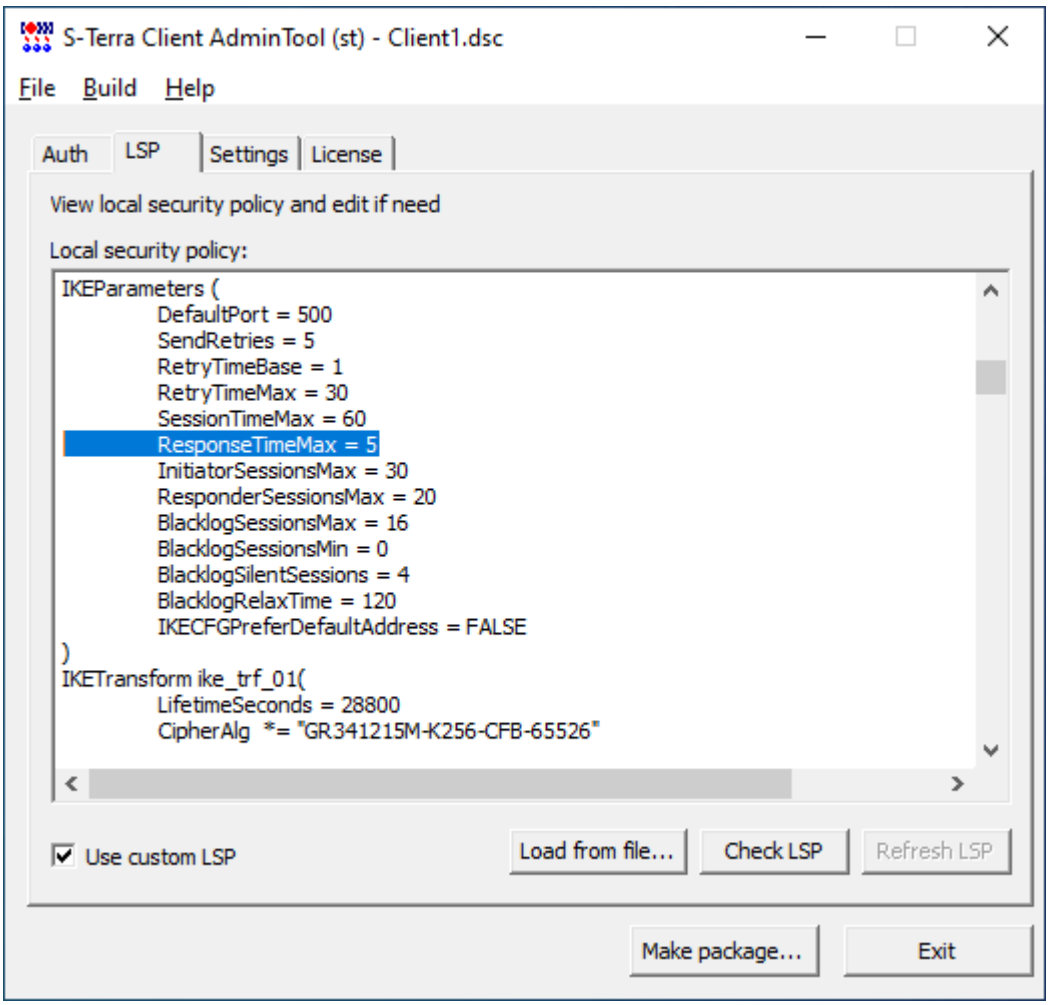


Рисунок 5

В Приложении представлены тексты конфигураций для Client1:

- текст LSP.

Проверка работоспособности стенда

Проверку работоспособности нужно выполнять после завершения настройки всех устройств стенда.

Проверка IP связности

1. Проверьте, что с защищаемых устройств Host-b-hub1, Host-b-spoke1, Host-b-spoke2 и Client1 доступен их соответствующий шлюз по умолчанию. Для этого выполните команду ping из консоли устройств:

```
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=0.259 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.227 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.172 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.186 ms

--- 192.168.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.172/0.211/0.259/0.034 ms
```

```
root@Host-b-spoke1:~# ping 192.168.1.1 -c 4
```

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.341 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.434 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.437 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.425 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.341/0.409/0.437/0.039 ms
```

```
root@Host-b-spoke2:~# ping 192.168.2.1 -c 4
```

```
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.229 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.242 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.282 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.303 ms

--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 0.229/0.264/0.303/0.029 ms
```

```
C:\Users\Administrator>ping 192.168.1.1
```

```
Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

2. Проверьте, что с криптошлюзов Spoke1 и Spoke2, а также с устройства Client1 доступны криптошлюзы Hub1-1 и Hub1-2 (по внешним интерфейсам). Для этого выполните команду ping из консоли устройств:

```
Spoke1#ping 172.16.100.10
```

```
PING 172.16.100.10 (172.16.100.10) 100(128) bytes of data.
108 bytes from 172.16.100.10: icmp_seq=1 ttl=63 time=0.669 ms
108 bytes from 172.16.100.10: icmp_seq=2 ttl=63 time=0.673 ms
```

```
108 bytes from 172.16.100.10: icmp_seq=3 ttl=63 time=0.852 ms
108 bytes from 172.16.100.10: icmp_seq=4 ttl=63 time=0.803 ms
108 bytes from 172.16.100.10: icmp_seq=5 ttl=63 time=0.809 ms

--- 172.16.100.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4097ms
rtt min/avg/max/mdev = 0.669/0.761/0.852/0.075 ms
```

```
Spoke1#ping 172.16.100.20
```

```
PING 172.16.100.20 (172.16.100.20) 100(128) bytes of data.
108 bytes from 172.16.100.20: icmp_seq=1 ttl=63 time=0.699 ms
108 bytes from 172.16.100.20: icmp_seq=2 ttl=63 time=0.707 ms
108 bytes from 172.16.100.20: icmp_seq=3 ttl=63 time=0.478 ms
108 bytes from 172.16.100.20: icmp_seq=4 ttl=63 time=0.915 ms
108 bytes from 172.16.100.20: icmp_seq=5 ttl=63 time=0.650 ms

--- 172.16.100.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4059ms
rtt min/avg/max/mdev = 0.478/0.689/0.915/0.139 ms
```

```
Spoke2#ping 172.16.100.10
```

```
PING 172.16.100.10 (172.16.100.10) 100(128) bytes of data.
108 bytes from 172.16.100.10: icmp_seq=1 ttl=63 time=0.617 ms
108 bytes from 172.16.100.10: icmp_seq=2 ttl=63 time=0.558 ms
108 bytes from 172.16.100.10: icmp_seq=3 ttl=63 time=0.627 ms
108 bytes from 172.16.100.10: icmp_seq=4 ttl=63 time=0.597 ms
108 bytes from 172.16.100.10: icmp_seq=5 ttl=63 time=0.669 ms

--- 172.16.100.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4085ms
rtt min/avg/max/mdev = 0.558/0.613/0.669/0.045 ms
```

```
Spoke2#ping 172.16.100.20
```

```
PING 172.16.100.20 (172.16.100.20) 100(128) bytes of data.
108 bytes from 172.16.100.20: icmp_seq=1 ttl=63 time=0.592 ms
108 bytes from 172.16.100.20: icmp_seq=2 ttl=63 time=0.608 ms
108 bytes from 172.16.100.20: icmp_seq=3 ttl=63 time=0.629 ms
108 bytes from 172.16.100.20: icmp_seq=4 ttl=63 time=0.490 ms
108 bytes from 172.16.100.20: icmp_seq=5 ttl=63 time=0.488 ms

--- 172.16.100.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4086ms
rtt min/avg/max/mdev = 0.488/0.561/0.629/0.063 ms
```

```
C:\Users\Administrator>ping 172.16.100.10
```

```
Обмен пакетами с 172.16.100.10 по с 32 байтами данных:
Ответ от 172.16.100.10: число байт=32 время=2мс TTL=62
Ответ от 172.16.100.10: число байт=32 время=2мс TTL=62
Ответ от 172.16.100.10: число байт=32 время=2мс TTL=62
Ответ от 172.16.100.10: число байт=32 время=2мс TTL=62

Статистика Ping для 172.16.100.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек
```

```
C:\Users\Administrator>ping 172.16.100.20
```

```
Обмен пакетами с 172.16.100.20 по с 32 байтами данных:
Ответ от 172.16.100.20: число байт=32 время=2мс TTL=62
Ответ от 172.16.100.20: число байт=32 время=2мс TTL=62
Ответ от 172.16.100.20: число байт=32 время=2мс TTL=62
```

```
Ответ от 172.16.100.20: число байт=32 время=2мс TTL=62

Статистика Ping для 172.16.100.20:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек
```

Проверка PKI

1. Проверьте, что на криптошлюзах Hub1-1, Hub1-2, Spoke1 и Spoke2 СОС импортирован в базу Продукта. Для этого выполните команду `run cert_mgr show` из cisco-like консоли криптошлюзов (пример вывода для Hub1-1):

```
Hub1-1#run cert_mgr show
```

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

2. Проверьте, что на криптошлюзах Hub1-1, Hub1-2, Spoke1 и Spoke2 статус всех сертификатов Active. Для этого выполните команду `run cert_mgr check` из cisco-like консоли криптошлюзов (пример вывода для Hub1-1):

```
Hub1-1#run cert_mgr check
```

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

3. Убедитесь, что на устройстве Client1 присутствуют локальный и доверенный сертификаты, и статус всех сертификатов Active:

```
C:\Program Files\S-Terra Client>cert_mgr.exe check
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Client1
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1-2
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1-1
```

Проверка построения защищенного соединения

1. Инициируйте построение защищенного соединения между криптошлюзами при помощи ICMP трафика, посылаемого с устройств Host-b-spoke1, Host-b-spoke2, Client1 на устройство Host-b-hub1. Для этого выполните команду `ping` из консоли защищаемых устройств:

```
root@Host-b-spoke1:~# ping 192.168.100.100 -c 5
```

```
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=64 time=6.70 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=3.97 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=3.69 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=2.44 ms
64 bytes from 192.168.100.100: icmp_seq=5 ttl=64 time=2.61 ms

--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 2.442/3.882/6.700/1.529 ms
```

```
root@Host-b-spoke2:~# ping 192.168.100.100 -c 4
```

```
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=61 time=1.36 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=61 time=1.16 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=61 time=1.30 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=61 time=1.53 ms

--- 192.168.100.100 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.159/1.337/1.534/0.135 ms
```

```
C:\Users\Administrator>ping 192.168.100.100
```

```
Обмен пакетами с 192.168.100.100 по с 32 байтами данных:
Ответ от 192.168.100.100: число байт=32 время=2мс TTL=61
Ответ от 192.168.100.100: число байт=32 время=2мс TTL=61
Ответ от 192.168.100.100: число байт=32 время=2мс TTL=61
Ответ от 192.168.100.100: число байт=32 время=2мс TTL=61

Статистика Ping для 192.168.100.100:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек
```

2. Проверьте, что на криптошлюзах и на устройстве Client1 установлены защищенные IPsec соединения. Для этого выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

```
Hub1-1#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 14 (172.16.100.10,500)-(172.16.1.2,500) active 1928 1960
2 15 (172.16.100.10,500)-(172.16.2.2,500) active 1916 1908

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 14 (192.168.100.0-192.168.100.255,*)-(192.168.1.0-192.168.1.255,*) * ESP tunn 616
704
2 15 (192.168.100.0-192.168.100.255,*)-(192.168.2.0-192.168.2.255,*) * ESP tunn
528 704
```

```
Hub1-2#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 1 (172.16.100.20,4500)-(172.16.3.2,4500) active 2016 2976

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (192.168.100.0-192.168.100.255,*)-(192.168.255.129,*) * ESP nat-t-tunn 512 512
```

```
Spoke1#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 10 (172.16.1.2,500)-(172.16.100.10,500) active 1960 1928

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 10 (192.168.1.0-192.168.1.255,*)-(192.168.100.0-192.168.100.255,*) * ESP tunn 704
616
```

```
Spoke2#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 3 (172.16.2.2,500)-(172.16.100.10,500) active 1908 1916

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3 (192.168.2.0-192.168.2.255,*)-(192.168.100.0-192.168.100.255,*) * ESP tunn 704 528
```

Для просмотра установленных защищенных соединений на устройстве Client1 кликните правой кнопкой мыши по иконке «С-Терра Клиент» в системном трее и выберите пункт Show SA Information в контекстном меню. Откроется окно VPN SA Monitor с информацией о текущих соединений (см. Рисунок 6):

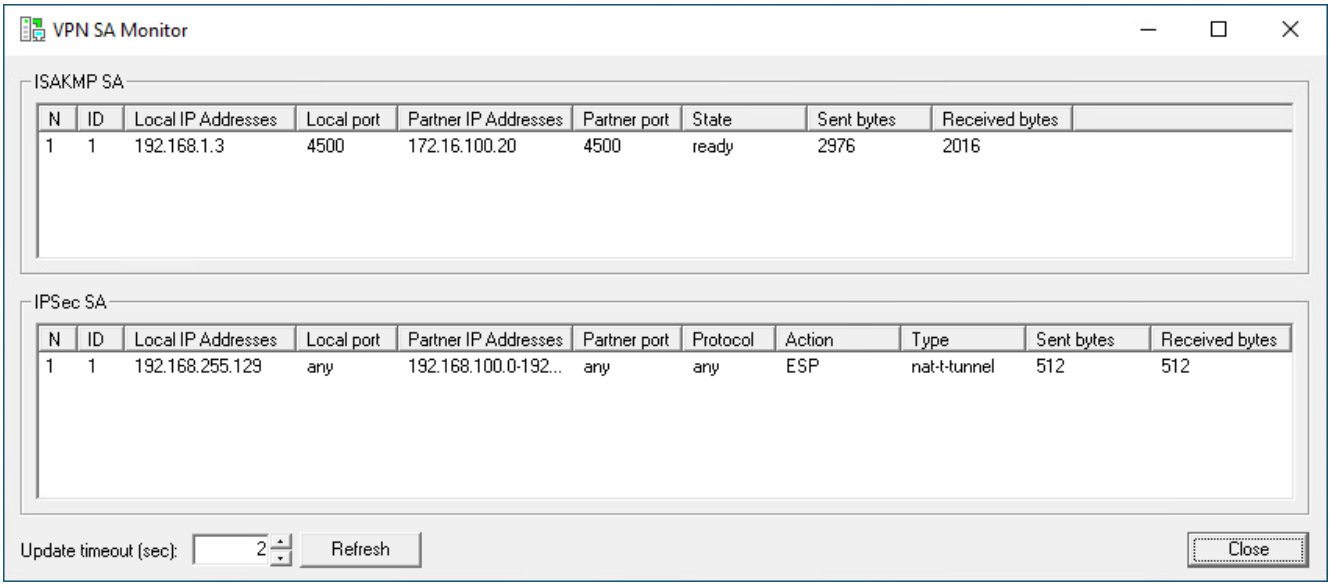


Рисунок 6

Видно, что на криптошлюзах и на устройстве Client1 установлены защищенные IPsec соединения. Если этого не произошло, то проверьте на криптошлюзах файл журнала (команда `run less /var/log/cspvpngate.log`). При необходимости увеличьте уровень логирования (команда `logging trap debugging` в консоли cisco-like) и заново инициируйте защищенное соединение.

Проверка динамической маршрутизации

1. Проверьте, что на криптошлюзах Hub1-1 и Hub1-2 в таблице маршрутизации появились маршруты до подсетей филиалов и до устройства Client1 (по IKECFG IP адресу). Для этого выполните следующую команду из cisco-like консоли криптошлюзов:

```
Hub1-1#run ip r
```

```
default via 172.16.100.1 dev eth0 proto st_policy
172.16.100.0/24 dev eth0 proto kernel scope link src 172.16.100.10
192.168.1.0/24 via 172.16.100.1 dev eth0 proto st_rri
192.168.2.0/24 via 172.16.100.1 dev eth0 proto st_rri
192.168.100.0/24 via 192.168.200.1 dev eth1 proto st_policy
192.168.200.0/24 dev eth1 proto kernel scope link src 192.168.200.10
```

```
Hub1-2#run ip r
```

```
default via 172.16.100.1 dev eth0 proto st_policy
172.16.100.0/24 dev eth0 proto kernel scope link src 172.16.100.20
192.168.100.0/24 via 192.168.200.1 dev eth1 proto st_policy
192.168.200.0/24 dev eth1 proto kernel scope link src 192.168.200.20
192.168.255.129 via 172.16.100.1 dev eth0 proto st_rri
```

2. Проверьте, что на маршрутизаторе Hub1-Router в таблице маршрутизации появились маршруты до подсетей филиалов и до устройства Client1 (по IKECFG IP адресу) через IP адреса LAN интерфейсов криптошлюзов Hub1-1 и Hub1-2, полученные по протоколу BGP. Для этого выполните следующую команду из консоли устройства Hub1-Router:

```
root@Hub1-Router:~# ip r
```

```
192.168.1.0/24 nhid 14 via 192.168.200.10 dev ens192 proto bgp metric 20
192.168.2.0/24 nhid 14 via 192.168.200.10 dev ens192 proto bgp metric 20
192.168.100.0/24 dev ens224 proto kernel scope link src 192.168.100.1
192.168.200.0/24 dev ens192 proto kernel scope link src 192.168.200.1
192.168.255.129 nhid 28 via 192.168.200.20 dev ens192 proto bgp metric 20
```

Проверка отказоустойчивого решения

1. Смоделируйте отказ на одном из центральных криптошлюзов, например отключите сетевой кабель от WAN интерфейса `GigabitEthernet0/0` на криптошлюзе Hub1-1 и убедитесь, что через некоторое время все защищенные соединения с партнерами Spoke1, Spoke2 и Client1 будут построены на криптошлюзе Hub1-2:

```
Hub1-2#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 3 (172.16.100.20,500)-(172.16.1.2,500) active 1928 1960
2 4 (172.16.100.20,4500)-(172.16.3.2,4500) active 2016 2976
3 5 (172.16.100.20,500)-(172.16.2.2,500) active 1916 1908

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 12 (192.168.100.0-192.168.100.255,*)-(192.168.1.0-192.168.1.255,*) * ESP tunn 704
1408
2 13 (192.168.100.0-192.168.100.255,*)-(192.168.255.129,*) * ESP nat-t-tunn 256 256
3 14 (192.168.100.0-192.168.100.255,*)-(192.168.2.0-192.168.2.255,*) * ESP tunn 528
1232
```

2. Убедитесь, что на маршрутизаторе Hub1-Router в таблице маршрутизации появились маршруты до подсетей филиалов и до устройства Client1 через IP адрес LAN интерфейса криптошлюза Hub1-2:

```
root@Hub1-Router:~# ip r
```

```
192.168.1.0/24 nhid 36 via 192.168.200.20 dev ens192 proto bgp metric 20
192.168.2.0/24 nhid 36 via 192.168.200.20 dev ens192 proto bgp metric 20
192.168.100.0/24 dev ens224 proto kernel scope link src 192.168.100.1
192.168.200.0/24 dev ens192 proto kernel scope link src 192.168.200.1
192.168.255.129 nhid 36 via 192.168.200.20 dev ens192 proto bgp metric 20
```

3. Исправьте причину отказа на криптошлюзе Hub1-1.

Проверка скорости переключения между криптошлюзами при отказе

1. С устройства Client1 постройте защищенное IPsec соединение. Определите, с каким из криптошлюзов центрального офиса построено соединение.
2. На криптошлюзе, с которым построено защищенное соединение, смоделируйте отказ.
3. На устройстве Client1 засеките время и начните отправку ICMP запросов на устройство Host-b-hub1 (пример для консоли PowerShell, команда `date` выводит текущее время на момент выполнения, параметр `-t` в команде `ping` задает бесконечную отправку запросов до прерывания выполнения пользователем):

```
PS C:\Windows\system32> date; ping 192.168.100.100 -t
```

```
2 июля 2024 г. 12:05:30

Обмен пакетами с 192.168.100.100 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
```

```
...
```

Это приведет к ситуации, когда в IPsec туннеле присутствует исходящий трафик, но отсутствует входящий. Засеките время, когда начнут приходить ICMP ответы:

```
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Ответ от 192.168.100.100: число байт=32 время=33мс TTL=61
Ответ от 192.168.100.100: число байт=32 время=1мс TTL=61
...
```

4. Проанализируйте лог на устройстве Client1 и определите время, прошедшее с момента начала отправки ICMP запросов до переключения на рабочий криптошлюз (индикатором успешного построения защищенного соединения является сообщение `IPSec connection <N> established`).

   В общем случае примерное время до переключения с отказавшего криптошлюза на рабочий вычисляется по следующей формуле (на основе параметров из LSP):

   ```
   DPDIdleDuration + DPDResponseDuration*DPDRetries + ResponseTimeMax
   ```

   В данном сценарии время переключения VPN клиента Client1 между криптошлюзами составляет примерно `2 + 1*3 + 5 = 10` секунд. Период восстановления IP связности между Client1 и Host-b-hub1 будет на несколько секунд дольше, так как потребуется еще некоторое время на анонсирование RRI маршрута с криптошлюза на маршрутизатор Hub1-Router.

5. Исправьте причину отказа на криптошлюзе.

Приложение

Конфигурация криптошлюза Hub1-1

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
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1-1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp policy 2
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto isakmp profile OLD_ALGS
 match identity dn
 set identity mapping
 set policy 2
!
ip local pool IKECFG_POOL 192.168.255.1 192.168.255.127
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.10
```

```
!
ip access-list extended IPSEC_ACl_HUB1_AND_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_AND_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_AND_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_AND_CLIENTS
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool IKECFG_POOL
 set security-association mss-fix out
 reverse-route
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer 172.16.1.2
 reverse-route
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 2 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE2
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile OLD_ALGS
 set security-association mss-fix out
 set peer 172.16.2.2
 reverse-route
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 3 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 172.16.100.10 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.200.10 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route 192.168.100.0 255.255.255.0 192.168.200.1
```

```
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Apr 12 16:46:56 2024

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Fri Apr 12 16:46:56 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.100.1
        ),
        Route(
            Destination = 192.168.100.0/24
            Gateway = 192.168.200.1
        )

)

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
)
```

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

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

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.100.10
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.10
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.10
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.10
        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
)

IdentityEntry Remote:OLD_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:OLD_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

AddressPool IKECFG_POOL
(
    IPAddresses = 192.168.255.1..192.168.255.127
)

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
```

```
)

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

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

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

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

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

IPsecAction IPsecAction:VPN:2
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.2.2
        Prefragmentation = ENABLE
    )
```

```
    ContainedProposals = ( GOST_ENCRYPT_AND_INTEGRITY:ESP )
    ReverseRoute = TRUE
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:2
)

IPsecAction IPsecAction:VPN:3:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    ReverseRoute = TRUE
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:3:DMAP:1
)

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_AND_SPOKE1"
    ),
    Filter (
        Label = "VPN:2:IPSEC_ACl_HUB1_AND_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_AND_SPOKE2"
    ),
    Filter (
        Label = "VPN:3:DMAP:1:IPSEC_ACL_HUB1_AND_CLIENTS"
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.255.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:3:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:3:DMAP:1:IPSEC_ACL_HUB1_AND_CLIENTS"
    )
)

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

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

3. Конфигурация FRR.

```
frr version 9.0.2
frr defaults traditional
hostname Hub1-1
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 192.168.200.10
 neighbor 192.168.200.1 remote-as 65000
 !
 address-family ipv4 unicast
  redistribute kernel
  neighbor 192.168.200.1 next-hop-self
  neighbor 192.168.200.1 distribute-list BGP_ROUTE_FILTER_OUT out
 exit-address-family
exit
!
access-list BGP_ROUTE_FILTER_OUT seq 5 permit 192.168.1.0/24
access-list BGP_ROUTE_FILTER_OUT seq 10 permit 192.168.2.0/24
access-list BGP_ROUTE_FILTER_OUT seq 15 permit 192.168.255.0/24
!
```

Конфигурация криптошлюза Hub1-2

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
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1-2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp policy 2
```

```
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto isakmp profile OLD_ALGS
 match identity dn
 set identity mapping
 set policy 2
!
ip local pool IKECFG_POOL 192.168.255.128 192.168.255.254
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.20
!
ip access-list extended IPSEC_ACl_HUB1_AND_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_AND_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_AND_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_AND_CLIENTS
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool IKECFG_POOL
 set security-association mss-fix out
 reverse-route
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
```

```
 set security-association mss-fix out
 set peer 172.16.1.2
 reverse-route
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 2 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE2
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile OLD_ALGS
 set security-association mss-fix out
 set peer 172.16.2.2
 reverse-route
 set pre-fragmentation
 set dead-connection history off
crypto map VPN 3 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 172.16.100.20 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.200.20 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route 192.168.100.0 255.255.255.0 192.168.200.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Apr 12 16:48:33 2024

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Fri Apr 12 16:48:33 2024 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

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

```
        Route(
            Destination = 192.168.100.0/24
            Gateway = 192.168.200.1
        )

)

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
)

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

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

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
```

```
        DestinationIP = 172.16.100.20
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.20
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.20
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.20
        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
)

IdentityEntry Remote:OLD_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:OLD_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

AddressPool IKECFG_POOL
(
    IPAddresses = 192.168.255.128..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:NEW_ALGS
(
    RemoteID             = Remote:NEW_ALGS
    LocalID              = Local:Cert:NEW_ALGS
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

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

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

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

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

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

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

IPsecAction IPsecAction:VPN:3:DMAP:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    ReverseRoute = TRUE
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
```

```
    IKERule = IKERule:VPN:3:DMAP:1
)

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_AND_SPOKE1"
    ),
    Filter (
        Label = "VPN:2:IPSEC_ACl_HUB1_AND_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_AND_SPOKE2"
    ),
    Filter (
        Label = "VPN:3:DMAP:1:IPSEC_ACL_HUB1_AND_CLIENTS"
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.255.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:3:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:3:DMAP:1:IPSEC_ACL_HUB1_AND_CLIENTS"
    )
)

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

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

3. Конфигурация FRR:

```
frr version 9.0.2
frr defaults traditional
hostname Hub1-2
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 192.168.200.20
 neighbor 192.168.200.1 remote-as 65000
 !
 address-family ipv4 unicast
  redistribute kernel
  neighbor 192.168.200.1 next-hop-self
```

```
  neighbor 192.168.200.1 distribute-list BGP_ROUTE_FILTER_OUT out
 exit-address-family
exit
!
access-list BGP_ROUTE_FILTER_OUT seq 5 permit 192.168.1.0/24
access-list BGP_ROUTE_FILTER_OUT seq 10 permit 192.168.2.0/24
access-list BGP_ROUTE_FILTER_OUT seq 15 permit 192.168.255.0/24
!
```

Конфигурация 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 unlimited
crypto isakmp keepalive 2 1
crypto isakmp keepalive retry-count 3
username          cscons          privilege          15          secret          5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke1
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_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.1.2
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
 permit ip 192.168.1.0 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_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer shuffle
 set peer 172.16.100.10
 set peer 172.16.100.20
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
!
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 ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Apr 12 16:50:02 2024

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Fri Apr 12 16:50:02 2024 (user: cscons)"
    Version                     = LSP_5_0
    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
    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_GOST_ENCRYPT_AND_INTEGRITY:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        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 = 172.16.100.10, 172.16.100.20
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 2
    DPDResponseDuration = 1
    DPDRetries          = 3
    Priority            = 10
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.10
        Prefragmentation = ENABLE
    ),
    TunnelEntry(
        PeerAddress = 172.16.100.20
        Prefragmentation = ENABLE
    )
    ShuffleTunnelEntries = TRUE
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = 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 = 192.168.1.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACl_HUB1_AND_SPOKE1"
    )
)

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

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

Конфигурация 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 4294967295
crypto isakmp keepalive 2 1
crypto isakmp keepalive retry-count 3
username          cscons          privilege          15          secret          5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke2
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_HUB1_AND_SPOKE2
 permit ip 192.168.2.0 0.0.0.255 192.168.100.0 0.0.0.255
!
!
crypto map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE2
 set transform-set GOST_ENCRYPT_AND_INTEGRITY
 set peer 172.16.100.10
 set peer 172.16.100.20
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
 crypto map VPN
!
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 ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
```

```
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Apr 12 16:51:14 2024

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Fri Apr 12 16:51:14 2024 (user: cscons)"
    Version                     = LSP_4_3
    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
)

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 = 172.16.100.10, 172.16.100.20
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign
    MainModeAuthMethod  = GOST:Sign
    DPDIdleDuration     = 2
    DPDResponseDuration = 1
    DPDRetries          = 3
    Priority            = 10
)

IPsecAction IPsecAction:VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.10
        DFHandling=COPY
        Assemble=TRUE
    ),
    TunnelEntry(
        PeerAddress = 172.16.100.20
        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 = 192.168.2.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACl_HUB1_AND_SPOKE2"
    )
)

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

Конфигурация Client1

1. Конфигурация LSP:

```
GlobalParameters (
    Title = "This LSP was automatically generated by S-Terra Client AdminTool (st) at
2025.11.10 14:22:02"
    Version = LSP_5_0
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
```

```
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
    DistinguishedName *= CertDescription(
        Subject *= COMPLETE,"C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Client1"
        )
)
CertDescription local_cert_dsc_01(
    Subject *= COMPLETE,"C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Client1"
    Issuer  *=  COMPLETE,"C=RU,L=Zelenograd,O=S-Terra  CSP,OU=RnD,CN=S-Terra  CSP  Test
Root CA"
    SerialNumber = "2F00005B65EA4888B6F348046B000000005B65"
    FingerprintMD5 = "22BA4AEB2E443BAF5EFEA81FD826A5A6"
)
CertDescription partner_cert_dsc_01(
)
AuthMethodGOSTSign auth_method_01(
    LocalID = auth_identity_01
    LocalCredential = local_cert_dsc_01
    RemoteCredential = partner_cert_dsc_01
    SendRequestMode = AUTO
    SendCertMode = AUTO
)
IKEParameters (
    DefaultPort = 500
    SendRetries = 5
    RetryTimeBase = 1
    RetryTimeMax = 30
    SessionTimeMax = 60
    ResponseTimeMax = 5
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    BlacklogRelaxTime = 120
    IKECFGPreferDefaultAddress = TRUE
    IKECFGDefaultAddress = 0.0.0.0
)
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
)
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
)
IKERule ike_rule_with_ikecfg_01(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 2
    DPDResponseDuration = 1
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03
    IKECFGRequestAddress = TRUE
)
IPsecAction ipsec_action_01(
    PersistentConnection = TRUE
    TunnelingParameters *=
        TunnelEntry(
            PeerAddress = 172.16.100.10
            Assemble = TRUE
            ReRoute = FALSE
            TCPEncapsulation = FALSE
        ),
        TunnelEntry(
            PeerAddress = 172.16.100.20
            Assemble = TRUE
            ReRoute = FALSE
            TCPEncapsulation = FALSE
        )
    ShuffleTunnelEntries = TRUE
    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 *= 172.16.100.10,172.16.100.20
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_03_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        SourceIP *= 172.16.100.10,172.16.100.20
        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 *= 172.16.100.10,172.16.100.20
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_06_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.10,172.16.100.20
        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 *= 172.16.100.10,172.16.100.20
        ProtocolID *= 50
        Action = PASS
        LogEventID = "pass_action_11_01"
        PacketType = LOCAL_UNICAST,LOCAL_MISDIRECTED
    ),Filter(
        DestinationIP *= 172.16.100.10,172.16.100.20
        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
)
```