Пример использования VRF в DMVPN (phase 2)

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего документа 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 документа, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Введение

Данный документ описывает настройку криптошлюзов «С-Терра Шлюз» для обеспечения безопасного взаимодействия между Центральным офисом и Филиалами. Рассматривается конфигурация сети на базе технологии DMVPN (phase 2) в условиях пересекающегося адресного пространства подсетей в Центральном офисе и Филиалах.

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

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

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

Предварительные требования

Требования к материально-техническому обеспечению

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

Требования к квалификации администратора

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

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

Требования к инфраструктуре

1. Требования к устройствам.

   1.1. «С-Терра Шлюз».

   1.1.1 Устройства «С-Терра Шлюз» должны быть инициализированы (подробнее на https://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

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

   1.2. Центр выпуска сертификатов.

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

   1.2.2 Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2016 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 5.0 (или новее).

   1.2.3 Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp).

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

   1.3. HTTP сервер для распространения списка отозванных сертификатов.

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

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

2. Требования к сетевому взаимодействию.

   2.1. Между устройствами стенда должна быть обеспечена IP связность.

© 2003-2026 S-Terra CSP

Общая схема стенда

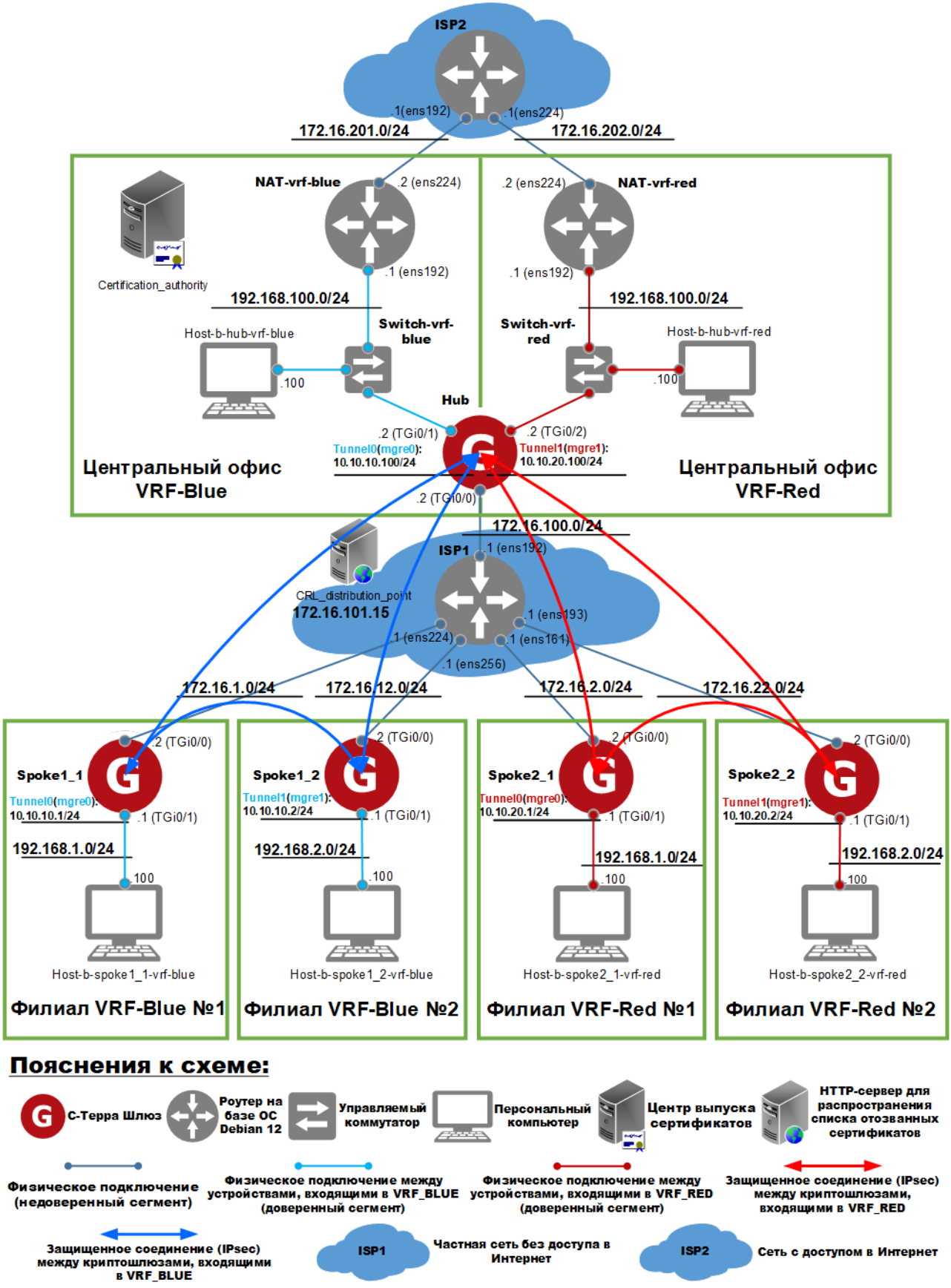


Рисунок 1. Общая схема стенда

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе VRF-Blue размещаются: криптошлюз «С-Терра Шлюз» (Hub), коммутатор (Int-switch-vrf-blue), натирующее устройство (NAT-vrf-blue), персональный компьютер (Host-b-hub-vrf-blue), центр выпуска сертификатов (Certification_authority).

   1.2. В центральном офисе VRF-Red размещаются: криптошлюз «С-Терра Шлюз» (Hub), коммутатор (Int-switch-vrf-red), натирующее устройство (NAT-vrf-red), персональный компьютер (Host-b-hub-vrf-red).

   1.3. В филиале VRF-Blue №1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1_1), персональный компьютер (Host-b-spoke1_1-vrf-blue).

   1.4. В филиале VRF-Blue №2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1_2), персональный компьютер (Host-b-spoke1_2-vrf-blue).

   1.5. В филиале VRF-Red №1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2_1), персональный компьютер (Host-b-spoke2_1-vrf-red).

   1.6. В филиале VRF-Red №2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2_2), персональный компьютер (Host-b-spoke2_2-vrf-red).

   1.7. В неконтролируемом сегменте сети ISP1 размещаются: HTTP-сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизатор (ISP1).

   1.8. В неконтролируемом сегменте сети ISP2 размещается маршрутизатор (ISP1).

2. Применение VRF.

   В данном документе использование VRF на Hub позволяет создать два независимых домена маршрутизации (VRF_BLUE и VRF_RED). Это логическое разделение дает возможность использовать пересекающиеся защищаемые подсети на криптошлюзах, относящихся к VRF_BLUE (Spoke1_1 и Spoke1_2), и криптошлюзах, относящихся к VRF_RED (Spoke2_1 и Spoke2_2). Кроме того, оно позволяет использовать пересекающиеся подсети за Hub.

   VRF на криптошлюзах Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 используется для обеспечения доступа устройств, находящихся за ними, в Интернет через Hub. Тогда как доступ к защищаемым подсетям осуществляется в соответствии с логикой работы DMVPN (phase 2).

3. Расположение интерфейсов в VRF.

   В VRF_BLUE находятся интерфейсы TenGigabitEthernet0/1 и Tunnel0 (mgre0), принадлежащие криптошлюзу Hub, а также LAN и mGRE интерфейсы, принадлежащие криптошлюзам Spoke1_1 и Spoke1_2.

   В VRF_RED находятся интерфейсы TenGigabitEthernet0/2, и Tunnel1 (mgre1), принадлежащие криптошлюзу Hub, а также LAN и mGRE интерфейсы, принадлежащие криптошлюзам Spoke2_1 и Spoke2_2.

4. Подлючение к сети Интернет.

   Доступ в Интернет для устройств за Hub обеспечивается статическими маршрутами по умолчанию на самом Hub. Трафик от Host-b-hub-vrf-blue уходит через NAT-vrf-blue, а от Host-b-hub-vrf-red — через NAT-vrf-red.

5. Параметры шифрования IPsec.

   Весь трафик между подсетью 192.168.100.0/24 (VRF_BLUE) и подсетями 192.168.1.0/24, 192.168.2.0/24 (VRF_BLUE) инкапсулируется в GRE. Также, весь трафик между подсетью 192.168.100.0/24 (VRF_RED) и подсетями 192.168.1.0/24, 192.168.2.0/24 (VRF_RED) инкапсулируется в GRE. GRE трафик защищается с использованием алгоритмов ГОСТ и протокола IPsec в транспортном IPv4 режиме.

© 2003-2026 S-Terra CSP

Между криптошлюзами Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 и криптошлюзом Hub устанавливаются статические IPsec туннели. Инициатором подключения является служебный трафик протоколов NHRP/BGP.

Между криптошлюзами Spoke1_1 и Spoke1_2, а также между криптошлюзами Spoke2_1 и Spoke2_2 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».

5.1. 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).

5.2. Параметры протокола ESP:

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

6. Параметры межсетевого экранирования.

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

6.1. На интерфейсах TenGigabitEthernet 0/1, TenGigabitEthernet 0/2 криптошлюза Hub и TenGigabitEthernet 0/1 интерфейсах криптошлюзов Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 IPv4 трафик не контролируется.

6.2. На интерфейсах TenGigabitEthernet 0/1, TenGigabitEthernet 0/2 криптошлюза Hub и TenGigabitEthernet 0/1 интерфейсах криптошлюзов Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 IPv6 трафик заблокирован.

6.3. На интерфейсах TenGigabitEthernet 0/0 криптошлюзов Hub, Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 разрешен входящий IPv4 трафик:

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

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

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

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

6.4. На интерфейсах TenGigabitEthernet 0/0 криптошлюзов Hub, Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 заблокирован исходящий незашифрованный GRE трафик и транзитный трафик до приватных IP адресов.

6.5. На интерфейсах TenGigabitEthernet 0/0 криптошлюзов Hub, Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 IPv6 трафик заблокирован.

6.6. На интерфейсах TenGigabitEthernet 0/0 криптошлюзов Hub, Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 инспектируются все исходящие локальные и транзитные IPv4 соединения для протоколов TCP и UDP. На основе результатов инспектирования осуществляется фильтрация входящего трафика с учетом состояния сессии (stateful).

7. Ограничения.

Из-за ограничений, связанных с conntrack таблицей, source NAT не может быть настроен на криптошлюзе Hub. Поэтому в качестве натирующих устройств используются выделенные устройства NAT-vrf-blue и NAT-vrf-red (это может быть одно устройство если оно поддерживает настройку NAT в VRF).

Настройка стенда

Настройка устройства Host-b-hub-vrf-blue

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.2

Настройка устройства Host-b-hub-vrf-red

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.2

Настройка устройства Host-b-spoke1_1-vrf-blue

1. Настройте IP адрес – 192.168.1.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.1.1

Настройка устройства Host-b-spoke1_2-vrf-blue

1. Настройте IP адрес – 192.168.2.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.2.1

Настройка устройства Host-b-spoke2_1-vrf-red

1. Настройте IP адрес – 192.168.1.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.1.1

Настройка устройства Host-b-spoke2_2-vrf-red

1. Настройте IP адрес – 192.168.2.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.2.1

Настройка устройства ISP1

1. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Настройте IP адрес – 172.16.12.1 и маску – 255.255.255.0 на сетевом интерфейсе ens256.
4. Настройте IP адрес – 172.16.2.1 и маску – 255.255.255.0 на сетевом интерфейсе ens161.
5. Настройте IP адрес – 172.16.22.1 и маску – 255.255.255.0 на сетевом интерфейсе ens193.
6. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства ISP2

1. Настройте IP адрес – 172.16.201.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.202.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.

© 2003-2026 S-Terra CSP

3. Настройте IP адрес – 172.10.0.1 и маску – 255.255.255.255 на сетевом интерфейсе ens256 (данный адрес приведен в качестве примера для проверки доступности сети Интернет с компьютеров, расположенных за криптошлюзами Центрального офиса и Филиалов).
4. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства NAT-vrf-blue

1. Настройте IP адрес – 192.168.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.201.2 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Задайте маршрут по умолчанию через 172.16.201.1
4. Настройте Source NAT на сетевом интерфейсе ens224. Пример команды для iptables:

```
iptables -t nat -A POSTROUTING -o ens224 -j SNAT --to-source 172.16.201.2
```

5. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства NAT-vrf-red

1. Настройте IP адрес – 192.168.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.202.2 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Задайте маршрут по умолчанию через 172.16.202.1
4. Настройте Source NAT на сетевом интерфейсе ens224. Пример команды для iptables:

```
iptables -t nat -A POSTROUTING -o ens224 -j SNAT --to-source 172.16.202.2
```

5. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Hub

Настройка сетевых параметров

1. Задайте имя устройства:

```
sterragate(config)#hostname Hub
```

2. Включите WAN и LAN интерфейсы и настройте IP адреса в соответствии со схемой стенда, а также задайте маршруты по умолчанию:

```
Hub(config)#interface TenGigabitEthernet0/0
Hub(config-if)# ip address 172.16.100.2 255.255.255.0
Hub(config-if)# no shutdown
Hub(config-if)#interface TenGigabitEthernet0/1
Hub(config-if)# ip address 192.168.100.2 255.255.255.0
Hub(config-if)# no shutdown
Hub(config-if)#interface TenGigabitEthernet0/2
Hub(config-if)# ip address 192.168.100.2 255.255.255.0
Hub(config-if)# no shutdown
Hub(config-if)# exit
Hub(config)#ip route 0.0.0.0 0.0.0.0 172.16.100.1
Hub(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1 table 10
Hub(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1 table 20
Hub(config)#end
```

Настройка шифрования

Настройки шифрования осуществляются из cisco-like консоли криптошлюза.

1. Параметры IKE:

   1.1. Задайте общие параметры IKE:

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

1.2. Создайте политику **1**, описывающую алгоритмы IKE туннеля:

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

1.3. Создайте профиль настроек ISAKMP (алгоритм IKE) под именем `ALGS_PROFILE`, чтобы далее его прикрепить к соответствующему разделу крипто-карты:

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

2. Параметры IPsec:

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

```
Hub(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:

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

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

```
Hub(config)#object-group network SELF
Hub(config-network-group)#description IP on WAN interface
Hub(config-network-group)#host 172.16.100.2
Hub(config-network-group)#exit
```

2.4. Создайте сетевой `object-group` с именем `PRIVATE` для хранения в нем приватных подсетей с целью дальнейшего его использования в ACL:

```
Hub(config)#object-group network PRIVATE
Hub(config-network-group)#description private LANs
Hub(config-network-group)#172.16.0.0 255.240.0.0
Hub(config-network-group)#192.168.0.0 255.255.0.0
Hub(config-network-group)#10.0.0.0 255.0.0.0
Hub(config-network-group)#exit
```

2.5. Создайте список доступа (ACL) для IPv4 трафика, который нужно защищать между центральным офисом и филиалом:

```
Hub(config)#ip access-list extended IPSEC_DMVPN
Hub(config-ext-nacl)# remark special DMVPN filter
```

```
Hub(config-ext-nacl)# permit gre object-group SELF each
Hub(config-ext-nacl)#exit
Hub(config)#
```

2.6. Создайте динамическую крипто-карту (имя DMAP, раздел 1) и привяжите её к статической (имя VPN, раздел 1):

```
Hub(config)#crypto dynamic-map DMAP 1
Hub(config-crypto-map)# match address IPSEC_DMVPN
Hub(config-crypto-map)# set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub(config-crypto-map)# set isakmp-profile ALGS_PROFILE
Hub(config-crypto-map)# set security-association mss-fix out
Hub(config-crypto-map)# set pre-fragmentation
Hub(config-crypto-map)# set dead-connection history off
Hub(config-crypto-map)#exit
Hub(config)#crypto map VPN 1 ipsec-isakmp dynamic DMAP
Hub(config)#
```

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

```
Hub(config)#interface TenGigabitEthernet0/0
Hub(config-if)#crypto map VPN
Hub(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

Настройка межсетевого экрана осуществляются из cisco-like консоли.

1. Создайте ACL с именем `FIREWALL_OUT` для исходящего с WAN интерфейса трафика:

   Список доступа для исходящего трафика должен блокировать открытый трафик из защищаемой подсети криптошлюза в подсети RFC1918/RFC6598 (считаем, что трафик непубличных подсетей должен обязательно шифроваться), а также незашифрованный GRE.

```
Hub(config)#ip access-list extended FIREWALL_OUT
Hub(config-ext-nacl)# permit ip object-group SELF object-group PRIVATE
Hub(config-ext-nacl)# deny ip any object-group PRIVATE
Hub(config-ext-nacl)# deny gre any any
Hub(config-ext-nacl)# permit ip any any
Hub(config-ext-nacl)#exit
```

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

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

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

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

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

```
Hub(config)#interface TenGigabitEthernet0/0
Hub(config-if)# ip access-group FIREWALL_IN in
Hub(config-if)# ip access-group FIREWALL_OUT out
Hub(config-if)# ip inspect INSPECT out
Hub(config-if)#exit
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка mGRE и VRF интерфейсов

В сборке 5.0.25337 консоль cisco-like некорректно работает с GRE-интерфейсами, на которых настроен настроен VRF, из-за чего неверно считывается часть параметров (tunnel mode, tunnel source, tunnel destination и tunnel key). Поэтому настройка GRE-интерфейсов должна осуществляться не в консоли, а в файле `/etc/network/interfaces.d/interfaces` по аналогии с VRF-интерфейсам.
Также **важно**, чтобы GRE-интерфейсы, которые входят в VRF, существовали в системе на момент включения VRF интерфейса, в противном случае VRF инстанс будет сконфигурирован неправильно.
По умолчанию, интерфейсы, описанные в конфигурационных файлах в директории `/etc/network/interfaces.d/`, включаются **до** интерфейсов, описанных в `/etc/network/interfaces`.
В связи с этим, если в VRF требуется добавить интерфейсы, которые создаются в конфигурационном файле `/etc/network/interfaces` и которые еще не существуют на момент включения соответствующего VRF интерфейса, то следует либо перенести описание VRF интерфейса в файл `/etc/network/interfaces` (после секции, обозначенной строками `###netifcfg-begin###` и `###netifcfg-end###`), либо в файле `/etc/network/interfaces` перенести строку `source /etc/network/interfaces.d/*` в конец файла (после строки `###netifcfg-end###`).

1. Приведите файл `/etc/network/interfaces.d/interfaces` к виду:

```
auto vrf_blue
iface vrf_blue inet manual
pre-up ip link del vrf_blue type vrf 2>/dev/null || true
pre-up ip route flush table 10 2>/dev/null || true
pre-up ip link add vrf_blue type vrf table 10
pre-up ip link set dev vrf_blue up
pre-up ip route add table 10 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_blue
pre-up ip link set dev mgre0 master vrf_blue 2>/dev/null || true
post-down ip link set dev vrf_blue down

auto vrf_red
iface vrf_red inet manual
pre-up ip link del vrf_red type vrf 2>/dev/null || true
pre-up ip route flush table 20 2>/dev/null || true
pre-up ip link add vrf_red type vrf table 20
pre-up ip link set dev vrf_red up
pre-up ip route add table 20 unreachable default metric 4278198272
pre-up ip link set dev eth2 master vrf_red
pre-up ip link set dev mgre1 master vrf_red 2>/dev/null || true
post-down ip link set dev vrf_red down

auto mgre0
iface mgre0 inet static
```

```
address 10.10.10.100
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_blue || true
post-down ip link del mgre0

auto mgre1
iface mgre1 inet static
address 10.10.20.100
netmask 255.255.255.0
pre-up ip tunnel add mgre1 mode gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 type gre nopmtudisc
pre-up ip link set mgre1 type gre ignore-df
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
pre-up ip link set dev mgre1 master vrf_red || true
post-down ip link del mgre1
```

Настройка NHRP

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

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

interface mgre1
 multicast dynamic
 holding-time 90
 cisco-authentication secret
```

2. Добавьте сервис OpenNHRP в автозагрузку и запустите его:

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

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

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

Настройка BGP

Динамическая маршрутизация настраивается через консоль сервиса FRR.

1. Добавьте сервис FRR в автозагрузку и запустите его:

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

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

```
root@Hub:~# vtysh
```

```

Hello, this is FRRouting (version 9.0.4).
```

```
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hub#
```

3. Настройте BGP:

```
Hub# configure terminal
```

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

```
Hub(config)# router bgp 65000 vrf vrf_blue
```

3.2. Установите идентификатор маршрутизатора:

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

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

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

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

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

3.5. Создайте группу `spokes-ibgp_cloud1` с номером автономной системы 65000 для BGP соседей из mgre подсети, входящую в vrf_blue:

```
Hub(config-router)# neighbor spokes-ibgp_cloud1 peer-group
Hub(config-router)# neighbor spokes-ibgp_cloud1 remote-as 65000
Hub(config-router)# bgp listen range 10.10.10.0/24 peer-group spokes-ibgp_cloud1
```

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

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

3.7. Включите анонсирование маршрута до защищаемой подсети Центрального офиса VRF_Blue:

```
Hub(config-router)#address-family ipv4 unicast
Hub(config-router-af)#network 192.168.100.0/24
```

3.8. Включите пересылку маршрутов для группы `spokes-ibgp_cloud1`:

```
Hub(config-router-af)# neighbor spokes-ibgp_cloud1 route-reflector-client
Hub(config-router-af)# exit
Hub(config-router)#exit
```

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

```
Hub(config)# router bgp 65000 vrf vrf_red
```

3.10. Установите идентификатор маршрутизатора:

```
Hub(config-router)# bgp router-id 10.10.20.100
```

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

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

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

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

3.13. Создайте группу `spokes-ibgp_cloud2` с номером автономной системы 65000 для BGP соседей из mgre подсети, входящую в vrf_red:

```
Hub(config-router)# neighbor spokes-ibgp_cloud2 peer-group
Hub(config-router)# neighbor spokes-ibgp_cloud2 remote-as 65000
Hub(config-router)# bgp listen range 10.10.20.0/24 peer-group spokes-ibgp_cloud1
```

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

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

3.15. Включите анонсирование маршрута до защищаемой подсети Центрального офиса VRF_Red:

```
Hub(config-router)#address-family ipv4 unicast
Hub(config-router-af)#network 192.168.100.0/24
```

3.16. Включите пересылку маршрутов для группы `spokes-ibgp_cloud2`:

```
Hub(config-router-af)# neighbor spokes-ibgp_cloud2 route-reflector-client
```

3.17. Сохраните изменения:

```
Hub(config-router-af)# end
Hub# 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]
```

Добавление mGRE-интерфейсов в файл /etc/ifaliases.cf

1. Добавьте mGRE-интерфейсы mgre0 и mgre1 в файл `/etc/ifaliases.cf` (выделено жирным):

```
root@Hub:~# nano /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="Tunnel1" pattern="mgre1")
interface (name="default" pattern="*")
```

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

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

```
SUCCESS:  Operation was successful.
```

3. Перезапустите VPN сервис:

```
root@Hub:~# systemctl restart vpngate.service
```

В Приложении представлены тексты конфигураций для криптошлюза Hub:

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

Настройка устройства Spoke1_1

Настройка сетевых параметров

1. Задайте имя устройства:

```
sterragate(config)#hostnameSpoke1-1
```

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

```
Spoke1_1(config)#interface TenGigabitEthernet0/0
```

```
Spoke1-1(config-if)# ip address 172.16.1.2 255.255.255.0
Spoke1-1(config-if)# no shutdown
Spoke1-1(config-if)#interface TenGigabitEthernet0/1
Spoke1-1(config-if)# description interface is included in VRF_BLUE
Spoke1-1(config-if)# ip address 192.168.1.1 255.255.255.0
Spoke1-1(config-if)# no shutdown
Spoke1-1(config-if)# exit
Spoke1-1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.1
Spoke1-1(config)#end
```

Настройка шифрования

Настройки шифрования происходят аналогично настройке Hub.

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

Настройка межсетевого экрана происходит аналогично настройке Hub.

Настройка mGRE и VRF интерфейсов

1. Привидите файл `/etc/network/interfaces.d/interfaces` к виду:

```
auto vrf_blue
iface vrf_blue inet manual
pre-up ip link del vrf_blue type vrf 2>/dev/null || true
pre-up ip route flush table 10 2>/dev/null || true
pre-up ip link add vrf_blue type vrf table 10
pre-up ip link set dev vrf_blue up
pre-up ip route add table 10 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_blue
pre-up ip link set dev mgre0 master vrf_blue 2>/dev/null || true
post-down ip link set dev vrf_blue down

auto mgre0
iface mgre0 inet static
address 10.10.10.1
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_blue || true
post-down ip link del mgre0
```

Настройка NHRP

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

```
interface mgre0
 map 10.10.10.100/24 172.16.100.2 register
 multicast nhs
 holding-time 90
```

```
 cisco-authentication secret
```

2. Добавьте сервис OpenNHRP в автозагрузку и запустите его:

```
root@Spoke1-1:~# systemctl enable opennhrp
```

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

```
root@Spoke1-1:~# systemctl start opennhrp
```

Настройка BGP

Динамическая маршрутизация настраивается через консоль сервиса FRR.

1. Добавьте сервис FRR в автозагрузку и запустите его:

```
root@Spoke1-1:~# systemctl enable frr
```

```
Synchronizing state of frr.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable frr
Created symlink /etc/systemd/system/multi-user.target.wants/frr.service → /lib/systemd/system/frr.service.
```

```
root@Spoke1-1:~# systemctl start frr
```

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

```
root@Spoke1-1:~# vtysh
```

```

Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

```

3. Настройте BGP:

```
Spoke1-1#configure terminal
```

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

```
Spoke1-1(config)# router bgp 65000 vrf vrf_blue
```

3.2. Установите идентификатор маршрутизатора:

```
Spoke1-1(config-router)# bgp router-id 10.10.10.1
```

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

```
Spoke1-1(config-router)#bgp log-neighbor-changes
```

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

```
Spoke1-1(config-router)# timers bgp 3 9
```

3.5. Добавьте mGRE-адрес Hub в качестве BGP соседа с номером автономной системы 65000 и установите время повторной попытки построения BGP соседства в 30 секунд:

```
Spoke1-1(config-router)# network 10.10.10.100 remote-as 65000
Spoke1-1(config-router)# neighbor 10.10.10.100 timers connect 30
```

3.6. Включите анонсирование маршрута до защищаемой подсети Филиала VRF-Blue:

```
Spoke1-1(config-router)#address-family ipv4 unicast
Spoke1-1(config-router-af)#network 192.168.1.0/24
```

3.7. Сохраните изменения:

```
Spoke1-1(config-router-af)# end
Spoke1-1# 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]
```

Добавление mGRE-интерфейсов в файл /etc/ifaliases.cf

1. Добавьте mGRE-интерфейсы mgre0 и mgre1 в файл `/etc/ifaliases.cf` (выделено жирным):

```
root@Spoke1-1:~# nano /etc/ifaliases.cf
```

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

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

```
root@Spoke1-1:~# integr_mgr calc -f /etc/ifaliases.cf
```

```
SUCCESS:  Operation was successful.
```

3. Перезапустите VPN сервис:

```
root@Spoke1-1:~# systemctl restart vpngate.service
```

В Приложении представлены тексты конфигураций для криптошлюза Spoke1_1:

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

Настройка устройства Spoke1_2

Настройка устройства Spoke1_2 осуществляется аналогично устройству Spoke1_1 с учетом соответствующих IP-адресов (см. Рисунок 1).

В Приложении представлены тексты конфигураций для криптошлюза Spoke1_2:

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

Настройка устройства Spoke2_1

Настройка устройства Spoke2_1 осуществляется аналогично устройству Spoke1_1 с учетом соответствующих IP-адресов (см. Рисунок 1).

В Приложении представлены тексты конфигураций для криптошлюза Spoke2_1:

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

- Содержимое `/etc/ifaliases.cf`.

Настройка устройства Spoke2_2

Настройка устройства Spoke2_2 осуществляется аналогично устройству Spoke2_1 с учетом соответствующих IP-адресов (см. Рисунок 1).

В Приложении представлены тексты конфигураций для криптошлюза Spoke2_2:

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

Проверка работоспособности стенда

До построения Spoke-to-Spoke туннелей

Проверка IP связности

1. Проверьте, что с защищаемых устройств Host-b-hub-vrf-blue, Host-b-hub-vrf-red, Host-b-spoke1_1-vrf-blue, Host-b-spoke1_2-vrf-blue, Host-b-spoke2_1-vrf-red, Host-b-spoke2_2-vrf-red доступен по ICMP соответствующий криптошлюз, который является шлюзом по умолчанию. Для этого выполните команду `ping` из консоли защищаемых устройств.

```
root@Host-b-hub-vrf-blue:~# ping 192.168.100.2
```

```
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.403 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.352 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.368 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.249 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.206 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.206/0.315/0.403/0.075 ms
```

```
root@Host-b-hub-vrf-red:~# ping 192.168.100.2
```

```
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.258 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.428 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.413 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.375 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.282 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 0.258/0.351/0.428/0.068 ms
```

```
root@Host-b-spoke1_1-vrf-blue:~# ping 192.168.1.1
```

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=1.51 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=1.22 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=1.39 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=1.27 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=1.29 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.222/1.336/1.513/0.103 ms
```

```
root@Host-b-spoke1_2-vrf-blue:~# ping 192.168.2.1
```

```
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=1.20 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=1.16 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=1.28 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=1.27 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=63 time=1.11 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.108/1.204/1.280/0.065 ms
```

```
root@Host-b-spoke2_1-vrf-red:~# ping 192.168.1.1
```

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.857 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=1.10 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=1.04 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=1.07 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.857/1.032/1.103/0.090 ms
```

```
root@Host-b-spoke2_2-vrf-red:~# ping 192.168.2.1
```

```
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=1.20 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=1.18 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=1.34 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=1.26 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=63 time=1.11 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.114/1.219/1.335/0.075 ms
```

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

2. Проверьте, что с криптошлюзов по ICMP доступен ISP1. Для этого выполните команду `ping` из cisco-like консоли соответствующего криптошлюза.

```
Hub#ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=0.937 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=1.43 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.771 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.802 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.698 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4024ms
rtt min/avg/max/mdev = 0.698/0.927/1.430/0.262 ms
```

```
Spoke1-1#ping 172.16.1.1
```

```
PING 172.16.1.1 (172.16.1.1) 100(128) bytes of data.
108 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.976 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.731 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.699 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=0.673 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=0.641 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4072ms
rtt min/avg/max/mdev = 0.641/0.744/0.976/0.119 ms
```

```
Spoke1-2#ping 172.16.12.1
```

```
PING 172.16.12.1 (172.16.12.1) 100(128) bytes of data.
108 bytes from 172.16.12.1: icmp_seq=1 ttl=64 time=1.56 ms
108 bytes from 172.16.12.1: icmp_seq=2 ttl=64 time=0.792 ms
108 bytes from 172.16.12.1: icmp_seq=3 ttl=64 time=0.784 ms
108 bytes from 172.16.12.1: icmp_seq=4 ttl=64 time=0.845 ms
108 bytes from 172.16.12.1: icmp_seq=5 ttl=64 time=0.845 ms
```

```
--- 172.16.12.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 0.784/0.965/1.563/0.299 ms
```

```
Spoke2-1#ping 172.16.2.1
```

```
PING 172.16.2.1 (172.16.2.1) 100(128) bytes of data.
108 bytes from 172.16.2.1: icmp_seq=1 ttl=64 time=1.14 ms
108 bytes from 172.16.2.1: icmp_seq=2 ttl=64 time=0.747 ms
108 bytes from 172.16.2.1: icmp_seq=3 ttl=64 time=0.484 ms
108 bytes from 172.16.2.1: icmp_seq=4 ttl=64 time=0.821 ms
108 bytes from 172.16.2.1: icmp_seq=5 ttl=64 time=0.762 ms

--- 172.16.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 0.484/0.790/1.137/0.208 ms
```

```
Spoke2-2#ping 172.16.22.1
```

```
PING 172.16.22.1 (172.16.22.1) 100(128) bytes of data.
108 bytes from 172.16.22.1: icmp_seq=1 ttl=64 time=1.17 ms
108 bytes from 172.16.22.1: icmp_seq=2 ttl=64 time=0.564 ms
108 bytes from 172.16.22.1: icmp_seq=3 ttl=64 time=0.846 ms
108 bytes from 172.16.22.1: icmp_seq=4 ttl=64 time=0.825 ms
108 bytes from 172.16.22.1: icmp_seq=5 ttl=64 time=0.569 ms

--- 172.16.22.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4034ms
rtt min/avg/max/mdev = 0.564/0.794/1.170/0.222 ms
```

Видно, что устройство ISP1 доступно по ICMP со всех криптошлюзов.

3. Проверьте, что с криптошлюза Hub по ICMP доступен ISP2 с интерфейсов TenGigabitEthernet 0/1 и TenGigabitEthernet 0/2. Для этого выполните команду `ping` из cisco-like консоли криптошлюза Hub (В качестве источника необходимо указывать интерфейс, а не IP-адрес. Это связано с ограничениями утилиты `ping`. В качестве IP-адреса источника, при использовании `ping`, можно указывать только IP-адреса интерфейсов из Global VRF.):

```
Hub#ping 172.16.201.1 source TenGigabitEthernet 0/1
```

```
PING 172.16.201.1 (172.16.201.1) from 192.168.100.2 eth1: 100(128) bytes of data.
108 bytes from 172.16.201.1: icmp_seq=1 ttl=63 time=3.17 ms
108 bytes from 172.16.201.1: icmp_seq=2 ttl=63 time=2.04 ms
108 bytes from 172.16.201.1: icmp_seq=3 ttl=63 time=2.17 ms
108 bytes from 172.16.201.1: icmp_seq=4 ttl=63 time=2.01 ms
108 bytes from 172.16.201.1: icmp_seq=5 ttl=63 time=2.40 ms

--- 172.16.201.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.014/2.356/3.166/0.427 ms
```

```
Hub#ping 172.16.202.1 source TenGigabitEthernet 0/2
```

```
PING 172.16.202.1 (172.16.202.1) from 192.168.100.2 eth2: 100(128) bytes of data.
108 bytes from 172.16.202.1: icmp_seq=1 ttl=63 time=3.07 ms
108 bytes from 172.16.202.1: icmp_seq=2 ttl=63 time=2.22 ms
108 bytes from 172.16.202.1: icmp_seq=3 ttl=63 time=2.05 ms
108 bytes from 172.16.202.1: icmp_seq=4 ttl=63 time=1.97 ms
108 bytes from 172.16.202.1: icmp_seq=5 ttl=63 time=2.89 ms

--- 172.16.202.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.970/2.439/3.071/0.451 ms
```

Видно, что устройство ISP2 доступно по ICMP с криптошлюза Hub.

Проверка PKI

1. Убедитесь, что на всех криптошлюзах получены необходимые сертификаты. А также, что статус всех сертификатов Active. Для этого в linux bash консоли введите следующие команды:

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

```
Found 6 certificates. Found 1 CRL.
1 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
4 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
5 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
6 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
7 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Hub:~# 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=Hub
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
5 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
6 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
```

```
root@Spoke1-1:~# cert_mgr show
```

```
Found 3 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke1-1:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
2 State: Active    C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

```
root@Spoke1-2:~# cert_mgr show
```

```
Found 3 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke1-2:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
2 State: Active    C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

```
root@Spoke2-1:~# cert_mgr show
```

```
Found 3 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke2-1:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

```
root@Spoke2-2:~# cert_mgr show
```

```
Found 3 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke2-2:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

Проверка добавления маршрутов в VRF

1. Убедитесь, что на криптошлюзе Hub все маршруты находятся в нужном VRF.

   1.1. Global VRF. На криптошлюзе Hub в Global VRF должен находиться default-маршрут до устройства ISP1.

```
root@Hub:~# ip route
```

```
default via 172.16.100.1 dev eth0 proto st_policy
172.16.100.0/24 dev eth0 proto kernel scope link src 172.16.100.2
```

   1.2. VRF_BLUE. На криптошлюзе Hub в VRF_BLUE должен находиться default-маршрут до устройства NAT-vrf-blue. А также маршруты, добавляемые в таблицу маршрутизации, при добавлении интерфейсов Tunnel0 (mgre0) и TenGigabitEthernet 0/1 (eth1) в VRF_BLUE.

```
root@Hub:~# ip route show table 10
```

```
default via 192.168.100.1 dev eth1 proto st_policy
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.100
local 10.10.10.100 dev mgre0 proto kernel scope host src 10.10.10.100
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.100
192.168.1.0/24 nhid 33 via 10.10.10.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 nhid 34 via 10.10.10.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 dev eth1 proto kernel scope link src 192.168.100.2
local 192.168.100.2 dev eth1 proto kernel scope host src 192.168.100.2
broadcast 192.168.100.255 dev eth1 proto kernel scope link src 192.168.100.2
```

   1.3. VRF_RED. На криптошлюзе Hub в VRF_RED должен находиться default-маршрут до устройства NAT-vrf-red. А также маршруты, добавляемые в таблицу маршрутизации, при добавлении интерфейсов Tunnel1 (mgre1) и TenGigabitEthernet 0/2 (eth2) в VRF_RED.

```
root@Hub:~# ip route show table 20
```

```
default via 192.168.100.1 dev eth2 proto st_policy
unreachable default metric 4278198272
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.100
local 10.10.20.100 dev mgre1 proto kernel scope host src 10.10.20.100
broadcast 10.10.20.255 dev mgre1 proto kernel scope link src 10.10.20.100
192.168.1.0/24 nhid 37 via 10.10.20.1 dev mgre1 proto bgp metric 20
192.168.2.0/24 nhid 38 via 10.10.20.2 dev mgre1 proto bgp metric 20
192.168.100.0/24 dev eth2 proto kernel scope link src 192.168.100.2
```

```
local 192.168.100.2 dev eth2 proto kernel scope host src 192.168.100.2
broadcast 192.168.100.255 dev eth2 proto kernel scope link src 192.168.100.2
```

2. Убедитесь, что на криптошлюзах Spoke1_1 Spoke1_2 Spoke2_1 и Spoke2_2 все маршруты находятся в нужном VRF.

2.1. Global VRF. На криптошлюзах Spoke1_1 Spoke1_2 Spoke2_1 и Spoke2_2 в Global VRF должен находиться default-маршрут до устройства ISP1.

```
root@Spoke1-1:~# ip route
```

```
default via 172.16.1.1 dev eth0 proto st_policy
172.16.1.0/24 dev eth0 proto kernel scope link src 172.16.1.2
```

```
root@Spoke1-2:~# ip route
```

```
default via 172.16.12.1 dev eth0 proto st_policy
172.16.12.0/24 dev eth0 proto kernel scope link src 172.16.12.2
```

```
root@Spoke2-1:~# ip route
```

```
default via 172.16.2.1 dev eth0 proto st_policy
172.16.2.0/24 dev eth0 proto kernel scope link src 172.16.2.2
```

```
root@Spoke2-2:~# ip route
```

```
default via 172.16.22.1 dev eth0 proto st_policy
172.16.22.0/24 dev eth0 proto kernel scope link src 172.16.22.2
```

2.2. VRF_BLUE. На криптошлюзах Spoke1_1 и Spoke1_2 в VRF_BLUE должны находиться маршруты, добавляемые в таблицу маршрутизации, при добавлении интерфейсов Tunnel0 (mgre0) и TenGigabitEthernet0/1 (eth1) в VRF_BLUE.

```
root@Spoke1-1:~# ip route show table 10
```

```
default nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.1
local 10.10.10.1 dev mgre0 proto kernel scope host src 10.10.10.1
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
local 192.168.1.1 dev eth1 proto kernel scope host src 192.168.1.1
broadcast 192.168.1.255 dev eth1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 nhid 27 via 10.10.10.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

```
root@Spoke1-2:~# ip route show table 10
```

```
default nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.2
local 10.10.10.2 dev mgre0 proto kernel scope host src 10.10.10.2
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.2
192.168.1.0/24 nhid 27 via 10.10.10.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 dev eth1 proto kernel scope link src 192.168.2.1
local 192.168.2.1 dev eth1 proto kernel scope host src 192.168.2.1
broadcast 192.168.2.255 dev eth1 proto kernel scope link src 192.168.2.1
192.168.100.0/24 nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

2.3. VRF_RED. На криптошлюзах Spoke2_1 и Spoke2_2 в VRF_RED должны находиться маршруты, добавляемые в таблицу маршрутизации, при добавлении интерфейсов Tunnel0 (mgre0) и TenGigabitEthernet0/1 (eth1) в VRF_RED.

```
root@Spoke2-1:~# ip route show table 20
```

```
default nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.20.0/24 dev mgre0 proto kernel scope link src 10.10.20.1
```

```
local 10.10.20.1 dev mgre0 proto kernel scope host src 10.10.20.1
broadcast 10.10.20.255 dev mgre0 proto kernel scope link src 10.10.20.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
local 192.168.1.1 dev eth1 proto kernel scope host src 192.168.1.1
broadcast 192.168.1.255 dev eth1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 nhid 26 via 10.10.20.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
```

```
root@Spoke2-2:~# ip route show table 20
```

```
default nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.20.0/24 dev mgre0 proto kernel scope link src 10.10.20.2
local 10.10.20.2 dev mgre0 proto kernel scope host src 10.10.20.2
broadcast 10.10.20.255 dev mgre0 proto kernel scope link src 10.10.20.2
192.168.1.0/24 nhid 26 via 10.10.20.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 dev eth1 proto kernel scope link src 192.168.2.1
local 192.168.2.1 dev eth1 proto kernel scope host src 192.168.2.1
broadcast 192.168.2.255 dev eth1 proto kernel scope link src 192.168.2.1
192.168.100.0/24 nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
```

Проверка работы NHRP

1. Убедитесь, что на криптошлюзе Hub по протоколу NHRP зарегистрировались все Spoke-устройства. Для этого в linux bash консоли введите следующую команду:

```
root@Hub:~# opennhrpctl show dynamic
```

```
Status: ok

Interface: mgre1
Type: dynamic
Protocol-Address: 10.10.20.1/32
NBMA-Address: 172.16.2.2
Flags: up
Expires-In: 1:15

Interface: mgre1
Type: dynamic
Protocol-Address: 10.10.20.2/32
NBMA-Address: 172.16.22.2
Flags: up
Expires-In: 1:10

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.1/32
NBMA-Address: 172.16.1.2
Flags: up
Expires-In: 1:24

Interface: mgre0
Type: dynamic
Protocol-Address: 10.10.10.2/32
NBMA-Address: 172.16.12.2
Flags: up
Expires-In: 1:07

Entries found: 4
```

2. Убедитесь, что для криптошлюзов Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2 криптошлюз Hub является next-hop сервером в рамках протокола NHRP и имеет флаг up. Для этого в linux bash консоли соответствующего криптошлюза введите следующую команду:

```
root@Spoke1-1:~# opennhrpctl nhs show
```

```
Status: ok

Interface: mgre0
Type: static
Protocol-Address: 10.10.10.100/24
NBMA-Address: 172.16.100.2
Server priority: 0
Flags: used up

Entries found: 1
```

```
root@Spoke1-2:~# opennhrpctl nhs show
```

```
Status: ok

Interface: mgre0
Type: static
Protocol-Address: 10.10.10.100/24
NBMA-Address: 172.16.100.2
Server priority: 0
Flags: used up

Entries found: 1
```

```
root@Spoke2-1:~# opennhrpctl nhs show
```

```
Status: ok

Interface: mgre0
Type: static
Protocol-Address: 10.10.20.100/24
NBMA-Address: 172.16.100.2
Server priority: 0
Flags: used up

Entries found: 1
```

```
root@Spoke2-2:~# opennhrpctl nhs show
```

```
Status: ok

Interface: mgre0
Type: static
Protocol-Address: 10.10.20.100/24
NBMA-Address: 172.16.100.2
Server priority: 0
Flags: used up

Entries found: 1
```

Видно, что все Spoke-устройства успешно зарегистрировались на криптошлюзе Hub.

Проверка работы BGP

1. Убедитесь, что на Hub корректно работает протокол BGP, для этого зайдите в linux bash выполните следующие команды:

```
root@Hub:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
Hub# sh ip bgp vrf vrf_blue summary
```

```
IPv4 Unicast Summary (VRF vrf_blue):
BGP router identifier 10.10.10.100, local AS number 65000 vrf-id 8
BGP table version 3
RIB entries 5, using 960 bytes of memory
Peers 2, using 41 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down Stc
*10.10.10.1     4      65000       804       807        3    0    0 00:40:02   A
*10.10.10.2     4      65000       803       806        3    0    0 00:39:59   A

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

```
Hub# sh ip bgp vrf vrf_red summary
```

```
IPv4 Unicast Summary (VRF vrf_red):
BGP router identifier 10.10.20.100, local AS number 65000 vrf-id 9
BGP table version 3
RIB entries 5, using 960 bytes of memory
Peers 2, using 41 KiB of memory
Peer groups 1, using 64 bytes of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down Stc
*10.10.20.1     4      65000       819       822        3    0    0 00:40:48   A
*10.10.20.2     4      65000       815       818        3    0    0 00:40:36   A

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

```
Hub# show ip bgp vrf vrf_blue
```

```
BGP table version is 3, local router ID is 10.10.10.100, vrf id 8
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 192.168.1.0/24   10.10.10.1               0    100      0 i
 *>i 192.168.2.0/24   10.10.10.2               0    100      0 i
 *>  192.168.100.0/24 0.0.0.0                  0         32768 i

Displayed 3 routes and 3 total paths
```

```
Hub# show ip bgp vrf vrf_red
```

```
BGP table version is 3, local router ID is 10.10.20.100, vrf id 9
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 192.168.1.0/24   10.10.20.1               0    100      0 i
 *>i 192.168.2.0/24   10.10.20.2               0    100      0 i
```

```
 *>  192.168.100.0/24 0.0.0.0                  0         32768 i

Displayed 3 routes and 3 total paths
```

Видно, что на Hub по протоколу BGP установлено соседство с криптошлюзами Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2, и получены маршруты до всех защищаемых подсетей.

2. Убедитесь, что на Hub маршруты, полученные по протоколу BGP, добавлены в нужные таблицы маршрутизации. Для этого зайдите в linux bash выполните следующие команды:

```
root@Hub:~# ip route show table 10
```

```
default via 192.168.100.1 dev eth1 proto st_policy
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.100
local 10.10.10.100 dev mgre0 proto kernel scope host src 10.10.10.100
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.100
192.168.1.0/24 nhid 33 via 10.10.10.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 nhid 34 via 10.10.10.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 dev eth1 proto kernel scope link src 192.168.100.2
local 192.168.100.2 dev eth1 proto kernel scope host src 192.168.100.2
broadcast 192.168.100.255 dev eth1 proto kernel scope link src 192.168.100.2
```

```
root@Hub:~# ip route show table 20
```

```
default via 192.168.100.1 dev eth2 proto st_policy
unreachable default metric 4278198272
10.10.20.0/24 dev mgre1 proto kernel scope link src 10.10.20.100
local 10.10.20.100 dev mgre1 proto kernel scope host src 10.10.20.100
broadcast 10.10.20.255 dev mgre1 proto kernel scope link src 10.10.20.100
192.168.1.0/24 nhid 37 via 10.10.20.1 dev mgre1 proto bgp metric 20
192.168.2.0/24 nhid 38 via 10.10.20.2 dev mgre1 proto bgp metric 20
192.168.100.0/24 dev eth2 proto kernel scope link src 192.168.100.2
local 192.168.100.2 dev eth2 proto kernel scope host src 192.168.100.2
broadcast 192.168.100.255 dev eth2 proto kernel scope link src 192.168.100.2
```

3. Убедитесь, что на Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2 корректно работает протокол BGP. Для этого зайдите в linux bash выполните следующие команды:

```
root@Spoke1-1:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
Spoke1-1# show ip bgp vrf vrf_blue summary
```

```
IPv4 Unicast Summary:
BGP router identifier 10.10.10.1, local AS number 65000 VRF vrf_blue vrf-id 8
BGP table version 12
RIB entries 6, using 768 bytes of memory
Peers 1, using 23 KiB of memory

Neighbor      V  AS   MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down State/PfxRcd  PfxSnt Desc
10.10.10.100  4  65000   23539     23531   12    0    0 01:17:24    3   1 FRRouting/10.3.1

Total number of neighbors 1
```

```
root@Spoke1-2:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
Spoke1-2# show ip bgp vrf vrf_blue summary
```

```
IPv4 Unicast Summary:
BGP router identifier 10.10.10.2, local AS number 65000 VRF vrf_blue vrf-id 8
BGP table version 12
```

```
RIB entries 6, using 768 bytes of memory
Peers 1, using 23 KiB of memory

Neighbor      V  AS   MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.10.10.100  4 65000  23704  23696     12      0      0 01:21:19    3    1 FRRouting/10.3.1

Total number of neighbors 1
```

```
root@Spoke2-1:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
Spoke2-1# show ip bgp vrf vrf_red summary
```

```
IPv4 Unicast Summary:
BGP router identifier 10.10.20.1, local AS number 65000 VRF vrf_red vrf-id 8
BGP table version 10
RIB entries 6, using 768 bytes of memory
Peers 1, using 23 KiB of memory

Neighbor      V  AS   MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.10.20.100  4 65000  23731  23725     10      0      0 01:27:30    3    1 FRRouting/10.3.1

Total number of neighbors 1
```

```
root@Spoke2-2:~# vtysh
```

```
Hello, this is FRRouting (version 9.0.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
Spoke2-2# sh ip bgp vrf vrf_red summary
```

```
IPv4 Unicast Summary:
BGP router identifier 10.10.20.2, local AS number 65000 VRF vrf_red vrf-id 8
BGP table version 10
RIB entries 6, using 768 bytes of memory
Peers 1, using 23 KiB of memory

Neighbor      V  AS   MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
10.10.20.100  4 65000  23944  23938     10      0      0 01:30:16    3    1 FRRouting/10.3.1

Total number of neighbors 1
```

```
Spoke1-1# show ip bgp vrf vrf_blue
```

```
BGP table version is 12, local router ID is 10.10.10.1, vrf id 8
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0/0        10.10.10.100             0    100      0 i
 *>  192.168.1.0/24   0.0.0.0                  0         32768 i
 *>i 192.168.2.0/24   10.10.10.2               0    100      0 i
 *>i 192.168.100.0/24 10.10.10.100             0    100      0 i

Displayed 4 routes and 4 total paths
```

```
Spoke1-2# show ip bgp vrf vrf_blue
```

```
BGP table version is 12, local router ID is 10.10.10.2, vrf id 8
```

```
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0/0        10.10.10.100             0    100      0 i
 *>i 192.168.1.0/24   10.10.10.1               0    100      0 i
 *>  192.168.2.0/24   0.0.0.0                  0         32768 i
 *>i 192.168.100.0/24 10.10.10.100             0    100      0 i

Displayed 4 routes and 4 total paths
```

```
Spoke2-1# show ip bgp vrf vrf_red
```

```
BGP table version is 10, local router ID is 10.10.20.1, vrf id 5
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0/0        10.10.20.100             0    100      0 i
 *>  192.168.1.0/24   0.0.0.0                  0         32768 i
 *>i 192.168.2.0/24   10.10.20.2               0    100      0 i
 *>i 192.168.100.0/24 10.10.20.100             0    100      0 i

Displayed 4 routes and 4 total paths
```

```
Spoke2-2# sh ip bgp vrf vrf_red
```

```
BGP table version is 10, local router ID is 10.10.20.2, vrf id 5
Default local pref 100, local AS 65000
Status codes:  s suppressed, d damped, h history, u unsorted, * valid, > best, =
multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0/0        10.10.20.100             0    100      0 i
 *>i 192.168.1.0/24   10.10.20.1               0    100      0 i
 *>  192.168.2.0/24   0.0.0.0                  0         32768 i
 *>i 192.168.100.0/24 10.10.20.100             0    100      0 i

Displayed 4 routes and 4 total paths
```

Видно, что на криптошлюзах Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2 по протоколу BGP установлено соседство с Hub и получены все необходимые маршруты.

4. Убедитесь, что на Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2 маршруты, полученные по протоколу BGP добавлены в нужные таблицы маршрутизации, для этого зайдите в linux bash консоль соответствующего криптошлюза и выполните следующие команды:

```
root@Spoke1-1:~# ip route show table 10
```

```
default nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

```
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.1
local 10.10.10.1 dev mgre0 proto kernel scope host src 10.10.10.1
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
local 192.168.1.1 dev eth1 proto kernel scope host src 192.168.1.1
broadcast 192.168.1.255 dev eth1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 nhid 27 via 10.10.10.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

```
root@Spoke1-2:~# ip route show table 10
```

```
default nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.10.0/24 dev mgre0 proto kernel scope link src 10.10.10.2
local 10.10.10.2 dev mgre0 proto kernel scope host src 10.10.10.2
broadcast 10.10.10.255 dev mgre0 proto kernel scope link src 10.10.10.2
192.168.1.0/24 nhid 27 via 10.10.10.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 dev eth1 proto kernel scope link src 192.168.2.1
local 192.168.2.1 dev eth1 proto kernel scope host src 192.168.2.1
broadcast 192.168.2.255 dev eth1 proto kernel scope link src 192.168.2.1
192.168.100.0/24 nhid 25 via 10.10.10.100 dev mgre0 proto bgp metric 20
```

```
root@Spoke2-1:~# ip route show table 20
```

```
default nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.20.0/24 dev mgre0 proto kernel scope link src 10.10.20.1
local 10.10.20.1 dev mgre0 proto kernel scope host src 10.10.20.1
broadcast 10.10.20.255 dev mgre0 proto kernel scope link src 10.10.20.1
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.1
local 192.168.1.1 dev eth1 proto kernel scope host src 192.168.1.1
broadcast 192.168.1.255 dev eth1 proto kernel scope link src 192.168.1.1
192.168.2.0/24 nhid 26 via 10.10.20.2 dev mgre0 proto bgp metric 20
192.168.100.0/24 nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
```

```
root@Spoke2-2:~# ip route show table 20
```

```
default nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
unreachable default metric 4278198272
10.10.20.0/24 dev mgre0 proto kernel scope link src 10.10.20.2
local 10.10.20.2 dev mgre0 proto kernel scope host src 10.10.20.2
broadcast 10.10.20.255 dev mgre0 proto kernel scope link src 10.10.20.2
192.168.1.0/24 nhid 26 via 10.10.20.1 dev mgre0 proto bgp metric 20
192.168.2.0/24 dev eth1 proto kernel scope link src 192.168.2.1
local 192.168.2.1 dev eth1 proto kernel scope host src 192.168.2.1
broadcast 192.168.2.255 dev eth1 proto kernel scope link src 192.168.2.1
192.168.100.0/24 nhid 24 via 10.10.20.100 dev mgre0 proto bgp metric 20
```

Проверка построения защищенного соединения

1. Убедитесь, что между Hub и Spoke1_1, Spoke1_2, Spoke2_1, Spoke2_2 установлено защищенное соединение:

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

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (172.16.100.2,500)-(172.16.2.2,500) active 1912 1960
2 2 (172.16.100.2,500)-(172.16.12.2,500) active 1912 1960
3 3 (172.16.100.2,500)-(172.16.1.2,500) active 1888 1936
4 4 (172.16.100.2,500)-(172.16.22.2,500) active 1912 1960
```

```
IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (172.16.100.2,*)-(172.16.2.2,*) 47 ESP trans 2164 1904
2 2 (172.16.100.2,*)-(172.16.12.2,*) 47 ESP trans 2164 1832
3 3 (172.16.100.2,*)-(172.16.1.2,*) 47 ESP trans 2448 2312
4 4 (172.16.100.2,*)-(172.16.22.2,*) 47 ESP trans 1804 1472
```

```
root@Spoke1-1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 33 (172.16.1.2,500)-(172.16.100.2,500) active 19676 16352

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 46 (172.16.1.2,*)-(172.16.100.2,*) 47 ESP trans 45084 67452
```

```
root@Spoke1-2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 98 (172.16.12.2,500)-(172.16.100.2,500) active 12564 10648

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (172.16.12.2,*)-(172.16.100.2,*) 47 ESP trans 1124 1912
```

```
root@Spoke2-1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 110 (172.16.2.2,500)-(172.16.100.2,500) active 1896 1932

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 33 (172.16.2.2,*)-(172.16.100.2,*) 47 ESP trans 8424 8076
```

```
root@Spoke2-2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 84 (172.16.22.2,500)-(172.16.100.2,500) active 6576 7704

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 44 (172.16.22.2,*)-(172.16.100.2,*) 47 ESP trans 64948 79240
```

Проверка доступности Интернета для устройств из защищаемых подсетей

1. Убедитесь, что устройства Host-b-hub-vrf-blue, Host-b-hub-vrf-red, Host-b-spoke1_1-vrf-blue, Host-b-spoke1_2-vrf-blue, Host-b-spoke2_1-vrf-red и Host-b-spoke2_2-vrf-red имеют доступ в Интернет через криптошлюз Hub. Для этого выполните команду `ping` из консоли защищаемых устройств и параллельно запустите `tcpdump` с указанными параметрами на криптошлюзе Hub:

```
root@Host-b-hub-vrf-blue:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=63 time=0.673 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=63 time=0.701 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=63 time=0.634 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=63 time=0.533 ms
64 bytes from 172.10.0.1: icmp_seq=5 ttl=63 time=0.719 ms

--- 172.10.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.533/0.652/0.719/0.066 ms
```

```
root@Hub:~# tcpdump -i eth1 -p icmp -Q in
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:29:17.734661 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 7586, seq 1, length 64
15:29:17.747974 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 7586, seq 1, length 64
15:29:18.750019 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 7842, seq 2, length 64
15:29:18.752836 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 7842, seq 2, length 64
15:29:19.754678 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 8098, seq 3, length 64
15:29:19.758868 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 8098, seq 3, length 64
15:29:20.761161 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 8354, seq 4, length 64
15:29:20.764658 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 8354, seq 4, length 64
15:29:21.766785 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 8610, seq 5, length 64
15:29:21.770440 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 8610, seq 5, length 64
...
```

```
root@Host-b-hub-vrf-red:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=63 time=0.782 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=63 time=0.653 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=63 time=0.969 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=63 time=0.522 ms
64 bytes from 172.10.0.1: icmp_seq=5 ttl=63 time=0.672 ms

--- 172.10.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.522/0.719/0.969/0.149 ms
```

```
root@Hub:~# tcpdump -i eth2 -p icmp -Q in
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:33:45.713908 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 10659, seq 1, length 64
15:33:45.717362 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 10659, seq 1, length 64
15:33:46.719292 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 10915, seq 2, length 64
15:33:46.721786 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 10915, seq 2, length 64
15:33:47.723819 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 11171, seq 3, length 64
15:33:47.726602 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 11171, seq 3, length 64
15:33:48.728178 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 11427, seq 4, length 64
15:33:48.731294 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 11427, seq 4, length 64
15:33:49.733016 IP 192.168.100.100 > 172.10.0.1: ICMP echo request, id 11683, seq 5, length 64
15:33:49.735978 IP 172.10.0.1 > 192.168.100.100: ICMP echo reply, id 11683, seq 5, length 64
...
```

```
root@Host-b-spoke1_1-vrf-blue:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=63 time=0.684 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=63 time=0.949 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=63 time=0.637 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=63 time=0.612 ms
```

```
64 bytes from 172.10.0.1: icmp_seq=5 ttl=63 time=0.634 ms
^C
--- 172.10.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.612/0.703/0.949/0.125 ms
```

```
root@Hub:~# tcpdump -i eth1 -p icmp
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:13:44.989072 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 30878, seq 1, length 64
15:13:44.994130 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 30878, seq 1, length 64
15:13:46.000459 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 31134, seq 2, length 64
15:13:46.003320 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 31134, seq 2, length 64
15:13:47.007121 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 31390, seq 3, length 64
15:13:47.009516 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 31390, seq 3, length 64
15:13:48.014431 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 31646, seq 4, length 64
15:13:48.017031 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 31646, seq 4, length 64
15:13:49.020176 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 31902, seq 5, length 64
15:13:49.023412 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 31902, seq 5, length 64
...
```

```
root@Host-b-spoke1_2-vrf-blue:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=63 time=0.679 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=63 time=0.618 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=63 time=0.620 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=63 time=0.599 ms
64 bytes from 172.10.0.1: icmp_seq=5 ttl=63 time=0.735 ms
^C
--- 172.10.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.599/0.650/0.735/0.050 ms
```

```
root@Hub:~# tcpdump -i eth1 -p icmp
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:35:30.849115 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 37539, seq 1, length 64
15:35:30.853011 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 37539, seq 1, length 64
15:35:31.855979 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 37795, seq 2, length 64
15:35:31.858011 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 37795, seq 2, length 64
15:35:32.861624 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 38051, seq 3, length 64
15:35:32.864534 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 38051, seq 3, length 64
15:35:33.868617 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 38307, seq 4, length 64
15:35:33.871316 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 38307, seq 4, length 64
15:35:34.874864 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 38563, seq 5, length 64
15:35:34.877021 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 38563, seq 5, length 64
...
```

```
root@Host-b-spoke2_1-vrf-red:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=61 time=1.64 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=61 time=1.64 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=61 time=1.81 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=61 time=1.78 ms
64 bytes from 172.10.0.1: icmp_seq=5 ttl=61 time=1.94 ms

--- 172.10.0.1 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.635/1.758/1.938/0.113 ms
```

```
root@Hub:~# tcpdump -i eth2 -p icmp
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:36:51.802158 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 58275, seq 1, length 64
15:36:51.804850 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 58275, seq 1, length 64
15:36:52.808130 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 58531, seq 2, length 64
15:36:52.810294 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 58531, seq 2, length 64
15:36:53.814521 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 58787, seq 3, length 64
15:36:53.816805 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 58787, seq 3, length 64
15:36:54.819836 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 59043, seq 4, length 64
15:36:54.822257 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 59043, seq 4, length 64
15:36:55.826000 IP 192.168.1.100 > 172.10.0.1: ICMP echo request, id 59299, seq 5, length 64
15:36:55.828343 IP 172.10.0.1 > 192.168.1.100: ICMP echo reply, id 59299, seq 5, length 64
...
```

```
root@Host-b-spoke2_2-vrf-red:~# ping 172.10.0.1
```

```
PING 172.10.0.1 (172.10.0.1) 56(84) bytes of data.
64 bytes from 172.10.0.1: icmp_seq=1 ttl=61 time=1.42 ms
64 bytes from 172.10.0.1: icmp_seq=2 ttl=61 time=1.69 ms
64 bytes from 172.10.0.1: icmp_seq=3 ttl=61 time=1.75 ms
64 bytes from 172.10.0.1: icmp_seq=4 ttl=61 time=1.63 ms
64 bytes from 172.10.0.1: icmp_seq=5 ttl=61 time=1.66 ms

--- 172.10.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.421/1.629/1.750/0.111 ms
```

```
root@Hub:~# tcpdump -i eth2 -p icmp
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:37:38.547926 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 4772, seq 1, length 64
15:37:38.550486 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 4772, seq 1, length 64
15:37:39.553606 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 5028, seq 2, length 64
15:37:39.556686 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 5028, seq 2, length 64
15:37:40.560495 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 5284, seq 3, length 64
15:37:40.562612 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 5284, seq 3, length 64
15:37:41.565968 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 5540, seq 4, length 64
15:37:41.569141 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 5540, seq 4, length 64
15:37:42.573058 IP 192.168.2.100 > 172.10.0.1: ICMP echo request, id 5796, seq 5, length 64
15:37:42.575644 IP 172.10.0.1 > 192.168.2.100: ICMP echo reply, id 5796, seq 5, length 64
...
```

Видно, что все устройства из защищаемых подсетей имеют выход в Интернет через криптошлюз Hub.

После построения Spoke-to-Spoke туннелей

Инициируйте построение spoke-to-spoke туннелей между криптошлюзами Spoke1_1 и Spoke1_2, а также между криптошлюзами Spoke2_1 и Spoke2_2 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke1_1-vrf-blue на Host-b-spoke1_2-vrf-blue (можно и наоборот) и с устройства Host-b-spoke2_1-vrf-red на Host-b-spoke2_2-vrf-red соответственно. Для этого выполните команду `ping` из консоли защищаемых устройств Host-b-spoke1_1-vrf-blue и Host-b-spoke2_1-vrf-red.

Проверка PKI

1. Убедитесь, что после установления Spoke-to-Spoke туннеля все Spoke-устройства получили сертификаты своих соседей. А также, что статус всех сертификатов Active.

```
root@Spoke1-1:~# cert_mgr show
```

```
Found 4 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
```

```
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
4 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
5 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke1-1:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

```
root@Spoke1-2:~# cert_mgr show
```

```
Found 4 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
4 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
5 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke1-2:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_2
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1_1
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
```

```
root@Spoke2-1:~# cert_mgr show
```

```
Found 4 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
5 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke2-1:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
```

```
root@Spoke2-2:~# cert_mgr show
```

```
Found 4 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 Status: remote  C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
5 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
root@Spoke2-2:~# cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_2
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root
CA
3 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub
4 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2_1
```

Проверка работы NHRP

1. Убедитесь, что на криптошлюзах Spoke1_1, Spoke1_2, Spoke2_1 и Spoke2_2, по протоколу NHRP, произошло разрешение NBMA-адресов соответствующих криптошлюзов. Для этого в linux bash консоли введите следующую команду:

```
root@Spoke1-1:~# opennhrpctl show cached
```

```
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.10.2/32
NBMA-Address: 172.16.12.2
Flags: used up
Expires-In: 1:03

Entries found: 1
```

```
root@Spoke1-2:~# opennhrpctl show cached
```

```
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.10.1/32
NBMA-Address: 172.16.1.2
Flags: up
Expires-In: 0:31

Entries found: 1
```

```
root@Spoke2-1:~# opennhrpctl show cached
```

```
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.20.2/32
NBMA-Address: 172.16.22.2
Flags: used up
Expires-In: 1:03

Entries found: 1
```

```
root@Spoke2-2:~# opennhrpctl show cached
```

```
Status: ok

Interface: mgre0
Type: cached
Protocol-Address: 10.10.20.1/32
NBMA-Address: 172.16.2.2
Flags: up
Expires-In: 0:41

Entries found: 1
```

Проверка построения защищенного соединения

1. Убедитесь, что защищенные соединения между криптошлюзами Spoke1_1 и Spoke1_2, а также между криптошлюзами Spoke2_1 и Spoke2_2 успешно построились. Для этого введите следующую команду из linux bash консоли соответствующего криптошлюза:

```
root@Spoke1-1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 33 (172.16.1.2,500)-(172.16.100.2,500) active 20120 16712
2 34 (172.16.1.2,500)-(172.16.12.2,500) active 1936 1904

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 47 (172.16.1.2,*)-(172.16.100.2,*) 47 ESP trans 60308 54540
2 48 (172.16.1.2,*)-(172.16.12.2,*) 47 ESP trans 288 288
```

```
root@Spoke1-2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 99 (172.16.12.2,500)-(172.16.1.2,500) active 1904 1936
2 100 (172.16.12.2,500)-(172.16.100.2,500) active 1504 1520

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 32 (172.16.12.2,*)-(172.16.100.2,*) 47 ESP trans 54144 91488
2 33 (172.16.12.2,*)-(172.16.1.2,*) 47 ESP trans 288 288
```

```
root@Spoke2-1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 110 (172.16.2.2,500)-(172.16.100.2,500) active 1896 1932
2 111 (172.16.2.2,500)-(172.16.22.2,500) active 1960 1928

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 33 (172.16.2.2,*)-(172.16.100.2,*) 47 ESP trans 96868 86440
2 34 (172.16.2.2,*)-(172.16.22.2,*) 47 ESP trans 288 288
```

```
root@Spoke2-2:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 84 (172.16.22.2,500)-(172.16.100.2,500) active 6936 8148
2 85 (172.16.22.2,500)-(172.16.2.2,500) active 1928 1960

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 45 (172.16.22.2,*)-(172.16.100.2,*) 47 ESP trans 46776 72380
2 46 (172.16.22.2,*)-(172.16.2.2,*) 47 ESP trans 288 288
```

2. Убидитесь, что пользовательский трафик, между криптошлюзами Spoke1_1 и Spoke1_2, а также между криптошлюзами Spoke2_1 и Spoke2_2, идет напрямую, а не через Hub. Для этого на устройствах Host-b-spoke1_1-vrf-blue и Host-b-spoke2_1-vrf-red запустите команду `traceroute` до устройств Host-b-spoke1_2-vrf-blue и Host-b-spoke2_2-vrf-blue соответственно:

```
root@Host-b-spoke1_1-vrf-blue:~# traceroute 192.168.2.100
```

```
traceroute to 192.168.2.100 (192.168.2.100), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.356 ms  0.284 ms  0.280 ms
```

```
 2  10.10.10.2 (10.10.10.2)  1.415 ms  1.344 ms  1.329 ms
 3  192.168.2.100 (192.168.2.100)  1.354 ms  1.370 ms  1.359 ms
```

```
root@Host-b-spoke2_1-vrf-red:~# traceroute 192.168.2.100
```

```
traceroute to 192.168.2.100 (192.168.2.100), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.534 ms  0.477 ms  0.458 ms
 2  10.10.20.2 (10.10.20.2)  1.887 ms  1.884 ms  1.895 ms
 3  192.168.2.100 (192.168.2.100)  2.186 ms  2.171 ms  2.165 ms
```

Видно, что пользовательский трафик, между криптошлюзами Spoke1_1 и Spoke1_2, а также между криптошлюзами Spoke2_1 и Spoke2_2, идет напрямую.

Приложение

Конфигурации криптошлюза Hub

1. Консоль cisco-like:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 csp
aaa new-model
!
hostname Hub
enable password csp
!
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 network PRIVATE
 description private LANs
 172.16.0.0 255.240.0.0
 192.168.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
!
object-group network SELF
 host 172.16.100.2
!
ip access-list extended IPSEC_DMVPN
 remark special DMVPN filter
 permit gre object-group SELF each
!
ip access-list extended FIREWALL_IN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FIREWALL_OUT
 permit ip object-group SELF object-group PRIVATE
 deny   ip any object-group PRIVATE
```

```
 deny   gre any any
 permit ip any any
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_DMVPN
 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 1 ipsec-isakmp dynamic DMAP
!
interface TenGigabitEthernet0/0
 ip address 172.16.100.2 255.255.255.0
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 crypto map VPN
 ip inspect INSPECT out
!
interface TenGigabitEthernet0/1
 description interface is included in VRF_BLUE
 ip address 192.168.100.2 255.255.255.0
!
interface TenGigabitEthernet0/2
 description interface is included in VRF_RED
 ip address 192.168.100.2 255.255.255.0
!
interface TenGigabitEthernet0/3
 no ip address
 shutdown
!
interface Tunnel0
 ip address 10.10.10.100 255.255.255.0
 mtu 1400
 tunnel mode gre multipoint
 tunnel key 1
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit
!
interface Tunnel1
 ip address 10.10.20.100 255.255.255.0
 mtu 1400
 tunnel mode gre multipoint
 tunnel key 2
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit
```

```
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route 0.0.0.0 0.0.0.0 192.168.100.1 table 10
ip route 0.0.0.0 0.0.0.0 192.168.100.1 table 20
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Feb  6 13:38:09 2026

GlobalParameters(
    Title                          = "This LSP was automatically generated by CSP
Converter at Fri Feb  6 13:38:09 2026 (user: cscons)"
    Version                    = LSP_5_0
    CRLHandlingMode            = ENABLE
    PreserveIPsecSA            = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.100.1
        ),
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.1
            Table = 10
        ),
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.1
            Table = 20
        )
)

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

```
    TCPSessionRateLow = 400
    TCPSessionRateMax = 500
    TCPSessionsMax = 256000
    TCPStrictnessLevel = 3
    UDPNotEstablishedTimeout = 30
    UDPEstablishedTimeout = 120
    UDPSessionsMax = 65536
)

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

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

FilterChain FilterChain:FIREWALL_IN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.100.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
```

```
        ProtocolID = 1
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        SourceIP = 172.16.100.2
        DestinationIP = 172.16.0.0/12
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.100.2
        DestinationIP = 192.168.0.0/16
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.100.2
        DestinationIP = 10.0.0.0/8
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.100.2
        DestinationIP = 100.64.0.0/10
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.0.0/12
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 192.168.0.0/16
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 10.0.0.0/8
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 100.64.0.0/10
```

```
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 47
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    ),
    Filter (
        Label = "INSPECT"
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain IPv6Default (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
```

```
        Action = PASS
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))

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

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

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    MainModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 3
    DPDRetries          = 3
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1:DMAP:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.100.2
        ProtocolID = 47
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_DMVPN"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
```

```
    InputFilter = FilterChain:FIREWALL_IN
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "Tunnel0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "Tunnel1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

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

interface mgre1
 multicast dynamic
 holding-time 90
 cisco-authentication secret
```

4. Содержимое файла `/etc/frr/frr.conf`:

```
frr version 9.0.4
frr defaults traditional
hostname Hub
log syslog informational
service integrated-vtysh-config
!
router bgp 65000 vrf vrf_blue
 bgp router-id 10.10.10.100
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor spokes-ibgp_cloud1 peer-group
 neighbor spokes-ibgp_cloud1 remote-as 65000
 bgp listen limit 5000
 bgp listen range 10.10.10.0/24 peer-group spokes-ibgp_cloud1
 !
 address-family ipv4 unicast
  network 192.168.100.0/24
  neighbor spokes-ibgp_cloud1 default-originate
  neighbor spokes-ibgp_cloud1 route-reflector-client
```

```
 exit-address-family
exit
!
router bgp 65000 vrf vrf_red
 bgp router-id 10.10.20.100
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor spokes-ibgp_cloud2 peer-group
 neighbor spokes-ibgp_cloud2 remote-as 65000
 bgp listen limit 5000
 bgp listen range 10.10.20.0/24 peer-group spokes-ibgp_cloud2
 !
 address-family ipv4 unicast
  network 192.168.100.0/24
  neighbor spokes-ibgp_cloud2 default-originate
  neighbor spokes-ibgp_cloud2 route-reflector-client
 exit-address-family
exit
!
end
```

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

```
auto vrf_blue
iface vrf_blue inet manual
pre-up ip link del vrf_blue type vrf 2>/dev/null || true
pre-up ip route flush table 10 2>/dev/null || true
pre-up ip link add vrf_blue type vrf table 10
pre-up ip link set dev vrf_blue up
pre-up ip route add table 10 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_blue
pre-up ip link set dev mgre0 master vrf_blue 2>/dev/null || true
post-down ip link set dev vrf_blue down

auto vrf_red
iface vrf_red inet manual
pre-up ip link del vrf_red type vrf 2>/dev/null || true
pre-up ip route flush table 20 2>/dev/null || true
pre-up ip link add vrf_red type vrf table 20
pre-up ip link set dev vrf_red up
pre-up ip route add table 20 unreachable default metric 4278198272
pre-up ip link set dev eth2 master vrf_red
pre-up ip link set dev mgre1 master vrf_red 2>/dev/null || true
post-down ip link set dev vrf_red down

auto mgre0
iface mgre0 inet static
address 10.10.10.100
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_blue || true
post-down ip link del mgre0

auto mgre1
iface mgre1 inet static
address 10.10.20.100
netmask 255.255.255.0
```

```
pre-up ip tunnel add mgre1 mode gre key 2 ttl 64 tos inherit
pre-up ip link set mgre1 type gre nopmtudisc
pre-up ip link set mgre1 type gre ignore-df
pre-up ip link set mgre1 mtu 1400
pre-up ip link set mgre1 multicast on
pre-up ip link set dev mgre1 master vrf_red || true
post-down ip link del mgre1
```

6. Содержимое файла `/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="Tunnel1" pattern="mgre1")
interface (name="default" pattern="*")
```

Конфигурации криптошлюза Spoke1_1

1. Консоль cisco-like:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname Spoke1-1
enable password csp
!
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 network SELF
 description IP on WAN interface
 host 172.16.1.2
!
object-group network PRIVATE
 description private LANs
 172.16.0.0 255.240.0.0
 192.168.0.0 255.255.0.0
```

```
 10.0.0.0 255.0.0.0
!
ip access-list extended IPSEC_DMVPN
 remark special DMVPN filter
 permit gre object-group SELF each
!
ip access-list extended FIREWALL_IN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FIREWALL_OUT
 permit ip object-group SELF object-group PRIVATE
 deny   ip any object-group PRIVATE
 deny   gre any any
 permit ip any any
!
ipv6 default filtering deny
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_DMVPN
 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 1 ipsec-isakmp dynamic DMAP
!
interface TenGigabitEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 crypto map VPN
 ip inspect INSPECT out
!
interface TenGigabitEthernet0/1
 description interface is included in VRF_BLUE
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 10.10.10.1 255.255.255.0
 mtu 1400
 tunnel mode gre multipoint
 tunnel key 1
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit
!
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
!
```

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

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Feb  6 15:29:31 2026

GlobalParameters(
    Title                          = "This LSP was automatically generated by CSP
Converter at Fri Feb  6 15:29:31 2026 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

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

)

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

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

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

FilterChain FilterChain:FIREWALL_IN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))

FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        SourceIP = 172.16.1.2
        DestinationIP = 172.16.0.0/12
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.1.2
```

```
        DestinationIP = 192.168.0.0/16
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.1.2
        DestinationIP = 10.0.0.0/8
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.0.0/12
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 192.168.0.0/16
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 10.0.0.0/8
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 47
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    ),
    Filter (
        Label = "INSPECT"
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
```

```
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

IKEParameters(
    FragmentSize = 0
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
    ResponderSessionsMax = 100
)

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

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    MainModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 3
    DPDRetries          = 3
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
```

```
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1:DMAP:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.1.2
        ProtocolID = 47
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_DMVPN"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "Tunnel0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

```
interface mgre0
 map 10.10.10.100/24 172.16.100.2 register
 multicast nhs
 holding-time 90
 cisco-authentication secret
```

4. Содержимое файла `/etc/frr/frr.conf`:

```
frr version 9.0.4
frr defaults traditional
hostname Spoke1-1
log syslog informational
service integrated-vtysh-config
!
router bgp 65000 vrf vrf_blue
 bgp router-id 10.10.10.1
 bgp log-neighbor-changes
 timers bgp 3 9
```

```
 neighbor 10.10.10.100 remote-as 65000
 neighbor 10.10.10.100 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.1.0/24
 exit-address-family
exit
!
end
```

5. Содержимое файла `/etc/network/interfaces.d/interface`:

```
auto vrf_blue
iface vrf_blue inet manual
pre-up ip link del vrf_blue type vrf 2>/dev/null || true
pre-up ip route flush table 10 2>/dev/null || true
pre-up ip link add vrf_blue type vrf table 10
pre-up ip link set dev vrf_blue up
pre-up ip route add table 10 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_blue
pre-up ip link set dev mgre0 master vrf_blue 2>/dev/null || true
post-down ip link set dev vrf_blue down

auto mgre0
iface mgre0 inet static
address 10.10.10.1
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_blue || true
post-down ip link del mgre0
```

6. Содержимое файла `/etc/ifaliases.cf`:

```
interface (name="GigabitEthernet0/0" pattern="eth0")
interface (name="GigabitEthernet0/1" pattern="eth1")
interface (name="Tunnel0" pattern="mgre0")
interface (name="default" pattern="*")
```

Конфигурации криптошлюза Spoke1_2

1. Консоль cisco-like

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 csp
aaa new-model
!
!
```

```
hostname Spoke1-2
enable password csp
!
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 network SELF
 description IP on WAN interface
 host 172.16.12.2
!
object-group network PRIVATE
 description private LANs
 172.16.0.0 255.240.0.0
 192.168.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
!
ip access-list extended IPSEC_DMVPN
 remark special DMVPN filter
 permit gre object-group SELF each
!
ip access-list extended FIREWALL_IN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FIREWALL_OUT
 permit ip object-group SELF object-group PRIVATE
 deny   ip any object-group PRIVATE
 deny   gre any any
 permit ip any any
!
ipv6 default filtering deny
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_DMVPN
 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 1 ipsec-isakmp dynamic DMAP
!
interface TenGigabitEthernet0/0
```

```
 ip address 172.16.12.2 255.255.255.0
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 crypto map VPN
 ip inspect INSPECT out
!
interface TenGigabitEthernet0/1
 description interface is included in VRF_BLUE
 ip address 192.168.2.1 255.255.255.0
!
interface Tunnel0
 ip address 10.10.10.2 255.255.255.0
 mtu 1400
 tunnel mode gre multipoint
 tunnel key 1
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit!
!
ip route 0.0.0.0 0.0.0.0 172.16.12.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Feb  6 15:30:48 2026

GlobalParameters(
    Title                           = "This LSP was automatically generated by CSP
Converter at Fri Feb  6 15:30:48 2026 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.12.1
        )

)

FirewallParameters(
```

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

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

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

FilterChain FilterChain:FIREWALL_IN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.12.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.12.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.12.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.12.2
```

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

FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        SourceIP = 172.16.12.2
        DestinationIP = 172.16.0.0/12
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.12.2
        DestinationIP = 192.168.0.0/16
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.12.2
        DestinationIP = 10.0.0.0/8
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.0.0/12
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 192.168.0.0/16
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 10.0.0.0/8
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 47
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
```

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

IdentityEntry Remote:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

IKEParameters(
    FragmentSize = 576
    SALifetimeDelta = 50
    InitiatorSessionsMax = 100
```

```
    ResponderSessionsMax = 100
)

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

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    MainModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 3
    DPDRetries          = 3
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1:DMAP:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.12.2
        ProtocolID = 47
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_DMVPN"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
```

```
    LogicalName = "Tunnel0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

```
interface mgre0
  map 10.10.10.100/24 172.16.100.2 register
  multicast nhs
  holding-time 90
  cisco-authentication secret
```

4. Содержимое файла `/etc/frr/frr.conf`:

```
frr version 9.0.4
frr defaults traditional
hostname sterragate
log syslog informational
hostname Spoke1-2
service integrated-vtysh-config
!
router bgp 65000 vrf vrf_blue
 bgp router-id 10.10.10.2
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor 10.10.10.100 remote-as 65000
 neighbor 10.10.10.100 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.2.0/24
 exit-address-family
exit
!
end
```

5. Содержимое файла `/etc/network/interfaces.s/interfaces`:

```
auto vrf_blue
iface vrf_blue inet manual
pre-up ip link del vrf_blue type vrf 2>/dev/null || true
pre-up ip route flush table 10 2>/dev/null || true
pre-up ip link add vrf_blue type vrf table 10
pre-up ip link set dev vrf_blue up
pre-up ip route add table 10 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_blue
pre-up ip link set dev mgre0 master vrf_blue 2>/dev/null || true
post-down ip link set dev vrf_blue down

auto mgre0
iface mgre0 inet static
address 10.10.10.2
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 1 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_blue || true
post-down ip link del mgre0
```

6. Содержимое файла `/etc/ifaliases.cf`:

```
interface (name="TenGigabitEthernet0/0" pattern="eth0")
```

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

Конфигурации криптошлюза Spoke2_1

1. Консоль cisco-like:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname Spoke2-1
enable password csp
!
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 network SELF
 description IP on WAN interface
 host 172.16.2.2
!
object-group network PRIVATE
 description private LANs
 172.16.0.0 255.240.0.0
 192.168.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
!
ip access-list extended IPSEC_DMVPN
 remark special DMVPN filter
 permit gre object-group SELF each
!
ip access-list extended FIREWALL_IN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
```

```
ip access-list extended FIREWALL_OUT
 permit ip object-group SELF object-group PRIVATE
 deny   ip any object-group PRIVATE
 deny   gre any any
 permit ip any any
!
ipv6 default filtering deny
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_DMVPN
 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 1 ipsec-isakmp dynamic DMAP
!
interface TenGigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.0
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 crypto map VPN
 ip inspect INSPECT out
!
interface TenGigabitEthernet0/1
 description interface is included in VRF_RED
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 10.10.20.1 255.255.255.0
 mtu 1400
 tunnel mode gre multipoint
 tunnel key 2
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit!
!
ip route 0.0.0.0 0.0.0.0 172.16.2.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Feb  6 15:31:49 2026

GlobalParameters(
    Title                          = "This LSP was automatically generated by CSP
Converter at Fri Feb  6 15:31:49 2026 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

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

)

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

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

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

FilterChain FilterChain:FIREWALL_IN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
```

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

FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        SourceIP = 172.16.2.2
        DestinationIP = 172.16.0.0/12
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.2.2
        DestinationIP = 192.168.0.0/16
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.2.2
        DestinationIP = 10.0.0.0/8
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.0.0/12
```

```
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 192.168.0.0/16
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 10.0.0.0/8
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 47
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    ),
    Filter (
        Label = "INSPECT"
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
        Action = PASS
        ExtendedAction = inspect_tcp<>
        LogEventID = "Inspect:INSPECT:tcp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 17
        Action = PASS
        ExtendedAction = inspect_udp<>
        LogEventID = "Inspect:INSPECT:udp"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = PASS
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))
```

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

IdentityEntry Local:Cert:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

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

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    MainModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 3
    DPDRetries          = 3
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1:DMAP:1
)

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

```
    ),
    Filter (
        SourceIP = 172.16.2.2
        ProtocolID = 47
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_DMVPN"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "Tunnel0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

```
interface mgre0
  map 10.10.20.100/24 172.16.100.2 register
  multicast nhs
  holding-time 90
  cisco-authentication secret
```

4. Содержимое файла `/etc/frr/frr.conf`:

```
frr version 9.0.4
frr defaults traditional
hostname Spoke2-1
log syslog informational
service integrated-vtysh-config
!
router bgp 65000 vrf vrf_red
 bgp router-id 10.10.20.1
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor 10.10.20.100 remote-as 65000
 neighbor 10.10.20.100 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.1.0/24
  neighbor 10.10.20.100 next-hop-self force
 exit-address-family
exit
!
end
```

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

```
auto vrf_red
```

```
iface vrf_red inet manual
pre-up ip link del vrf_red type vrf 2>/dev/null || true
pre-up ip route flush table 20 2>/dev/null || true
pre-up ip link add vrf_red type vrf table 20
pre-up ip link set dev vrf_red up
pre-up ip route add table 20 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_red
pre-up ip link set dev mgre0 master vrf_red 2>/dev/null || true
post-down ip link set dev vrf_red down

auto mgre0
iface mgre0 inet static
address 10.10.20.1
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 2 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_red || true
post-down ip link del mgre0
```

6. Содержимое файла `/etc/ifaliases.cf`:

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

Конфигурации криптошлюза Spoke2_2

1. Консоль cisco-like:

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname Spoke2-2
enable password csp
!
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 network SELF
 description IP on WAN interface
 host 172.16.22.2
!
object-group network PRIVATE
 description private LANs
 172.16.0.0 255.240.0.0
 192.168.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
!
ip access-list extended IPSEC_DMVPN
 remark special DMVPN filter
 permit gre object-group SELF each
!
ip access-list extended FIREWALL_IN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FIREWALL_OUT
 permit ip object-group SELF object-group PRIVATE
 deny   ip any object-group PRIVATE
 deny   gre any any
 permit ip any any
!
ipv6 default filtering deny
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_DMVPN
 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 1 ipsec-isakmp dynamic DMAP
!
interface TenGigabitEthernet0/0
 ip address 172.16.22.2 255.255.255.0
 ip access-group FIREWALL_IN in
 ip access-group FIREWALL_OUT out
 crypto map VPN
 ip inspect INSPECT out
!
interface TenGigabitEthernet0/1
 description interface is included in VRF_RED
 ip address 192.168.2.1 255.255.255.0
!
interface Tunnel0
 ip address 10.10.20.2 255.255.255.0
 mtu 1400
```

```
 tunnel mode gre multipoint
 tunnel key 2
 offloading tx-checksumming
 no tunnel path-mtu-discovery
 tunnel ignore-df
 tunnel ttl 64
 tunnel tos inherit !
ip route 0.0.0.0 0.0.0.0 172.16.22.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Feb  6 15:32:55 2026

GlobalParameters(
    Title                           = "This LSP was automatically generated by CSP
Converter at Fri Feb  6 15:32:55 2026 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.22.1
        )

)

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

```
)

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

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

FilterChain FilterChain:FIREWALL_IN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.22.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.22.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.22.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.22.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FIREWALL_IN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))
```

```
FilterChain FilterChain:FIREWALL_OUT (
    Filters = Filter (
        SourceIP = 172.16.22.2
        DestinationIP = 172.16.0.0/12
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.22.2
        DestinationIP = 192.168.0.0/16
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 172.16.22.2
        DestinationIP = 10.0.0.0/8
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.0.0/12
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 192.168.0.0/16
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 10.0.0.0/8
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 47
        Action = DROP
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = "INSPECT"
        LogEventID = "FIREWALL_OUT"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    ),
    Filter (
        Label = "INSPECT"
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        ProtocolID = 6
```

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

IdentityEntry Remote:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:ALGS_PROFILE(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

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

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
```

```
    AggrModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    MainModeAuthMethod  = GOST:Sign:ALGS_PROFILE
    DPDIdleDuration     = 3
    DPDResponseDuration = 3
    DPDRetries          = 3
    Priority            = 100
)

IPsecAction IPsecAction:VPN:1:DMAP:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1:DMAP:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.22.2
        ProtocolID = 47
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_DMVPN"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = FilterChain:FIREWALL_IN
    OutputFilter = FilterChain:FIREWALL_OUT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "Tunnel0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

```
interface mgre0
  map 10.10.20.100/24 172.16.100.2 register
  multicast nhs
  holding-time 90
  cisco-authentication secret
```

4. Содержимое файла `/etc/frr/frr.conf`:

```
frr version 9.0.4
frr defaults traditional
hostname sterragate
log syslog informational
hostname Spoke2-2
service integrated-vtysh-config
!
router bgp 65000 vrf vrf_red
 bgp router-id 10.10.20.2
 bgp log-neighbor-changes
 timers bgp 3 9
 neighbor 10.10.20.100 remote-as 65000
 neighbor 10.10.20.100 timers connect 30
 !
 address-family ipv4 unicast
  network 192.168.2.0/24
 exit-address-family
exit
!
end
```

5. Содержимое файла `/etc/networkk/interfaces.d/interfaces`:

```
auto vrf_red
iface vrf_red inet manual
pre-up ip link del vrf_red type vrf 2>/dev/null || true
pre-up ip route flush table 20 2>/dev/null || true
pre-up ip link add vrf_red type vrf table 20
pre-up ip link set dev vrf_red up
pre-up ip route add table 20 unreachable default metric 4278198272
pre-up ip link set dev eth1 master vrf_red
pre-up ip link set dev mgre0 master vrf_red 2>/dev/null || true
post-down ip link set dev vrf_red down

auto mgre0
iface mgre0 inet static
address 10.10.20.2
netmask 255.255.255.0
pre-up ip tunnel add mgre0 mode gre key 2 ttl 64 tos inherit
pre-up ip link set mgre0 type gre nopmtudisc
pre-up ip link set mgre0 type gre ignore-df
pre-up ip link set mgre0 mtu 1400
pre-up ip link set mgre0 multicast on
pre-up ip link set dev mgre0 master vrf_red || true
post-down ip link del mgre0
```

6. Содержимое файла `/etc/ifaliases.cf`:

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