Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (протокол IPv6)

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 криптошлюзов «С-Терра Шлюз» для обеспечения безопасного взаимодействия между защищаемыми подсетями центрального офиса и двух филиалов (подсети филиалом между собой взаимодействовать не могут). Защищаемые подсети в LAN сегменте и недоверенные подсети в WAN сегменте – IPv6. Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec.

Партнеры по IPsec, в настоящем документе – криптошлюзы, для аутентификации будут использовать сертификаты в формате x509. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Криптошлюзы в центральном офисе, филиале № 1 и филиале № 2 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.

Требования к инфраструктуре

1. Требования к устройствам.

   1.1. «С-Терра Шлюз».

      1.1.1 Устройства «С-Терра Шлюз» должны быть инициализированы (подробнее на http://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 R2 (или новее).

      1.2.3 Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp), либо утилиту ca-tool, входящую в состав пакета auxiliary-tools (пакет auxiliary-tools предназначен для установки на «С-Терра Шлюз» 5.0, документация на ca-tool приведена в инструкции «Центр выпуска тестовых ГОСТ сертификатов для IPsec», документацию и пакет можно загрузить на портале https://doc.s-terra.ru).

      > 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 (СОС). Устройство с именем CRL_distribution_point на схеме. Если по объективным причинам использование СОС не представляется возможным или не требуется, то проверку СОС можно отключить в CLI «С-Терра Шлюз» (при соблюдении правил пользования).

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

2. Требования к сетевому взаимодействию.

   2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

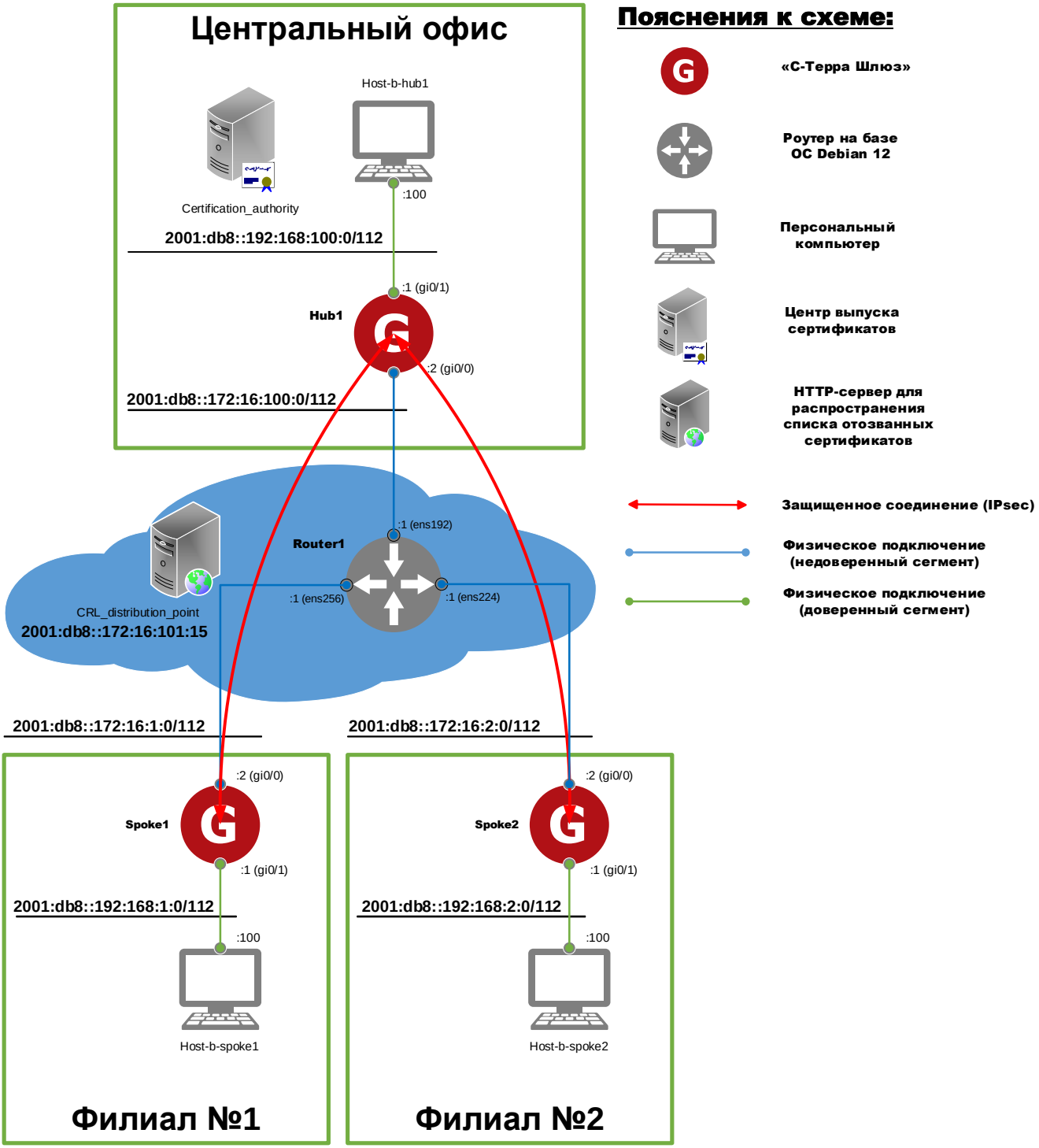


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюз «С-Терра Шлюз» (Hub1) версии 5.0 и персональный компьютер (Host-b-hub1).

   1.2. В филиале № 1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) версии 5.0 и персональный компьютер (Host-b-spoke1).

   1.3. В филиале № 2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2) версии 5.0 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), маршрутизатор (Router1).

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. Параметры шифрования IPsec.

   Весь IPv6 трафик между подсетями центрального офиса (2001:db8::192:168:100:0/112) и филиалов (2001:db8::192:168:1:0/112, 2001:db8::192:168:2:0/112) защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном IPv6 режиме.

   Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke1 может трафик из подсети филиала (2001:db8::192:168:1:0/112) в подсеть центра (2001:db8::192:168:100:0/112) и наоборот из центра в филиал.

   Инициировать защищенное соединение между криптошлюзами Hub1 и Spoke2 может трафик из подсети филиала (2001:db8::192:168:2:0/112) в подсеть центра (2001:db8::192:168:100:0/112) и наоборот из центра в филиал.

   3.1. Параметры протокола IKE:

   - 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).

   3.2. Параметры протокола ESP:

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

4. Параметры межсетевого экранирования.

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

   4.1. Для «С-Терра Шлюз» версии 5.0:

   4.1.1 На LAN интерфейсах IPv6 трафик не контролируется.

4.1.2 На LAN интерфейсах IPv4 трафик не заблокирован. При необходимости трафик IPv4 может быть заблокирован по аналогии с блокировкой трафика IPv4 на WAN интерфейсе в настоящем сценарии.

4.1.3 На WAN интерфейсах разрешен входящий IPv6 трафик:

4.1.3.1 Пакеты сообщений Neighbor Solicitation (NS) и Neighbor Advertisement (NA) протокола Neighbor Discovery (ND). Разрешение приема сообщений ND-NS необходимо для обнаружения криптошлюза смежным сетевым оборудованием (Router1 в настоящем сценарии) в случае, если инициатором обмена данными является не сам криптошлюз, а партнер. Прием сообщений ND-NA разрешается для случая, когда сообщение ND-NS посылается криптошлюзом, который инициирует обмен данными с партнером, а смежное сетевое оборудование посылает ND-NA с link-local адреса IPv6.

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

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

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

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

4.1.4 На WAN интерфейсах весь IPv4 трафик заблокирован – входящий и исходящий.

4.1.5 На WAN интерфейсах инспектируются все исходящие локальные и транзитные IPv6 соединения для протоколов TCP и UDP. На основе результатов инспектирования осуществляется фильтрация входящего трафика с учетом состояния сессии (stateful).

Настройка стенда

Настройка устройства Router1

1. Настройте IP адрес и маску – 2001:db8::172:16:1:1/112 на сетевом интерфейсе ens256.
2. Настройте IP адрес и маску – 2001:db8::172:16:100:1/112 на сетевом интерфейсе ens192.
3. Настройте IP адрес и маску – 2001:db8::172:16:2:1/112 на сетевом интерфейсе ens224.
4. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Host-b-hub1

1. Настройте IP адрес и маску 2001:db8::192:168:100:100/112 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 2001:db8::192:168:100:1.
3. Разрешите прием и отправку ICMP пакетов (если заблокировано).

Настройка устройства Host-b-spoke1

1. Настройте IP адрес и маску 2001:db8::192:168:1:100/112 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 2001:db8::192:168:1:1.
3. Разрешите прием и отправку ICMP пакетов (если заблокировано).

Настройка устройства Host-b-spoke2

1. Настройте IP адрес и маску 2001:db8::192:168:2:100/112 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 2001:db8::192:168:2:1.
3. Разрешите прием и отправку ICMP пакетов (если заблокировано).

Настройка криптошлюза Hub1

Настройка будет происходить локально при помощи консольного подключения.

Настройка может осуществляться и удаленно (по SSH), но исключительно по доверенному каналу связи. Доверенным каналом связи может считаться канал в пределах контролируемой зоны в случае отсутствия в нем нарушителя (в нашем примере это подсеть 2001:db8::192:168:100:0/112 для центрального офиса, подсеть 2001:db8::192:168:1:0/112 для филиала № 1 и 2001:db8::192:168:2:0/112 для филиала № 2). Доверенным каналом связи также считается канал, защищенный при помощи протокола IPsec (например, после настройки шифрования между подсетью 2001:db8::192:168:100:0/112 и подсетями 2001:db8::192:168:1:0/112, 2001:db8::192:168:2:0/112 разрешается выполнять настройку критошлюзов Spoke1 и Spoke2 из подсети 2001:db8::192:168:100:0/112 центрального офиса).

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 шлюз 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 применяются сразу после ввода соответствующих команд. **Политика безопасности применяются после выхода из режима конфигурирования**.

1. Проверьте включена ли маршрутизация IPv6:

```
root@Hub1:~# sysctl net.ipv6.conf.all.forwarding
```

```
net.ipv6.conf.all.forwarding = 1
```

Маршрутизация должна быть включена при инициализации криптошлюза. При необходимости маршрутизация IPv6 может быть включена позднее записью настройки `net.ipv6.conf.all.forwarding=1` в файл `/etc/sysctl.d/02-sterra_internet_settings.conf` с последующей перезагрузкой криптошлюза.

2. Задайте имя устройства в cisco-like консоли:

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

3. Включите внешний `GigabitEthernet0/0` и внутренний `GigabitEthernet0/1` интерфейсы:

В зависимости от параметров сетевого интерфейса его имя может отличаться от `GigabitEthernetN/M` и иметь имена, например `FastEthernetN/M`, `TenGigabitEthernetN/M`.

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

4. Разрешите IPv6 трафик независимо от наличия списков доступа на интерфейсах:

```
Hub1(config)#ipv6 default filtering permit
```

В рамках настоящего сценария команда по умолчанию `ipv6 default filtering deny` приведет и к блокировке трафика IPv6 на LAN интерфейсе, так как на WAN интерфейсе будет задан список доступа, а на LAN интерфейсе список доступа IPv6 не предполагается.

Примечание – Описание команды `ipv6 default filtering deny|permit`.

Команда `ipv6 default filtering deny` запрещает прохождение трафика IPv6 во всех направлениях на интерфейсах без списков доступа IPv6. Рекомендуется использовать эту команду в сетях, где используется исключительно IPv4, так как в целях повышения безопасности в таких сетях целесообразно заблокировать любые попытки подключения к криптошлюзу по IPv6 или передачи через него трафика IPv6. Команда активна по умолчанию после инициализации криптошлюза.

Если администратор криптошлюза явно указал возможность использования IPv6 путем привязки хотя бы одного списка доступа IPv6 к интерфейсу в любом направлении, то команда `ipv6 default filtering deny` не действует на этом интерфейсе. На интерфейсах, к которым не привязан ни один список доступа IPv6 команда `ipv6 default filtering deny` будет по-прежнему запрещать прохождение любого IPv6 трафика в любом направлении.

Если команда `ipv6 default filtering deny` активна, то на интерфейсах, к которым привязаны списки доступа IPv6, фильтрация трафика IPv6 будет производится в соответствии с правилами, указанными в списке доступа с неявным drop all в конце списка.

Если требуется разрешить IPv6 трафик на всех интерфейсах независимо от наличия списков доступа на них, то нужно выполнить команду `ipv6 default filtering permit` и далее уже фильтровать IPv6 трафик по аналогии с IPv4. Команду `ipv6 default filtering permit` рекомендуется использовать, если администратором предполагается использование IPv6 на всех интерфейсах.

Независимо от используемой команды (`ipv6 default filtering deny` или `ipv6 default filtering permit`) справедливо правило - если список доступа IPv6 на интерфейсе объявлен только в одном направлении, а в противоположном направлении список доступа IPv6 отсутствует, то для противоположного направления используется неявная политика pass all. Если неявная политика pass all нежелательна в соответствии с политиками безопасности, принятыми на объекте внедрения, то следует определить дополнительный список доступа IPv6, в котором явным образом указать правила фильтрации трафика IPv6 в противоположном направлении, и привязать его к интерфейсу.

5. Задайте IP адреса в соответствии со схемой стенда на внешнем `GigabitEthernet0/0` и внутреннем `GigabitEthernet0/1` интерфейсах:

```
Hub1(config)#interface GigabitEthernet 0/0
Hub1(config-if)#no ip address
Hub1(config-if)#ipv6 address 2001:db8::172:16:100:2/112
Hub1(config-if)#exit
Hub1(config)#interface GigabitEthernet 0/1
Hub1(config-if)#no ip address
Hub1(config-if)#ipv6 address 2001:db8::192:168:100:1/112
Hub1(config-if)#exit
```

6. Задайте маршрут по умолчанию через устройство Router1:

```
Hub1(config)#ipv6 route ::/0 2001:db8::172:16:100:1
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка шифрования

1. Параметры IKE.

   1.1. Задайте общие параметры IKE:

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

   1.2. Создайте политику, описывающую параметры IKE туннеля:

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

   1.3. Создайте профиль настроек ISAKMP под именем `NEW_ALGS`:

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

2. Параметры IPsec.

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

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

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

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

   2.3. Создайте список доступа (ACL) для IPv6 трафика, который нужно защищать между центральным офисом и филиалом №1:

```
Hub1(config)#ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
Hub1(config-ext-nacl)#permit             ipv6             2001:db8::192:168:100:0/112
2001:db8::192:168:1:0/112
Hub1(config-ext-nacl)#exit
```

   2.4. Создайте список доступа (ACL) для IPv6 трафика, который нужно защищать между центральным офисом и филиалом №2:

```
Hub1(config)#ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE2_IPV6
Hub1(config-ext-nacl)#permit            ipv6            2001:db8::192:168:100:0/112
2001:db8::192:168:2:0/112
Hub1(config-ext-nacl)#exit
```

2.5. Создайте крипто-карту (имя VPN_IPV6, раздел 1) для построения IPsec туннеля между центральным офисом и филиалом №1:

```
Hub1(config)#crypto map VPN_IPV6 1 ipsec-isakmp
Hub1(config-crypto-map)#match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
Hub1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)#set peer ipv6 2001:db8::172:16:1:2
Hub1(config-crypto-map)#set isakmp-profile NEW_ALGS
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#exit
```

2.6. Добавьте в созданную крипто-карту `VPN_IPV6`, в раздел 2 настройки для построения IPsec туннеля между центральным офисом и филиалом №2:

```
Hub1(config)#crypto map VPN_IPV6 2 ipsec-isakmp
Hub1(config-crypto-map)#match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE2_IPV6
Hub1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)#set isakmp-profile NEW_ALGS
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#set peer ipv6 2001:db8::172:16:2:2
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

2.7. Прикрепите созданную крипто-карту `VPN_IPV6` к внешнему WAN интерфейсу `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#crypto map VPN_IPV6
```

3. Примените настройки:

```
Hub1(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 (обратите внимание на формат задания IPv6 адреса):

```
Hub1(ca-trustpoint)#          crl          download          group          ROOTCA
http://[2001:db8::172:16:101:15]/certcrl.crl
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка межсетевого экрана

1. Создайте сетевой `object-group` с именем `SELF-IPV6` для хранения в нем WAN адресов криптошлюза:

```
Hub1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hub1(config)#object-group v6-network SELF-IPV6
Hub1(config-network-group)# remark WAN IP
Hub1(config-network-group)# host 2001:db8::172:16:100:2
Hub1(config-network-group)#exit
```

2. Создайте ACL с именем `FW_INPUT_WAN_IPV6` для входящего на WAN интерфейс трафика:

```
Hub1(config)# ipv6 access-list FW_INPUT_WAN_IPV6
Hub1(config-ipv6-acl)#permit icmp any any nd-ns
Hub1(config-ipv6-acl)#permit icmp any any nd-na
Hub1(config-ipv6-acl)#permit udp any object-group SELF-IPV6 eq 500
Hub1(config-ipv6-acl)#permit udp any object-group SELF-IPV6 eq 4500
Hub1(config-ipv6-acl)#permit icmp any object-group SELF-IPV6
Hub1(config-ipv6-acl)#permit esp any object-group SELF-IPV6
Hub1(config-ipv6-acl)# exit
```

3. Создайте ACL'и с именами `FIREWALL_OUT` и `FIREWALL_IN` для запрета исходящего и входящего IPv4 трафика на WAN интерфейсе:

```
Hub1(config)#ip access-list extended FIREWALL_OUT
Hub1(config-ext-nacl)#deny ip any any
Hub1(config-ext-nacl)#ip access-list extended FIREWALL_IN
Hub1(config-ext-nacl)#deny ip any any
```

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

```
Hub1(config)#ip inspect tcp sessions-max 256000
Hub1(config)#ip inspect udp sessions-max 65536
Hub1(config)#ipv6 inspect name INSPECT tcp
Hub1(config)#ipv6 inspect name INSPECT udp
```

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

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#ipv6 access-group FW_INPUT_WAN_IPV6 in
Hub1(config-if)#ip access-group FIREWALL_IN in
Hub1(config-if)#ip access-group FIREWALL_OUT out
Hub1(config-if)#ipv6 inspect INSPECT out
```

6. Примените настройки:

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

Подробная настройка с описанием команд приведена в базовом сценарии.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke1

Настройка криптошлюза Spoke1 происходит аналогично настройке Hub1.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke2

Настройка криптошлюза Spoke2 происходит аналогично настройке Spoke1.

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP.

Проверка работоспособности стенда

Проверку работоспособности нужно выполнять после завершения настройки всех устройств стенда.

Проверка IP связности

1. Проверьте, что с криптошлюзов по ICMP доступен шлюз по умолчанию (Router1). Для этого выполните команду `ping` из cisco-like консоли соответствующего криптошлюза.

```
Hub1#ping 2001:db8::172:16:100:1
```

```
PING 2001:db8::172:16:100:1(2001:db8::172:16:100:1) 100 data bytes
108 bytes from 2001:db8::172:16:100:1: icmp_seq=1 ttl=64 time=0.273 ms
108 bytes from 2001:db8::172:16:100:1: icmp_seq=2 ttl=64 time=0.365 ms
108 bytes from 2001:db8::172:16:100:1: icmp_seq=3 ttl=64 time=0.406 ms
108 bytes from 2001:db8::172:16:100:1: icmp_seq=4 ttl=64 time=0.257 ms
108 bytes from 2001:db8::172:16:100:1: icmp_seq=5 ttl=64 time=0.387 ms

--- 2001:db8::172:16:100:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.257/0.337/0.406/0.060 ms
```

```
Spoke1#ping 2001:db8::172:16:1:1
```

```
PING 2001:db8::172:16:1:1(2001:db8::172:16:1:1) 100 data bytes
108 bytes from 2001:db8::172:16:1:1: icmp_seq=1 ttl=64 time=0.900 ms
108 bytes from 2001:db8::172:16:1:1: icmp_seq=2 ttl=64 time=0.268 ms
108 bytes from 2001:db8::172:16:1:1: icmp_seq=3 ttl=64 time=0.448 ms
108 bytes from 2001:db8::172:16:1:1: icmp_seq=4 ttl=64 time=0.366 ms
108 bytes from 2001:db8::172:16:1:1: icmp_seq=5 ttl=64 time=0.347 ms

--- 2001:db8::172:16:1:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.268/0.465/0.900/0.224 ms
```

```
Spoke2#ping 2001:db8::172:16:2:1
```

```
PING 2001:db8::172:16:2:1(2001:db8::172:16:2:1) 100 data bytes
108 bytes from 2001:db8::172:16:2:1: icmp_seq=1 ttl=64 time=0.235 ms
108 bytes from 2001:db8::172:16:2:1: icmp_seq=2 ttl=64 time=0.301 ms
108 bytes from 2001:db8::172:16:2:1: icmp_seq=3 ttl=64 time=0.295 ms
108 bytes from 2001:db8::172:16:2:1: icmp_seq=4 ttl=64 time=0.229 ms
108 bytes from 2001:db8::172:16:2:1: icmp_seq=5 ttl=64 time=0.547 ms

--- 2001:db8::172:16:2:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4048ms
rtt min/avg/max/mdev = 0.229/0.321/0.547/0.116 ms
```

Видно, что устройство Router1 доступно по ICMP со всех криптошлюзов.

2. Проверьте, что с защищаемых устройств Host-b-hub1, Host-b-spoke1, Host-b-spoke2 доступен по ICMP соответствующий криптошлюз, который является шлюзом по умолчанию. Для этого выполните команду `ping` из linux bash консоли защищаемых устройств.

```
root@Host-b-hub1:~# ping 2001:db8::192:168:100:1 -c 5
```

```
PING 2001:db8::192:168:100:1(2001:db8::192:168:100:1) 56 data bytes
64 bytes from 2001:db8::192:168:100:1: icmp_seq=1 ttl=64 time=0.260 ms
64 bytes from 2001:db8::192:168:100:1: icmp_seq=2 ttl=64 time=0.182 ms
64 bytes from 2001:db8::192:168:100:1: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 2001:db8::192:168:100:1: icmp_seq=4 ttl=64 time=0.393 ms
64 bytes from 2001:db8::192:168:100:1: icmp_seq=5 ttl=64 time=0.369 ms

--- 2001:db8::192:168:100:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.182/0.317/0.393/0.083 ms
```

```
root@Host-b-spoke1:~# ping 2001:db8::192:168:1:1 -c 5
```

```
PING 2001:db8::192:168:1:1(2001:db8::192:168:1:1) 56 data bytes
64 bytes from 2001:db8::192:168:1:1: icmp_seq=1 ttl=64 time=0.961 ms
64 bytes from 2001:db8::192:168:1:1: icmp_seq=2 ttl=64 time=0.376 ms
64 bytes from 2001:db8::192:168:1:1: icmp_seq=3 ttl=64 time=0.323 ms
64 bytes from 2001:db8::192:168:1:1: icmp_seq=4 ttl=64 time=0.249 ms
64 bytes from 2001:db8::192:168:1:1: icmp_seq=5 ttl=64 time=0.188 ms

--- 2001:db8::192:168:1:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.188/0.419/0.961/0.278 ms
```

```
root@Host-b-spoke2:~# ping 2001:db8::192:168:2:1 -c 5
```

```
PING 2001:db8::192:168:2:1(2001:db8::192:168:2:1) 56 data bytes
64 bytes from 2001:db8::192:168:2:1: icmp_seq=1 ttl=64 time=0.345 ms
64 bytes from 2001:db8::192:168:2:1: icmp_seq=2 ttl=64 time=0.385 ms
64 bytes from 2001:db8::192:168:2:1: icmp_seq=3 ttl=64 time=0.283 ms
64 bytes from 2001:db8::192:168:2:1: icmp_seq=4 ttl=64 time=0.247 ms
64 bytes from 2001:db8::192:168:2:1: icmp_seq=5 ttl=64 time=0.369 ms

--- 2001:db8::192:168:2:1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.247/0.325/0.385/0.052 ms
```

Видно, что со всех защищаемых устройств соответствующие криптошлюзы доступны по ICMP.

3. Проверьте, что с криптошлюза Hub1 доступны по ICMP криптошлюзы Spoke1 и Spoke2 (по внешним интерфейсам). Для этого выполните команду `ping` из cisco-like консоли соответствующего криптошлюза.

```
Hub1#ping 2001:db8::172:16:1:2
```

```
PING 2001:db8::172:16:1:2(2001:db8::172:16:1:2) 100 data bytes
108 bytes from 2001:db8::172:16:1:2: icmp_seq=1 ttl=63 time=1.11 ms
108 bytes from 2001:db8::172:16:1:2: icmp_seq=2 ttl=63 time=0.911 ms
108 bytes from 2001:db8::172:16:1:2: icmp_seq=3 ttl=63 time=0.820 ms
108 bytes from 2001:db8::172:16:1:2: icmp_seq=4 ttl=63 time=0.625 ms
108 bytes from 2001:db8::172:16:1:2: icmp_seq=5 ttl=63 time=0.536 ms

--- 2001:db8::172:16:1:2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4023ms
rtt min/avg/max/mdev = 0.536/0.801/1.113/0.205 ms
```

```
Hub1#ping 2001:db8::172:16:2:2
```

```
PING 2001:db8::172:16:2:2(2001:db8::172:16:2:2) 100 data bytes
108 bytes from 2001:db8::172:16:2:2: icmp_seq=1 ttl=63 time=1.09 ms
108 bytes from 2001:db8::172:16:2:2: icmp_seq=2 ttl=63 time=0.527 ms
108 bytes from 2001:db8::172:16:2:2: icmp_seq=3 ttl=63 time=0.552 ms
108 bytes from 2001:db8::172:16:2:2: icmp_seq=4 ttl=63 time=0.773 ms
108 bytes from 2001:db8::172:16:2:2: icmp_seq=5 ttl=63 time=0.462 ms

--- 2001:db8::172:16:2:2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.462/0.679/1.085/0.228 ms
```

Видно, что с криптошлюза Hub1 доступны по ICMP криптошлюзы Spoke1 и Spoke2.

Проверка PKI

1. Проверьте, что на криптошлюзах СОС импортирован в базу Продукта. Для этого выполните команду `run cert_mgr show` из cisco-like консоли соответствующего криптошлюза.

```
Hub1#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
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
```

```
Spoke1#run cert_mgr show
```

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

```
Spoke2#run cert_mgr show
```

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

Видно, что на криптошлюзах СОС импортирован в базу Продукта. Если этого не произошло, то проверьте файл журнала (команда `run grep getcrls_daemon /var/log/cspvpngate.log`) и, при необходимости, перезапустите сервис автоматической загрузки СОС (команда `run systemctl restart getcrls.service`).

2. Проверьте, что на криптошлюзах статус всех сертификатов Active. Для этого выполните команду `run cert_mgr check` из cisco-like консоли соответствующего криптошлюза.

```
Hub1#run cert_mgr check
```

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

```
Spoke1#run cert_mgr check
```

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

```
Spoke2#run cert_mgr check
```

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

Видно, что на криптошлюзах статус всех сертификатов Active. Если статус Inactive, то проверьте:

- загружен ли СОС в базу Продукта;
- правильны и одинаковы ли дата и время на всех криптошлюзах.

Проверка построения защищенного соединения между подсетями Hub1 и Spoke1, Hub1 и Spoke2

1. Инициируйте построение защищенного соединения между криптошлюзами Hub1 и Spoke1 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke1 на Host-b-hub1 (можно и наоборот). Для этого выполните команду `ping` из linux bash консоли защищаемого устройства Host-b-spoke1.

```
root@Host-b-spoke1:~# ping 2001:db8::192:168:100:100 -c 5
```

```
PING 2001:db8::192:168:100:100(2001:db8::192:168:100:100) 56 data bytes
64 bytes from 2001:db8::192:168:100:100: icmp_seq=1 ttl=63 time=1002 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=2 ttl=63 time=10.1 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=3 ttl=63 time=1.88 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=4 ttl=63 time=1.34 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=5 ttl=63 time=1.42 ms

--- 2001:db8::192:168:100:100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.343/203.285/1001.681/399.211 ms
```

2. Проверьте, что на криптошлюзах Hub1 и Spoke1 установлено защищенное IPsec соединение. Для этого выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

```
Hub1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (2001:db8::172:16:100:2,500)-(2001:db8::172:16:1:2,500) active 1976 2008

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1   1   (2001:db8::192:168:100:0-2001:db8::192:168:100:ffff,*)-(2001:db8::192:168:1:0-
2001:db8::192:168:1:ffff,*) * ESP tunn 540 540
```

```
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 1 (2001:db8::172:16:1:2,500)-(2001:db8::172:16:100:2,500) active 2008 1976

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1    1    (2001:db8::192:168:1:0-2001:db8::192:168:1:ffff,*)-(2001:db8::192:168:100:0-
2001:db8::192:168:100:ffff,*) * ESP tunn 540 540
```

3. Инициируйте построение защищенного соединения между криптошлюзами Hub1 и Spoke2 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke2 на Host-b-hub1 (можно и наоборот). Для этого выполните команду `ping` из linux bash консоли защищаемого устройства Host-b-spoke2.

```
root@Host-b-spoke2:~# ping 2001:db8::192:168:100:100 -c 5
```

```
PING 2001:db8::192:168:100:100(2001:db8::192:168:100:100) 56 data bytes
64 bytes from 2001:db8::192:168:100:100: icmp_seq=1 ttl=62 time=870 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=2 ttl=62 time=1.65 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=3 ttl=62 time=1.69 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=4 ttl=62 time=1.59 ms
64 bytes from 2001:db8::192:168:100:100: icmp_seq=5 ttl=62 time=1.75 ms

--- 2001:db8::192:168:100:100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.592/175.399/870.313/347.456 ms
```

4. Проверьте, что на криптошлюзах Hub1 и Spoke2 установлено защищенное IPsec соединение. Для этого выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

```
Hub1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (2001:db8::172:16:100:2,500)-(2001:db8::172:16:1:2,500) active 1976 2008
2 2 (2001:db8::172:16:100:2,500)-(2001:db8::172:16:2:2,500) active 1976 2008

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1   1   (2001:db8::192:168:100:0-2001:db8::192:168:100:ffff,*)-(2001:db8::192:168:1:0-
2001:db8::192:168:1:ffff,*) * ESP tunn 1080 1080
2   2   (2001:db8::192:168:100:0-2001:db8::192:168:100:ffff,*)-(2001:db8::192:168:2:0-
2001:db8::192:168:2:ffff,*) * ESP tunn 540 540
```

```
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 1 (2001:db8::172:16:2:2,500)-(2001:db8::172:16:100:2,500) active 2008 1976

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1    1    (2001:db8::192:168:2:0-2001:db8::192:168:2:ffff,*)-(2001:db8::192:168:100:0-
2001:db8::192:168:100:ffff,*) * ESP tunn 540 540
```

Видно, что между криптошлюзами Hub1, Spoke1 и Hub1, Spoke2 установлено защищенное IPsec соединение. Если этого не произошло, то проверьте 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 работы межсетевого экрана

Для проверки работы межсетевого экрана выполните последовательно следующие команды из cisco-like консоли криптошлюзов и проанализируйте их вывод.

```
Hub1#run fwconn_mgr show
Hub1#run klogview -f FW,drop
```

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1
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 v6-network SELF-IPV6
 remark WAN IP
 host 2001:db8::172:16:100:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering permit
!
ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 permit ipv6 2001:db8::192:168:100:0/112 2001:db8::192:168:1:0/112
!
```

```
ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE2_IPV6
 permit ipv6 2001:db8::192:168:100:0/112 2001:db8::192:168:2:0/112
!
ipv6 access-list FW_INPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit udp any object-group SELF-IPV6 eq isakmp
 permit udp any object-group SELF-IPV6 eq non500-isakmp
 permit icmp any object-group SELF-IPV6
 permit esp any object-group SELF-IPV6
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto map VPN_IPV6 1 ipsec-isakmp
 match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer ipv6 2001:db8::172:16:1:2
 set pre-fragmentation
 set dead-connection history off
crypto map VPN_IPV6 2 ipsec-isakmp
 match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE2_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer ipv6 2001:db8::172:16:2:2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::172:16:100:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface GigabitEthernet0/1
 no ip address
 ipv6 address 2001:db8::192:168:100:1/112
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::172:16:100:1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://[2001:db8::172:16:101:15]/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
```

```
0A06082A85030701010302306931 0B300906035504061302525531133011 0603
550407130A5A656C656E6F6772616431143012060355040A130B532D54657272
6120435350310C300A060355040B1303526E443121301F06035504031318532D
5465727261204353502054657374205 26F6F74204341301E170D313931303131
3036353230305A170D333931303131303730313539 5A3069310B300906035504
0613025255311330110603550407130A5A656C656E6F6772616431143012060 3
55040A130B532D5465727261204353503 10C300A060355040B1303526E443121
301F06035504031318532D5465727261204353502054657374205 26F6F742043
413066301F06082A85030701010101301306072A85030202301060 82A850307
0101020203430004404D765AA83710D69F7C61A5AC9C875BC67EBD77EBD9ECA7
2F87EE655C9F8D15F57E86190229309899FDDED212CF0EF482C9B1FDC03B0224
CF745280875C2742A8A351304F300B0603551D0F040403020186300F0603551D
130101FF040530030101FF301D0603551D0E041604149481B6585600F773A290
4D575026EDC82AAD04E1301006092B060104018237150104030201003 00A0608
2A85030701010302034100464986BFF801832B3F3DE1BD725DA9E065A8098425
ADE9BB6B223814A76CEC9E9BD24ECA72A6AE472E96144F5AAA08F9CDC3DA5457
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Mar 27 15:51:07 2024

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP Converter
at Wed Mar 27 15:51:07 2024 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    IPv6Routes =
        Route(
            Destination = ::/0
            Gateway = 2001:db8::172:16:100:1
        )

)

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

```
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:FIREWALL_IN:FW_INPUT_WAN_IPV6 (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 135
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 136
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:100:2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:100:2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:100:2
        ProtocolID = 58
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
```

```
    Filter (
        DestinationIP = 2001:db8::172:16:100:2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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_IPV6:1
(
    IKEPeerIPFilter = 2001:db8::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_IPV6:2
(
    IKEPeerIPFilter = 2001:db8::172:16:2:2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 20
)

IPsecAction IPsecAction:VPN_IPV6:1
(
    TunnelingParameters = IPv6TunnelEntry(
        PeerAddress = 2001:db8::172:16:1:2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN_IPV6:1
)

IPsecAction IPsecAction:VPN_IPV6:2
(
    TunnelingParameters = IPv6TunnelEntry(
        PeerAddress = 2001:db8::172:16:2:2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN_IPV6:2
)

FilterChain IPsecPolicy:VPN_IPV6 (
    IPv6Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 2001:db8::192:168:100:0/112
        DestinationIP = 2001:db8::192:168:1:0/112
        Action = PASS
```

```
        ExtendedAction = ipsec< sa = IPsecAction:VPN_IPV6:1 >
        LogEventID = "IPsec:Protect:VPN_IPV6:1:IPSEC_ACL_HUB1_AND_SPOKE1_IPV6"
    ),
    Filter (
        Label = "VPN_IPV6:2:IPSEC_ACL_HUB1_AND_SPOKE2_IPV6"
        SourceIP = 2001:db8::192:168:100:0/112
        DestinationIP = 2001:db8::192:168:2:0/112
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN_IPV6:2 >
        LogEventID = "IPsec:Protect:VPN_IPV6:2:IPSEC_ACL_HUB1_AND_SPOKE2_IPV6"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN:FW_INPUT_WAN_IPV6
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN_IPV6
)
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/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 v6-network SELF-IPV6
 remark WAN IP
 host 2001:db8::172:16:1:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering permit
!
ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 permit ipv6 2001:db8::192:168:1:0/112 2001:db8::192:168:100:0/112
!
ipv6 access-list FW_INPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit udp any object-group SELF-IPV6 eq isakmp
 permit udp any object-group SELF-IPV6 eq non500-isakmp
 permit icmp any object-group SELF-IPV6
 permit esp any object-group SELF-IPV6
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto map VPN_IPV6 1 ipsec-isakmp
 match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer ipv6 2001:db8::172:16:100:2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::172:16:1:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface GigabitEthernet0/1
 no ip address
 ipv6 address 2001:db8::192:168:1:1/112
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::172:16:1:1
!
crypto pki trustpoint s-terra_technological_trustpoint
```

```
 revocation-check crl
 crl download group ROOTCA http://[2001:db8::172:16:101:15]/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
0A06082A850307010103023069310B300906035504061302525531133011060
550407130A5A656C656E6F6772616431143012060355040A130B532D54657272
6120435350310C300A060355040B1303526E443121301F06035504031318532D
5465727261204353502054657374205265737420526F6F74204341301E170D313931303131
3036353230305A170D3339313031313037303135395A3069310B300906035504
0613025255311330110603550407130A5A656C656E6F67726164311430120603
55040A130B532D5465727261204353502054657374205265737420526F6F742043
413066301F06082A850307010101013013060728A8503020223010608 2A850307
0101020203430004404D765AA83710D69F7C61A5AC9C875BC67EBD77EBD9ECA7
2F87EE655C9F8D15F57E86190229309899FDDED212CF0EF482C9B1FDC03B0224
CF745280875C2742A8A351304F300B0603551D0F040403020186300F0603551D
130101FF040530030101FF301D0603551D0E041604149481B6585600F773A290
4D575026EDC82AAD04E1301006092B06010401823715010403020100300A0608
2A850307010103020341004649868FF801832B3F3DE1BD725DA9E065A8098425
ADE9BB6B223814A76CEC9E9BD24ECA72A6AE472E96144F5AAA08F9CDC3DA5457
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Mar 27 14:38:14 2024

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Wed Mar 27 14:38:14 2024 (user: cscons)"
    Version                       = LSP_5_0
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

RoutingTable(
    IPv6Routes =
        Route(
            Destination = ::/0
            Gateway = 2001:db8::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:FIREWALL_IN:FW_INPUT_WAN_IPV6 (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 135
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 136
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:1:2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:1:2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
```

```
        DestinationIP = 2001:db8::172:16:1:2
        ProtocolID = 58
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:1:2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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_IPV6:1
(
    IKEPeerIPFilter = 2001:db8::172:16:100:2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:VPN_IPV6:1
(
    TunnelingParameters = IPv6TunnelEntry(
        PeerAddress = 2001:db8::172:16:100:2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN_IPV6:1
)

FilterChain IPsecPolicy:VPN_IPV6 (
    IPv6Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 2001:db8::192:168:1:0/112
        DestinationIP = 2001:db8::192:168:100:0/112
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN_IPV6:1 >
        LogEventID = "IPsec:Protect:VPN_IPV6:1:IPSEC_ACL_HUB1_AND_SPOKE1_IPV6"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN:FW_INPUT_WAN_IPV6
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN_IPV6
)
```

Конфигурации криптошлюза Spoke2

1. Консоль cisco-like:

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

```
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group v6-network SELF-IPV6
 remark WAN IP
 host 2001:db8::172:16:2:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering permit
!
ipv6 access-list IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 permit ipv6 2001:db8::192:168:2:0/112 2001:db8::192:168:100:0/112
!
ipv6 access-list FW_INPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit udp any object-group SELF-IPV6 eq isakmp
 permit udp any object-group SELF-IPV6 eq non500-isakmp
 permit icmp any object-group SELF-IPV6
 permit esp any object-group SELF-IPV6
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
```

```
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto map VPN_IPV6 1 ipsec-isakmp
 match ipv6 address IPSEC_ACL_HUB1_AND_SPOKE1_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer ipv6 2001:db8::172:16:100:2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::172:16:2:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface GigabitEthernet0/1
 no ip address
 ipv6 address 2001:db8::192:168:2:1/112
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::172:16:2:1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://[2001:db8::172:16:101:15]/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
0A06082A850307010103023069310B300906035504061302525531133011060603
550407130A5A656C656E6F6772616431143012060355040A130B532D54657272
6120435350310C300A060355040B1303526E443121301F06035504031318532D
5465727261204353502054657374205261F6F74204341301E170D313931303131
3036353230305A170D333931303131303730313539 5A3069310B300906035504
0613025255311330110603550407130A5A656C656E6F67726164311430120603
55040A130B532D5465727261204353502054657374205261F6F742043
413066301F06082A850307010101013013060 72A850302022301060 82A850307
0101020203430004404D765AA83710D69F7C61A5AC9C875BC67EBD77EBD9ECA7
2F87EE655C9F8D15F57E86190229309899FDDED212CF0EF482C9B1FDC03B0224
CF745280875C2742A8A351304F300B0603551D0F040403020186300F0603551D
130101FF040530030101FF301D0603551D0E041604149481B6585600F773A290
4D575026EDC82AAD04E1301006092B06010401823715010403020100300A0608
2A850307010103020341004649 86BFF801832B3F3DE1BD725DA9E065A8098425
ADE9BB6B223814A76CEC9E9BD24ECA72A6AE472E96144F5AAA08F9CDC3DA5457
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Mar 27 14:39:39 2024

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Wed Mar 27 14:39:39 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    IPv6Routes =
        Route(
            Destination = ::/0
            Gateway = 2001:db8::172:16:2:1
        )

)

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

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

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

FilterChain FilterChain:FIREWALL_IN:FW_INPUT_WAN_IPV6 (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
```

```
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 135
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        ProtocolID = 58
        ICMPType = 136
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:2:2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:2:2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:2:2
        ProtocolID = 58
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = 2001:db8::172:16:2:2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN_IPV6"
    ),
    Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
```

```
        DestinationIP = ::/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        DestinationIP = ::/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        DestinationIP = ::/0
        Action = PASS
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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_IPV6:1
(
    IKEPeerIPFilter = 2001:db8::172:16:100:2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:VPN_IPV6:1
(
    TunnelingParameters = IPv6TunnelEntry(
        PeerAddress = 2001:db8::172:16:100:2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
```

```
    DFHandling = COPY
    IKERule = IKERule:VPN_IPV6:1
)

FilterChain IPsecPolicy:VPN_IPV6 (
    IPv6Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 2001:db8::192:168:2:0/112
        DestinationIP = 2001:db8::192:168:100:0/112
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN_IPV6:1 >
        LogEventID = "IPsec:Protect:VPN_IPV6:1:IPSEC_ACL_HUB1_AND_SPOKE1_IPV6"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN:FW_INPUT_WAN_IPV6
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN_IPV6
)
```