Настройка DMVPN (phase 2) dual cloud с протоколом динамической маршрутизации iBGP (IPv4 через 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

Данная инструкция описывает настройку DMVPN IPv4 (LAN) через IPv6 (WAN), для сетевых инженеров, знакомых с данной технологией по оборудованию Cisco, а также разбирающихся в базовых настройках «С-Терра Шлюз».

Краткое описание технологии DMVPN

Технология DMVPN (англ. Dynamic Multipoint Virtual Private Network – динамическая многоточечная виртуальная частная сеть) позволяет динамически строить защищенные соединения без необходимости описывать каждое соединение в политике безопасности, что существенно упрощает масштабирование крупных сетей с полносвязной топологией. Автоматическое построение полносвязной защищенной топологии достигается за счет применения динамических протоколов маршрутизации и таких протоколов как NHRP (англ. Next Hop Resolution Protocol – протокол разрешения следующего узла) и multipoint GRE (англ. Generic Routing Encapsulation).

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, NHRP, GRE, OSPF, BGP, VRRP.

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.

© 2003-2025 S-Terra CSP

Также Администратор должен быть ознакомлен со сценарием «Настройка DMVPN (phase 2) dual cloud с протоколом динамической маршрутизации iBGP». Далее по тексту он будет называться базовым сценарием DMVPN IPv4.

Дополнительно, Администратор должен быть ознакомлен со сценариями «Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (IPv4 через IPv6)» и «Настройка DMVPN (phase 2) dual cloud с протоколом динамической маршрутизации iBGP (протокол IPv6)».

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.

      1.1.2. При использовании «С-Терра Шлюз» на виртуальных машинах тип сетевого адаптера виртуальной машины должен быть “VMXNET 3”. Работа на других типах адаптеров не гарантируется.

   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).

      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 устройствами стенда должна быть обеспечена IP связность.

© 2003-2025 S-Terra CSP

Общая схема стенда

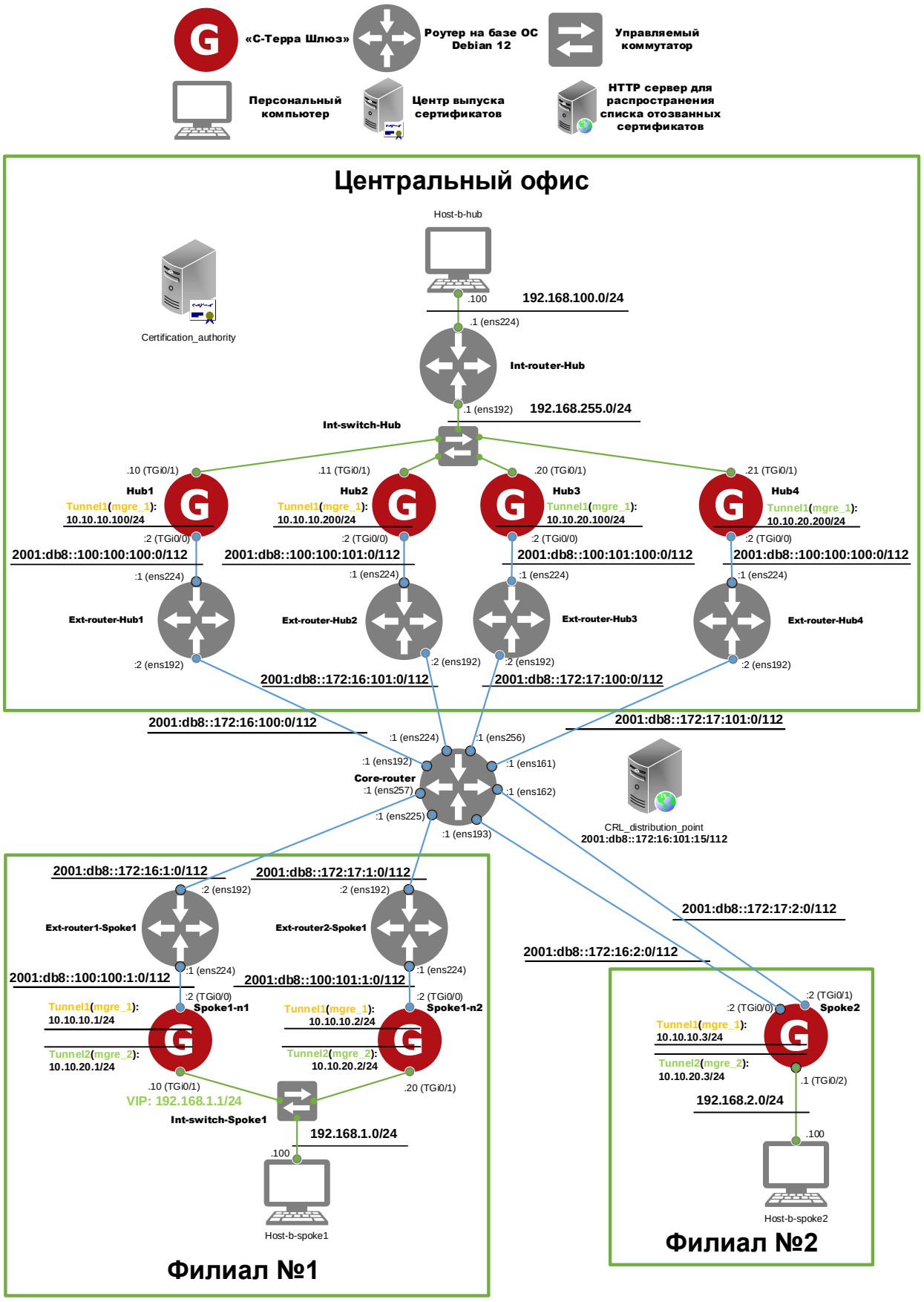


Рисунок 1. Общая схема стенда

Общая логика работы

Данная инструкция описывает настройку технологии DMVPN на криптошлюзах безопасности «С-Терра Шлюз» 5.0. Будет настроено две mGRE подсети (dual cloud) и использован протокол динамической маршрутизации iBGP. В каждой mGRE подсети будет по два Hub. По окончании настройки реализуется возможность построения динамических защищенных соединений между всеми подсетями филиалов, а также подсетями филиалов и центрального офиса (см. Рисунок 1).

Стенд состоит из 20 устройств:

- «С-Терра Шлюз» версии 5.0: Hub1, Hub2, Hub3, Hub4, Spoke1-n1, Spoke1-n2, Spoke2.
- Роутеры на базе ОС Debian 12: Int-router-Hub, Ext-router-Hub1, Ext-router-Hub2, Ext-router-Hub3, Ext-router-Hub4, Core-router, Ext-router1-Spoke1, Ext-router2-Spoke1.
- Управляемые коммутаторы: Int-switch-Hub, Int-switch-Spoke1.
- Персональные компьютеры: Host-b-hub, Host-b-spoke1, Host-b-spoke2.

Роутеры на базе ОС Debian 12 выбраны в качестве примера. В общем случае могут быть использованы любые маршрутизаторы, поддерживающие функции NAT и динамической маршрутизации (NAT в ОС Debian 12 будет реализован при помощи iptables, а динамическая маршрутизация при помощи пакета FRR).

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), 4 криптошлюза «С-Терра Шлюз» (Hub1, Hub2, Hub3 и Hub4) версии 5.0, 4 маршрутизатора, преобразующие IPv6 адреса (Ext-router-Hub1, Ext-router-Hub2, Ext-router-Hub3, Ext-router-Hub4), маршрутизатор, анонсирующий в BGP маршрут до защищаемой подсети центрального офиса (Int-router-Hub), и персональный компьютер (Host-b-hub).

   1.2. В филиале № 1 размещаются: 2 криптошлюза «С-Терра Шлюз» (Spoke1-n1 и Spoke1-n2) версии 5.0, 2 маршрутизатора, преобразующие IPv6 адрес, 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 размещаются: маршрутизатор (Core-router) и HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point).

2. Подключение к сети Интернет.

   В данном сценарии для эмуляции сети Интернет используется маршрутизатор Core-router.

   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. Криптошлюзы Hub1, Hub2, Hub3 и Hub4 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизаторы Ext-router-Hub1, Ext-router-Hub2, Ext-router-Hub3 и Ext-router-Hub4 соответственно).

   2.2. Криптошлюзы Spoke1-n1 и Spoke1-n2 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Ext-router1-Spoke и Ext-router2-Spoke соответственно).

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

3. Параметры шифрования IPsec.

   Весь трафик между центральным офисом (192.168.100.0/24) и филиалами (192.168.1.0/24, 192.168.2.0/24) инкапсулируется в GRE, а GRE трафик защищается с использованием алгоритмов ГОСТ и протокола IPsec в транспортном IPv6 режиме.

© 2003-2025 S-Terra CSP

Между криптошлюзами в филиалах и центральным офисом устанавливаются статические IPsec туннели. Инициатором подключения является служебный трафик протоколов NHRP/BGP.

Между филиальными криптошлюзами устанавливаются динамические IPsec туннели. Инициатором построения туннелей является реальный трафик защищаемых подсетей филиалов.

Режим работы IPsec туннеля должен быть транспортным. Работа IPsec туннеля в туннельном режиме не поддерживается для сети DMVPN на криптошлюзах безопасности «С-Терра Шлюз 5.0».

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 заблокирован.

4.1.2. На LAN интерфейсах IPv4 трафик не заблокирован.

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 заблокирован исходящий незашифрованный GRE трафик и транзитный трафик до приватных IP адресов.

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).

4.1.6. На WAN интерфейсах IPv4 трафик заблокирован – входящий и исходящий.

5. Отказоустойчивость.

Отказоустойчивость обеспечивается протоколом NHRP и протоколом динамической маршрутизации BGP. Филиальные криптошлюзы одновременно регистрируются по протоколу NHRP на Hub1, Hub2, Hub3 и Hub4. Hub1 и Hub2 находятся в одной mGRE-подсети (10.10.10.0/24), а Hub3 и Hub4 находятся во второй mGRE-подсети (10.10.20.0/24).

Поддержка нескольких Hub в одной mGRE-подсети осуществляется, начиная с «С-Терра Шлюз» версии 5.0.

5.1. Динамическая маршрутизация.

Динамическая маршрутизация между криптошлюзами филиалов и центрального офиса обеспечивается протоколом Internal BGP. Все криптошлюзы безопасности находятся в одной автономной системе №65000.

Криптошлюзы безопасности, установленные в филиалах, отсылают маршрутную информацию о защищаемых подсетях только криптошлюзам в центральный офис, соответственно, получение маршрутной информации происходит тоже только из центрального офиса. Маршруты до защищаемых подсетей устанавливаются через mGRE-интерфейсы. Центральные криптошлюзы являются роут-рефлекторами (route-reflector), а филиальные – роут-рефлектор клиентами (route-reflector client).

Между криптошлюзами в центральном офисе и роутером Int-router-Hub (AS №65001) передача маршрутной информации обеспечивается при помощи External BGP. Между криптошлюзами в центральном офисе передача маршрутной информации не обеспечивается.

На каждом криптошлюзе филиала и на роутере Int-router-Hub будет набор резервирующих друг друга маршрутов для каждой из защищаемых подсетей, из которых будет использоваться лучший из доступных в настоящий момент. Выбор лучшего из доступных маршрутов будет настроен по правилу статического приоритета, которые будут определены при конфигурировании.

5.2. Отказоустойчивость филиала № 1.

Повышение отказоустойчивости Филиала № 1 обеспечивается использованием протокола VRRP на LAN интерфейсах криптошлюзов. Криптошлюзы Spoke1-n1 и Spoke1-n2 объединяются в отказоустойчивый кластер, работающий на базе протокола VRRP в режиме Master/Backup. Протокол VRRP реализуется сервисом keepalived.

Конфигурация между нодами кластера не синхронизируется. При изменении настроек на одной ноде нужно выполнить аналогичные настройки на другой.

Нода, находящаяся в состоянии Master, владеет VIP адресом в доверенном сегменте и, соответственно, обрабатывает трафик. Нода, находящаяся в состоянии Backup или Fault, не владеет VIP адресом.

При помощи скрипта `/etc/keepalived/scripts/check_ping` сервис `keepalived` дополнительно контролирует состояние канала Интернет-провайдера посредством проверки доступности заданных узлов по протоколу ICMP. Если все заданные узлы недоступны определенное время, то нода кластера переходит в состояние FAULT, что приводит к переключению кластера на резервную ноду (в случае, если она была в состоянии BACKUP), которая подключена к другому Интернет-провайдеру. Резервирование подключения к Интернет обеспечивается следующим принципом – каждая нода кластера филиала подключается к соответствующему Интернет-провайдеру.

При помощи конфигурационного файла `/etc/keepalived/notify_common.conf` и скрипта `/etc/keepalived/scripts/notify_common` обеспечивается следующая логика. Если нода переходит в состояние BACKUP или FAULT, то BGP пиринг с центральными

криптошлюзами выключается. Если нода переходит в состояние MASTER, то BGP пиринг с центральными криптошлюзами включается.

Также в настройках FRR добавляется маршрут до защищаемой сети центрального офиса через VIP адрес с дистанцией 240. Таким образом, если был получен маршрут по BGP, то он будет более приоритетным, чем маршрут через VIP адрес.

На портах коммутатора Int-switch-Spoke1, подключенных к криптошлюзам, обязательно должен быть включен режим `portfast`.

5.3. Отказоустойчивость филиала № 2.

Отказоустойчивость филиала реализована резервированием каналов связи и управлением резервированными каналами связи при помощи сервиса «multiwan». Режим работы каналов основной/резервный. При отказе основного канала связи происходит переключение на работу через резервный канал связи (если он был доступен). При восстановлении работы основного канала связи происходит переключение на работу через основной канал связи.

Настройка стенда

Настройка устройства Host-b-hub

На данном устройстве должны быть настроены IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).

Настройка устройства Host-b-spoke1

На данном устройстве должны быть настроены IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).

Настройка устройства Host-b-spoke2

На данном устройстве должны быть настроены IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).

Настройка устройства Int-switch-Hub

На данном устройстве сетевые интерфейсы, коммутирующие криптошлюзы Hub1, Hub2, Hub3, Hub4 и роутер Int-router-Hub, должны быть в одном VLAN и в режиме portfast.

Настройка устройства Int-switch-Spoke1

На данном устройстве сетевые интерфейсы, коммутирующие криптошлюзы Spoke1-n1, Spoke1-n2 и персональный компьютер Host-b-spoke1, должны быть в одном VLAN и в режиме portfast.

Настройка устройства Core-router

На данном устройстве должны быть настроены IP-адреса в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).

Настройка устройства Ext-router-Hub1

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Ext-router-Hub2

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Ext-router-Hub3

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Ext-router-Hub4

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Ext-router1-Spoke1

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Ext-router2-Spoke1

На данном устройстве должно быть настроено:

1. IP-адреса и маршрутизация в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Source NAT/Destination NAT. В приложении представлены настройки iptables (содержимое файла `/etc/iptables.rules`).

Настройка устройства Int-router-Hub

На данном устройстве должно быть настроено:

1. IP-адреса в соответствии с общей схемой стенда (см. Рисунок 1). В приложении представлены сетевые настройки (содержимое файла `/etc/network/interfaces`).
2. Динамическая маршрутизация. В приложении представлены настройки FRR.

Настройка устройства Hub1

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 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.

© 2003-2025 S-Terra CSP

Настройка сетевых параметров

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

1. Проверьте включена ли маршрутизация IPv6, выполнив следующую команду:

```
root@sterragate:~# 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:

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

3. Включите внешний `TenGigabitEthernet0/0` (WAN) и внутренний `TenGigabitEthernet0/1` (LAN) интерфейсы:

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

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

4. Настройте IPv6 адрес на WAN интерфейсе и IPv4 адрес на LAN интерфейсе в соответствии со схемой стенда и маршрут по умолчанию:

```
Hub1(config)#interface TenGigabitEthernet0/0
Hub1(config-if)# no ip address
Hub1(config-if)# ipv6 address 2001:db8::100:100:100:2/112
Hub1(config-if)#interface TenGigabitEthernet0/1
Hub1(config-if)# no ip address
Hub1(config-if)# ip address 192.168.255.10 255.255.255.0
Hub1(config-if)# exit
Hub1(config)# ipv6 route ::/0 2001:db8::100:100:100:1
Hub1(config)#end
```

Примечание – В отличие от сценария «Настройка DMVPN (phase 2) dual cloud с протоколом динамической маршрутизации iBGP (протокол IPv6)» проверка доступности маршрута по умолчанию на данном этапе не производится, так как команда `ipv6 default filtering permit` не применялась. В связи с этим проверка доступности маршрута по умолчанию будет произведена после настройки правил межсетевого экранирования, когда будут созданы списки доступа IPv6 на WAN интерфейсе.

Настройка шифрования

Настройки шифрования осуществляются из cisco-like консоли криптошлюза.

1. Параметры IKE:

1.1. Задайте общие параметры IKE:

```
Hub1(config)#crypto isakmp identity dn
Hub1(config)#crypto isakmp keepalive 3 3
Hub1(config)#crypto isakmp keepalive retry-count 3
```

```
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 алгоритмы 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 (алгоритм IKE) под именем `ALGS_PROFILE`:

```
Hub1(config)#crypto isakmp profile ALGS_PROFILE
% A profile is deemed incomplete until it has match identity statements
Hub1(conf-isa-prof)# match identity dn
Hub1(conf-isa-prof)# set identity mapping
Hub1(conf-isa-prof)# set policy 1
Hub1(conf-isa-prof)#exit
```

Примечание - В настоящем сценарии в отличии от базового сценария DMVPN IPv4 используется один раздел криптокарты с одним isakmp профилем, к которому привязана только одна isakmp политика. В базовом сценарии DMVPN IPv4 вторая isakmp политика использовалась для подключения криптошлюзов версии 4.3. Однако, криптошлюзы версии 4.3 не поддерживают IPv6 и поэтому в настоящем сценарии не рассматриваются.

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

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

Режим работы IPsec туннеля должен быть транспортным. В отличие от криптошлюзов версии 4.3 туннельный режим IPsec в сценарии DMVPN для криптошлюзов версии 5.0 не поддерживается и не может быть использован даже при отсутствии NAT.

2.3. Создайте сетевой `object-group` с именем `SELF-IPV6` для хранения в нем WAN адресов криптошлюза с целью дальнейшего его использования в ACL:

```
Hub1(config)# object-group v6-network SELF-IPV6
Hub1(config-v6network-group)#description IP on WAN interface
Hub1(config-v6network-group)# host 2001:db8::100:100:100:2
Hub1(config-v6network-group)#exit
```

2.4. Создайте список доступа (ACL) для IPv6 трафика, который нужно защищать между центральным офисом и филиалами:

```
Hub1(config)# ipv6 access-list IPSEC_DMVPN_IPV6
Hub1(config-ipv6-acl)# remark special DMVPN filter
Hub1(config-ipv6-acl)# permit gre object-group SELF-IPV6 each
Hub1(config-ipv6-acl)#exit
```

```
Hub1(config)#
```

Примечание - Ключевое слово `each` позволяет строить узкие IPsec туннели для любого адреса назначения. Адрес назначения берется из IP заголовка GRE пакета, в котором находится NBMA адрес криптошлюза.

2.5. Создайте динамическую крипто-карту (имя DMAP_IPV6, раздел 1) и привяжите её к статической (имя VPN_IPV6, раздел 1):

```
Hub1(config)# crypto dynamic-map DMAP_IPV6 1
Hub1(config-crypto-map)# match ipv6 address IPSEC_DMVPN_IPV6
Hub1(config-crypto-map)# set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)# set isakmp-profile ALGS_PROFILE
Hub1(config-crypto-map)# set security-association mss-fix out
Hub1(config-crypto-map)# set pre-fragmentation
Hub1(config-crypto-map)# set dead-connection history off
Hub1(config-crypto-map)#exit
Hub1(config)#crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
Hub1(config)#
```

2.6. Прикрепите созданную статическую крипто-карту к внешнему интерфейсу `TenGigabitEthernet0/0`:

```
Hub1(config)#interface TenGigabitEthernet0/0
Hub1(config-if)#crypto map VPN_IPV6
Hub1(config-if)#exit
```

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

По умолчанию на всех сетевых интерфейсах IPv6 трафик заблокирован – команда `ipv6 default filtering deny`. Команда `ipv6 default filtering deny` запрещает прохождение трафика IPv6 во всех направлениях на интерфейсах без списков доступа IPv6. Ниже будут созданы списки доступа IPv6 на WAN интерфейсе. Описание команды `ipv6 default filtering deny|permit` приведено в сценарии «Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (протокол IPv6)».

Настройка межсетевого экрана осуществляются из cisco-like консоли.

1. Создайте ACL с именем `FW_OUTPUT_WAN_IPV6` для исходящего с WAN интерфейс IPv6 трафика:

Список доступа IPv6 для исходящего трафика должен блокировать весь транзитный трафик и незашифрованный GRE IPv6, в который инкапсулирован открытый трафик IPv4 из защищаемой подсети криптошлюза 192.168.100.100/24 в защищаемые подсети филиалов 192.168.1.100/24 и 192.168.2.100/24 (считаем, что трафик защищаемых криптошлюзами подсетей должен обязательно шифроваться), а также открытый служебный трафик NHRP и BGP.

```
Hub1(config)# ipv6 access-list FW_OUTPUT_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)#deny gre any any
Hub1(config-ipv6-acl)#permit ipv6 object-group SELF-IPV6 any
Hub1(config-ipv6-acl)#exit
```

2. Создайте ACL с именем `FW_INPUT_WAN_IPV6` для входящего на WAN интерфейс IPv6 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 isakmp
Hub1(config-ipv6-acl)#permit udp any object-group SELF-IPV6 eq non500-isakmp
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
```

Примечание - Список доступа для входящего трафика разрешает пакеты сообщений NS и NA протокола Neighbor Discovery (подробнее смотри п. 4.1.3.1 в “Общая логика работы”), входящие пакеты протоколов IKE, ESP, ICMP, а остальные блокирует только для случая, когда криптошлюз является ответчиком **впервые.** Если криптошлюз является инициатором или ответчиком в рамках ранее созданной сессии, то ответные пакеты будут разрешены, так как согласно алгоритму работы stateful фильтрации динамические разрешающие правила более приоритетны чем статические. Stateful фильтрация будет настроена далее в данном разделе. Динамические правила stateful фильтрации в cisco-like консоли НЕ отображаются, их можно посмотреть при помощи утилиты `fwconn_mgr` с параметром `show`.

3. Создайте ACL 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)#exit
Hub1(config)#ip access-list extended FIREWALL_IN
Hub1(config-ext-nacl)#deny ip any any
Hub1(config-ext-nacl)#exit
```

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 tcp
```

5. Прикрепите списки доступа и правила инспектирования на внешний интерфейс:

```
Hub1(config)#interface TenGigabitEthernet0/0
Hub1(config-if)#ipv6 access-group FW_OUTPUT_WAN_IPV6 out
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
Hub1(config-if)#exit
```

6. Проверьте доступность маршрута по умолчанию:

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

```
PING 2001:db8::100:100:100:1(2001:db8::100:100:100:1) 100 data bytes
108 bytes from 2001:db8::100:100:100:1: icmp_seq=1 ttl=64 time=0.297 ms
108 bytes from 2001:db8::100:100:100:1: icmp_seq=2 ttl=64 time=0.520 ms
108 bytes from 2001:db8::100:100:100:1: icmp_seq=3 ttl=64 time=0.331 ms
108 bytes from 2001:db8::100:100:100:1: icmp_seq=4 ttl=64 time=0.360 ms
108 bytes from 2001:db8::100:100:100:1: icmp_seq=5 ttl=64 time=0.534 ms

--- 2001:db8::100:100:100:1 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4074ms
rtt min/avg/max/mdev = 0.297/0.408/0.534/0.098 ms
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка mGRE-интерфейса

На центральных шлюзах должно быть по одному mGRE-интерфейсу.

1. Настройки mGRE интерфейсов осуществляются из linux bash, чтобы попасть в linux bash выполните следующую команду в CLI разграничения доступа (предварительно нужно выйти из консоли cisco-like):

```
Hub1#exit
administrator@Hub1] system
```

```
Entering system shell...
root@Hub1:~#
```

2. Создайте файл `/etc/network/interfaces.d/mgre0` и добавьте в него следующее содержимое:

Имя mGRE-интерфейса должно соответствовать шаблону: mgreN, где N – целое число.

```
auto mgre0
iface mgre0 inet static
address 10.10.10.100/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

При необходимости использовать явно заданную привязку физического адреса для отправки пакетов mGRE-туннеля не допускается использовать dev без local в комманде ip tunnel.

Пример правильной команды:

pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit **dev** eth0 **local** 2001:db8::100:100:100:2

3. Поднимите mGRE-интерфейс:

```
root@Hub1:~# ifup mgre0
```

4. Убедитесь, что mGRE-интерфейс создан с нужными параметрами:

```
root@Hub1:~# ip -6 tunnel show mgre0
```

```
mgre0: gre/ipv6 remote :: local :: encaplimit 4 hoplimit 64 tclass inherit flowlabel
0x00000 (flowinfo 0x00000000) key 1
```

```
root@Hub1:~# ip address show dev mgre0
```

```
7: mgre0@NONE: <MULTICAST,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group
default qlen 10000
    link/gre6 :: brd :: permaddr 4232:e564:3172::
    inet 10.10.10.100/24 brd 10.10.10.255 scope global mgre0
       valid_lft forever preferred_lft forever
    inet6 fe80::a0a:a64/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::7f00:1/64 scope host
       valid_lft forever preferred_lft forever
```

Настройка NHRP

Настройки NHRP интерфейсов осуществляются из linux bash в следующей последовательности:

1. Приведите файл `/etc/opennhrp/opennhrp.conf` к виду:

```
interface mgre0
 multicast dynamic
 holding-time 90
 cisco-authentication secret
 non-caching
```

Примечание – Допустимый диапазон значения `holding-time` – от 30 до 150 секунд. Подробное описание параметра `holding-time` и ограничения по его изменению приведено в Базовом сценарии DMVPN IPv4 в разделе Описание параметра holding-time.

2. Добавьте сервис OpenNHRP в автозагрузку и запустите его:

```
root@Hub1:~# systemctl enable opennhrp
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/opennhrp.service -> /lib/systemd/system/opennhrp.service.
```

```
root@Hub1:~# systemctl start opennhrp
```

Настройка BGP

Динамическая маршрутизация настраивается через консоль сервиса FRR.

1. Добавьте сервис FRR в автозагрузку и запустите его:

```
root@Hub1:~# 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
Created symlink /etc/systemd/system/multi-user.target.wants/frr.service → /lib/systemd/system/frr.service.
```

```
root@Hub1:~# systemctl start frr
```

2. Войдите в консоль сервиса FRR, для этого нужно из linux bash набрать следующую команду:

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

```

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

Hub1#
```

3. Настройте BGP (см. описание http://docs.frrouting.org):

```
Hub1# configure terminal
```

3.1. Создайте route-map `FROM-HUB1-OUT`, которая будет менять `local-preference` для маршрутов, которые Hub1 получает из автономной системы 65001 (192.168.100.0/24) и ретранслирует в криптошлюзы филиалов:

```
Hub1(config)# route-map FROM-HUB1-OUT permit 1
Hub1(config-route-map)# set local-preference 100
Hub1(config-route-map)# exit
```

Примечание - route-map будет изменять статический приоритет (`local-preference`) для объявляемых маршрутов или маршрутов, полученных по eBGP и не будет влиять на `local-preference` маршрутов, полученных от Spoke-ов. Подробнее – смотри в базовом сценарии DMVPN IPv4.

3.2. Включите процесс протокола BGP для автономной системы 65000 и перейдите в режим его конфигурирования:

```
Hub1(config)# router bgp 65000
```

3.3. Установите идентификатор маршрутизатора:

```
Hub1(config-router)# bgp router-id 10.10.10.100
```

3.4. Включите логирование изменения статуса (например, up, down и другие) BGP соседа в журнале работы:

```
Hub1(config-router)# bgp log-neighbor-changes
```

3.5. Отключите обязательное наличие BGP фильтров для обмена маршрутами по eBGP сессий:

```
Hub1(config-router)# no bgp ebgp-requires-policy
```

Примечание - Команда `bgp ebgp-requires-policy` включена по умолчанию и требует наличие фильтров при работе с eBGP соседями. В настоящем сценарии отключение ebgp-requires-policy производится с целью упрощения конфигурирования. Подробнее – смотри в базовом сценарии DMVPN IPv4.

3.6. Установите таймеры keepalive и hold time для BGP соседей:

```
Hub1(config-router)# timers bgp 3 9
```

Примечание - Данные настройки производятся с целью ускорения сходимости iBGP и по согласованию с Производителем могут изменяться.

3.7. Создайте группу spokes-ibgp с номером автономной системы 65000 для BGP соседей из mgre подсети (криптошлюзов филиалов):

```
Hub1(config-router)# neighbor spokes-ibgp peer-group
Hub1(config-router)# neighbor spokes-ibgp remote-as 65000
Hub1(config-router)# bgp listen range 10.10.10.0/24 peer-group spokes-ibgp
```

3.8. Измените максимальное количество BGP соседей, которые могут подключиться к криптошлюзу по BGP одновременно:

```
Hub1(config-router)# bgp listen limit 5000
```

3.9. Добавьте bgp соседа 192.168.255.1 с номером автономной системы 65001:

```
Hub1(config-router)# neighbor 192.168.255.1 remote-as 65001
```

3.10. Включите пересылку маршрутов для группы `spokes-ibgp`:

```
Hub1(config-router)# address-family ipv4 unicast
Hub1(config-router-af)# neighbor spokes-ibgp route-reflector-client
```

3.11. Включите изменение nexthop адреса для маршрутов, полученных по eBGP, на адрес Hub1:

```
Hub1(config-router-af)# neighbor spokes-ibgp next-hop-self
```

Примечание - Чтобы изменять next-hop адреса маршрутов, полученных по iBGP, можно использовать команду «`neighbor spokes-ibgp next-hop-self force`». В этом случае трафик между филиалами будет идти через центр (Аналог первой фазы DMVPN).

3.12. Примените route-map `FROM-HUB1-OUT` на отправленные маршруты к соседям из группы `spokes-ibgp`:

```
Hub1(config-router-af)# neighbor spokes-ibgp route-map FROM-HUB1-OUT out
```

Примечание - Для данного сценария `local-preference` будет изменён для ретранслируемого маршрута до 192.168.100.0/24.

3.13. Сохраните изменения:

```
Hub1(config-router-af)# end
```

```
Hub1# write

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

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`.

Настройка устройства Hub2

Настройка устройства Hub2 осуществляется аналогично устройству Hub1 с учетом соответствующих IP-адресов (см. Рисунок 1). В настройках FRR значение `local-preference` должно быть равно 75.

Значение mGRE key на Hub1 и на Hub2 должны совпадать. Но должен отличаться от значения mGRE key на Hub3 и Hub4.

В Приложении представлены тексты конфигураций для криптошлюза Hub2:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`.

Настройка устройства Hub3

Настройка устройства Hub3 осуществляется аналогично устройству Hub1 с учетом соответствующих IP-адресов (см. Рисунок 1). В настройках FRR значение `local-preference` должно быть равно 50.

Значение mGRE key на Hub3 и на Hub4 должны совпадать. Но должен отличаться от значения mGRE key на Hub1 и Hub2.

В Приложении представлены тексты конфигураций для криптошлюза Hub3:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`.

Настройка устройства Hub4

Настройка устройства Hub4 осуществляется аналогично устройству Hub1 с учетом соответствующих IP-адресов (см. Рисунок 1). В настройках FRR значение `local-preference` должно быть равно 25.

Значение mGRE key на Hub3 и на Hub4 должны совпадать. Но должен отличаться от значения mGRE key на Hub1 и Hub2.

В Приложении представлены тексты конфигураций для криптошлюза Hub4:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;

- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`.

Настройка устройства Spoke1-n1

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, настройки PKI, настройка паролей доступа к консоли cisco-like, настройка сетевых параметров, настройка шифрования, настройка политики обработки COC (CRL) и настройка межсетевого экрана осуществляется аналогично устройству Hub1 с учетом соответствующих IP-адресов (см. Рисунок 1).

Настройка mGRE-интерфейсов

На филиальных шлюзах должно быть по два mGRE-интерфейса (по два на каждый центральный шлюз).

1. Настройки mGRE интерфейсов осуществляются из linux bash, чтобы попасть в linux bash выполните следующую команду в CLI разграничения доступа (предварительно нужно выйти из консоли cisco-like):

```
Spoke1-n1#exit
administrator@Spoke1-n1] system
```

```
Entering system shell...
root@Spoke1-n1:~#
```

2. Создайте файл `/etc/network/interfaces.d/mgre0` и добавьте в него следующее содержимое:

Имя mGRE-интерфейса должно соответствовать шаблону: mgreN, где N – целое число.

```
auto mgre0
iface mgre0 inet static
address 10.10.10.1/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

3. Создайте файл `/etc/network/interfaces.d/mgre1` и добавьте в него следующее содержимое:

Имя mGRE-интерфейса должно соответствовать шаблону: mgreN, где N – целое число.

```
auto mgre1
iface mgre1 inet static
address 10.10.20.1/24
pre-up ip link del mgre1 2> /dev/null || true
pre-up ip tunnel add mgre1 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
post-up ethtool -K mgre1 tx-checksumming off > /dev/null
post-down ip link del mgre1
```

4. Поднимите mGRE-интерфейс:

```
root@Spoke1-n1:~# ifup mgre0
root@Spoke1-n1:~# ifup mgre1
```

5. Убедитесь, что mGRE-интерфейс создан с нужными параметрами:

```
root@Spoke1-n1:~# ip -6 tunnel show mgre0
mgre0: gre/ipv6 remote :: local :: encaplimit 4 hoplimit 64 tclass inherit flowlabel
0x00000 (flowinfo 0x00000000) key 1
root@Spoke1-n1:~# ip -6 tunnel show mgre1
mgre1: gre/ipv6 remote :: local :: encaplimit 4 hoplimit 64 tclass inherit flowlabel
0x00000 (flowinfo 0x00000000) key 2
root@Spoke1-n1:~# ip address show dev mgre0
7: mgre0@NONE: <MULTICAST,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group
default qlen 10000
    link/gre6 :: brd :: permaddr 2e4e:df9e:a4d6::
    inet 10.10.10.1/24 brd 10.10.10.255 scope global mgre0
       valid_lft forever preferred_lft forever
    inet6 fe80::a0a:a01/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::7f00:1/64 scope host
       valid_lft forever preferred_lft forever
root@Spoke1-n1:~# ip address show dev mgre1
8: mgre1@NONE: <MULTICAST,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group
default qlen 10000
    link/gre6 :: brd :: permaddr ae1:c6d7:ab19::
    inet 10.10.20.1/24 brd 10.10.20.255 scope global mgre1
       valid_lft forever preferred_lft forever
    inet6 fe80::a0a:1401/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::a0a:a01/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::7f00:1/64 scope host
       valid_lft forever preferred_lft forever
```

Настройка NHRP

Настройка NHRP осуществляются из linux bash.

1. Приведите файл `/etc/opennhrp/opennhrp.conf` к виду:

Маска в настройках opennhrp должна совпадать с маской на mgre интерфейсе.

```
interface mgre0
 map 10.10.10.100/24 2001:db8::172:16:100:2 register
 map 10.10.10.200/24 2001:db8::172:16:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
interface mgre1
 map 10.10.20.100/24 2001:db8::172:17:100:2 register
 map 10.10.20.200/24 2001:db8::172:17:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
```

Примечание – В больших DMVPN сетях, содержащих более сотни устройств, может наблюдаться повышение нагрузки на криптошлюзы Центрального офиса после потери связи со всеми или большинством филиалов, например, из-за отказа провайдера. В этом случае криптошлюзы филиалов могут направлять Registration Request на Hub практически одновременно создавая пик нагрузки на него. Для повышения равномерности распределения по времени запросов Registration Request от филиальных криптошлюзов введен параметр `reregister-time` – время до начала перерегистрации Spoke на Hub после потери связи между ними. Пример настроек с использованием `reregister-time`:

```
interface mgre0
 map 10.10.10.100/24 2001:db8::172:16:100:2 register register reregister-time 60
 map 10.10.10.200/24 2001:db8::172:16:101:2 register reregister-time 45-75
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
```

По умолчанию время перерегистрации берётся из диапазона 60-180 секунд.

Подробнее – смотри в базовом сценарии DMVPN IPv4.

2. Добавьте сервис OpenNHRP в автозагрузку и запустите его:

```
root@Spoke1-n1:~# systemctl enable opennhrp
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/opennhrp.service -> /lib/systemd/system/opennhrp.service.
```

```
root@Spoke1-n1:~# systemctl start opennhrp
```

3. Через некоторое время проверьте, что между Spoke1-n1 и центральными криптошлюзами Hub1, Hub2, Hub3, Hub4 поднялись IPsec туннели (если туннели не поднялись – проверьте настройки сети/IPsec/Firewall/NHRP, лог-файлы `/var/log/cspvpngate.log` и `/var/log/syslog`):

```
root@Spoke1-n1:~# 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 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 7192 6312
2 11 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 6160 5448
3 12 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 7108 6312
4 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 46 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 101780
105684
2 47 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 38804
27104
3 48 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 23420
22204
4 49 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 15616
16192
5 50 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 296 296
```

Настройка BGP

Динамическая маршрутизация настраивается через консоль сервиса FRR.

1. Добавьте сервис FRR в автозагрузку и запустите его:

```
root@Spoke1-n1:~# systemctl enable frr
```

```
Synchronizing state of frr.service with SysV service script with /lib/system/system-sysv-install.
Executing: /lib/system/system-sysv-install enable frr
```

```
root@Spoke1-n1:~# systemctl start frr
```

2. Войдите в консоль сервиса FRR, для этого нужно из linux bash набрать следующую команду:

```
root@Spoke1-n1:~# vtysh
```

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

3. Добавьте маршрут 192.168.100.0/24 через VIP адрес (192.168.1.20) с дистанцией 240:

```
Spoke1-n1#configure terminal
Spoke1-n1(config)# ip route 192.168.100.0/24 192.168.1.20 240
```

Примечания:

- В DMVPN IPv4 через IPv6 в отличие от базового сценария DMVPN IPv4 маршруты должны указывать не на кластерный адрес VRRP, а на адрес LAN-интерфейса смежного устройства.
- Данный маршрут будет устанавливаться в систему на резервной ноде кластера VRRP для обеспечения возможности опроса ее LAN интерфейса из подсети Центрального офиса, например, с целью централизованного сбора диагностической информации из Центрального офиса. Подробнее – смотри в базовом сценарии DMVPN IPv4.

4. Настройте BGP (см. описание http://docs.frrouting.org):

4.1. Создайте route-map `TO-HUB1-OUT`, `TO-HUB2-OUT`, `TO-HUB3-OUT`, `TO-HUB4-OUT`. Данные route-map будет менять `local-preference` для маршрутов, анонсируемые филиалом в сторону криптошлюзов Центрального офиса (192.168.1.0/24):

```
Spoke1-n1(config)# route-map TO-HUB1-OUT permit 1
Spoke1-n1(config-route-map)#set local-preference 100
Spoke1-n1(config-route-map)#exit
Spoke1-n1(config)#route-map TO-HUB2-OUT permit 1
Spoke1-n1(config-route-map)#set local-preference 75
Spoke1-n1(config-route-map)#exit
Spoke1-n1(config)#route-map TO-HUB3-OUT permit 1
Spoke1-n1(config-route-map)#set local-preference 50
Spoke1-n1(config-route-map)#exit
Spoke1-n1(config)#route-map TO-HUB4-OUT permit 1
Spoke1-n1(config-route-map)#set local-preference 25
Spoke1-n1(config-route-map)#exit
```

Примечание - На криптошлюзах всех остальных филиалах маршрут до защищаемой подсети Spoke1-n1, полученный через Hub1, будет иметь наибольший приоритет, а маршрут до защищаемой подсети Spoke1-n1, полученный через Hub4, будет иметь наименьший приоритет.

4.2. Включите процесс протокола BGP для автономной системы 65000 и перейдите в режим его конфигурирования:

```
Spoke1-n1(config)#router bgp 65000
```

4.3. Установите идентификатор маршрутизатора:

```
Spoke1-n1(config-router)#bgp router-id 192.168.1.10
```

4.4. Включите логирование изменения статуса (например, up, down и другие) BGP соседа в журнале работы:

```
Spoke1-n1(config-router)#bgp log-neighbor-changes
```

4.5. Установите таймеры keepalive и holdtime для BGP соседа:

```
Spoke1-n1(config-router)#timers bgp 3 9
```

4.6. Добавьте mGRE-адреса Hub-ов в качестве BGP соседей с номером автономной системы 65000 и установите время повторной попытки построения BGP соседства в 30 секунд:

```
Spoke1-n1(config-router)#neighbor 10.10.10.100 remote-as 65000
Spoke1-n1(config-router)#neighbor 10.10.10.100 timers connect 30
Spoke1-n1(config-router)#neighbor 10.10.10.200 remote-as 65000
Spoke1-n1(config-router)#neighbor 10.10.10.200 timers connect 30
Spoke1-n1(config-router)#neighbor 10.10.20.100 remote-as 65000
Spoke1-n1(config-router)#neighbor 10.10.20.100 timers connect 30
Spoke1-n1(config-router)#neighbor 10.10.20.200 remote-as 65000
Spoke1-n1(config-router)#neighbor 10.10.20.200 timers connect 30
```

4.7. Включите анонсирование маршрута до защищаемой подсети Филиала №1:

```
Spoke1-n1(config-router)#address-family ipv4 unicast
Spoke1-n1(config-router-af)#network network 192.168.1.0/24
```

4.8. Примените route-map к соседям:

```
Spoke1-n1(config-router-af)#neighbor 10.10.10.100 activate
Spoke1-n1(config-router-af)#neighbor 10.10.10.100 route-map TO-HUB1-OUT out
Spoke1-n1(config-router-af)# neighbor 10.10.10.200 activate
Spoke1-n1(config-router-af)#neighbor 10.10.10.200 route-map TO-HUB2-OUT out
Spoke1-n1(config-router-af)# neighbor 10.10.20.100 activate
Spoke1-n1(config-router-af)#neighbor 10.10.20.100 route-map TO-HUB3-OUT out
Spoke1-n1(config-router-af)# neighbor 10.10.20.200 activate
Spoke1-n1(config-router-af)#neighbor 10.10.20.200 route-map TO-HUB4-OUT out
```

4.9. Сохраните изменения:

```
Spoke1-n1(config-router-af)#end
Spoke1-n1(config-router)# exit
Spoke1-n1# write
```

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

Настройка VRRP

В отличие от версии 4.3 в версии 5.0 значительная часть настроек VRRP перенесена в cisco-like консоль. Но настройка VRRP конфигурационного файла `/etc/keepalived/notify_common.conf` осуществляется из linux bash.

1. Сохраните копию файла `/etc/keepalived/notify_common.conf` в `/etc/keepalived/notify_common.conf.backup` и приведите файл `/etc/keepalived/notify_common.conf` к виду:

```
############################################   specific   to   DMVPN   scenario
############################################################
# Flag indicate that DMVPN scenario is using on clustered spokes.
# Used to mange BGP neighbors shutdown state or OSPF interfaces passive mode when
VRRP node changes it STATE.
FLAG_DMVPN_SCENARIO_ON_CLUSTERED_SPOKE="true"

### IBGP specific options ###
# Internal routing protocol for DMVPN (IBGP or OSPF).
DMVPN_INTERNAL_ROUTING_PROTOCOL="IBGP"

# Local BGP AS Number. Set it if internal routing protocol is IBGP.
```

```
DMVPN_LOCAl_ASN="65000"

# BGP neighbors (separated by space) which must be shutted down if VRRP node transit
to BACKUP of FAULT state,
# and no shutted down if VRRP node transit to MASTER state.
# Set it if internal routing protocol is IBGP.
DMVPN_BGP_NEIGHBORS="10.10.10.100 10.10.10.200 10.10.20.100 10.10.20.200"
```

Конфигурационный файл `/etc/keepalived/notify_common.conf` управляет скриптом `/etc/keepalived/scripts/notify_common`. Логика следующая: если нода переходит в состояние BACKUP или FAULT, то BGP пиринг с центральными криптошлюзами (10.10.10.100, 10.10.10.200, 10.10.20.100, 10.10.20.200) выключается. Если нода переходит в состояние MASTER, то BGP пиринг с центральными криптошлюзами включается.

Изменение параметров DMVPN в файле `/etc/keepalived/notify_common.conf` **после настройки keepalived (в процессе работы)**:
При необходимости изменения параметров следует:
1) Перезапустить FRR с помощью команды "`systemctl restart frr`" (это действие загрузит конфигурацию, которая соответствует состоянию MASTER). ВАЖНО: после перезапуска FRR может возникнуть ассиметричная маршрутизация. Это связано с тем, что устройство в состоянии BACKUP или FAULT будет участвовать в обмене BGP маршрутами;
2) Изменить требуемые настройки FRR, которые соответствует состоянию MASTER;
3) Сохранить настройки FRR (команда write).
4) После настройки FRR требуется изменить соответствующие параметры DMVPN в файле `/etc/keepalived/notify_common.conf`.
5) Для устройств, находящихся в состоянии BACKUP или FAULT, следует перезапустить сервис keepalived, чтобы применить настройки из файла `/etc/keepalived/notify_common.conf`. Для устройства в состоянии MASTER настройки применяются после перехода в состояние BACKUP или FAULT.
Если была допущена ошибка в файле `/etc/keepalived/notify_common.conf` в части DMVPN (например, номер автономной системы или IP-адрес BGP пира не совпадает с настройками FRR), то при переходе ноды в состояние BACKUP или FAULT в логах `/var/log/cspvpngate.log` появится сообщение "`VRRP notify common script: ERROR: can not set shutdown on neighbor`". После исправления ошибок в файле достаточно перезапустить сервис keepalived.

2. Остальные настройки VRRP осуществляются из cisco-like консоли криптошлюза. Включите использование vrrp v3:

```
Spoke1-n1# configure terminal
Spoke1-n1(config)# fhrp version vrrp v3
```

3. Включите запуск общего скрипт-файла (`/etc/keepalived/scripts/notify_common`) при переходе VRRP инстанса между состояниями:

```
Spoke1-n1(config)# vrrp notify common
```

4. Создайте правило SLA (по умолчанию для IPv6):

```
Spoke1-n1(config)#vrrp track sla check_isp_link ipv6
```

5. Укажите целевые хосты для проверки связи:

```
Spoke1-n1(vrrp-track-sla)# host 2001:db8::172:16:1:1
Spoke1-n1(vrrp-track-sla)# host 2001:db8::172:16:101:15
```

6. Укажите режим SLA на проверку с помощью ICMP:

```
Spoke1-n1(vrrp-track-sla)# mode icmp-echo
```

7. Задайте условие успешности проверки, как доступность любого из указанного хостов:

```
Spoke1-n1(vrrp-track-sla)# reachability any
```

8. Задайте интерфейс, с которого будут отправляться ICMP:

```
Spoke1-n1(vrrp-track-sla)# source TenGigabitEthernet0/0
```

9. Задайте количество допустимых неуспешных попыток проверки доступности хостов:

```
Spoke1-n1(vrrp-track-sla)# fall 15
```

10. Задайте количество необходимых успешных попыток проверки доступности хостов:

```
Spoke1-n1(vrrp-track-sla)# rise 10
```

11. Задайте время ожидания проверки доступности хоста:

```
Spoke1-n1(vrrp-track-sla)# timeout 2
```

12. Интервал между проверками доступности хоста:

```
Spoke1-n1(vrrp-track-sla)# interval 3
Spoke1-n1(vrrp-track-sla)# exit
```

13. Включите VRRP на внутреннем интерфейсе (создает VRRP инстанс):

```
Spoke1-n1(config)# interface TenGigabitEthernet0/1
Spoke1-n1(config-if)# vrrp 1 address-family ipv4
Spoke1-n1(config-if-vrrp)#
```

14. Задайте кластерный IPv4 адрес:

```
Spoke1-n1(config-if-vrrp)# address 192.168.1.1 255.255.255.0
```

15. Установите интервал отправки advertisement-сообщений:

```
Spoke1-n1(config-if-vrrp)# timers advertise 3
```

16. Установите интервал отправки gratuitous ARP-сообщения:

```
Spoke1-n1(config-if-vrrp)# timers garp 5
```

17. Прикрепите к интерфейсу SLA правило:

```
Spoke1-n1(config-if-vrrp)# track sla check_isp_link
```

18. Включите отслеживание внешнего интерфейса:

```
Spoke1-n1(config-if-vrrp)# track interface TenGigabitEthernet0/0
```

19. Отключите preempt mode:

```
Spoke1-n1(config-if-vrrp)# no preempt
```

20. Установите приоритет для VRRP инстанса:

```
Spoke1-n1(config-if-vrrp)# priority 100
Spoke1-n1(config-if-vrrp)#end
```

21. Убедитесь, что нода перешла в состояние MASTER. Для этого войдите в cisco-like консоль криптошлюза и посмотрите настройки VRRP:

```
Spoke1-n1#show vrrp
```

```
Interface                     VRID  State   AddrFamily
------------------------------------------------------
TenGigabitEthernet0/1         1     Master  IPv4
```

22. Убедитесь, что доступен один из хостов, указанных в SLA:

```
Spoke1-n1#show vrrp sla check_isp_link
```

```

Rule name: check_isp_link
Result:    Success
```

```
Hostname                                State       Last checked at
2001:db8::172:16:1:1                    reachable   2024-05-28|09:23:25.032
2001:db8::172:16:101:15                 unknown     None
```

Примечание - Из-за того, что проверяется доступность любого хоста, после получения ответа от 2001:db8::172:16:1:1 проверка второго хоста не происходит.

23. Убедитесь, что на внутреннем интерфейсе eth1 появился кластерный VIP-адрес:

```
root@Spoke1-n1:~# ip address show dev eth1
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 10000
    link/ether 00:50:56:9e:e8:2f brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    altname ens192
    altname TenGigabitEthernet0_1
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 192.168.1.1/24 scope global secondary eth1:900
       valid_lft forever preferred_lft forever
    inet6 fe80::4287:6f0e:1e99:45c5/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

В Приложении представлены тексты конфигураций для криптошлюза Spoke1-n1:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/network/interfaces.d/mgre1`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/keepalived/keepalived.conf`.

Настройка устройства Spoke1-n2

Настройка устройства Spoke1-n2 осуществляется аналогично устройству Spoke1-n1 с учетом соответствующих IP-адресов (см. Рисунок 1).

Значение bgp router-id у резервной ноды должно отличаться от значения основной ноды (Spoke1-n1). Значение priority в VRRP у резервной ноды должно быть меньше, чем у основной ноды.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1-n1:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/network/interfaces.d/mgre1`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/keepalived/keepalived.conf`.

Настройка устройства Spoke2

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, настройки PKI, настройка паролей доступа к консоли cisco-like, настройка политики обработки COC (CRL), настройка межсетевого экрана, настройка mGRE-интерфейсов, настройка NHRP и настройка BGP осуществляется аналогично устройству Spoke1-n1 с учетом соответствующих IP-адресов (см. Рисунок 1). Настройки VRRP на Spoke2 не выполняются. Соответственно в настройках BGP не нужно добавлять маршрут через VIP адрес.

Из-за отсутствия маршрута по умолчанию до настройки multiwan, COC не будет загружен в базу Продукта во время настройки политики обработки COC (CRL).

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. Проверьте включена ли маршрутизация IPv6, выполнив следующую команду:

```
root@sterragate:~# 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:

```
sterragate(config)#hostname Spoke2
```

3. Включите WAN и LAN интерфейсы и настройте IP адрес на WAN и LAN интерфейсах в соответствии со схемой стенда:

```
Spoke2(config)#interface TenGigabitEthernet0/0
Spoke2(config-if)# no ip address
Spoke2(config-if)# ipv6 address 2001:db8::172:16:2:2/112
Spoke2(config-if)# no shutdown
Spoke2(config-if)#interface TenGigabitEthernet0/1
Spoke2(config-if)# no ip address
Spoke2(config-if)# ipv6 address 2001:db8::172:16:2:2/112
Spoke2(config-if)# no shutdown
Spoke2(config-if)#interface TenGigabitEthernet0/2
Spoke2(config-if)# ip address 192.168.2.1 255.255.255.0
Spoke2(config-if)# no shutdown
Spoke2(config)#end
```

   Примечание – маршрут по умолчанию будет добавлен с помощью сервиса multiwan.

Настройка шифрования

Настройка шифрования осуществляется аналогично устройству Spoke1-n1 с учетом соответствующих IP-адресов (см. Рисунок 1) и наличия двух WAN интерфейсов у Spoke2. В отличие от базового сценария DMVPN IPv4, в данном сценарии IPv6 адреса двух WAN интерфейсов Spoke2 разнесены в две `object-group` с именами `SELF-ISP1-IPV6` и `SELF-ISP2-IPV6`. Наличие двух `object-group` в данном сценарии по одному WAN IPv6 адресу в каждой не является обязательным и принципиальным отличием от базового сценария DMVPN IPv4. При необходимости и целесообразности может

использоваться одна `object-group` с двумя WAN адресами с соответствующими изменения в других частях cisco-like конфигурации.

Настройки шифрования осуществляются из cisco-like консоли криптошлюза.

1. Параметры IKE выполните аналогично устройствам Hub1 и Spoke1-n1.
2. Параметры IPsec:

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

   ```
   Spoke2(config)# crypto ipsec security-association lifetime kilobytes unlimited
   ```

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

   ```
   Spoke2(config)#crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
   Spoke2(cfg-crypto-trans)# mode transport
   Spoke2(cfg-crypto-trans)#exit
   ```

   Режим работы IPsec туннеля должен быть транспортным. В отличие от криптошлюзов версии 4.3 туннельный режим IPsec в сценарии DMVPN для криптошлюзов версии 5.0 не поддерживается и не может быть использован даже при отсутствии NAT.

   2.3. Создайте сетевые `object-group` с именами `SELF-ISP1-IPV6` и `SELF-ISP2-IPV6` для хранения в каждом из них одного из двух WAN адресов криптошлюза с целью дальнейшего его использования в ACL:

   ```
   Spoke2(config)#object-group v6-network SELF-ISP1-IPV6
   Spoke2(config-v6network-group)# description IP on WAN interface for ISP1
   Spoke2(config-v6network-group)# host 2001:db8::172:16:2:2
   Spoke2(config-v6network-group)# exit
   Spoke2(config)#object-group v6-network SELF-ISP2-IPV6
   Spoke2(config-v6network-group)# description IP on WAN interface for ISP2
   Spoke2(config-v6network-group)# host 2001:db8::172:17:2:2
   Spoke2(config-v6network-group)# exit
   ```

   2.4. Создайте два списка доступа (ACL) для IPv6 трафика, который нужно защищать между филиалом №2 и смежными филиалами (центральным офисом и филиалом №1):

   ```
   Spoke2(config)# ipv6 access-list IPSEC_DMVPN_ISP1_IPV6
   Spoke2(config-ipv6-acl)# remark special DMVPN filter for ISP1
   Spoke2(config-ipv6-acl)# permit gre object-group SELF-ISP1-IPV6 each
   Spoke2(config-ipv6-acl)#exit
   Spoke2(config)# ipv6 access-list IPSEC_DMVPN_ISP2_IPV6
   Spoke2(config-ipv6-acl)# remark special DMVPN filter for ISP2
   Spoke2(config-ipv6-acl)# permit gre object-group SELF-ISP2-IPV6 each
   Spoke2(config-ipv6-acl)#exit
   Spoke2(config)#
   ```

   Примечание - Ключевое слово `each` позволяет строить узкие IPsec туннели для любого адреса назначения. Адрес назначения берется из IP заголовка GRE пакета, в котором находится NBMA адрес криптошлюза.

   2.5. Создайте динамические крипто-карты (имена `DMAP_ISP1_IPV6`, раздел 1 и `DMAP_ISP1_IPV6`, раздел 1) и привяжите их к соответствующим статическим (имена `VPN_ISP1_IPV6`, раздел 1 и `VPN_ISP2_IPV6`, раздел 1):

   ```
   Spoke2(config)# crypto dynamic-map DMAP_ISP1_IPV6 1
   Spoke2(config-crypto-map)# match ipv6 address IPSEC_DMVPN_ISP1_IPV6
   Spoke2(config-crypto-map)# set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
   ```

```
Spoke2(config-crypto-map)# set isakmp-profile ALGS_PROFILE
Spoke2(config-crypto-map)# set security-association mss-fix out
Spoke2(config-crypto-map)# set pre-fragmentation
Spoke2(config-crypto-map)# set dead-connection history off
Spoke2(config-crypto-map)#exit
Spoke2(config)#crypto map VPN_ISP1_IPV6 1 ipsec-isakmp dynamic DMAP_ISP1_IPV6
Spoke2(config)# crypto dynamic-map DMAP_ISP2_IPV6 1
Spoke2(config-crypto-map)# match ipv6 address IPSEC_DMVPN_ISP2_IPV6
Spoke2(config-crypto-map)# set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Spoke2(config-crypto-map)# set isakmp-profile ALGS_PROFILE
Spoke2(config-crypto-map)# set security-association mss-fix out
Spoke2(config-crypto-map)# set pre-fragmentation
Spoke2(config-crypto-map)# set dead-connection history off
Spoke2(config-crypto-map)#exit
Spoke2(config)#crypto map VPN_ISP2_IPV6 1 ipsec-isakmp dynamic DMAP_ISP2_IPV6
Spoke2(config)#
```

2.6. Прикрепите созданные статические крипто-карты `VPN_ISP1_IPV6` и `VPN_ISP2_IPV6` к внешним интерфейсам `TenGigabitEthernet0/0` и `TenGigabitEthernet0/1`:

```
Spoke2(config)#interface TenGigabitEthernet0/0
Spoke2(config-if)#crypto map VPN_ISP1_IPV6
Spoke2(config-if)#exit
Spoke2(config)#interface TenGigabitEthernet0/1
Spoke2(config-if)#crypto map VPN_ISP2_IPV6
Spoke2(config-if)#exit
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка multiwan

Настройка осуществляются из linux bash. Подробное описание параметров приведено в сценарии «Резервирование каналов связи при помощи пакета «multiwan» (протокол IPv6)».

1. Приведите файл `/etc/multiwan/config.yaml` к виду:

```
config_format_version: 1
links_params:
  links:
  - name: ISP1
    check:
      hosts_reachability: any
      ipv6:
        hosts:
        - 2001:db8::172:16:101:15
        - 2001:db8::172:16:2:1
        source_address: 2001:db8::172:16:2:2
      method:
        icmp:
          max_rtt: 100
          interval: 3
          restore_interval: 1
          restore_count: 10
          failure_count: 10
          tos: 184
          data_size: 56
    iface_name: eth0
    prio: 300
    routes:
      ipv6:
        networks:
        - ::/0
```

```
      nexthop: 2001:db8::172:16:2:1
      source_address: 2001:db8::172:16:2:2
    watch_foreign_routes: true
- name: ISP2
  check:
    hosts_reachability: any
    ipv6:
      hosts:
      - 2001:db8::172:16:101:15
      - 2001:db8::172:17:2:1
      source_address: 2001:db8::172:17:2:2
    method:
      icmp:
        max_rtt: 100
        interval: 3
        restore_interval: 1
        restore_count: 10
        failure_count: 10
        tos: 184
        data_size: 56
  iface_name: eth1
  prio: 200
  routes:
    ipv6:
      networks:
      - ::/0
      nexthop: 2001:db8::172:17:2:1
      source_address: 2001:db8::172:17:2:2
    watch_foreign_routes: True
```

Завершение настройки Spoke2

1. После настройки запустите сервис `multiwan`, а также добавьте его в автозагрузку:

```
root@Spoke2:~# systemctl start multiwan.service
root@Spoke2:~# systemctl enable multiwan.service
```

2. Посмотреть лог работы сервиса можно в файле `/var/log/cspvpngate.log`:

```
root@Spoke2:~# tail -n 1000 /var/log/cspvpngate.log | grep multiwan
```

```
2024-05-28T10:58:10.042075+03:00 Spoke2 multiwan: INFO: Starting multiwan...
2024-05-28T10:58:11.421765+03:00 Spoke2 multiwan: INFO: NAT translations table has
been cleared.
2024-05-28T10:58:12.438633+03:00 Spoke2 multiwan: INFO: LSP was reloaded.
2024-05-28T10:58:12.445774+03:00 Spoke2 multiwan: INFO: Used interface "eth0".
Nexthop "2001:db8::172:16:2:1".
```

3. Проверьте, что добавлены маршруты объявлены в настройках `multiwan`:

```
root@Spoke2:~# ip -6 route show proto multiwan
```

```
default via 2001:db8::172:16:2:1 dev eth0 src 2001:db8::172:16:2:2 metric 700 pref
medium
```

4. Проверьте что маршрут до IP адреса HTTP сервера CRL_distribution_point в системе:

```
root@Spoke2:~# ip -6 route get 2001:db8::172:16:101:15
```

```
2001:db8::172:16:101:15 from :: via 2001:db8::172:16:2:1 dev eth0 proto multiwan src
2001:db8::172:16:2:2 metric 700 pref medium
```

5. Если всё настроено верно, то перезагрузите сервис `getcrls` для загрузки СОС в базу Продукта:

```
root@Spoke2:~# systemctl restart getcrls.service
```

6. Выполните проверку статуса сертификатов в базе Продукта:

```
root@Spoke2:~# cert_mgr 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=Spoke2
```

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- Содержимое `/etc/network/interfaces.d/mgre0`;
- Содержимое `/etc/network/interfaces.d/mgre1`;
- Содержимое `/etc/opennhrp/opennhrp.conf`;
- Содержимое `/etc/frr/frr.conf`;
- Содержимое `/etc/multiwan/multiwan.yaml`

Проверка работоспособности стенда

Проверка работоспособности стенда проводится в трех состояниях:

1. Все узлы в центральном офисе и филиалах функционируют и исправны.
2. Проблема на основном криптошлюзе в центральном офисе: отказ центрального криптошлюза, отказ внешнего сетевого интерфейса.
3. Проблема на основной ноде кластера в филиале: отказ основной ноды кластера, недоступность Интернет-провайдера, недоступность сервиса opennhrp.

Все узлы в центральном офисе и филиалах функционируют и исправны

1. Убедитесь, что криптошлюз второго филиала работает через основной интерфейс:

```
root@Spoke2:~# mwan_mgr show --links_status
```

```
Link: 1
    Name: ISP1
    Interface: eth0
    Priority: 300
    State: reachable
    Active: True
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:16:2:1"
Link: 2
    Name: ISP2
    Interface: eth1
    Priority: 200
    State: reachable
    Active: False
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:17:2:1"
```

   Видно, что активным интерфейсом является eth0.

2. Убедитесь, что на центральных криптошлюзах установлены IPsec-туннели со всеми филиальными криптошлюзами, для этого в linux bash выполните следующую команду:

```
root@Hub1:~# 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 (2001:db8::100:100:100:2,4500)-(2001:db8::172:16:1:2,4500) active 2520 2496
2 11 (2001:db8::100:100:100:2,4500)-(2001:db8::172:16:2:2,4500) active 2456 2424
3 12 (2001:db8::100:100:100:2,4500)-(2001:db8::172:17:1:2,4500) active 1992 2032

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 6 (2001:db8::100:100:100:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 0 1564
2 7 (2001:db8::100:100:100:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 1064 0
3 8 (2001:db8::100:100:100:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 168 140
4 9 (2001:db8::100:100:100:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 1248
1268
5 10 (2001:db8::100:100:100:2,*)-(2001:db8::172:17:1:2,*) 47 ESP nat-t-trans 204 140
```

```
root@Hub2:~# 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::100:100:101:2,4500)-(2001:db8::172:17:1:2,4500) active 1992 2032
2 2 (2001:db8::100:100:101:2,4500)-(2001:db8::172:16:1:2,4500) active 1992 2032
3 3 (2001:db8::100:100:101:2,4500)-(2001:db8::172:16:2:2,4500) active 1992 2024

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (2001:db8::100:100:101:2,*)-(2001:db8::172:17:1:2,*) 47 ESP nat-t-trans 204 140
2 2 (2001:db8::100:100:101:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 1512
1576
3 3 (2001:db8::100:100:101:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 1608
1588
```

```
root@Hub3:~# 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 (2001:db8::100:101:100:2,4500)-(2001:db8::172:16:2:2,4500) active 2488 2520
2 4 (2001:db8::100:101:100:2,4500)-(2001:db8::172:17:1:2,4500) active 1992 2032
3 9 (2001:db8::100:101:100:2,4500)-(2001:db8::172:16:1:2,4500) active 1992 2032

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3 (2001:db8::100:101:100:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 0 7380
2 4 (2001:db8::100:101:100:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 12224 0
3 5 (2001:db8::100:101:100:2,*)-(2001:db8::172:17:1:2,*) 47 ESP nat-t-trans 1428 980
4 6 (2001:db8::100:101:100:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 7172
6840
```

```
root@Hub4:~# 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 (2001:db8::100:101:101:2,4500)-(2001:db8::172:16:1:2,4500) active 1992 2032
2 4 (2001:db8::100:101:101:2,4500)-(2001:db8::172:16:2:2,4500) active 2424 2456
3 5 (2001:db8::100:101:101:2,4500)-(2001:db8::172:17:1:2,4500) active 1992 2032

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3 (2001:db8::100:101:101:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 12384
14020
2 4 (2001:db8::100:101:101:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 392 232
3 5 (2001:db8::100:101:101:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 13348
9376
4 6 (2001:db8::100:101:101:2,*)-(2001:db8::172:17:1:2,*) 47 ESP nat-t-trans 1632
1120
```

Видно, что на каждом центральном криптошлюзе установлено по три IPsec-туннеля – два с нодами кластера в первом филиале (IP-адреса 2001:db8::172:16:1:2, 2001:db8::172:17:1:2) и третий с криптошлюзом во втором филиале (IP-адрес: 2001:db8::172:16:2:2). Строка «`ESP nat-t-trans`» свидетельствует о том, что IPsec-туннель работает в транспортном режиме через NAT. Состояние, когда один IPsec-туннель отображается как два IPsec-туннеля (один для входящего трафика, другой для исходящего) является нормальным. Так же состояние, когда происходит дублирование записи IPsec-туннеля и счётчики меняются только у последней записи, является нормальным.

3. Убедитесь, что на центральных криптошлюзах протокол NHRP верно отображает информацию о филиальных криптошлюзах, для этого в linux bash выполните следующую команду:

```
root@Hub1:~# opennhrpctl show
```

```
Status: ok

Interface: mgre0
Type: local
Protocol-Address: 10.10.10.255/32
Alias-Address: 10.10.10.100
Flags: up

Interface: mgre0
Type: local
Protocol-Address: 10.10.10.100/32
Flags: up

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:06

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.1/32
NBMA-Address: 2001:db8::172:16:1:2
NBMA-NAT-OA-Address: 2001:db8::100:100:1:2
Flags: up
Expires-In: 1:06

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.2/32
NBMA-Address: 2001:db8::172:17:1:2
NBMA-NAT-OA-Address: 2001:db8::100:101:1:2
Flags: used up
Expires-In: 1:05
```

```
root@Hub2:~# opennhrpctl show
```

```
Status: ok

Interface: mgre0
Type: local
Protocol-Address: 10.10.10.255/32
Alias-Address: 10.10.10.200
Flags: up

Interface: mgre0
Type: local
Protocol-Address: 10.10.10.200/32
Flags: up

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
```

```
Expires-In: 1:29

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.1/32
NBMA-Address: 2001:db8::172:16:1:2
NBMA-NAT-OA-Address: 2001:db8::100:100:1:2
Flags: up
Expires-In: 1:16

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.2/32
NBMA-Address: 2001:db8::172:17:1:2
NBMA-NAT-OA-Address: 2001:db8::100:101:1:2
Flags: used up
Expires-In: 1:05
```

```
root@Hub3:~# opennhrpctl show
```

```
Status: ok

Interface: mgre0
Type: local
Protocol-Address: 10.10.20.255/32
Alias-Address: 10.10.20.100
Flags: up

Interface: mgre0
Type: local
Protocol-Address: 10.10.20.100/32
Flags: up

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.1/32
NBMA-Address: 2001:db8::172:16:1:2
NBMA-NAT-OA-Address: 2001:db8::100:100:1:2
Flags: up
Expires-In: 1:23

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.2/32
NBMA-Address: 2001:db8::172:17:1:2
NBMA-NAT-OA-Address: 2001:db8::100:101:1:2
Flags: up
Expires-In: 1:08

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:08
```

```
root@Hub4:~# opennhrpctl show
```

```
Status: ok

Interface: mgre0
```

```
Type: local
Protocol-Address: 10.10.20.255/32
Alias-Address: 10.10.20.200
Flags: up

Interface: mgre0
Type: local
Protocol-Address: 10.10.20.200/32
Flags: up

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.1/32
NBMA-Address: 2001:db8::172:16:1:2
NBMA-NAT-OA-Address: 2001:db8::100:100:1:2
Flags: up
Expires-In: 1:19

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.2/32
NBMA-Address: 2001:db8::172:17:1:2
NBMA-NAT-OA-Address: 2001:db8::100:101:1:2
Flags: used up
Expires-In: 1:17

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:09
```

Видно, что на каждом центральном криптошлюзе протокол NHRP корректно отображает информацию о филиальных криптошлюзах (записи с пометкой «`Type: dynamic`»), а именно mGRE-адрес (`Protocol-Address`) соответствует NBMA IP-адресу (`NBMA-Address`). Также правильно отображается информация об исходном IP-адресе до выполнения процедуры трансляции (`NBMA-NAT-OA-Address`) для тех криптошлюзов, которые находятся за устройствами, выполняющими функции NAT.

4. Убедитесь, что на центральных криптошлюзах подсистема ip neighbor ядра ОС Linux корректно отображает информацию о маппинге mGRE-адреса в NBMA-адрес филиальных криптошлюзов, для этого в linux bash выполните следующую команду:

```
root@Hub1:~# ip neighbor show
```

```
10.10.10.1 dev mgre0 lladdr 2001:db8::172:16:1:2 REACHABLE
192.168.255.1 dev eth1 lladdr 00:50:56:9e:fd:81 REACHABLE
10.10.10.3 dev mgre0 lladdr 2001:db8::172:16:2:2 REACHABLE
10.10.10.2 dev mgre0 lladdr 2001:db8::172:17:1:2 REACHABLE
fe80::250:56ff:fe9e:527a dev eth0 lladdr 00:50:56:9e:52:7a router REACHABLE
2001:db8::100:100:100:1 dev eth0 lladdr 00:50:56:9e:52:7a router REACHABLE
```

```
root@Hub2:~# ip neighbor show
```

```
10.10.10.1 dev mgre0 lladdr 2001:db8::172:16:1:2 REACHABLE
10.10.10.3 dev mgre0 lladdr 2001:db8::172:16:2:2 REACHABLE
10.10.10.2 dev mgre0 lladdr 2001:db8::172:17:1:2 REACHABLE
192.168.255.1 dev eth1 lladdr 00:50:56:9e:fd:81 REACHABLE
2001:db8::100:100:101:1 dev eth0 lladdr 00:50:56:9e:9a:f3 router REACHABLE
fe80::250:56ff:fe9e:9af3 dev eth0 lladdr 00:50:56:9e:9a:f3 router DELAY
```

```
root@Hub3:~# ip neighbor show
```

```
192.168.255.1 dev eth1 lladdr 00:50:56:9e:fd:81 REACHABLE
10.10.20.1 dev mgre0 lladdr 2001:db8::172:16:1:2 REACHABLE
10.10.20.2 dev mgre0 lladdr 2001:db8::172:17:1:2 REACHABLE
10.10.20.3 dev mgre0 lladdr 2001:db8::172:16:2:2 REACHABLE
2001:db8::100:101:100:1 dev eth0 lladdr 00:50:56:9e:4f:8b router STALE
fe80::250:56ff:fe9e:4f8b dev eth0 lladdr 00:50:56:9e:4f:8b router REACHABLE
```

```
root@Hub4:~# ip neighbor show
```

```
10.10.20.2 dev mgre0 lladdr 2001:db8::172:17:1:2 REACHABLE
10.10.20.1 dev mgre0 lladdr 2001:db8::172:16:1:2 REACHABLE
192.168.255.1 dev eth1 lladdr 00:50:56:9e:fd:81 REACHABLE
10.10.20.3 dev mgre0 lladdr 2001:db8::172:16:2:2 REACHABLE
fe80::250:56ff:fe9e:e411 dev eth0 lladdr 00:50:56:9e:e4:11 router STALE
2001:db8::100:101:101:1 dev eth0 lladdr 00:50:56:9e:e4:11 router REACHABLE
```

Видно, что на каждом центральном криптошлюзе маппинг mGRE-адреса в NBMA-адрес филиальных криптошлюзов выполнен верно.

5. Убедитесь, что на центральных криптошлюзах корректно работает протокол BGP, для этого зайдите в linux bash выполните следующие команды:

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

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

```
Hub1# show ip bgp summary
```

```
IPv4 Unicast Summary (VRF default):
BGP router identifier 10.10.10.100, local AS number 65000 vrf-id 0
BGP table version 3
RIB entries 5, using 960 bytes of memory
Peers 3, using 61 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor          V           AS    MsgRcvd    MsgSent    TblVer   InQ OutQ   Up/Down
State/PfxRcd   PfxSnt Desc
*10.10.10.1      4       65000        309        311         3     0     0 00:15:15
1        3 N/A
*10.10.10.3      4       65000        308        310         3     0     0 00:15:14
1        3 N/A
192.168.255.1    4       65001        315        315         3     0     0 00:15:27
1        3 N/A

Total number of neighbors 3
* - dynamic neighbor
2 dynamic neighbor(s), limit 5000
```

```
Hub1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.10.1, mgre0, weight 1, 00:17:25
B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:17:24
```

```
B>* 192.168.100.0/24 [20/0] via 192.168.255.1, eth1, weight 1, 00:17:37
```

```
root@Hub2:~# vtysh
```

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

```
Hub2# show ip bgp summary
```

```
IPv4 Unicast Summary (VRF default):
BGP router identifier 10.10.10.200, local AS number 65000 vrf-id 0
BGP table version 7
RIB entries 5, using 960 bytes of memory
Peers 3, using 61 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor          V           AS    MsgRcvd    MsgSent    TblVer   InQ OutQ   Up/Down
State/PfxRcd   PfxSnt Desc
*10.10.10.1      4       65000        249        251         7     0     0 00:12:18
1        3 N/A
*10.10.10.3      4       65000        259        261         7     0     0 00:12:48
1        3 N/A
192.168.255.1    4       65001        304        309         7     0     0 00:15:00
1        3 N/A

Total number of neighbors 3
* - dynamic neighbor
2 dynamic neighbor(s), limit 5000
```

```
Hub2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.10.1, mgre0, weight 1, 00:14:00
B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:14:30
B>* 192.168.100.0/24 [20/0] via 192.168.255.1, eth1, weight 1, 00:16:42
```

```
root@Hub3:~# vtysh
```

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

```
Hub3# show ip bgp summary
```

```
IPv4 Unicast Summary (VRF default):
BGP router identifier 10.10.20.100, local AS number 65000 vrf-id 0
BGP table version 3
RIB entries 5, using 960 bytes of memory
Peers 3, using 61 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor          V           AS    MsgRcvd    MsgSent    TblVer   InQ OutQ   Up/Down
State/PfxRcd   PfxSnt Desc
```

```
*10.10.20.1      4       65000         308         310          3     0     0 00:15:15
1        3 N/A
*10.10.20.3      4       65000         345         347          3     0     0 00:17:06
1        3 N/A
192.168.255.1    4       65001         350         347          3     0     0 00:17:05
1        3 N/A

Total number of neighbors 3
* - dynamic neighbor
2 dynamic neighbor(s), limit 5000
```

```
Hub3# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.20.1, mgre0, weight 1, 00:16:44
B>* 192.168.2.0/24 [200/0] via 10.10.20.3, mgre0, weight 1, 00:18:35
B>* 192.168.100.0/24 [20/0] via 192.168.255.1, eth1, weight 1, 00:18:35
```

```
root@Hub4:~# vtysh
```

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

```
Hub4# show ip bgp summary
```

```
IPv4 Unicast Summary (VRF default):
BGP router identifier 10.10.20.200, local AS number 65000 vrf-id 0
BGP table version 3
RIB entries 5, using 960 bytes of memory
Peers 3, using 61 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor          V           AS    MsgRcvd    MsgSent    TblVer   InQ OutQ   Up/Down
State/PfxRcd   PfxSnt Desc
*10.10.20.1      4       65000         339         341          3     0     0 00:16:47
1        3 N/A
*10.10.20.3      4       65000         344         346          3     0     0 00:17:02
1        3 N/A
192.168.255.1    4       65001         350         347          3     0     0 00:17:04
1        3 N/A

Total number of neighbors 3
* - dynamic neighbor
2 dynamic neighbor(s), limit 5000
```

```
Hub4# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.20.1, mgre0, weight 1, 00:18:16
B>* 192.168.2.0/24 [200/0] via 10.10.20.3, mgre0, weight 1, 00:18:31
```

```
B>* 192.168.100.0/24 [20/0] via 192.168.255.1, eth1, weight 1, 00:18:33
```

Видно, что на каждом центральном криптошлюзе по протоколу BGP установлено соседство с основной нодой кластера в филиале №1, с криптошлюзом в филиале №2 и роутером Int-router-Hub. Соседство с резервной нодой кластера в филиале №1 отсутствует, как и требуется (нода, которая находится в состоянии BACKUP/FAULT не участвует в BGP).

Маршруты до филиальных подсетей (192.168.1.0/24 и 192.168.2.0/24) и до 192.168.100.0/24 в таблице маршрутизации присутствуют.

6. Убедитесь, что основная нода кластера в филиале №1 находится в состоянии MASTER, для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# ip address show dev eth1
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 10000
    link/ether 00:50:56:9e:e8:2f brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    altname ens192
    altname TenGigabitEthernet0_1
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet 192.168.1.1/24 scope global secondary eth1:900
       valid_lft forever preferred_lft forever
    inet6 fe80::c148:7e29:5b8d:9b58/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

```
root@Spoke1-n1:~# tcpdump -i eth1 -n -c 4 vrrp
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:27:59.766702 IP 192.168.1.10 > 224.0.0.18: VRRPv3, Advertisement, vrid 1, prio
100, intvl 300cs, length 12
13:28:02.766860 IP 192.168.1.10 > 224.0.0.18: VRRPv3, Advertisement, vrid 1, prio
100, intvl 300cs, length 12
13:28:05.767208 IP 192.168.1.10 > 224.0.0.18: VRRPv3, Advertisement, vrid 1, prio
100, intvl 300cs, length 12
13:28:08.767444 IP 192.168.1.10 > 224.0.0.18: VRRPv3, Advertisement, vrid 1, prio
100, intvl 300cs, length 12
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

```
root@Spoke1-n1:~# ip route show
```

```
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.1
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.10
192.168.2.0/24 nhid 26 via 10.10.10.3 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 21 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

Видно, что на внутреннем интерфейсе eth1 имеется VIP-адрес 192.168.1.1, а также с данного интерфейса (с IP-адреса 192.168.1.10) отсылаются VRRP пакеты. В таблице маршрутизации присутствуют маршруты до защищаемых подсетей центрального офиса и филиала №2.

Также в cisco-like консоли криптошлюза можно увидеть состояние VRRP:

```
Spoke1-n1#show vrrp
```

```
Interface                     VRID  State   AddrFamily
-----------------------------------------------------
TenGigabitEthernet0/1         1     Master  IPv4
```

7. Убедитесь, что на резервной ноде есть маршрут до 192.168.100.0/24 через IP адрес LAN-интерфейса основной ноды.

```
root@Spoke1-n2:~# ip route show
```

```
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.2
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.2
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.20
192.168.100.0/24 nhid 15 via 192.168.1.10 dev eth1 proto static metric 20
```

8. Убедитесь, что на внутреннем маршрутизаторе центрального офиса есть марштрты до защищищаемых подсетей филиалов через Hub1.

```
root@Int-router1-Hub:~# ip route show
192.168.1.0/24 nhid 10 via 192.168.255.10 dev ens192 proto bgp metric 20
192.168.2.0/24 nhid 10 via 192.168.255.10 dev ens192 proto bgp metric 20
192.168.100.0/24 dev ens224 proto kernel scope link src 192.168.100.1
192.168.255.0/24 dev ens192 proto kernel scope link src 192.168.255.1
```

9. Убедитесь, что присутствует трафик между защищаемым подсетями филиала №1 и центрального офиса. Для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-hub и удостоверьтесь в прохождении пакетов:

```
root@Host-b-spoke1:~# 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=2.66 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=61 time=2.38 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=61 time=2.38 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=61 time=2.40 ms

--- 192.168.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.377/2.455/2.663/0.120 ms
```

10. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно строится, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=4.22 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=336 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.26 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=2.16 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.161/86.122/335.850/144.182 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 2548 2424
2 24 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2548 2424
3 26 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 3048 2924
4 27 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2548 2424
5 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 26 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 41312
52748
```

```
2 27 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 49636
46052
3 28 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 38148
39620
4 29 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 22384
23172
5 30 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
```

Видно, что пакеты успешно дошли от Host-b-spoke1 до Host-b-spoke2, а также построился IPsec-туннель между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2.

Проблема на криптошлюзах в центральном офисе

Смоделируем поочерёдный отказ внешнего сетевого интерфейса eth0 на криптошлюзах центрального офиса Hub1, Hub2 и Hub3 и проверим работоспособность стенда.

1. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub1 в состояние DOWN, для этого в linux bash выполните следующую команду:

   ```
   root@Hub1:~# ip -6 link set dev eth0 down
   ```

2. Подождите некоторое время и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub1 отсутствует. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre0. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub2. Для этого в linux bash выполните следующие команды:

   ```
   root@Spoke1-n1:~# sa_mgr show
   ```

   ```
   ISAKMP sessions: 0 initiated, 0 responded

   ISAKMP connections:
   Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
   1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 2548 2424
   2 26 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 3048 2924
   3 27 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2548 2424
   4 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

   IPsec connections:
   Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
   1 27 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 70556
   64796
   2 28 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 59068
   61308
   3 29 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 44156
   46000
   4 30 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
   ```

   ```
   root@Spoke1-n1:~# vtysh
   ```

   ```

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

   ```
   Spoke1-n1# show ip route bgp
   ```

   ```
   Codes: K - kernel route, C - connected, S - static, R - RIP,
          O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
          T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
          f - OpenFabric,
          > - selected route, * - FIB route, q - queued, r - rejected, b - backup
          t - trapped, o - offload failure

   B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:06:00
   ```

```
B>* 192.168.100.0/24 [200/0] via 10.10.10.200, mgre0, weight 1, 00:06:00
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 41 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:100:2,4500) active 3552 3352
2 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 2888 2940
3 47 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:101:2,4500) active 3040 2924
4 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 1992 2032

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 22 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 77064
74984
2 23 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 74764
76472
3 25 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 288 288
4 26 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 18644
25076
```

```
root@Spoke2:~# vtysh
```

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

```
Spoke2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.10.1, mgre0, weight 1, 00:07:29
B>* 192.168.100.0/24 [200/0] via 10.10.10.200, mgre0, weight 1, 00:07:29
```

3. Убедитесь, что ходит трафик между защищаемым подсетями филиала №1 и центрального офиса, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-hub и удостоверьтесь в прохождении пакетов:

```
root@Host-b-spoke1:~# 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=2.47 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=61 time=2.22 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=61 time=1.95 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=61 time=1.96 ms

--- 192.168.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.951/2.150/2.472/0.216 ms
```

4. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно строится, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=3.23 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=976 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.10 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=2.00 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 2.003/245.891/976.238/421.665 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 2548 2424
2 26 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 3048 2924
3 27 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2548 2424
4 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 27 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 102956
93228
2 28 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 91320
94840
3 29 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 78988
82720
4 30 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
```

Видно, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно построилось.

5. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub2 в состояние DOWN, для этого в linux bash выполните следующую команду:

```
root@Hub2:~# ip -6 link set dev eth0 down
```

6. Подождите некоторое время и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub2 отсутствует. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre1. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub3. Для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 27 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 3064 2856
3 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 30 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
2 31 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 56620
58924
3 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 29012
30164
```

```
root@Spoke1-n1:~# vtysh
```

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

```
Spoke1-n1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.20.3, mgre1, weight 1, 00:20:25
B>* 192.168.100.0/24 [200/0] via 10.10.20.100, mgre1, weight 1, 00:20:25
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 41 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:100:2,4500) active 4068 3784
2 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 3320 3456
3 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 2424 2548

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 27 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 42860
43692
2 28 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 36824
33752
3 30 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 0 0
```

```
root@Spoke2:~# vtysh
```

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

```
Spoke2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.20.1, mgre1, weight 1, 00:22:24
B>* 192.168.100.0/24 [200/0] via 10.10.20.100, mgre1, weight 1, 00:22:24
```

7. Убедитесь, что ходит трафик между защищаемым подсетями филиала №1 и центрального офиса, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-hub и удостоверьтесь в прохождении пакетов:

```
root@Host-b-spoke1:~# 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=2.47 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=61 time=2.04 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=61 time=2.16 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=61 time=2.59 ms
```

```
--- 192.168.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.042/2.313/2.590/0.222 ms
```

8. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 функционирует исправно, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=3.31 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=2.33 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.30 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=2.39 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 2.302/2.583/3.313/0.422 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 27 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 3064 2856
3 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 31 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 71776
74764
2 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 43732
45416
3 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
```

Так как туннель был до проведения теста, то после отправки пакетов с помощью PING увеличились счётчики отправки и получения в туннеле.

9. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub3 в состояние DOWN, для этого в linux bash выполните следующую команду:

```
root@Hub3:~# ip -6 link set dev eth0 down
```

10. Подождите некоторое время и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub3 отсутствует. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre1. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub4. Для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 2 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424
3 176 (2001:db8::100:100:1:2,500)-(2001:db8::172:16:100:2,500) incompleted 356 0
4 177 (2001:db8::100:100:1:2,500)-(2001:db8::172:16:101:2,500) incompleted 356 0

IPsec connections:
```

```
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 81200
84648
2 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
```

```
root@Spoke1-n1:~# vtysh
```

```

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

```

```
Spoke1-n1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.20.3, mgre1, weight 1, 00:10:31
B>* 192.168.100.0/24 [200/0] via 10.10.20.200, mgre1, weight 1, 00:10:31
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 1 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 3320 3456
2 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 2424 2548
3 207 (2001:db8::172:16:2:2,500)-(2001:db8::172:16:101:2,500) incompleted 356 0

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 27 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 93120
95696
2 30 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 288 288
```

```
root@Spoke2:~# vtysh
```

```

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

```

```
Spoke2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.20.1, mgre1, weight 1, 00:11:24
B>* 192.168.100.0/24 [200/0] via 10.10.20.200, mgre1, weight 1, 00:11:24
```

11. Убедитесь, что ходит трафик между защищаемым подсетями филиала №1 и центрального офиса, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-hub и удостоверьтесь в прохождении пакетов:

```
root@Host-b-spoke1:~# 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=2.62 ms
```

```
64 bytes from 192.168.100.100: icmp_seq=2 ttl=61 time=2.59 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=61 time=3.06 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=61 time=2.99 ms

--- 192.168.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.585/2.813/3.058/0.213 ms
```

12. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 функционирует исправно, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=24.6 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=2.42 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=1.75 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=1.52 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.515/7.561/24.564/9.821 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 93448
97484
2 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
```

Так как туннель был до проведения теста, то после отправки пакетов с помощью PING увеличились счётчики отправки и получения в туннеле.

13. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub3 в состояние UP, для этого в linux bash выполните следующую команду:

```
root@Hub3:~# ip -6 link set dev eth0 up
```

14. Подождите некоторое время (до пяти минут) и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub3 создан. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre1. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub3. Для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424
3 200 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2032 1992
```

```
IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 104492
109024
2 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
3 34 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 3052
4528
```

```
root@Spoke1-n1:~# vtysh
```

```

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

```

```
Spoke1-n1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.20.3, mgre1, weight 1, 00:01:33
B>* 192.168.100.0/24 [200/0] via 10.10.20.100, mgre1, weight 1, 00:02:51
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 3320 3456
2 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 2424 2548
3 226 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:100:2,4500) active 2124 2092

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 27 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 120376
124080
2 30 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 576 576
3 31 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 7708
7660
```

```
root@Spoke2:~# vtysh
```

```

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

```

```
Spoke2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.20.1, mgre1, weight 1, 00:02:34
B>* 192.168.100.0/24 [200/0] via 10.10.20.100, mgre1, weight 1, 00:02:34
```

15. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub2 в состояние UP, для этого в linux bash выполните следующую команду:

```
root@Hub2:~# ip -6 link set dev eth0 up
```

16. Подождите некоторое время (до пяти минут) и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub2 создан. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre0. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub2. Для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3064 2856
2 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424
3 200 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2032 1992
4 214 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 121136
126308
2 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
3 34 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 18800
21944
4 35 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 3316
4832
```

```
root@Spoke1-n1:~# vtysh
```

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

```
Spoke1-n1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:00:19
B>* 192.168.100.0/24 [200/0] via 10.10.10.200, mgre0, weight 1, 00:01:18
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 3320 3456
2 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 2424 2548
3 226 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:100:2,4500) active 2124 2092
4 247 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:101:2,4500) active 2024 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 27 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 133040
137000
2 30 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 576 576
```

```
3 31 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 20084
20260
4 32 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 3888
4088
```

```
root@Spoke2:~# vtysh
```

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

```
Spoke2# show ip6 route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.10.1, mgre0, weight 1, 00:01:34
B>* 192.168.100.0/24 [200/0] via 10.10.10.200, mgre0, weight 1, 00:01:34
```

17. Переведите внешний сетевой интерфейс eth0 на криптошлюзе Hub1 в состояние UP, для этого в linux bash выполните следующую команду:

```
root@Hub1:~# ip -6 link set dev eth0 up
```

18. Подождите некоторое время (до пяти минут) и убедитесь в том, что на основной ноде кластера в филиале №1 и на криптошлюзе в филиале №2 IPsec-туннель с Hub1 создан. Маршруты в защищаемые подсети доступны через mGRE-интерфейс mgre0. Маршрут до защищаемую подсеть центрального офиса доступна через mGRE-адрес Hub1. Для этого в linux bash выполните следующие команды:

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 21 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 3580 3288
2 28 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2548 2424
3 200 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2032 1992
4 214 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 2032 1992
5 219 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 33 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 576 576
2 34 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 62844
67652
3 35 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 30992
51672
4 36 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 33788
25352
5 37 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 11488
11936
```

```
root@Spoke1-n1:~# vtysh
```

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

```
Spoke1-n1# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:11:01
B>* 192.168.100.0/24 [200/0] via 10.10.10.100, mgre0, weight 1, 00:11:01
```

```
root@Spoke2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 42 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:101:2,4500) active 3752 3972
2 48 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:1:2,4500) active 2424 2548
3 226 (2001:db8::172:16:2:2,4500)-(2001:db8::172:17:100:2,4500) active 2124 2092
4 247 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:101:2,4500) active 2024 1992
5 251 (2001:db8::172:16:2:2,4500)-(2001:db8::172:16:100:2,4500) active 2024 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 30 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:1:2,*) 47 ESP nat-t-trans 576 576
2 31 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 65156
60820
3 32 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 49248
50424
4 33 (2001:db8::172:16:2:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 24016
38812
5 34 (2001:db8::172:16:2:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 26808
27320
```

```
root@Spoke2:~# vtysh
```

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

```
Spoke2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.1.0/24 [200/0] via 10.10.10.1, mgre0, weight 1, 00:12:04
B>* 192.168.100.0/24 [200/0] via 10.10.10.100, mgre0, weight 1, 00:12:06
```

Видно, что в случае отказа внешнего сетевого интерфейса eth0 на криптошлюзах Hub1, Hub2 и Hub3 в центральном офисе динамическое построение защищенных соединений продолжает функционировать, защищаемая подсеть центрального офиса доступна с филиальных криптошлюзов.

19. При восстановлении внешнего сетевого интерфейса eth0 все также корректно отрабатывает. Проверку с полным отключением Hub1, Hub2, Hub3 повторите по аналогии.

Проблема на основной ноде кластера в филиале

Смоделируем полный отказ основной ноды кластера в филиале №1, а также отказ Интернет-провайдера и проверим работоспособность стенда.

1. Полный отказ основной ноды кластера в филиале №1.

   1.1. Выключите основную ноду, для этого в linux bash выполните следующую команду:

   ```
   root@Spoke1-n1:~# poweroff
   ```

   1.2. Убедитесь, что резервная нода перешла в состояние MASTER, для этого проверьте наличие VIP адреса на внутреннем интерфейсе и состояние VRRP в cisco-like консоли криптошлюза:

   ```
   root@Spoke1-n2:~# ip address show dev eth1
   ```

   ```
   3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
   qlen 10000
       link/ether 00:50:56:9e:f2:09 brd ff:ff:ff:ff:ff:ff
       altname enp11s0
       altname ens192
       altname TenGigabitEthernet0_1
       inet 192.168.1.20/24 brd 192.168.1.255 scope global eth1
          valid_lft forever preferred_lft forever
       inet 192.168.1.1/24 scope global secondary eth1:900
          valid_lft forever preferred_lft forever
       inet6 fe80::2a0e:d5e1:c290:e543/64 scope link stable-privacy
          valid_lft forever preferred_lft forever
   ```

   ```
   Spoke1-n2#show vrrp
   ```

   ```
   Interface                       VRID  State   AddrFamily
   ------------------------------------------------------
   TenGigabitEthernet0/1           1     Master  IPv4
   ```

   Видно, что кластерный VIP-адрес (192.168.1.1) присутствует на внутреннем интерфейсе eth1 и VRRP находится в состоянии MASTER.

   1.3. Убедитесь, что на резервной ноде по протоколу BGP установлено соседство с центральными криптошлюзами и получены маршруты в защищаемые подсети, для этого в linux bash выполните следующие команды:

   ```
   root@Spoke1-n2:~# vtysh
   ```

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

   ```
   Spoke1-n2# show ip bgp summary
   ```

   ```
   IPv4 Unicast Summary (VRF default):
   BGP router identifier 192.168.1.20, local AS number 65000 vrf-id 0
   BGP table version 3
   RIB entries 5, using 960 bytes of memory
   Peers 4, using 82 KiB of memory

   Neighbor          V           AS    MsgRcvd    MsgSent    TblVer   InQ OutQ   Up/Down
   State/PfxRcd   PfxSnt Desc
   10.10.10.100     4       65000        141        138         3     0     0 00:06:43
   2        1 N/A
   10.10.10.200     4       65000        141        138         3     0     0 00:06:43
   2        1 N/A
   10.10.20.100     4       65000        141        138         3     0     0 00:06:43
   2        1 N/A
   ```

```
10.10.20.200    4       65000        141        138         3     0     0 00:06:43
2        1 N/A

Total number of neighbors 4
```

```
Spoke1-n2# show ip route bgp
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

B>* 192.168.2.0/24 [200/0] via 10.10.10.3, mgre0, weight 1, 00:07:09
B>* 192.168.100.0/24 [200/0] via 10.10.10.100, mgre0, weight 1, 00:07:09
```

1.4. Убедитесь, что защищенное соединение между резервной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно строится, для этого запустите ping с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на резервной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=3.09 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=414 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.16 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=1.31 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.310/105.065/413.709/178.196 ms
```

```
root@Spoke1-n2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 139 (2001:db8::100:101:1:2,4500)-(2001:db8::172:17:101:2,4500) active 2432 2456
2 140 (2001:db8::100:101:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2432 2456
3 141 (2001:db8::100:101:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2528 2488
4 142 (2001:db8::100:101:1:2,4500)-(2001:db8::172:16:101:2,4500) active 2032 1928
5 143 (2001:db8::100:101:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 33 (2001:db8::100:101:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 296 280
2 34 (2001:db8::100:101:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 512 300
3 35 (2001:db8::100:101:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 31900
30536
4 36 (2001:db8::100:101:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 31816
33032
5 37 (2001:db8::100:101:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 0 34240
6 38 (2001:db8::100:101:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 32284
0
7 39 (2001:db8::100:101:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 19540
33260
8 40 (2001:db8::100:101:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
```

1.5. Запустите основную ноду кластера, дождитесь ее полной загрузки и убедитесь, что она перешла в состояние BACKUP (основная нода не перехватит роль MASTER, так как в

настройках VRRP стоит опция `nopreempt`), для этого проверьте отсутствие VIP адреса на внутреннем интерфейсе, и состояние VRRP в cisco-like консоли криптошлюза:

```
root@Spoke1-n1:~# ip -6 address show dev eth1
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 10000
    link/ether 00:50:56:9e:e8:2f brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    altname ens192
    altname TenGigabitEthernet0_1
    inet 192.168.1.10/24 brd 192.168.1.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::4a9:8a39:d052:8803/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

```
Spoke1-n1#show vrrp
```

```
Interface                     VRID  State   AddrFamily
------------------------------------------------------
TenGigabitEthernet0/1         1     Backup  IPv4
```

Видно, что в случае полного отказа основной ноды кластера роль MASTER на себя берет резервная нода и успешно обрабатывает трафик.

2. Отказ Интернет-провайдера.

2.1. Чтобы смоделировать отказ Интернет-провайдера заблокируем ICMP пакеты от резервной ноды кластера (предполагается, что резервная нода находится в состоянии MASTER, а основная в BACKUP) на роутере Core_router, для этого в linux bash выполните следующую команду:

```
root@Core-router:~# ip6tables -A INPUT -s 2001:db8::172:17:1:2 -p icmpv6 -j DROP
```

2.2. Убедитесь, что резервная нода кластера перешла в состояние FAULT, для этого состояние VRRP в cisco-like консоли криптошлюза:

```
Spoke1-n2#show vrrp
```

```
Interface                     VRID  State   AddrFamily
------------------------------------------------------
TenGigabitEthernet0/1         1     Fault   IPv4
```

2.3. Убедитесь, что основная нода кластера перешла в состояние MASTER, для этого в linux bash выполните следующую команду:

```
Spoke1-n1#show vrrp
```

```
Interface                     VRID  State   AddrFamily
------------------------------------------------------
TenGigabitEthernet0/1         1     Master  IPv4
```

2.4. Удалите на роутере Core_router правила, блокирующие ICMP добавленные ранее, для этого в linux bash выполните следующую команду:

```
root@Core-router:~# ip6tables -D INPUT -s 2001:db8::172:17:1:2 -p icmpv6 -j DROP
```

2.5. Убедитесь, что резервная нода кластера перешла в состояние BACKUP, для этого в linux bash выполните следующую команду:

```
Spoke1-n2#show vrrp
```

```
Interface                     VRID  State   AddrFamily
------------------------------------------------------
TenGigabitEthernet0/1         1     Backup  IPv4
```

При отказе Интернет-провайдера нода кластера переходит в состояние FAULT, а в случае восстановления в BACKUP.

Отказ интернет-провайдера второго филиала

1. Чтобы смоделировать отказ Интернет-провайдера заблокируем ICMP пакеты от основного интерфейса на роутере Core_router, для этого в linux bash выполните следующую команду:

```
root@Core-router:~# ip6tables -A INPUT -s 2001:db8::172:16:2:2 -p icmpv6 -j DROP
```

2. Проверьте состояние линков:

```
root@Spoke2:~# mwan_mgr show --links_status
```

```
Link: 1
    Name: ISP1
    Interface: eth0
    Priority: 300
    State: unreachable
    Active: False
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:16:2:1"
Link: 2
    Name: ISP2
    Interface: eth1
    Priority: 200
    State: reachable
    Active: True
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:17:2:1"
```

Видно, что хосты стали недоступны через основной интерфейс (eth0) и активным стал второй интерфейс (eth1).

3. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно строится, для этого запустите `ping` с устройства Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=3.72 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=489 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.24 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=1.70 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.703/124.180/489.056/210.662 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 9 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 2000 2024
2 10 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2496 2520
3 11 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 2464 2424
4 12 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 2432 2456
5 13 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:2:2,4500) active 2032 1992

IPsec connections:
```

```
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1  9  (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*)  47 ESP  nat-t-trans 28916
30120
2 10 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 0 23296
3  11  (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*)  47 ESP  nat-t-trans 29172
0
4  12  (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*)  47 ESP  nat-t-trans 84 64
5  13  (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*)  47 ESP  nat-t-trans 28908
30068
6 14 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 308 168
7  15  (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*)  47 ESP  nat-t-trans 28788
25664
8 16 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:2:2,*) 47 ESP nat-t-trans 288 288
```

4. Проверьте правильность определения NBMA адреса криптошлюза филиала №2 в OpenNHRP на смежных ему устройствах:

```
root@Hub1:~# opennhrpctl show nbma 2001:db8::172:16:2:2
```

```
Status: ok
```

```
root@Hub1:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:17:2:2
Flags: up
Expires-In: 1:10
```

```
root@Hub2:~# opennhrpctl show nbma 2001:db8::172:16:2:2
```

```
Status: ok
```

```
root@Hub2:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:17:2:2
Flags: up
Expires-In: 1:19
```

```
root@Hub3:~# opennhrpctl show nbma 2001:db8::172:16:2:2
```

```
Status: ok
```

```
root@Hub3:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:17:2:2
Flags: up
Expires-In: 1:12
```

```
root@Hub4:~# opennhrpctl show nbma 2001:db8::172:16:2:2
```

```
Status: ok
```

```
root@Hub4:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:17:2:2
Flags: up
Expires-In: 1:26
```

```
root@Spoke1-n1:~# opennhrpctl show nbma 172.17.2.2
```

```
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:17:2:2
Flags: used up
Expires-In: 1:23
```

Видно, что все устройства правильно определяют NBMA адрес криптошлюза филиала №2.

5. Удалите на роутере Core_router правила, блокирующие ICMP, добавленные ранее, для этого в linux bash выполните следующую команду:

```
root@Core-router:~# ip6tables -D INPUT -s 2001:db8::172:16:2:2 -p icmpv6 -j DROP
```

6. Проверьте состояние линков:

```
root@Spoke2:~# mwan_mgr show --links_status
```

```
Link: 1
    Name: ISP1
    Interface: eth0
    Priority: 300
    State: reachable
    Active: True
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:16:2:1"
Link: 2
    Name: ISP2
    Interface: eth1
    Priority: 200
    State: reachable
    Active: False
    Hosts reachability: any
    IPv4 hosts: None
    IPv6 hosts: "2001:db8::172:16:101:15", "2001:db8::172:17:2:1"
```

Видно, что хосты стали доступны через основной интерфейс (eth0), и канал связи 1 (ISP1) стал активным.

7. Убедитесь, что защищенное соединение между основной нодой кластера в филиале №1 и криптошлюзом в филиале №2 успешно строится, для этого запустите `ping` с устройства

Host-b-spoke1 на устройство Host-b-spoke2 и проверьте наличие IPsec-туннеля на основной ноде кластера в филиале №1:

```
root@Host-b-spoke1:~# ping 192.168.2.100 -c 4
```

```
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=61 time=3.58 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=62 time=117 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=62 time=2.22 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=62 time=1.65 ms

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.654/31.222/117.432/49.777 ms
```

```
root@Spoke1-n1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 9 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:101:2,4500) active 9344 10796
2 11 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:101:2,4500) active 11104 12744
3 12 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:100:2,4500) active 11204 9800
4 14 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:100:2,4500) active 2368 2560
5 15 (2001:db8::100:100:1:2,4500)-(2001:db8::172:17:2:2,4500) active 2032 1992
6 16 (2001:db8::100:100:1:2,4500)-(2001:db8::172:16:2:2,4500) active 2032 1992

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 92 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:101:2,*) 47 ESP nat-t-trans 116848
121444
2 93 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:100:2,*) 47 ESP nat-t-trans 110220
114560
3 94 (2001:db8::100:100:1:2,*)-(2001:db8::172:17:2:2,*) 47 ESP nat-t-trans 288 288
4 95 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:101:2,*) 47 ESP nat-t-trans 48240
50192
5 96 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:2:2,*) 47 ESP nat-t-trans 288 288
6 97 (2001:db8::100:100:1:2,*)-(2001:db8::172:16:100:2,*) 47 ESP nat-t-trans 3092
2132
```

8. Проверьте правильность определения NBMA адреса криптошлюза филиала №2 в OpenNHRP на смежных ему устройствах:

```
root@Hub1:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok
```

```
root@Hub1:~# opennhrpctl show nbma 2001:db8::172:16:2:2
```

```
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:25
```

```
root@Hub2:~# opennhrpctl show nbma 2001:db8::172:17:2:2
```

```
Status: ok
```

```
root@Hub2:~# opennhrpctl show nbma 2001:db8::172:16:2:2
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:24

root@Hub3:~# opennhrpctl show nbma 2001:db8::172:17:2:2
Status: ok

root@Hub3:~# opennhrpctl show nbma 2001:db8::172:16:2:2
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:21

root@Hub4:~# opennhrpctl show nbma 2001:db8::172:17:2:2
Status: ok

root@Hub4:~# opennhrpctl show nbma 2001:db8::172:16:2:2
Status: ok

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.20.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: up
Expires-In: 1:11

root@Spoke1-n1:~# opennhrpctl show nbma 2001:db8::172:17:2:2
Status: ok

root@Spoke1-n1:~# opennhrpctl show nbma 2001:db8::172:16:2:2
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.10.3/32
NBMA-Address: 2001:db8::172:16:2:2
Flags: used up
Expires-In: 1:24
```

Видно, что все устройства правильно определяют NBMA адрес криптошлюза филиала №2. Дополнительно видно, что все криптошлюзы определяют, что криптошлюз филиала №2 не находится за NAT.

Дополнение

Балансировка нагрузки от филиальных криптошлюзов на центральные криптошлюзы

В данной главе будет описана настройка балансировки пакетов от филиальных криптошлюзов между криптошлюзами центрального офиса.

На устройстве Int-router-Hub должны отсутствовать route-map, регулирующие приоритет входящих маршрутов, полученных от Hub1, Hub2, Hub3 и Hub4. В таком случае в таблице маршрутизации Int-router-Hub будут присутствовать маршруты, полученные от всех Hub-ов.

На всех криптошлюзах центрального офиса требуется изменить настройки FRR. Далее показана настройка Hub1.

1. Войдите в консоль сервиса FRR, для этого нужно из linux bash набрать следующую команду:

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

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

Hub1#
```

2. Требуется удалить route-map вида `FROM-HUB1-OUT` на Hub1, Hub2, Hub3 и Hub4. После этого криптошлюзы филиалов будут получать маршруты до защищаемых подсетей центрального офиса с одинаковым приоритетом:

```
Hub1# conf t
Hub1(config)# no route-map FROM-HUB1-OUT
Hub1(config)# router bgp 65000
Hub1(config-router)# address-family ipv4 unicast
Hub1(config-router-af)# no neighbor spokes-ibgp route-map FROM-HUB1-OUT out
Hub1(config-router-af)# end
```

3. Сохраните настройки FRR:

```
Hub1# write
```

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

После настройки на устройстве Int-router-Hub должно быть по четыре маршрута до защищаемых сетей филиалов, а на криптошлюзах филиалов будет четыре маршрута до защищаемой сети центрального офиса.

```
root@Int-router-Hub:~# ip route show
```

```
192.168.1.0/24 nhid 30 proto bgp metric 20
        nexthop via 192.168.255.10 dev ens192 weight 1
        nexthop via 192.168.255.11 dev ens192 weight 1
        nexthop via 192.168.255.20 dev ens192 weight 1
        nexthop via 192.168.255.21 dev ens192 weight 1
192.168.2.0/24 nhid 30 proto bgp metric 20
        nexthop via 192.168.255.10 dev ens192 weight 1
        nexthop via 192.168.255.11 dev ens192 weight 1
        nexthop via 192.168.255.20 dev ens192 weight 1
        nexthop via 192.168.255.21 dev ens192 weight 1
192.168.100.0/24 dev ens224 proto kernel scope link src 192.168.100.1
192.168.255.0/24 dev ens192 proto kernel scope link src 192.168.255.1
```

```
root@Spoke1-n1:~# ip route show
```

```
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.1
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.10
192.168.2.0/24 nhid 28 via 10.10.10.3 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 46 proto bgp metric 20
        nexthop via 10.10.10.100 dev mgre0 weight 1
        nexthop via 10.10.10.200 dev mgre0 weight 1
        nexthop via 10.10.20.100 dev mgre1 weight 1
        nexthop via 10.10.20.200 dev mgre1 weight 1
```

```
root@Spoke2:~# ip route show
```

```
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.3
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.3
192.168.1.0/24 nhid 247 via 10.10.10.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 dev eth2 proto kernel scope link src 192.168.2.1
192.168.100.0/24 nhid 10683 proto bgp metric 20
        nexthop via 10.10.10.100 dev mgre0 weight 1
        nexthop via 10.10.10.200 dev mgre0 weight 1
        nexthop via 10.10.20.100 dev mgre1 weight 1
        nexthop via 10.10.20.200 dev mgre1 weight 1
```

Ограничение полосы пропускания (shaping) на mGRE интерфейсе.

В данном разделе будет описано конфигурирование ограничения полосы пропускания до 100 Мбит/с суммарно по всем типам трафика, из них 10 на UDP, 85 на TCP и 5 на остальной трафик.

Подробнее об ограничениях при настройке полосы пропускания описано в инструкции «Обеспечение качества обслуживания для трафика (QoS)».

Для исключения срабатываний механизма защиты от атак воспроизведения на принимающем криптошлюзе при перегрузке полосы пропускания на передающем криптошлюзе (подробнее в разделе «Ограничение полосы пропускания (shaping)» инструкции «Обеспечение качества обслуживания для трафика (QoS)») рекомендуется отказаться от shaping на WAN-интерфейсе и выполнять его ДО зашифрования трафика, например, на внешнем оборудовании (LAN-сегмент) или mGRE-интерфейсе.

Примечание - Срабатывание механизма защиты от атак воспроизведения на приемной стороне можно диагностировать по увеличению счетчика потерь «ipsec replay drops» в утилите «kstat_show».

Для начала нужно маркировать UDP и TCP трафик. Настройка маркирования осуществляется в cisco-like консоли криптошлюза и должна производиться на внутреннем интерфейсе. В данном сценарии маркирование будет производиться на интерфейсе `mgre0`. Однако, криптошлюзы версии 5.0 не позволяют настраивать туннельные интерфейсы IPv6 через cisco-like консоль. В связи с этим необходимо в linux bash добавить возможность привязки mgre-интерфейса в cisco-like к спискам доступа. Для добавления возможности привязки mgre выполните следующие действия:

1. Добавьте GRE интерфейс mgre0 в файл /etc/ifaliases.cf (выделено жирным):

```
root@Hub1:~# vim.tiny /etc/ifaliases.cf
```

```
interface (name="TenGigabitEthernet0/0" pattern="eth0")
interface (name="TenGigabitEthernet0/1" pattern="eth1")
interface (name="TenGigabitEthernet0/2" pattern="eth2")
interface (name="Tunnel0" pattern="mgre0")
interface (name="default" pattern="*")
```

- значение параметра `name` должно быть задано в виде TunnelN.

- значение параметра `pattern` должно соответствовать имени GRE интерфейса в нотации Linux.

Конфигурирование mgre-интерфейса IPv6 из cisco-like консоли не поддерживается и должно выполняться из linux bash. Попытка настройки mgre-интерфейса IPv6 из cisco-like консоли приведет к созданию mgre-интерфейса IPv4.

2. Пересчитайте контрольную сумму файла `/etc/ifaliases.cf`:

```
root@Hub1:~# integr_mgr calc -f /etc/ifaliases.cf


SUCCESS:  Operation was successful.
```

Настройка маркирования осуществляется в cisco-like консоли криптошлюза:

1. Создайте необходимые списки доступа, которые описывают маркируемый трафик:

```
Hub1#conf t
Hub1(config)#ip access-list extended SET_DSCP_AF11
Hub1(config-ext-nacl)#permit tcp 192.168.100.0 0.0.0.255 any
Hub1(config-ext-nacl)#ip access-list extended SET_DSCP_AF12
Hub1(config-ext-nacl)#permit udp 192.168.100.0 0.0.0.255 any
Hub1(config-ext-nacl)#ip access-list extended CLEAR_DSCP
Hub1(config-ext-nacl)#deny tcp 192.168.100.0 0.0.0.255 any
Hub1(config-ext-nacl)#deny udp 192.168.100.0 0.0.0.255 any
Hub1(config-ext-nacl)#permit ip any any
Hub1(config-ext-nacl)#exit
Hub1(config)#
```

2. Опишите классы трафика на основе списков доступа:

```
Hub1(config)#class-map match-all CLEAR_DSCP
Hub1(config-cmap)#match access-group name CLEAR_DSCP
Hub1(config-cmap)#class-map match-all SET_DSCP_AF11
Hub1(config-cmap)#match access-group name SET_DSCP_AF11
Hub1(config-cmap)#class-map match-all SET_DSCP_AF12
Hub1(config-cmap)#match access-group name SET_DSCP_AF12
Hub1(config-cmap)#exit
```

3. Опишите политику для трафика (выставление DSCP метки):

```
Hub1(config)#policy-map DSCP_POLICY
Hub1(config-pmap)#class SET_DSCP_AF11
Hub1(config-pmap-c)#set dscp af11
Hub1(config-pmap-c)#class SET_DSCP_AF12
Hub1(config-pmap-c)#set dscp af12
Hub1(config-pmap-c)#class CLEAR_DSCP
Hub1(config-pmap-c)#set dscp default
Hub1(config-pmap-c)#exit
Hub1(config-pmap)#exit
Hub1(config)#
```

4. Привяжите политику для трафика к mgre интерфейсу на исходящее направление:

```
Hub1(config)#interface Tunnel0
Hub1(config-if)#service-policy output DSCP_POLICY
Hub1(config-if)#end
```

Настройка ограничения полосы пропускания осуществляется из linux bash.

1. Добавьте следующее содержимое в файл `/etc/network/if-up.d/zshaper`:

Скрипты из `/etc/network/if-up.d/` выполняются в лексикографическом порядке. Скрипт должен выполняться позже `st-virtual-if`.

```
#!/bin/bash

function enable_shaper(){
# del root queue discipline
tc qdisc del dev $IFACE root || true

# add root queue discipline
tc qdisc add dev $IFACE root handle 1:0 htb default 4

# add root class
tc class add dev $IFACE parent 1:0 classid 1:1 htb rate 100mbit ceil 100mbit

# add sub classes
tc class add dev $IFACE parent 1:1 classid 1:2 htb rate 85mbit ceil 100mbit
tc class add dev $IFACE parent 1:1 classid 1:3 htb rate 10mbit ceil 100mbit
tc class add dev $IFACE parent 1:1 classid 1:4 htb rate 5mbit ceil 100mbit

# add filters for traffic
tc filter add dev $IFACE parent 1:0 protocol ip prio 0 u32 match ip tos 0x28 0xfc
flowid 1:2
tc filter add dev $IFACE parent 1:0 protocol ip prio 0 u32 match ip tos 0x30 0xfc
flowid 1:3
}

if [[ $IFACE == "mgre0" ]]; then
    enable_shaper $IFACE
fi
```

Пояснения:

1.1. Удалить корневую дисциплину с интерфейса:

```
tc qdisc del dev $IFACE root || true
```

Примечание – При включении интерфейса с IPv6 адресом включается алгоритм Duplicate Address Detection (DAD), который обеспечивает уникальность IPv6 адреса в пределах сети. При попытке удаления корневой дисциплины (команда `tc qdisc del dev $IFACE root`) в период работы DAD возможно появление сообщений об ошибках следующего вида:

```
Error: Cannot delete qdisc with handle of zero.
```

Для безусловного выполнения других команд скрипта даже при выполнении команды `tc qdisc del dev $IFACE root` в период работы механизма DAD добавлены команды `|| true`.

1.2. Добавить подкласс 4 по умолчанию в корневую дисциплину интерфейса с классом HTB (трафик, который не попал под фильтры, направляется в этот класс):

```
tc qdisc add dev $IFACE root handle 1:0 htb default 4
```

1.3. Ограничить скорость на интерфейсе до 100 Мбит/с:

```
tc class add dev $IFACE parent 1:0 classid 1:1 htb rate 100mbit ceil 100mbit
```

1.4. Определить подклассы (1:2, 1:3, 1:4) и ограничить в них скорость:

```
tc class add dev $IFACE parent 1:1 classid 1:2 htb rate 85mbit ceil 100mbit
tc class add dev $IFACE parent 1:1 classid 1:3 htb rate 10mbit ceil 100mbit
tc class add dev $IFACE parent 1:1 classid 1:4 htb rate 5mbit ceil 100mbit
```

1.5. При помощи фильтров направить трафик в нужные классы. Пакеты с меткой AF11 (0x28) должны попадать в класс 1:2 (`flowid 1:2`). Пакеты с меткой AF12 (0x30) должны попадать в класс 1:3 (`flowid 1:3`):

Требуется указывать шестнадцатеричное значение ToS байта. Для двоичного значения DSCP добавляются два нуля справа и переводится полученное значение в шестнадцатеричное представление:

- двоичное представление для AF11 001010 -> 00101000 -> 0x28;
- двоичное представление для AF12 001100 -> 00110000 -> 0x30.

```
tc filter add dev $IFACE parent 1:0 protocol ip prio 0 u32 match ip tos 0x28 0xfc
flowid 1:2
tc filter add dev $IFACE parent 1:0 protocol ip prio 0 u32 match ip tos 0x30 0xfc
flowid 1:3
```

1.6. В данном сценарии shaping будет производиться на внутреннем интерфейсе `mgre0` до зашифрования трафика.

2. Дайте файлу `/etc/network/if-up.d/zshaper` права на исполнение:

```
root@Hub1:~# chmod u+x /etc/network/if-up.d/zshaper
```

Примечание - Данный файл будет запускаться автоматически при старте системы во время конфигурирования интерфейса `mgre0` (а также при выполнении команды `ifup mgre0`).

3. Примените настройки ограничения полосы пропускания:

```
root@Hub1:~# ifdown mgre0; ifup mgre0
```

```
Waiting for DAD... Done
Error: Cannot delete qdisc with handle of zero.
```

4. Посмотреть статистику можно при помощи команд:

```
root@Hub1:~# tc -s qdisc show dev mgre0
root@Hub1:~# tc -s filter show dev mgre0
root@Hub1:~# tc -s class show dev mgre0
```

Примечание - Из-за ограничения полосы пропускания в `kstat_show` будут расти как счётчики `tx errors`, так и количество отброшенных пакетов (`dropped`) в `tc -s qdisc show dev mgre0`. Допускается небольшое отклонение между количеством отброшенных пакетов и `tx error`.

Настройки для других криптошлюзов будут отличаться количеством интерфейсов и защищаемой подсетью.

Приложение

Устройство Core-router

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
# To Ext-router-Hub1
auto ens192
iface ens192 inet6 static
address 2001:db8::172:16:100:1/112

# To Ext-router-Hub2
auto ens224
iface ens224 inet6 static
address 2001:db8::172:16:101:1/112

# To Ext-router-Hub3
auto ens256
iface ens256 inet6 static
address 2001:db8::172:17:100:1/112

# To Ext-router-Hub4
auto ens161
iface ens161 inet6 static
address 2001:db8::172:17:101:1/112

# To Spoke2 (ISP1)
auto ens193
iface ens193 inet6 static
address 2001:db8::172:16:2:1/112

# To Spoke1-n2
auto ens225
iface ens225 inet6 static
address 2001:db8::172:17:1:1/112

# To Spoke1-n1
auto ens257
iface ens257 inet6 static
address 2001:db8::172:16:1:1/112

# To Spoke2 (ISP2)
auto ens162
iface ens162 inet6 static
address 2001:db8::172:17:2:1/112

# For CDP.
auto ens224:0
iface ens224:0 inet6 static
address 2001:db8::172:16:101:15/112
```

Устройство Ext-router-Hub1

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
# To Core-router
auto ens192
iface ens192 inet6 static
address 2001:db8::172:16:100:2/112
gateway 2001:db8::172:16:100:1

# To Hub1
auto ens224
iface ens224 inet6 static
address 2001:db8::100:100:100:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:16:100:2"
IPSECGW="2001:db8::100:100:100:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Ext-router-Hub2

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# To Core-router
auto ens192
iface ens192 inet6 static
address 2001:db8::172:16:101:2/112
gateway 2001:db8::172:16:101:1

# To Hub2
auto ens224
iface ens224 inet6 static
address 2001:db8::100:100:101:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:16:101:2"
IPSECGW="2001:db8::100:100:101:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Ext-router-Hub3

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# To Core-router
auto ens192
iface ens192 inet6 static
address 2001:db8::172:17:100:2/112
gateway 2001:db8::172:17:100:1

# To Hub3
auto ens224
iface ens224 inet6 static
address 2001:db8::100:101:100:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:17:100:2"
IPSECGW="2001:db8::100:101:100:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Ext-router-Hub4

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# To Core-router
auto ens192
iface ens192 inet6 static
address 2001:db8::172:17:101:2/112
gateway 2001:db8::172:17:101:1

# To Hub4
auto ens224
iface ens224 inet6 static
address 2001:db8::100:101:101:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:17:101:2"
IPSECGW="2001:db8::100:101:101:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Ext-router1-Spoke1

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
# To Core-router
auto ens192
iface ens192 inet6 static
address 2001:db8::172:16:1:2/112
gateway 2001:db8::172:16:1:1

# To Spoke1-n1
auto ens224
iface ens224 inet6 static
address 2001:db8::100:100:1:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:16:1:2"
IPSECGW="2001:db8::100:100:1:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Ext-router2-Spoke1

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# To Core_couter
auto ens192
iface ens192 inet6 static
address 2001:db8::172:17:1:2/112
gateway 2001:db8::172:17:1:1

# To Spoke1-n2
auto ens224
iface ens224 inet6 static
address 2001:db8::100:101:1:1/112
```

Настройки iptables

Содержимое файла `/etc/iptables.rules`:

```
EXTIF="ens192"
INTIF="ens224"
INET_IP1="2001:db8::172:17:1:2"
IPSECGW="2001:db8::100:101:1:2"
### SNAT ###
ip6tables -t nat -A POSTROUTING -o $EXTIF -j SNAT --to-source $INET_IP1
### DNAT ###
# IKE/500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 500 -j DNAT --to-
destination [$IPSECGW]:500
# NAT-T/4500
ip6tables -t nat -A PREROUTING --dst $INET_IP1 -p udp --dport 4500 -j DNAT --to-
destination [$IPSECGW]:4500
```

Устройство Host-b-hub

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 192.168.100.100/24
gateway 192.168.100.1
```

Устройство Host-b-spoke1

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 192.168.1.100/24
gateway 192.168.1.1
```

Устройство Host-b-spoke2

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens192
iface ens192 inet static
address 192.168.2.100/24
gateway 192.168.2.1
```

Устройство Int-router-Hub

Сетевые настройки

Содержимое файла `/etc/network/interfaces`:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# To Hubs
auto ens192
iface ens192 inet static
address 192.168.255.1/24

# To LAN
auto ens224
iface ens224 inet static
address 192.168.100.1/24
```

Настройки динамической маршрутизации

Настройки сервиса FRR (`vtysh`):

```
!
frr version 8.4.4
frr defaults traditional
hostname Int-router1-Hub
log syslog informational
service integrated-vtysh-config
!
router bgp 65001
 bgp router-id 192.168.255.1
```

```
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 no bgp suppress-duplicates
 coalesce-time 1000
 timers bgp 3 9
 neighbor 192.168.255.10 remote-as 65000
 neighbor 192.168.255.11 remote-as 65000
 neighbor 192.168.255.20 remote-as 65000
 neighbor 192.168.255.21 remote-as 65000
 !
 address-family ipv4 unicast
  network 192.168.100.0/24
  neighbor 192.168.255.10 route-map FROM-HUB1-IN in
  neighbor 192.168.255.11 route-map FROM-HUB2-IN in
  neighbor 192.168.255.20 route-map FROM-HUB3-IN in
  neighbor 192.168.255.21 route-map FROM-HUB4-IN in
 exit-address-family
exit
!
route-map FROM-HUB1-IN permit 1
 set local-preference 100
exit
!
route-map FROM-HUB2-IN permit 1
 set local-preference 75
exit
!
route-map FROM-HUB3-IN permit 1
 set local-preference 50
exit
!
route-map FROM-HUB4-IN permit 1
 set local-preference 25
exit
!
end
```

Устройство Hub1

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1
```

```
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:100:100:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
```

```
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:100:100:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.255.10 255.255.255.0
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:100:100:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.10.100/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 multicast dynamic
 holding-time 90
```

```
 cisco-authentication secret
 non-caching
```

Настройки BGP

Содержимое файла `/etc/frr/frr.conf`:

```
!
frr version 9.0.2
frr defaults traditional
hostname Hub1
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 10.10.10.100
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor spokes-ibgp peer-group
 neighbor spokes-ibgp remote-as 65000
 neighbor 192.168.255.1 remote-as 65001
 bgp listen limit 5000
 bgp listen range 10.10.10.0/24 peer-group spokes-ibgp
 !
 address-family ipv4 unicast
  neighbor spokes-ibgp route-reflector-client
  neighbor spokes-ibgp next-hop-self
  neighbor spokes-ibgp route-map FROM-HUB1-OUT out
 exit-address-family
exit
!
route-map FROM-HUB1-OUT permit 1
 set local-preference 100
exit
!
end
```

Устройство Hub2

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Hub2
```

```
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:100:101:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
```

```
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:100:101:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.255.11 255.255.255.0
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:100:101:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.10.200/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 multicast dynamic
 holding-time 90
```

```
 cisco-authentication secret
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Hub2
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 10.10.10.200
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor spokes-ibgp peer-group
 neighbor spokes-ibgp remote-as 65000
 neighbor 192.168.255.1 remote-as 65001
 bgp listen limit 5000
 bgp listen range 10.10.10.0/24 peer-group spokes-ibgp
 !
 address-family ipv4 unicast
  neighbor spokes-ibgp route-reflector-client
  neighbor spokes-ibgp next-hop-self
  neighbor spokes-ibgp route-map FROM-HUB2-OUT out
 exit-address-family
exit
!
route-map FROM-HUB2-OUT permit 1
 set local-preference 75
exit
!
end
```

Устройство Hub3

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Hub3
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
```

```
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:101:100:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
```

```
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:101:100:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.255.20 255.255.255.0
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:101:100:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.20.100/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 multicast dynamic
 holding-time 90
 cisco-authentication secret
```

```
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Hub3
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 10.10.20.100
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor spokes-ibgp peer-group
 neighbor spokes-ibgp remote-as 65000
 neighbor 192.168.255.1 remote-as 65001
 bgp listen limit 5000
 bgp listen range 10.10.20.0/24 peer-group spokes-ibgp
 !
 address-family ipv4 unicast
  neighbor spokes-ibgp route-reflector-client
  neighbor spokes-ibgp next-hop-self
  neighbor spokes-ibgp route-map FROM-HUB3-OUT out
 exit-address-family
exit
!
route-map FROM-HUB3-OUT permit 1
 set local-preference 50
exit
!
end
```

Устройство Hub4

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Hub4
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
```

```
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:101:101:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
```

```
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:101:101:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.255.21 255.255.255.0
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:101:101:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.20.200/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 multicast dynamic
 holding-time 90
 cisco-authentication secret
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Hub4
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 10.10.20.200
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor spokes-ibgp peer-group
 neighbor spokes-ibgp remote-as 65000
 neighbor 192.168.255.1 remote-as 65001
 bgp listen limit 5000
 bgp listen range 10.10.20.0/24 peer-group spokes-ibgp
 !
 address-family ipv4 unicast
  neighbor spokes-ibgp route-reflector-client
  neighbor spokes-ibgp next-hop-self
  neighbor spokes-ibgp route-map FROM-HUB4-OUT out
 exit-address-family
exit
!
route-map FROM-HUB4-OUT permit 1
 set local-preference 25
exit
!
end
```

Устройство Spoke1-n1

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
fhrp version vrrp v3
hostname Spoke1-n1
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
!
```

```
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:100:1:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
```

```
 set dead-connection history off
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:100:1:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.1.10 255.255.255.0
 vrrp 1 address-family ipv4
  timers advertise 3
  timers garp 5
  no preempt
  track sla check_isp_link
  track interface TenGigabitEthernet0/0
  address 192.168.1.1 255.255.255.0
  exit-vrrp
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:100:1:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
vrrp track sla check_isp_link ipv6
 host 2001:db8::172:16:1:1
 host 2001:db8::172:16:101:15
 mode icmp-echo
 reachability any
 source TenGigabitEthernet0/0
 fall 15
 rise 10
 timeout 2
 interval 3
!
vrrp notify common
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.10.1/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Содержимое файла `/etc/network/interfaces.d/mgre1`:

```
auto mgre1
iface mgre1 inet static
address 10.10.20.1/24
pre-up ip link del mgre1 2> /dev/null || true
pre-up ip tunnel add mgre1 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
post-up ethtool -K mgre1 tx-checksumming off > /dev/null
post-down ip link del mgre1
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 map 10.10.10.100/24 2001:db8::172:16:100:2 register
 map 10.10.10.200/24 2001:db8::172:16:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
interface mgre1
 map 10.10.20.100/24 2001:db8::172:17:100:2 register
 map 10.10.20.200/24 2001:db8::172:17:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Spoke1-n1
log syslog informational
service integrated-vtysh-config
!
ip route 192.168.100.0/24 192.168.1.20 240
!
router bgp 65000
 bgp router-id 192.168.1.10
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor 10.10.10.100 remote-as 65000
 neighbor 10.10.10.100 timers connect 30
 neighbor 10.10.10.200 remote-as 65000
 neighbor 10.10.10.200 timers connect 30
 neighbor 10.10.20.100 remote-as 65000
```

```
 neighbor 10.10.20.100 timers connect 30
 neighbor 10.10.20.200 remote-as 65000
 neighbor 10.10.20.200 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.1.0/24
  neighbor 10.10.10.100 route-map TO-HUB1-OUT out
  neighbor 10.10.10.200 route-map TO-HUB2-OUT out
  neighbor 10.10.20.100 route-map TO-HUB3-OUT out
  neighbor 10.10.20.200 route-map TO-HUB4-OUT out
 exit-address-family
exit
!
route-map TO-HUB1-OUT permit 1
 set local-preference 100
exit
!
route-map TO-HUB2-OUT permit 1
 set local-preference 75
exit
!
route-map TO-HUB3-OUT permit 1
 set local-preference 50
exit
!
route-map TO-HUB4-OUT permit 1
 set local-preference 25
exit
!
end
```

Настройки VRRP

Содержимое файла `/etc/keepalived/notify_common.conf`:

```
################################################   specific   to   DMVPN   scenario
#############################################################
# Flag indicate that DMVPN scenario is using on clustered spokes.
# Used to mange BGP neighbors shutdown state or OSPF interfaces passive mode when
VRRP node changes it STATE.
FLAG_DMVPN_SCENARIO_ON_CLUSTERED_SPOKE="true"

### IBGP specific options ###
# Internal routing protocol for DMVPN (IBGP or OSPF).
DMVPN_INTERNAL_ROUTING_PROTOCOL="IBGP"

# Local BGP AS Number. Set it if internal routing protocol is IBGP.
DMVPN_LOCAl_ASN="65000"

# BGP neighbors (separated by space) which must be shutted down if VRRP node transit
to BACKUP of FAULT state,
# and no shutted down if VRRP node transit to MASTER state.
# Set it if internal routing protocol is IBGP.
DMVPN_BGP_NEIGHBORS="10.10.10.100 10.10.10.200 10.10.20.100 10.10.20.200"
```

Содержимое файла `/etc/keepalived/keepalived.conf`:

```
global_defs {
  enable_dbus
}
vrrp_sync_group 0 {
  notify "/etc/keepalived/scripts/notify_common"
```

```
  group {
    eth1_1
  }
}
vrrp_script check_isp_link {
  script "/etc/keepalived/scripts/sla check --ip-version 6 --mode icmp-echo --hosts
2001:db8::172:16:1:1 2001:db8::172:17:1:1 --reachability any --source-iface eth0 -
-tos 0xB8 --data-size 56 --name check_isp_link"
  fall 15
  rise 10
  timeout 2
  interval 3
}
vrrp_instance eth1_1 {
  version 3
  interface eth1
  track_interface {
    eth0
  }
  virtual_ipaddress {
    192.168.1.1/24 label eth1:900
  }
  nopreempt
  priority 100
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 1
  track_script {
    check_isp_link
  }
}
```

Устройство Spoke1-n2

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
fhrp version vrrp v3
hostname Spoke1-n2
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
!
!
```

```
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-IPV6
 description IP on WAN interface
 host 2001:db8::100:101:1:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-IPV6 any
!
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
!
ipv6 access-list IPSEC_DMVPN_IPV6
 remark special DMVPN filter
 permit gre object-group SELF-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_IPV6 1
 match ipv6 address IPSEC_DMVPN_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
```

```
!
crypto map VPN_IPV6 1 ipsec-isakmp dynamic DMAP_IPV6
!
interface TenGigabitEthernet0/0
 no ip address
 ipv6 address 2001:db8::100:101:1:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_IPV6 out
 crypto map VPN_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 ip address 192.168.1.20 255.255.255.0
 vrrp 1 address-family ipv4
  timers advertise 3
  timers garp 5
  no preempt
  priority 50
  track sla check_isp_link
  track interface TenGigabitEthernet0/0
  address 192.168.1.1 255.255.255.0
  exit-vrrp
!
interface TenGigabitEthernet0/2
 no ip address
 shutdown
!
!
!
ipv6 route ::/0 2001:db8::100:101:1:1
!
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
...
AD4F8901771632E0A0AF83

quit
!
vrrp track sla check_isp_link ipv6
 host 2001:db8::172:17:1:1
 host 2001:db8::172:16:101:15
 mode icmp-echo
 reachability any
 source TenGigabitEthernet0/0
 fall 15
 rise 10
 timeout 2
 interval 3
!
vrrp notify common
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.10.2/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Содержимое файла `/etc/network/interfaces.d/mgre1`:

```
auto mgre1
iface mgre1 inet static
address 10.10.20.2/24
pre-up ip link del mgre1 2> /dev/null || true
pre-up ip tunnel add mgre1 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
post-up ethtool -K mgre1 tx-checksumming off > /dev/null
post-down ip link del mgre1
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 map 10.10.10.100/24 2001:db8::172:16:100:2 register
 map 10.10.10.200/24 2001:db8::172:16:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
interface mgre1
 map 10.10.20.100/24 2001:db8::172:17:100:2 register
 map 10.10.20.200/24 2001:db8::172:17:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Spoke1-n2
service integrated-vtysh-config
!
ip route 192.168.100.0/24 192.168.1.10 240
!
router bgp 65000
 bgp router-id 192.168.1.20
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor 10.10.10.100 remote-as 65000
 neighbor 10.10.10.100 shutdown
 neighbor 10.10.10.100 timers connect 30
 neighbor 10.10.10.200 remote-as 65000
 neighbor 10.10.10.200 shutdown
 neighbor 10.10.10.200 timers connect 30
```

```
 neighbor 10.10.20.100 remote-as 65000
 neighbor 10.10.20.100 shutdown
 neighbor 10.10.20.100 timers connect 30
 neighbor 10.10.20.200 remote-as 65000
 neighbor 10.10.20.200 shutdown
 neighbor 10.10.20.200 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.1.0/24
  neighbor 10.10.10.100 route-map TO-HUB1-OUT out
  neighbor 10.10.10.200 route-map TO-HUB2-OUT out
  neighbor 10.10.20.100 route-map TO-HUB3-OUT out
  neighbor 10.10.20.200 route-map TO-HUB4-OUT out
 exit-address-family
exit
!
route-map TO-HUB1-OUT permit 1
 set local-preference 100
exit
!
route-map TO-HUB2-OUT permit 1
 set local-preference 75
exit
!
route-map TO-HUB3-OUT permit 1
 set local-preference 50
exit
!
route-map TO-HUB4-OUT permit 1
 set local-preference 25
exit
!
end
```

Настройки VRRP

Содержимое файла `/etc/keepalived/notify_common.conf`:

```
############################################### specific to DMVPN scenario
############################################################
# Flag indicate that DMVPN scenario is using on clustered spokes.
# Used to mange BGP neighbors shutdown state or OSPF interfaces passive mode when
VRRP node changes it STATE.
FLAG_DMVPN_SCENARIO_ON_CLUSTERED_SPOKE="true"

### IBGP specific options ###
# Internal routing protocol for DMVPN (IBGP or OSPF).
DMVPN_INTERNAL_ROUTING_PROTOCOL="IBGP"

# Local BGP AS Number. Set it if internal routing protocol is IBGP.
DMVPN_LOCAl_ASN="65000"

# BGP neighbors (separated by space) which must be shutted down if VRRP node transit
to BACKUP of FAULT state,
# and no shutted down if VRRP node transit to MASTER state.
# Set it if internal routing protocol is IBGP.
DMVPN_BGP_NEIGHBORS="10.10.10.100 10.10.10.200 10.10.20.100 10.10.20.200"
```

Содержимое файла `/etc/keepalived/keepalived.conf`:

```
global_defs {
  enable_dbus
```

```
}
vrrp_sync_group 0 {
  notify "/etc/keepalived/scripts/notify_common"
  group {
    eth1_1
  }
}
vrrp_script check_isp_link {
  script "/etc/keepalived/scripts/sla check --ip-version 6 --mode icmp-echo --hosts
2001:db8::172:16:1:1 2001:db8::172:17:1:1 --reachability any --source-iface eth0 -
-tos 0xB8 --data-size 56 --name check_isp_link"
  fall 15
  rise 10
  timeout 2
  interval 3
}
vrrp_instance eth1_1 {
  version 3
  interface eth1
  track_interface {
    eth0
  }
  virtual_ipaddress {
    192.168.1.1/24 label eth1:900
  }
  nopreempt
  priority 50
  advert_int 3
  garp_master_refresh 5
  virtual_router_id 1
  track_script {
    check_isp_link
  }
}
```

Устройство Spoke2

cisco-like консоль

```
!
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 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 secret 5 $6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/x
heIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXWA9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke2
enable secret 5 PC9d7N5HlAyLrzuA3qRJvQ==
!
```

```
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile ALGS_PROFILE
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
 mode transport
!
object-group v6-network SELF-ISP1-IPV6
 description IP on WAN interface for ISP1
 host 2001:db8::172:16:2:2
!
object-group v6-network SELF-ISP2-IPV6
 description IP on WAN interface for ISP2
 host 2001:db8::172:17:2:2
!
ip access-list extended FIREWALL_OUT
 deny   ip any any
!
ip access-list extended FIREWALL_IN
 deny   ip any any
!
ipv6 default filtering deny
!
ipv6 access-list FW_OUTPUT_WAN_ISP1_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-ISP1-IPV6 any
!
ipv6 access-list FW_INPUT_WAN_ISP1_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit udp any object-group SELF-ISP1-IPV6 eq isakmp
 permit udp any object-group SELF-ISP1-IPV6 eq non500-isakmp
 permit icmp any object-group SELF-ISP1-IPV6
 permit esp any object-group SELF-ISP1-IPV6
!
ipv6 access-list FW_OUTPUT_WAN_ISP2_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 deny   gre any any
 permit ipv6 object-group SELF-ISP2-IPV6 any
!
ipv6 access-list FW_INPUT_WAN_ISP2_IPV6
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit udp any object-group SELF-ISP2-IPV6 eq isakmp
 permit udp any object-group SELF-ISP2-IPV6 eq non500-isakmp
```

```
 permit icmp any object-group SELF-ISP2-IPV6
 permit esp any object-group SELF-ISP2-IPV6
!
ipv6 access-list IPSEC_DMVPN_ISP1_IPV6
 remark special DMVPN filter for ISP1
 permit gre object-group SELF-ISP1-IPV6 each
!
ipv6 access-list IPSEC_DMVPN_ISP2_IPV6
 remark special DMVPN filter for ISP2
 permit gre object-group SELF-ISP2-IPV6 each
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ipv6 inspect name INSPECT tcp
ipv6 inspect name INSPECT udp
!
crypto dynamic-map DMAP_ISP1_IPV6 1
 match ipv6 address IPSEC_DMVPN_ISP1_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto dynamic-map DMAP_ISP2_IPV6 1
 match ipv6 address IPSEC_DMVPN_ISP2_IPV6
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile ALGS_PROFILE
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN_ISP1_IPV6 1 ipsec-isakmp dynamic DMAP_ISP1_IPV6
!
crypto map VPN_ISP2_IPV6 2 ipsec-isakmp dynamic DMAP_ISP2_IPV6
!
interface TenGigabitEthernet0/0
 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_ISP1_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_ISP1_IPV6 out
 crypto map VPN_ISP1_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/1
 no ip address
 ipv6 address 2001:db8::172:17:2:2/112
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 ipv6 access-group FW_INPUT_WAN_ISP2_IPV6 in
 ipv6 access-group FW_OUTPUT_WAN_ISP2_IPV6 out
 crypto map VPN_ISP2_IPV6
 ipv6 inspect INSPECT out
!
interface TenGigabitEthernet0/2
 ip address 192.168.2.1 255.255.255.0
!
interface TenGigabitEthernet0/3
```

```
 no ip address
 shutdown
!
!
!
!
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
...
AD4F8901771632E0A0AF83

quit
!
end
```

Настройки mGRE

Содержимое файла `/etc/network/interfaces.d/mgre0`:

```
auto mgre0
iface mgre0 inet static
address 10.10.10.3/24
pre-up ip link del mgre0 2> /dev/null || true
pre-up ip tunnel add mgre0 mode ip6gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
post-up ethtool -K mgre0 tx-checksumming off > /dev/null
post-down ip link del mgre0
```

Содержимое файла `/etc/network/interfaces.d/mgre1`:

```
auto mgre1
iface mgre1 inet static
address 10.10.20.3/24
pre-up ip link del mgre1 2> /dev/null || true
pre-up ip tunnel add mgre1 mode ip6gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
post-up ethtool -K mgre1 tx-checksumming off > /dev/null
post-down ip link del mgre1
```

Настройки NHRP

Содержимое файла `/etc/opennhrp/opennhrp.conf`:

```
interface mgre0
 map 10.10.10.100/24 2001:db8::172:16:100:2 register
 map 10.10.10.200/24 2001:db8::172:16:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
 non-caching
interface mgre1
 map 10.10.20.100/24 2001:db8::172:17:100:2 register
 map 10.10.20.200/24 2001:db8::172:17:101:2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
```

```
 non-caching
```

Настройки BGP

```
!
frr version 9.0.2
frr defaults traditional
hostname Spoke2
log syslog informational
service integrated-vtysh-config
!
router bgp 65000
 bgp router-id 192.168.2.1
 bgp log-neighbor-changes
 no bgp ebgp-requires-policy
 timers bgp 3 9
 neighbor 10.10.10.100 remote-as 65000
 neighbor 10.10.10.100 timers connect 30
 neighbor 10.10.10.200 remote-as 65000
 neighbor 10.10.10.200 timers connect 30
 neighbor 10.10.20.100 remote-as 65000
 neighbor 10.10.20.100 timers connect 30
 neighbor 10.10.20.200 remote-as 65000
 neighbor 10.10.20.200 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.2.0/24
  neighbor 10.10.10.100 route-map TO-HUB1-OUT out
  neighbor 10.10.10.200 route-map TO-HUB2-OUT out
  neighbor 10.10.20.100 route-map TO-HUB3-OUT out
  neighbor 10.10.20.200 route-map TO-HUB4-OUT out
 exit-address-family
exit
!
route-map TO-HUB1-OUT permit 1
 set local-preference 100
exit
!
route-map TO-HUB2-OUT permit 1
 set local-preference 75
exit
!
route-map TO-HUB3-OUT permit 1
 set local-preference 50
exit
!
route-map TO-HUB4-OUT permit 1
 set local-preference 25
exit
!
end
```

Настройки multiwan

```
config_format_version: 1
links_params:
  links:
  - name: ISP1
    check:
      hosts_reachability: any
      ipv6:
```

```
      hosts:
      - 2001:db8::172:16:101:15
      - 2001:db8::172:16:2:1
      source_address: 2001:db8::172:16:2:2
    method:
      icmp:
        max_rtt: 100
        interval: 3
        restore_interval: 1
        restore_count: 10
        failure_count: 10
        tos: 184
        data_size: 56
  iface_name: eth0
  prio: 300
  routes:
    ipv6:
      networks:
      - ::/0
      nexthop: 2001:db8::172:16:2:1
      source_address: 2001:db8::172:16:2:2
    watch_foreign_routes: true
- name: ISP2
  check:
    hosts_reachability: any
    ipv6:
      hosts:
      - 2001:db8::172:16:101:15
      - 2001:db8::172:17:2:1
      source_address: 2001:db8::172:17:2:2
    method:
      icmp:
        max_rtt: 100
        interval: 3
        restore_interval: 1
        restore_count: 10
        failure_count: 10
        tos: 184
        data_size: 56
  iface_name: eth1
  prio: 200
  routes:
    ipv6:
      networks:
      - ::/0
      nexthop: 2001:db8::172:17:2:1
      source_address: 2001:db8::172:17:2:2
    watch_foreign_routes: True
```