Построение L2 VPN туннеля между несколькими шлюзами «С-Терра Шлюз DP» в топологии звезда

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

Введение

Данный сценарий описывает настройку «С-Терра Шлюз DP» для безопасного взаимодействия между защищаемыми подсетями центрального офиса и филиалов на втором уровне модели OSI (L2 VPN).

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. Безопасное взаимодействие между защищаемыми подсетями филиалов осуществляется через криптошлюз центрального офиса.

Все остальные соединения на третьем уровне модели OSI от/на «С-Терра Шлюз DP» разрешены, но защищаться при помощи IPsec не будут.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Криптошлюзы – «С-Терра Шлюз DP» версии 5.0.

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, routing, switching.

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

Администратор должен быть ознакомлен со сценарием «Построение L2 VPN туннеля между двумя «С-Терра Шлюз DP».

Требования к инфраструктуре

1. Требования к устройствам.

1.1. «С-Терра Шлюз DP».

1.1.1. Устройства «С-Терра Шлюз DP» должны быть инициализированы (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз DP -> С-Терра Шлюз DP <версия> -> «Подключение АП и инициализация ПК С-Терра Шлюз DP на вычислительных системах архитектуры Intel x86-64»).

1.2. Центр выпуска сертификатов.

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

1.2.2. Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2016 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 5.0 R2 (или новее).

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

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

1.3. HTTP сервер для распространения списка отозванных сертификатов.

1.3.1. Функционирующий HTTP сервер для распространения списка отозванных сертификатов (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 DP» (при соблюдении правил пользования).

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

2. Требования к сетевому взаимодействию.

2.1. Между криптошлюзами должна быть обеспечена IP связность.

Схема взаимодействия

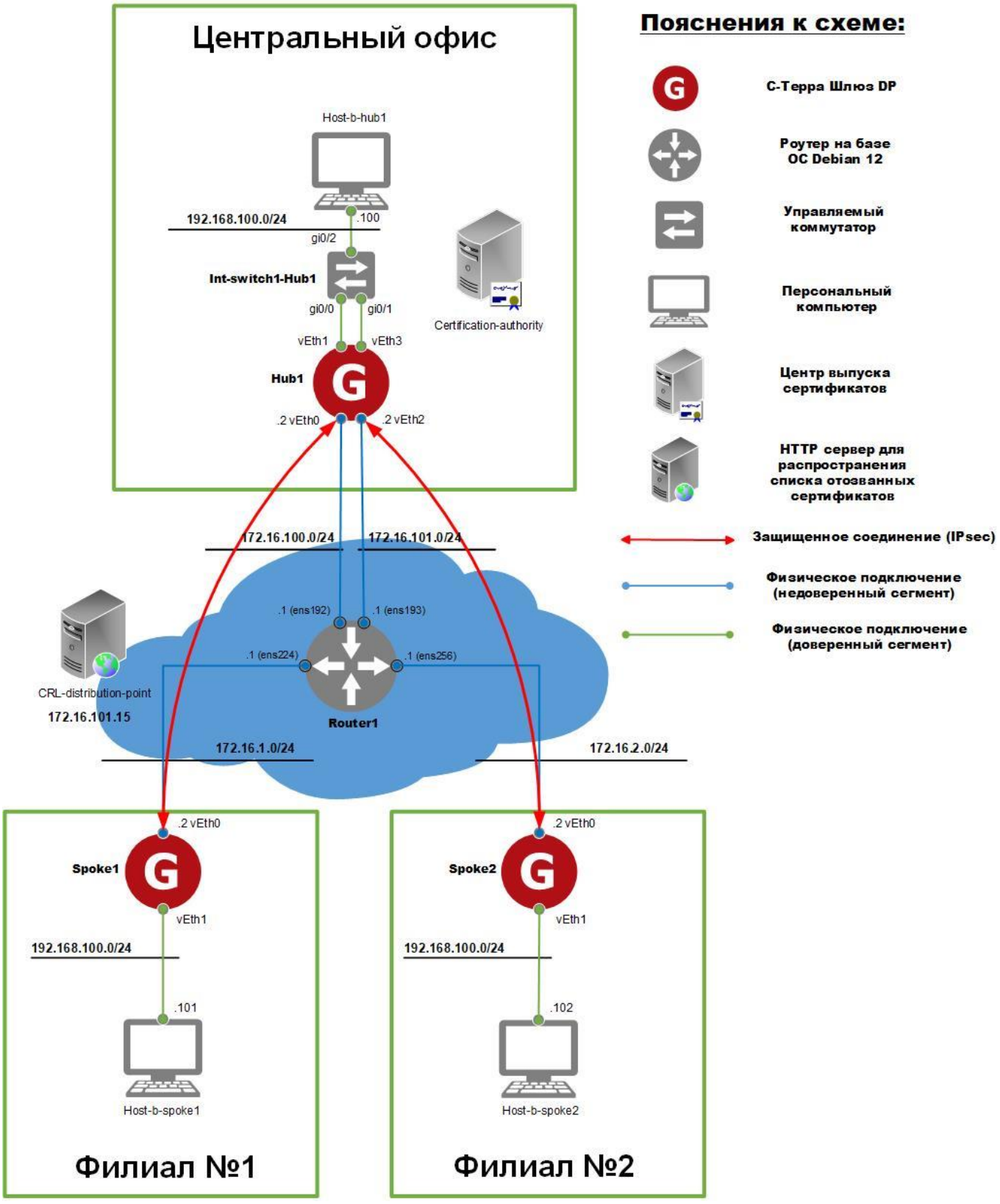


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification-authority), криптошлюз «С-Терра Шлюз 40G» (Hub1), коммутатор (Int-switch1-Hub1) и персональный компьютер (Host-b-hub1).

   1.2. В филиалах размещаются: криптошлюзы «С-Терра Шлюз 10G» (Spoke1 и Spoke2) и персональные компьютеры (Host-b-spoke1 и Host-b-spoke2).

   1.3. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL-distribution-point) и маршрутизатор (Router1).

2. Подключение к сети Интернет.
   В данном сценарии для эмуляции сети Интернет используются маршрутизатор Router1.

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

   2.1. Криптошлюз Hub1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1). Для корректной работы WAN интерфейсы криптошлюза Hub1 должны находиться в разных широковещательных доменах (например, как на схеме стенда или в разных VLAN сегментах).

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

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

3. L2 VPN/L3 VPN.

   Общие сведения

   Высокопроизводительный L2 VPN реализуется самим Продуктом «С-Терра Шлюз DP». Главное отличие «С-Терра Шлюз DP» от модуля «С-Терра L2», который реализует аналогичный функционал, – это производительность шифрования, которая может достигать 100 Gbit/s. Также важно понимать, что защищаемый при помощи «С-Терра Шлюз DP» транзитный L2 трафик не может быть обработан TCP/IP стеком операционной системы (например, нельзя применить к такому трафику правила iptables).

   На этапе ввода в эксплуатацию «С-Терра Шлюз DP» нужно определить какой из сетевых интерфейсов будет подключен к доверенной сети – LAN, а какой к недоверенной – WAN (при необходимости может быть несколько пар LAN/WAN интерфейсов).

   Логика обработка фреймов/пакетов

   «С-Терра Шлюз DP» обрабатывает фреймы/пакеты следующим образом. Все фреймы, поступившие на LAN интерфейс, упаковываются в пакеты протокола EtherIP (протокол 97), далее эти пакеты зашифровываются в соответствии с политикой безопасности и отправляются с WAN интерфейса (пакеты с LAN интерфейса не могут попасть в TCP/IP стек ОС). Пакеты, поступившие на WAN интерфейс, делятся на две группы. К первой группе относятся транзитные зашифрованные пакеты L2 VPN, они расшифровываются и отправляются с LAN интерфейса, данные пакеты никогда не попадают в TCP/IP стек ОС. Ко второй группе относятся пакеты, которые предназначены в TCP/IP стек ОС, как правило — это зашифрованный трафик (L3 VPN) для удаленного управления «С-Терра Шлюз DP» и открытый трафик (с некоторыми исключениями при работе криптошлюза за NAT).

   Логика настройки шифрования

Настройка шифрования трафика производится в два этапа. Этап первый – настройка L2 части (либо data plane), которая частично осуществляется в процессе инициализации «С-Терра Шлюз DP» мастером настроек, либо полностью через конфигурационный файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`. На втором этапе настраивается политика безопасности через консоль cisco-like.

Для шифрования транзитного L2 трафика (L2 VPN) крипто-карту нужно прикреплять **ко всем** специальным интерфейсам, которые имеют имя `DP<N>` (данные интерфейсы по сути являются ядрами процессора). Пример:

```
interface DP0
 crypto map L2VPN
 crypto ipsec stream-id 1000
!
interface DP1
 crypto map L2VPN
 crypto ipsec stream-id 1001
!
...
!
interface DP44
 crypto map L2VPN
 crypto ipsec stream-id 1044
!
```

Для организации защиты удаленного управления «С-Терра Шлюз DP» (L3 VPN) крипто-карту нужно прикреплять к интерфейсу, который имеет имя `vEthernet<N>` и соответствует WAN. Пример:

```
interface vEthernet0
 crypto map L3VPN
 ip address 172.16.1.2 255.255.255.0
 mtu 9000
!
```

Если для удаленного управления используется «С-Терра Клиент» под Windows с IKECFG адресом, то в качестве защищаемого Mgmt адреса «С-Терра Шлюз DP» нельзя указывать IP адрес на WAN интерфейсе. Создайте для этого на «С-Терра Шлюз DP» либо loopback интерфейс, либо назначьте адрес на свободный сетевой интерфейс (выполняется средствами ОС).

4. Параметры межсетевого экранирования.

   Для пакетов применяются следующие правила фильтрации:

   4.1. На LAN интерфейсах vEthernet1 (порты L2) IPv4 и IPv6 трафик не контролируется.

   4.2. На WAN интерфейсах vEthernet0 разрешен входящий IPv4 трафик:

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

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

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

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

   4.3. На WAN интерфейсах vEthernet0 IPv6 трафик заблокирован.

   4.4. На WAN интерфейсах vEthernet0 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).

   4.5. На DP интерфейсах разрешен входящий IPv4 трафик:

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

4.5.2 Протокол UDP порт 4500 – NAT-Traversal (ESP in UDP).

4.6. На DP интерфейсах IPv6 трафик заблокирован.

4.7. На всех остальных интерфейсах, не задействованных в L2, IPv4 и IPv6 трафик **не контролируется.**

5. Параметры безопасного взаимодействия.

Весь трафик на втором уровне модели OSI подсети 192.168.100.0/24, который передается между центральным офисом и филиалами защищается с использованием алгоритмов ГОСТ и протокола IPsec в транспортном режиме, трафик управления (L3 VPN) – в туннельном режиме.

Инициировать защищенное соединение может как трафик из филиала в центр, так и наоборот, из центра в филиал.

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 для L2 VPN:

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

5.3. Параметры протокола ESP для L3 VPN:

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

Настройка стенда

Настройка устройства Router1

1. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.101.1 и маску – 255.255.255.0 на сетевом интерфейсе ens193.
3. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
4. Настройте IP адрес – 172.16.2.1 и маску – 255.255.255.0 на сетевом интерфейсе ens256.
5. Разрешите прохождение IP трафика.

Настройка устройства Host-b-hub1

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke1

1. Настройте IP адрес – 192.168.100.101 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke2

1. Настройте IP адрес – 192.168.100.102 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Разрешите прием и отправку ICMP пакетов.

Настройка криптошлюза Hub1

Настройка будет происходить локально при помощи консольного подключения.

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

Начальные настройки

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

1. Войдите в CLI разграничения доступа. Для этого, после появления сообщения:

   ```
   S-Terra administrative console
   ```

   введите логин и пароль для CLI разграничения доступа:

   Пользователь и пароль по умолчанию: `administrator`, `s-terra`. Обязательно смените пароль для пользователя `administrator` при помощи команды `change user password`.

   ```
   login as: administrator
   ```

   ```
   administrator's password:

   ############################################################
   System is not initialized. Please run "initialize" command to start initializat
   ion procedure.
   ############################################################

   administrator@sterragate]
   ```

2. Установите правильный тип терминала (для `putty` тип терминала `xterm`) и требуемую ширину (для удобства работы), например:

   ```
   administrator@sterragate] terminal terminal-type xterm
   administrator@sterragate] terminal width 150
   ```

3. Установите нужную временную зону и правильные дату и время на криптошлюзе, используя консоль linux bash. Для этого выполните следующие команды.

   3.1. Войдите в linux bash.

   ```
   administrator@ sterragate]system
   ```

   ```
   Entering system shell...
   ```

   3.2. Установите нужную временную зону:

   ```
   root@sterragate:~# dpkg-reconfigure tzdata
   ```

   3.3. Проверьте при помощи команды `date` дату и время и если они неправильные то, установите верные значения (формат – месяц/день/год часы:минуты):

   ```
   root@sterragate:~# date -s "22/10/2024 12:32"
   ```

   ```
   Tue Oct 22 12:09:30 MSK 2024
   ```

4. Установите надежный пароль для пользователя root (под данным пользователем осуществляется доступ по SSH в linux bash):

```
root@sterragate:~# passwd
```

```
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

5. Выйдите из linux bash обратно в CLI разграничения доступа:

```
root@sterragate:~# exit
```

```
logout
Leaving system shell...
administrator@sterragate]
```

6. Запустите процедуру инициализации, в процессе которой будет запущен мастер начальных настроек L2 (data plane):

```
administrator@sterragate] initialize
```

6.1. Пройдите инициализацию биологического ДСЧ, нажимая предлагаемые клавиши:

```
Progress: [********  ]
Press key: i
```

6.2. Введите лицензию на Продукт GATEDP:

```
You have to enter license for S-Terra Gate DP
Available product codes:
GATE
GATEDP
MVPN
```

```
Enter product code: GATEDP
Enter customer code: Customer
Enter license number: 1XX
Enter license code: 50XXX-XXXXX- XXXXX - XXXXX - XXXXX
```

```
Your license:
  CustomerCode = Customer
  ProductCode  = GATEDP
  LicenseNumber= 1XX
  LicenseCode  = 50XXX-XXXXX- XXXXX - XXXXX - XXXXX
```

```
Is the above data correct? Yes
```

```
INFO: License accepted

################################################################################
################################################################
ssh-keygen: generating new host keys: RSA ECDSA ED25519
INFO: SSH server was successfully enabled and started
```

6.3. На вопрос включать ли маршрутизацию пакетов IPv6 ответить отрицательно (`no`):

```
Would you like to enable IPv6 forwarding? [No] no
```

```
INFO: IP forwarding status:
INFO: IPv4: enabled
INFO: IPv6: disabled.
```

6.4. Нажмите Enter, после чего запустится мастер начальных настроек L2 (data plane). Данный мастер изменяет файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`, который используется сервисом `ipsmapp`:

```
WARNING: This script will stop ipsmapp daemon and create new ipsm_dpdk.cfg. All ipsmapp
settings will be reset.
```

```
Do you want to continue? [yes]
```

```
INFO: Binding network devices to their original drivers
INFO: Device "0000:03:00.0" is already bound to driver "vmxnet3". Skipping
```

```
INFO: Device "0000:04:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:0b:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:13:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:1b:00.0" is already bound to driver "vmxnet3". Skipping
```

В зависимости от аппаратной платформы драйвер может отличаться.

6.4.1 Укажите количество портов (количество физических LAN и WAN интерфейсов для L2 (Mgmt интерфейсы не учитываются):

```
Enter amount of ports (2-4) [2] : 4
```

6.4.2 Введите количество потоков для обработки трафика (количество потоков соответствует количеству `DP<N>` интерфейсов):

По умолчанию, число потоков (threads) N для обработки трафика вычисляется по следующей формуле:
`N = nproc_all - 2 - 3*ports_num`,
где:
`nproc_all` – количество вычислительных потоков процессоров (это значение можно посмотреть в выводе команды `nproc --all` в линукс консоли шлюза или рассчитать исходя из спецификации установленных в конкретную платформу процессоров),
`ports_num` – количество портов для L2, заданное на предыдущем шаге.

В зависимости от ситуации, это число можно изменять (только **в меньшую** сторону). В схеме звезда, число потоков (threads) на шлюзах следует задавать так, чтобы число потоков (threads) на центральном шлюзе соответствовало сумме потоков на филиальных шлюзах. Подробнее в примерах ниже.

Пример 1 (схема «звезда» с двумя лучами; центральный шлюз – DP 40G, филиальные шлюзы – DP 25G):
На центральном шлюзе установлены два 64-х ядерных процессора с включенным Hyper-Threading. Суммарное количество вычислительных потоков процессоров: 2*64*2 = 256. Число потоков (threads) доступных для L2 по умолчанию: 256 - 2 - 3*4 = 242.
На каждом из двух филиальных шлюзов установлен один 64-х ядерный процессор с включенным Hyper-Threading. Количество вычислительных потоков процессоров на каждом из этих шлюзов: 64*2 = 128, сответственно, число потоков для обработки трафика (threads) по умолчанию: 128 - 2 - 3*2 = 120. Следовательно, сумма потоков для обработки трафика (threads) на всех филиальных шлюзах: 240.
Таким образом, на центральном шлюзе число потоков для обработки трафика (threads) следует сделать равным 240, на каждом филиальном шлюзе оставить по умолчанию (120).

Пример 2 (схема «звезда» с тремя лучами; центральный шлюз – DP 40G, филиальные шлюзы – DP 10G):
На центральном шлюзе установлены два 64-х ядерных процессора с включенным Hyper-Threading. Суммарное количество вычислительных потоков процессоров: 2*64*2 = 256. Число потоков (threads) доступных для L2 по умолчанию: 256 - 2 - 3*6 = 236.
На каждом из трех филиальных шлюзов установлены два 22-х ядерных процессора с включенным Hyper-Threading. Количество вычислительных потоков процессоров на каждом из этих шлюзов: 2*22*2 = 88, сответственно, число потоков для обработки трафика (threads) по умолчанию: 88 - 2 - 3*2 = 80. Следовательно, сумма потоков для обработки трафика (threads) на всех филиальных шлюзах: 240.
Таким образом, на центральном шлюзе число потоков для обработки трафика (threads) следует сделать равным 234, на каждом филиальном шлюзе: 78.

В данном сценарии число потоков (threads) N для обработки трафика будет уменьшено в целях снижения объема конфигурации, и будет составлять 16 для центрального шлюза и 8 для каждого филиального шлюза.

```
threads (1-30) [30] : 16
```

6.4.3 Выберите из предложенного списка PCI адрес для WAN порта. PORT0 – первый WAN интерфейс.

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |       -       | vmxnet3 |
| 1 | 0000:04:00.0 |       -       | vmxnet3 |
| 2 | 0000:0b:00.0 |       -       | vmxnet3 |
| 3 | 0000:13:00.0 |       -       | vmxnet3 |
| 4 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

Данный список сформирован из всех физических сетевых интерфейсов, которые есть в криптошлюзе. В каждом конкретном случае PCI адреса могут отличаться. PCI адреса интерфейсов для WAN и LAN портов указаны в документации на ПАК.

```
Enter device index to be configured as WAN interface "PORT0" (0-4): 0
```

```
INFO: Configuring device "0000:03:00.0" as "PORT0"
```

6.4.4 Укажите IP адрес для первого WAN интерфейса (в данном сценарии - 172.16.100.2). Данный IP адрес будет назначен на интерфейс `vEthernet0`:

Обратите внимание, что в данном сценарии для корректной работы WAN интерфейсы криптошлюза Hub1 должны находиться в разных широковещательных доменах (например, как на схеме стенда или в разных VLAN сегментах).

```
Enter IP-address for WAN interface (l3_ip/l3_ip6) (allowed_protocols: ipv4,ipv6):
172.16.100.2
```

6.4.5 Укажите маску для IP адреса первого WAN интерфейса (в данном сценарии - 24):

```
Enter netmask for WAN interface (0-32) [24] : 24
```

6.4.6 Укажите адрес шлюза по умолчанию для транзитного L2 (data plane) зашифрованного трафика (в данном сценарии – 172.16.100.1):

```
Enter default gateway IP-address (gw_ip) (allowed_protocols: ipv4): 172.16.100.1
```

6.4.7 Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

6.4.8 Выберите из вновь предложенного списка PCI адрес для первого LAN порта. PORT1 – первый LAN интерфейс:

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:04:00.0 |       -       | vmxnet3 |
| 2 | 0000:0b:00.0 |       -       | vmxnet3 |
| 3 | 0000:13:00.0 |       -       | vmxnet3 |
| 4 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

Из списка выше видно, что первый WAN порт уже сконфигурирован («`PORT0`» в столбце «Configured as»):

```
Enter device index to be configured as LAN interface "PORT1" and paired with "PORT0"
(0-3): 3
```

6.4.9 Укажите IP адрес источника для EtherIP туннеля (в данном сценарии – 172.16.100.2):

Для транспортного режима IPsec здесь следует указывать адрес первого WAN интерфейса криптошлюза Hub1. В случае использования туннельного режима IPsec, данный адрес может не присутствовать в системе и быть любым. Во всех случаях этот адрес должен совпадать с l2_dst_ip на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke1.

```
Enter source IP-address for l2-tunnel (l2_src_ip) : 172.16.100.2
```

6.4.10 Укажите IP адрес назначения для EtherIP туннеля (в данном сценарии – 172.16.1.2):

Для транспортного режима IPsec здесь следует указывать адрес WAN интерфейса криптошлюза Spoke1. В случае использования туннельного режима IPsec, данный адрес может быть любым. Во всех случаях этот адрес должен совпадать с `l2_src_ip` на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke1.

```
Enter destination IP-address for l2-tunnel (l2_dst_ip) : 172.16.1.2
```

6.4.11 Задайте MTU для WAN и LAN интерфейсов (в данном сценарии – 9000):

Если есть возможность, то всегда указывайте MTU на WAN интерфейсе минимум на 100 (сто) байт больше, чем максимальный MTU на защищаемых устройствах, чтобы избежать фрагментации и увеличить производительность. В этом случае MTU на LAN интерфейсе указывайте как максимальный MTU на защищаемых устройствах. Например, если MTU на защищаемых устройствах 9000, то MTU для WAN – 9100, MTU для LAN – 9000. Проверить наличие или отсутствие фрагментации можно при помощи утилиты `kstat_show` (параметр «frag ok»).

```
Enter MTU for WAN interface (68-9700) [9700] : 9000
Enter MTU for LAN interface (68-9700) [9600] : 9000
```

6.4.12 Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

6.4.13 Выберите из списка PCI адрес для второго WAN порта. PORT2 – второй WAN интерфейс.

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:04:00.0 |       -       | vmxnet3 |
| 2 | 0000:0b:00.0 |       -       | vmxnet3 |
| 3 | 0000:13:00.0 |     PORT1     | vmxnet3 |
| 4 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

```
Enter device index to be configured as WAN interface "PORT2" (0-4): 2
```

```
INFO: Configuring device "0000:0b:00.0" as "PORT2"
```

6.4.14 Укажите IP адрес для второго WAN интерфейса (в данном сценарии - 172.16.101.2). Данный IP адрес будет назначен на интерфейс `vEthernet2`:

```
Enter IP-address for WAN interface (l3_ip/l3_ip6) (allowed_protocols: ipv4,ipv6):
172.16.101.2
```

6.4.15 Укажите маску для IP адреса второго WAN интерфейса (в данном сценарии - 24):

```
Enter netmask for WAN interface (0-32) [24] 24
```

6.4.16 Укажите адрес шлюза по умолчанию для транзитного L2 (data plane) зашифрованного трафика (в данном сценарии – 172.16.101.1):

```
Enter default gateway IP-address (gw_ip) (allowed_protocols: ipv4): 172.16.101.1
```

6.4.17 Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

6.4.18 Выберите из вновь предложенного списка PCI адрес для второго LAN порта. PORT3 – второй LAN интерфейс:

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:04:00.0 |       -       | vmxnet3 |
| 2 | 0000:0b:00.0 |     PORT2     | vmxnet3 |
| 3 | 0000:13:00.0 |     PORT1     | vmxnet3 |
| 4 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

```
Enter device index to be configured as LAN interface "PORT3" and paired with "PORT2"
(0-4): 4
```

6.4.19 Укажите IP адрес источника для EtherIP туннеля (в данном сценарии – 172.16.101.2):

Для транспортного режима IPsec здесь следует указывать адрес второго WAN интерфейса криптошлюза Hub1. В случае использования туннельного режима IPsec, данный адрес может не присутствовать в системе и быть любым. Во всех случаях этот адрес должен совпадать с l2_dst_ip на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke2.

```
Enter source IP-address for l2-tunnel (l2_src_ip) (allowed_protocols: ipv4,ipv6):
172.16.101.2
```

6.4.20 Укажите IP адрес назначения для EtherIP туннеля (в данном сценарии – 172.16.2.2):

Для транспортного режима IPsec здесь следует указывать адрес WAN интерфейса криптошлюза Spoke2. В случае использования туннельного режима IPsec, данный адрес может быть любым. Во всех случаях этот адрес должен совпадать с `l2_src_ip` на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke2.

```
Enter destination IP-address for l2-tunnel (l2_dst_ip) (allowed_protocols: ipv4):
172.16.2.2
```

6.4.21 Задайте MTU для WAN и LAN интерфейсов (в данном сценарии – 9000):

```
Enter MTU for WAN interface (68-9700) [9700] 9000
Enter MTU for LAN interface (68-9700) [8900] 9000
```

6.4.22 Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

6.4.23 Дождитесь окончания процедуры инициализации и мастера настроек:

```
---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:04:00.0 |       -       | vmxnet3 |
| 2 | 0000:0b:00.0 |     PORT2     | vmxnet3 |
| 3 | 0000:13:00.0 |     PORT1     | vmxnet3 |
| 4 | 0000:1b:00.0 |     PORT3     | vmxnet3 |
+---+--------------+--------------+---------+
```

```
INFO: Operation completed successfully. Restart your system to apply the changes
INFO: OK

################################################################################
INFO: Reset product settings was completed successfully
```

6.4.24 После мастер настроек предложит поменять пароль пользователя root. Установите надежный пароль. После этого процедура инициализации будет завершена:

```
Do you want to change the password for root user? [Yes]
New password:
Retype new password:
```

```
passwd: password updated successfully
INFO: S-Terra VPN services were successfully enabled and started
NOTICE:
Network traffic is blocked, except on management interface (if using one).
To unblock network traffic, please setup the network security policy
or use "run csconf_mgr activate" command to activate the predefined
permissive network security policy now.

INFO: Initialization completed.
NOTICE: Some settings will take effect after OS reboot only.
```

6.4.25 Включите прохождение сетевого трафика, загрузив предопределенную разрешающую политику:

```
administrator@sterragate]run csconf_mgr activate
```

Начальные настройки завершены.

Если вы хотите заново запустить мастер начальных настроек L2 (data plane), то выполните:
`administrator@sterragate] run /opt/VPNagent/bin/init.sh.d/25_run_configure_dp.sh`

Настройка L2

В данном разделе будут описаны:

- настройка фрагментации;
- настройка механизма Path MTU Discovery;
- настройка механизма изменения MSS в TCP пакетах;
- настройка распределения потоков обработки трафика по портам.

1. Перейдите в linux bash:

```
administrator@Hub1] system
```

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

2. Уменьшите время сборки фрагментированных пакетов:

```
root@sterragate:~# drv_mgr set frag_reassemble_timeout 2
```

```
Value of "frag_reassemble_timeout" is set to 2.
```

3. Дальнейшие настройки осуществляются через файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`:

```
root@sterragate:~# vim.tiny /opt/VPNagent/etc/ipsm_dpdk.cfg
```

3.1. Включите механизм Path MTU Discovery и изменение MSS в TCP пакетах на LAN портах (PORT1 и PORT3). Для этого раскомментируйте параметры `pmtud`, `mssfix` и выставите им значения: для `pmtud` - «значение MTU порта минус 100» (в данном сценарии – это значение 8900), для `mssfix` - «значение MTU порта минус 140» (в данном сценарии – это значение 8860):

```
[PORT1]
pci_id = 0000:13:00.0
l2_src_ip = 100.100.101.1
```

```
l2_dst_ip = 100.100.101.2
pair_port = 0
mtu = 9000
...
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
...



[PORT3]
pci_id = 0000:1b:00.0
l2_src_ip = 100.100.102.1
l2_dst_ip = 100.100.102.2
pair_port = 2
mtu = 9000
...
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
...
```

3.2. Распределите потоки обработки трафика между LAN портами (PORT1 и PORT3). В данном сценарии на шлюзе Hub1 задано 16 потоков (threads), сответственно, на каждый порт будет отведено по 8 потоков. Раскомментируйте параметры `thr_count` (число потоков на данном порту) и `thr_start` (порядковый номер (начиная с нуля) потока обработки трафика, с которого начинается отсчет указанного в `thr_count` числа потоков) и выставите им следующие значения. Для порта PORT1: `thr_start` – 0, `thr_count` – 8. Для порта PORT3: `thr_start` – 8, `thr_count` – 8.

```
[PORT1]
pci_id = 0000:13:00.0
l2_src_ip = 100.100.101.1
l2_dst_ip = 100.100.101.2
pair_port = 0
mtu = 9000
thr_start = 0 ;min: 0 max: <threads - 1> -- first processing thread for this port
thr_count = 8 ;min: 1 max: <threads - thr_start> -- number of processing threads for
this port...



[PORT3]
pci_id = 0000:1b:00.0
l2_src_ip = 100.100.102.1
l2_dst_ip = 100.100.102.2
pair_port = 2
mtu = 9000
thr_start = 8 ;min: 0 max: <threads - 1> -- first processing thread for this port
thr_count = 8 ;min: 1 max: <threads - thr_start> -- number of processing threads for
this port
```

Таким образом для первого LAN порта будут назначены потоки 0-7, для второго – 8-15.

3.3. Для применения настроек перезапустите сервис `ipsmapp`:

```
root@sterragate:~# systemctl restart ipsmapp.service
```

4. Выйдите из linux bash:

```
root@sterragate:~# exit
```

```
logout
Leaving system shell...
```

Настройка L2 (data plane) завершена.

Настройки PKI (запросы и сертификаты)

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

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

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка паролей доступа к консоли cisco-like

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка сетевых параметров

Настройка сетевых параметров проходит в два этапа. Первый – настройка Mgmt интерфейса (`TenGigabitEthernet0/0`) в cisco-like консоли (данный интерфейс не представлен на схеме). Второй – настройка маршрутизации в cisco-like консоли.

Первый этап.

1. Выведите список всех интерфейсов, доступных в cisco-like консоли и выберите незадействованный в L2. Незадействованные в L2 интерфейсы будут иметь имя `TenGigabitEthernet0/N`, а задействованные `vEthernetN`:

```
sterragate#show interfaces
```

```
TenGigabitEthernet0/0 is down, line protocol is down
  Hardware address is 0050.569e.47ab
  MTU 1500 bytes
DP0
  Virtual data plane interface (pattern "10G_000")
DP1
  Virtual data plane interface (pattern "10G_001")
DP2
...
DP15
  Virtual data plane interface (pattern "10G_015")
vEthernet0 is up, line protocol is up
  Hardware address is 0050.569e.0d52
  Description: WAN
  Internet address is 172.16.100.2/24
  MTU 9000 bytes
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.26ec
  MTU 9000 bytes
vEthernet2 is up, line protocol is up
  Hardware address is 0050.569e.a832
  Internet address is 172.16.101.2/24
  MTU 9000 bytes
```

```
vEthernet3 is up, line protocol is up
  Hardware address is 0050.569e.fe19
  MTU 9000 bytes
```

Видно, что интерфейс `TenGigabitEthernet0/0` не задействован в L2. Интерфейсы `vEthernetN` задействованы в L2, `vEthernet0` и `vEthernet2` соответствуют WAN интерфейсам, а `vEthernet1` и `vEthernet3` – LAN.

2. Настройте Mgmt интерфейс:

Mgmt интерфейс запрещено подключать к недоверенным сетям, так как Mgmt интерфейсы не контролируются средствами Продукта и соответственно отсутствует возможность фильтровать пакеты и использовать криптокарты через cisco-like. Через cisco-like доступна только настройка IP адреса.
Если требуется фильтровать пакеты, то используйте iptables (см. документ «Использование утилиты «iptables»). Соответствие интерфейса в cisco-like нотации интерфейсу в linux нотации можно увидеть в файле `/etc/ifaliases.cf`.
Всё то же относится к любому интерфейсу кроме тех, которые в нотации cisco-like начинаются на vEthernet и на DP.

```
sterragate#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sterragate(config)#interface TenGigabitEthernet0/1
sterragate(config-if)#ip address 192.168.253.1 255.255.255.0
sterragate(config-if)#exit
```

Второй этап.

Изменения сетевых настроек в cisco-like консоли применяются сразу после ввода соответствующих команд. Политика безопасности применяется после выхода из режима конфигурирования.

1. Задайте имя устройства:

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

2. Убедитесь, что WAN и LAN интерфейсы административно включены и line protocol (способность интерфейса передавать пакеты в данный момент) находится в состоянии up, а также на интерфейсе `vEthernet0` присутствует WAN адрес криптошлюза:

```
Hub1(config)#do show interfaces vEthernet0
vEthernet0 is up, line protocol is up
  Hardware address is 0050.569e.0d52
  Description: WAN
  Internet address is 172.16.100.2/24
  MTU 9000 bytes
Hub1(config)#do show interfaces vEthernet1
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.26ec
  MTU 9000 bytes
Hub1(config)#do show interfaces vEthernet2
vEthernet2 is up, line protocol is up
  Hardware address is 0050.569e.a832
  Internet address is 172.16.101.2/24
  MTU 9000 bytes
Hub1(config)#do show interfaces vEthernet3
vEthernet3 is up, line protocol is up
  Hardware address is 0050.569e.fe19
  MTU 9000 bytes
```

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

3. Задайте маршрут по умолчанию через устройство Router1 для исходящего из TCP/IP стека ОС и транзитного Mgmt трафика (шлюз по умолчанию для зашифрованного транзитного L2 трафика задается в файле `/opt/VPNagent/etc/ipsm_dpdk.cfg`):

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

4. Задайте статический маршрут до устройства Spoke1 через соответствующий интерфейс устройства Router1.

```
Hub1(config)#ip route 172.16.1.2 255.255.255.255 172.16.100.1
```

5. Задайте статический маршрут до устройства Spoke2 через соответствующий интерфейс устройства Router1.

```
Hub1(config)#ip route 172.16.2.2 255.255.255.255 172.16.101.1
```

6. Проверьте доступность устройства Router1:

```
Hub1(config)#do ping 172.16.100.1
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=1.13 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.237 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.192 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.200 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.299 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.192/0.411/1.131/0.362 ms
```

```
Hub1(config)#do ping 172.16.101.1
PING 172.16.101.1 (172.16.101.1) 100(128) bytes of data.
108 bytes from 172.16.101.1: icmp_seq=1 ttl=64 time=0.288 ms
108 bytes from 172.16.101.1: icmp_seq=2 ttl=64 time=0.415 ms
108 bytes from 172.16.101.1: icmp_seq=3 ttl=64 time=0.494 ms
108 bytes from 172.16.101.1: icmp_seq=4 ttl=64 time=0.926 ms
108 bytes from 172.16.101.1: icmp_seq=5 ttl=64 time=0.534 ms

--- 172.16.101.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 0.288/0.531/0.926/0.214 ms
```

Настройка шифрования

1. Настройте параметры IKE.

1.1. Задайте общие параметры IKE:

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

1.2. Создайте политику, описывающую параметры IKE туннеля:

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

```
Hub1(config-isakmp)#exit
```

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

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

2. Параметры IPsec для защиты транзитного L2 трафика.

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

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

2.2. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика, которым будет защищаться L3 трафик управления:

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

2.3. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика (транспортный режим), которым будет защищаться L2 трафик между центральным офисом и филиалами:

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

2.4. Создайте список доступа (ACL) для транзитного инкапсулированного в EtherIP пользовательского трафика, который нужно защищать между центральным офисом и первым филиалом:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
Hub1(config-ext-nacl)#remark EtherIP L2 tunnel
Hub1(config-ext-nacl)#permit 97 host 172.16.100.2 host 172.16.1.2
Hub1(config-ext-nacl)#exit
Hub1(config)#
```

2.5. Создайте список доступа (ACL) для транзитного инкапсулированного в EtherIP пользовательского трафика, который нужно защищать между центральным офисом и вторым филиалом:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE2
Hub1(config-ext-nacl)#remark EtherIP L2 tunnel
Hub1(config-ext-nacl)#permit 97 host 172.16.101.2 host 172.16.2.2
Hub1(config-ext-nacl)#exit
Hub1(config)#
```

2.6. Создайте крипто-карту (имя L2VPN_HUB1_AND_SPOKE1, раздел 1):

```
Hub1(config)#crypto map L2VPN_HUB1_AND_SPOKE1 1 ipsec-isakmp
```

2.6.1. Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_SPOKE1
```

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

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

2.6.3. Укажите IP адрес партнера по IPsec, это внешний IP адрес устройства Spoke1:

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

2.6.4. Задайте локальный IP адрес для IKE и IPsec пакетов.

```
Hub1(config-crypto-map)#set local-address 172.16.100.2
```

2.6.5. Прикрепите ISAKMP профиль NEW_ALGS к криптокарте:

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

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

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

2.6.7. Включите префрагментацию:

```
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#exit
```

2.7. Создайте крипто-карту (имя L2VPN_HUB1_AND_SPOKE2, раздел 1):

```
Hub1(config)#crypto map L2VPN_HUB1_AND_SPOKE2 1 ipsec-isakmp
```

2.7.1. Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_SPOKE2
```

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

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

2.7.3. Укажите IP адрес партнера по IPsec, это внешний IP адрес устройства Spoke2:

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

2.7.4. Задайте локальный IP адрес для IKE и IPsec пакетов.

```
Hub1(config-crypto-map)#set local-address 172.16.101.2
```

2.7.5. Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте :

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

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

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

2.7.7. Включите префрагментацию:

```
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#exit
```

2.8. Прикрепите крипто-карту `L2VPN_HUB1_AND_SPOKE1` к `DP` интерфейсам из диапазона 0 – 7 (эти номера соответствуют потокам обработки трафика первого LAN порта (PORT1 в ipsm_dpdk.cfg)):

```
Hub1(config)#interface range DP 0 - 7
Hub1(config-if)#crypto map L2VPN_HUB1_AND_SPOKE1
Hub1(config-if)#exit
```

2.9. Прикрепите крипто-карту `L2VPN_HUB1_AND_SPOKE2` к `DP` интерфейсам из диапазона 8 – 15 (эти номера соответствуют потокам обработки трафика второго LAN порта (PORT3 в ipsm_dpdk.cfg)):

```
Hub1(config)#interface range DP 8 - 15
Hub1(config-if)#crypto map L2VPN_HUB1_AND_SPOKE2
Hub1(config-if)#exit
```

2.10. Примените настройки:

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

3. Параметры IPsec для защиты удаленного управления криптошлюзом.

3.1. Задайте IKECFG пул, из которого будет выдаваться IP адрес компьютеру администратора

```
Hub1(config)#ip local pool ADMIN_ADDRESS 192.168.255.1
```

3.2. Создайте расширенный список доступа (ACL) для трафика, который требуется защищать (в качестве локального адреса указывается адрес Mgmt интерфейса, а в качестве удаленного адреса – адрес из IKECFG пула):

```
Hub1(config)#ip access-list extended ADMIN_ACL
Hub1(config-ext-nacl)#remark MGMT IP
Hub1(config-ext-nacl)#permit ip host 192.168.253.1 host 192.168.255.1
```

```
Hub1(config-ext-nacl)#exit
```

3.3. Создайте динамическую криптокарту (имя `MGMT`, раздел 1):

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

3.3.1. Укажите список доступа для защищаемого трафика:

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

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

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

3.3.3. Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

3.3.4. Укажите IKECFG пул:

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

3.3.5. Включите префрагментацию:

```
Hub1(config-crypto-map)#set pre-fragmentation
```

3.3.6. Включите автоматическую и интеллектуальную корректировку значения MSS:

```
Hub1(config-crypto-map)#set security-association mss-fix out
```

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

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

3.4. Создайте криптокарту (имя L3VPN, раздел 1) и добавьте туда динамическую криптокарту MGMT:

```
Hub1(config)#crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
```

3.5. Прикрепите созданную криптокарту `L3VPN` к внешнему интерфейсу `vEthernet0`:

```
Hub1(config)#interface vEthernet 0
Hub1(config-if)#description WAN
Hub1(config-if)#crypto map L3VPN
```

3.6. Примените настройки:

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

Настройка политики обработки COC (CRL)

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

Включите проверку COC и настройте автоматическую загрузку и импортирование в базу Продукта списка отозванных сертификатов с HTTP сервера CRL-distribution-point.

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка межсетевого экрана

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

```
Hub1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hub1(config)#object-group network SELF
Hub1(config-network-group)#remark WAN IP
Hub1(config-network-group)#host 172.16.100.2
Hub1(config-network-group)#host 172.16.101.2
Hub1(config-network-group)#exit
```

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

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

3. Создайте ACL с именем FW_INPUT_DP для входящего на DP интерфейсы трафика:

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

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

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

5. Прикрепите правила межсетевого экранирования на WAN интерфейсы `vEthernet0 и vEthernet2`:

```
Hub1(config)#interface vEthernet0
Hub1(config-if)#ip access-group FW_INPUT_WAN in
Hub1(config-if)#ip inspect INSPECT out
Hub1(config-if)#exit
Hub1(config)#interface vEthernet2
Hub1(config-if)#ip access-group FW_INPUT_WAN in
Hub1(config-if)#ip inspect INSPECT out
Hub1(config-if)#exit
```

6. Прикрепите правила межсетевого экранирования на все DP интерфейсы:

```
Hub1(config)#interface range DP 0 - 15
Hub1(config-if-range)#ip access-group FW_INPUT_DP in
Hub1(config-if-range)#exit
```

7. Примените настройки:

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

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP;
- Конфигурация L2 (data plane).

Настройка криптошлюза Spoke1

Начальные настройки

Начальные настройки производятся аналогично соответствующим настройкам на криптошлюзе Hub1 до момента настройки мастера настроек L2 (data plane).

1. Нажмите Enter, после чего запустится мастер начальных настроек L2 (data plane). Данный мастер изменяет файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`, который используется сервисом `ipsmapp`:

```
Configuring IPSM:
```

```
This script will stop ipsmapp daemon and create new ipsm_dpdk.cfg. All ipsmapp settings
will be reset. Do you want to continue? [Yes]
```

```
INFO: Binding network devices to their original drivers
INFO: Device "0000:03:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:0b:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:13:00.0" is already bound to driver "vmxnet3". Skipping
```

1.1. Укажите количество портов (количество физических LAN и WAN интерфейсов для L2, Mgmt интерфейсы не учитываются):

```
Enter amount of ports (2-2) [2] : 2
```

1.2. Введите количество потоков обработки трафика (количество потоков соответствует количеству `DP<N>` интерфейсов):

Обратите внимание, что число потоков должно совпадать с числом потоков на первом LAN порту криптошлюза Hub1 (в данном сценарии это число – 8).

```
threads (1-36) [36] : 8
```

1.3. Выберите из предложенного списка PCI адрес для WAN порта. PORT0 – WAN интерфейс.

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |       -       | vmxnet3 |
| 1 | 0000:0b:00.0 |       -       | vmxnet3 |
| 2 | 0000:13:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

Данный список сформирован из всех физических сетевых интерфейсов, которые есть в криптошлюзе. В каждом конкретном случае PCI адреса могут отличаться.

```
Enter device index to be configured as WAN interface "PORT0" (0-2): 0
```

```
INFO: Configuring device "0000:03:00.0" as "PORT0"
```

1.4. Укажите IP адрес WAN интерфейса (в данном сценарии - 172.16.1.2). Данный IP адрес будет назначен на интерфейс `vEthernet0`:

```
Enter IP-address for WAN interface (l3_ip/l3_ip6) (allowed_protocols: ipv4,ipv6):
172.16.1.2
```

1.5. Укажите маску для IP адреса WAN интерфейса (в данном сценарии - 24):

```
Enter netmask for WAN interface (0-32) [24] 24
```

1.6. Укажите адрес шлюза по умолчанию для транзитного L2 (data plane) зашифрованного трафика (в данном сценарии – 172.16.1.1):

```
Enter default gateway IP-address (gw_ip) (allowed_protocols: ipv4): 172.16.1.1
```

1.7. Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

1.8. Выберите из вновь предложенного списка PCI адрес для LAN порта. PORT1 – LAN интерфейс:

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:0b:00.0 |       -       | vmxnet3 |
| 2 | 0000:13:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

Из списка выше видно, что WAN порт уже сконфигурирован («PORT0» в столбце «Configured as»):

```
Enter device index to be configured as LAN interface "PORT1" and paired with "PORT0"
(0-2): 1
```

1.9. Укажите IP адрес источника для EtherIP туннеля (в данном сценарии – 172.16.1.2):

```
Enter source IP-address for l2-tunnel (l2_src_ip) (allowed_protocols: ipv4,ipv6):
172.16.1.2
```

1.10. Укажите IP адрес назначения для EtherIP туннеля (в данном сценарии – 172.16.100.2):

```
Enter destination IP-address for l2-tunnel (l2_dst_ip) (allowed_protocols: ipv4):
172.16.100.2
```

1.11. Задайте MTU для WAN и LAN интерфейсов (в данном сценарии – 9000):

```
Enter MTU for WAN interface (68-9700) [9700] : 9000
Enter MTU for LAN interface (68-9700) [9600] : 9000
```

1.12. Нажмите Enter, если все параметры введены верно:

```
Is the above data correct? [Yes]
```

1.13. Дождитесь окончания процедуры инициализации и мастера настроек:

```
+---+--------------+--------------+---------+
|   |    PCI id    | Configured as | driver  |
+---+--------------+--------------+---------+
| 0 | 0000:03:00.0 |     PORT0     | vmxnet3 |
| 1 | 0000:0b:00.0 |     PORT1     | vmxnet3 |
| 2 | 0000:13:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
INFO: Operation completed successfully. Restart your system to apply the changes
INFO: OK

################################################################################
Network traffic is blocked.
To unblock network traffic, please setup the network security policy
or use "run csconf_mgr activate" command to activate the predefined
permissive network security policy now.
```

1.14. Включите прохождение сетевого трафика, загрузив предопределенную разрешающую политику:

```
administrator@sterragate] run csconf_mgr activate
```

Начальные настройки завершены.

Настройка L2

Настройка параметров L2 производится аналогично настройкам L2 на криптошлюзе Hub1 до момента настройки распределения потоков обработки трафика по портам.

Параметры `thr_start` и `thr_count` задавать не требуется, по умолчанию все потоки будут назначены на LAN порт.

Настройки PKI (запросы и сертификаты)

Настройка производится аналогично настройкам на криптошлюзе Hub1.

Настройка паролей доступа к консоли cisco-like

Настройка производится аналогично настройкам на криптошлюзе Hub1.

Настройка сетевых параметров

Настройка производится аналогично настройкам на криптошлюзе Hub1.

Настройка шифрования

1. Параметры IKE.

   1.1 Задайте общие параметры IKE:

```
Spoke1(config)#crypto isakmp identity dn
Spoke1(config)#crypto isakmp keepalive 3 2
Spoke1(config)#crypto isakmp keepalive retry-count 5
Spoke1(config)#crypto isakmp fragmentation
Spoke1(config)#crypto isakmp security-association lifetime delta 50
Spoke1(config)#crypto isakmp initiator-sessions-max 100
Spoke1(config)#crypto isakmp responder-sessions-max 100
```

   1.2 Создайте политику, описывающую параметры IKE туннеля:

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

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

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

2. Параметры IPsec для защиты транзитного L2 трафика.

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

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

   2.2. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика, которым будет защищаться L3 трафик управления:

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

   2.3. Задайте комбинированный алгоритм шифрования и имитозащиты (набор преобразований) для трафика (транспортный режим), которым будет защищаться L2 трафик между центральным офисом и филиалом:

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

   2.4. Создайте список доступа (ACL) для транзитного инкапсулированного в EtherIP пользовательского трафика, который нужно защищать между центральным офисом и первым филиалом:

```
Spoke1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
Spoke1(config-ext-nacl)# remark EtherIP L2 tunnel
Spoke1(config-ext-nacl)# permit 97 host 172.16.1.2 host 172.16.100.2
```

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

2.5. Создайте крипто-карту (имя L2VPN_HUB1_AND_SPOKE1, раздел 1):

```
Spoke1(config)#crypto map L2VPN_HUB1_AND_SPOKE1 1 ipsec-isakmp
```

2.5.1 Укажите список доступа для защищаемого трафика:

```
Spoke1(config-crypto-map)# match address IPSEC_ACL_HUB1_AND_SPOKE1
```

2.5.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

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

2.5.3 Укажите IP адрес партнера по IPsec, это внешний IP адрес первого WAN интерфейса криптошлюза Hub1:

```
Spoke1(config-crypto-map)# set peer 172.16.100.1
```

2.5.4 Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

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

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

2.5.6 Включите префрагментацию:

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

2.6. Прикрепите крипто-карту `L2VPN_HUB1_AND_SPOKE1` ко всем `DP` интерфейсам (они соответствуют потокам обработки трафика LAN порта (PORT1 в ipsm_dpdk.cfg)):

```
Spoke1(config)# interface range DP 0 - 7
Spoke1(config-if)# crypto map L2VPN_HUB1_AND_SPOKE1
Spoke1(config-if)# exit
```

2.7. Примените настройки:

```
Spoke1(config-if)# end
```

2.8. **Важно!** Убедитесь, что значения параметра `crypto ipsec stream-id` на интерфейсах DP 0 – 7 криптошлюза Spoke1 совпадают со значениями на интерфейсах DP 0 – 7 криптошлюза Hub1. Проверить это можно в выводе команды `show running-config`:

```
Spoke1# show running-config
```

```
...
!
interface DP0
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1000
!
interface DP1
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1001
!
interface DP2
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1002
!
interface DP3
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1003
!
interface DP4
 crypto map L2VPN_HUB1_AND_SPOKE1
```

```
 crypto ipsec stream-id 1004
!
interface DP5
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1005
!
interface DP6
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1006
!
interface DP7
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1007
!
...
```

Видно, что значения `crypto ipsec stream-id` на соответствующих интерфейсах DP совпадают.

Если значения этого параметра на шлюзах различаются, то следует отредактировать значение на одном из криптошлюзов, например на Spoke1. Для этого перейдите обратно в режим конфигурации:

```
Spoke1#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Spoke1(config)#
```

Перейдите в режим конфигурации интерфейса, на котором следует изменить данный параметр (например, если нужно выставить значение `stream-id` равное 1023 на интерфейсе DP 0) и задайте нужное значение:

```
Spoke1(config)#interface dp 0
Spoke1(config-if)#crypto ipsec stream-id 1023
Spoke1(config-if)#exit
```

3. Параметры IPsec для защиты удаленного управления криптошлюзом.

3.1. Перейдите в режим конфигурации:

```
Spoke1#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

3.2. Задайте IKECFG пул, из которого будет выдаваться IP адрес компьютеру администратора

```
Spoke1(config)#ip local pool ADMIN_ADDRESS 192.168.255.2
```

3.3. Создайте расширенный список доступа (ACL) для трафика, который требуется защищать (в качестве локального адреса указывается адрес Mgmt интерфейса, а в качестве удаленного адреса – адрес из IKECFG пула):

```
Spoke1(config)#ip access-list extended ADMIN_ACL
Spoke1(config-ext-nacl)#remark MGMT IP
Spoke1(config-ext-nacl)#permit ip host 192.168.254.1 host 192.168.255.2
Spoke1(config-ext-nacl)#exit
```

3.4. Создайте динамическую криптокарту (имя `MGMT`, раздел 1):

```
Spoke1(config)#crypto dynamic-map MGMT 1
```

3.4.1. Укажите список доступа для защищаемого трафика:

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

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

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

3.4.3. Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

3.4.4. Укажите IKECFG пул:

```
Spoke1(config-crypto-map)#set pool ADMIN_ADDRESS
```

3.4.5. Включите префрагментацию:

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

3.4.6. Включите автоматическую и интеллектуальную корректировку значения MSS:

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

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

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

3.5. Создайте криптокарту (имя L3VPN, раздел 1) и добавьте туда динамическую криптокарту MGMT:

```
Spoke1(config)#crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
```

3.6. Прикрепите созданную криптокарту `L3VPN` к внешнему интерфейсу `vEthernet0`:

```
Spoke1(config)#interface vEthernet 0
Spoke1(config-if)#description WAN
Spoke1(config-if)#crypto map L3VPN
```

3.7. Примените настройки:

```
Spoke1(config-if)#end
```

Настройка политики обработки COC (CRL)

Настройка производится аналогично настройкам на криптошлюзе Hub1.

Настройка межсетевого экрана

Настройка производится аналогично настройкам на криптошлюзе Hub1.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP;
- Конфигурация L2 (data plane).

Настройка криптошлюза Spoke2

Настройка криптошлюза Spoke2 происходит аналогично настройке Spoke1.

Число потоков обработки трафика следует выставлять такое же, какое было задано для второго LAN порта криптошлюза Hub1.

Важно! После этапа настройки шифрования, убедитесь, что значения параметра `crypto ipsec stream-id` на интерфейсах DP 0 – 7 криптошлюза Spoke2 совпадают со значениями на интерфейсах DP 8 – 15 криптошлюза Hub1, в противном случае значения следует заменить на совпадающие.

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP;
- Конфигурация L2 (data plane).

Проверка работоспособности стенда

Проверку работоспособности нужно выполнять после завершения настройки всех устройств стенда.

Проверка IP связности

1. Проверьте, что с криптошлюзов Hub1, Spoke1 и Spoke2 по ICMP доступен шлюз по умолчанию (Router1). Для этого выполните команду `ping` из cisco-like консоли криптошлюзов.

```
Hub1#ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=1.64 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.999 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=2.55 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.856 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=1.36 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4035ms
rtt min/avg/max/mdev = 0.856/1.481/2.552/0.601 ms
```

```
Hub1#ping 172.16.101.1
```

```
PING 172.16.101.1 (172.16.101.1) 100(128) bytes of data.
108 bytes from 172.16.101.1: icmp_seq=1 ttl=64 time=1.67 ms
108 bytes from 172.16.101.1: icmp_seq=2 ttl=64 time=1.03 ms
108 bytes from 172.16.101.1: icmp_seq=3 ttl=64 time=0.712 ms
108 bytes from 172.16.101.1: icmp_seq=4 ttl=64 time=0.942 ms
108 bytes from 172.16.101.1: icmp_seq=5 ttl=64 time=0.941 ms

--- 172.16.101.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.712/1.060/1.673/0.324 ms
```

```
Spoke1#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=0.824 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.911 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.835 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=0.966 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=1.47 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.824/1.000/1.468/0.239 ms
```

```
Spoke2#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=0.556 ms
108 bytes from 172.16.2.1: icmp_seq=2 ttl=64 time=0.969 ms
108 bytes from 172.16.2.1: icmp_seq=3 ttl=64 time=1.16 ms
108 bytes from 172.16.2.1: icmp_seq=4 ttl=64 time=0.889 ms
108 bytes from 172.16.2.1: icmp_seq=5 ttl=64 time=0.782 ms

--- 172.16.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4030ms
rtt min/avg/max/mdev = 0.556/0.871/1.160/0.200 ms
```

   Видно, что устройство Router1 доступно по ICMP как с Hub1, так и со Spoke1 и Spoke2.

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

```
Hub1#ping 172.16.1.2
```

```
PING 172.16.1.2 (172.16.1.2) 100(128) bytes of data.
108 bytes from 172.16.1.2: icmp_seq=1 ttl=63 time=24.0 ms
108 bytes from 172.16.1.2: icmp_seq=2 ttl=63 time=15.0 ms
108 bytes from 172.16.1.2: icmp_seq=3 ttl=63 time=14.1 ms
108 bytes from 172.16.1.2: icmp_seq=4 ttl=63 time=9.63 ms
108 bytes from 172.16.1.2: icmp_seq=5 ttl=63 time=11.2 ms

--- 172.16.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 9.632/14.821/24.064/5.013 ms
```

```
Hub1#ping 172.16.2.2
```

```
PING 172.16.2.2 (172.16.2.2) 100(128) bytes of data.
108 bytes from 172.16.2.2: icmp_seq=1 ttl=63 time=8.14 ms
108 bytes from 172.16.2.2: icmp_seq=2 ttl=63 time=6.59 ms
108 bytes from 172.16.2.2: icmp_seq=3 ttl=63 time=4.67 ms
108 bytes from 172.16.2.2: icmp_seq=4 ttl=63 time=11.1 ms
108 bytes from 172.16.2.2: icmp_seq=5 ttl=63 time=9.85 ms

--- 172.16.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 4.676/8.093/11.195/2.308 ms
```

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

Проверка PKI

Проверьте, что на криптошлюзах СОС импортирован в базу Продукта и все сертификаты имеют статус Active. Подробная проверка приведена в базовом сценарии

Проверка построения защищенного L2 соединения между криптошлюзами

1. Инициируйте построение защищенного L2 соединения между криптошлюзами Hub1 и Spoke1, Hub1 и Spoke2 с любого из защищаемых устройств. Например, выполните проверку доступности устройств Host-b-hub1 и Host-b-spoke2 с устройства Host-b-spoke1.

   1.1. Выполните команду `ping` из linux bash консоли защищаемого устройства Host-b-spoke1.

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

```
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=64 time=1.83 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=1.74 ms
64 bytes from 192.168.100.100: icmp_seq=5 ttl=64 time=1.86 ms

--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 1.568/1.737/1.864/0.109 ms
```

   1.2. Выполните команду `ping` из linux bash консоли защищаемого устройства Host-b-spoke1.

```
root@Host-b-spoke1:~# ping 192.168.100.102 -c 5
```

```
PING 192.168.100.102 (192.168.100.102) 56(84) bytes of data.
64 bytes from 192.168.100.102: icmp_seq=1 ttl=64 time=3.71 ms
64 bytes from 192.168.100.102: icmp_seq=2 ttl=64 time=3.88 ms
64 bytes from 192.168.100.102: icmp_seq=3 ttl=64 time=4.18 ms
64 bytes from 192.168.100.102: icmp_seq=4 ttl=64 time=4.01 ms
64 bytes from 192.168.100.102: icmp_seq=5 ttl=64 time=3.82 ms

--- 192.168.100.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
```

```
rtt min/avg/max/mdev = 3.712/3.921/4.182/0.179 ms
```

2. Проверьте, что на криптошлюзах Hub1, Spoke1 и Spoke2 установлены защищенные IPsec соединения. Для этого выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

```
Hub1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 10 (172.16.101.2,500)-(172.16.2.2,500) active 4536 4492
2 11 (172.16.100.2,500)-(172.16.1.2,500) active 4556 4472

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 33 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 416
2 34 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 416 312
3 35 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 416
4 36 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 416 312
5 37 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
6 38 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
7 39 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
8 40 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
9 41 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
10 42 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
11 43 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
12 44 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
13 45 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
14 46 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
15 47 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
16 48 (172.16.101.2,*)-(172.16.2.2,*) 97 ESP trans 312 312
```

```
Spoke1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 5 (172.16.1.2,500)-(172.16.100.2,500) active 4472 4556

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 18 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 416
2 19 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 416 312
3 20 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
4 21 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
5 22 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
6 23 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
7 24 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
8 25 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 312 312
```

```
Spoke2#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 10 (172.16.2.2,500)-(172.16.101.2,500) active 4492 4536

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 16 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 416 312
2 17 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 416
3 18 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
```

```
4 19 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
5 20 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
6 21 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
7 22 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
8 23 (172.16.2.2,*)-(172.16.101.2,*) 97 ESP trans 312 312
```

Видно, что на криптошлюзах Hub1, Spoke1 и Spoke2 установлены защищенные IPsec соединения (количество защищенных IPsec соединений должно совпадать со значением параметра threads, указанно в мастере настроек L2). Если этого не произошло, то проверьте файл журнала (команда `run less /var/log/cspvpngate.log`). При необходимости увеличьте уровень логирования (команда `logging trap debugging` в консоли cisco-like) и заново инициируйте защищенное соединение.

Подробная проверка работоспособности стенда и диагностика описаны в сценарии «Построение L2 VPN туннеля между двумя «С-Терра Шлюз DP».

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username           cscons           privilege           15           secret           5
$y$j9T$6FE.F1idmCPYp3/uvlNVp0$ZEdonJTEpjrnfYFBgHlbh4dRVTK01n3ogE6EuohUUH2
aaa new-model
!
!
hostname Hub1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
ip local pool ADMIN_ADDRESS 192.168.255.1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT esp-magma-mgm
 mode transport
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
 host 172.16.101.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.100.2 host 172.16.1.2
!
```

```
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE2
 remark EtherIP L2 tunnel
 permit etherip host 172.16.101.2 host 172.16.2.2
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FW_INPUT_DP
 permit udp any object-group SELF eq non500-isakmp
 permit esp any object-group SELF
!
ip access-list extended ADMIN_ACL
 remark MGMT IP
 permit ip host 192.168.253.1 host 192.168.255.1
!
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 MGMT 1
 match address ADMIN_ACL
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool ADMIN_ADDRESS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN_HUB1_AND_SPOKE1 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set local-address 172.16.100.2
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN_HUB1_AND_SPOKE2 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE2
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set local-address 172.16.101.2
 set peer 172.16.2.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
!
interface TenGigabitEthernet0/0
 ip address 192.168.253.1 255.255.255.0
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1000
```

```
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1001
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1007
!
interface DP8
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1008
!
interface DP9
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1009
!
interface DP10
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1010
!
interface DP11
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1011
!
interface DP12
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1012
!
interface DP13
```

```
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1013
!
interface DP14
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1014
!
interface DP15
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1015
!
interface vEthernet0
 description WAN
 ip address 172.16.100.2 255.255.255.0
 mtu 9000
 ip access-group FW_INPUT_WAN in
 crypto map L3VPN
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
 no ip address
 mtu 9000
!
interface vEthernet2
 description WAN
 ip address 172.16.101.2 255.255.255.0
 mtu 9000
 ip access-group FW_INPUT_WAN in
 ip inspect INSPECT out
!
interface vEthernet3
 description LAN
 no ip address
 mtu 9000
!
!
ip route 172.16.1.2 255.255.255.255 172.16.100.1
ip route 172.16.2.2 255.255.255.255 172.16.101.1
ip route 0.0.0.0 0.0.0.0 172.16.100.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group 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:   Thu Dec 25 12:01:20 2025
```

```
GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Thu Dec 25 12:01:20 2025 (user: root)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 172.16.1.2/32
            Gateway = 172.16.100.1
        ),
        Route(
            Destination = 172.16.2.2/32
            Gateway = 172.16.101.1
        ),
        Route(
            Destination = 0.0.0.0/0
            Gateway = 172.16.100.1
        )

)

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

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

ESPProposal MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP
```

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

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

FilterChain FilterChain:FW_INPUT_DP (
    Filters = Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

```
FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.101.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))
```

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

AddressPool ADMIN_ADDRESS
(
    IPAddresses = 192.168.255.1
)

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

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

IKERule IKERule:L2VPN_HUB1_AND_SPOKE1:1
(
    IKEPeerIPFilter = 172.16.1.2
    IKELocalIPFilter = 172.16.100.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:L2VPN_HUB1_AND_SPOKE2:1
(
    IKEPeerIPFilter = 172.16.2.2
    IKELocalIPFilter = 172.16.101.2
    Transform = crypto:isakmp:policy:1
```

```
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 20
)

IKERule IKERule:L3VPN:1:MGMT:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    IKECFGPool          = ADMIN_ADDRESS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

IPsecAction IPsecAction:L2VPN_HUB1_AND_SPOKE1:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN_HUB1_AND_SPOKE1:1
)

IPsecAction IPsecAction:L2VPN_HUB1_AND_SPOKE2:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN_HUB1_AND_SPOKE2:1
)

IPsecAction IPsecAction:L3VPN:1:MGMT:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:L3VPN:1:MGMT:1
)

const IPsecPolicy:L2VPN_HUB1_AND_SPOKE1 = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.100.2
        DestinationIP = 172.16.1.2
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN_HUB1_AND_SPOKE1:1 >
```

```
        LogEventID                                                                  =
"IPsec:Protect:L2VPN_HUB1_AND_SPOKE1:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1000 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1001 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1002 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1003 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1004 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1005 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1006 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1007 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1007
)

const IPsecPolicy:L2VPN_HUB1_AND_SPOKE2 = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.101.2
        DestinationIP = 172.16.2.2
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN_HUB1_AND_SPOKE2:1 >
        LogEventID                                                                  =
"IPsec:Protect:L2VPN_HUB1_AND_SPOKE2:1:IPSEC_ACL_HUB1_AND_SPOKE2"
    )
)
```

```
FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1008 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1009 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1010 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1011 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1012 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1013 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1014 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1015 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1015
)

FilterChain IPsecPolicy:L3VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.253.1
        DestinationIP = 192.168.255.1
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L3VPN:1:MGMT:1 >
        LogEventID = "IPsec:Protect:L3VPN:1:MGMT:1:ADMIN_ACL"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1001
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1005
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1007
)
```

```
NetworkInterface (
    LogicalName = "DP8"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1008
)

NetworkInterface (
    LogicalName = "DP9"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1009
)

NetworkInterface (
    LogicalName = "DP10"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1010
)

NetworkInterface (
    LogicalName = "DP11"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1011
)

NetworkInterface (
    LogicalName = "DP12"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1012
)

NetworkInterface (
    LogicalName = "DP13"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1013
)

NetworkInterface (
    LogicalName = "DP14"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1014
)

NetworkInterface (
    LogicalName = "DP15"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1015
)

NetworkInterface (
    LogicalName = "vEthernet0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:L3VPN
```

```
)

NetworkInterface (
    LogicalName = "vEthernet1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "vEthernet2"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
)

NetworkInterface (
    LogicalName = "vEthernet3"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

3. Конфигурация L2 (data plane).

Файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`:

```
[PERFORMANCE]
threads = 16                        ;maximum: (cpu core num (maximum:254, including
HyperThreading) - 2 - 3 * ports_num) -- processing (encrypt/decrypt/filter) threads
number
no_max_freq = yes
;sendqueue_size = 64000     ;min: 1000 max: 200000 default: 64000 -- size of re-order
fixing queue
;disable_sendqueue = no     ;yes/no, default: no -- disable re-order fixing queue
;tx_retries = 10           ;min: 0 max: 1000 default: 10 -- retries count for outgoing
packets before drop
;tx_delay = 20                ;min: 0 max: 200 default: 20 -- delay in microseconds
before another retry of sending packet burst
;rx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of rx descriptors
in network adapter configuration
;tx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of tx descriptors
in network adapter configuration
;no_max_freq = no             ;yes/no, default: no -- disable setting max possible
frequency for our processor cores
;sendq_burst_threshold = 0   ;min: 100 max: 100000 default: 0 (disabled) -- make a
delay, if sending N packets from sendqueue in a row
;sendq_burst_delay = 10     ;min: 1 max: 200 default: 10 -- delay in microseconds when
sendq_burst_threshold activated
;pcap_mpool_size = 262143   ;min: 6736: max 4194303: default: auto -- number of buffers
in single memory pool, 1 pool per port
;rx_queue_len = 16          ;min: 1 max: 32 default: 16 -- size of thread queue (in
bursts)
;rx_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
rx thread if there are no packets incoming
;tx_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
tx thread if there are no packets to send
;wrk_sleep = 50            ;min: 0 max: 10000 default: 50 -- pause in microseconds on
wrk thread if there are no packets incoming
;kni_sleep = 50            ;min: 0 max: 10000 default: 50 -- pause in microseconds on
kni thread if there are no packets incoming or outgoing
;cb_wait = 50               ;min: 0 max: 10000 default: 50 -- wait in microseconds on
wrk thread if corresponding tx thread is busy
;rx_cache_size = 64000     ;min: 2000: max 200000: default: 64000 -- size of rx thread
packet cache
```

```
;wrk_overload_thresh = 90   ;min: 1: max 100: default: 90 -- threshold (in %) of wrk
thread queue fill when it counts as "overloaded"

[EAL]
corelist = 0-43
;coremask = 0x1              ;mask of cpu cores to run on, including HyperThreading
;corelist = 0-1             ;list of cpu cores to run on, including HyperThreading
;channels = 1               ;min: 1 max: 8 default: 1    -- memory channels number
;cpuset    =    (0-2,4)@(0-1)                    ;map    threads    to    cpu    cores:
<threads[@cpus]>[<,threads[@cpus]>...]
;eal_log_level = 4          ;min: 1 max: 8 default: 4    -- log level of dpdk messages
;rx_pthresh = 8               ;min: 0 max: 255 default: 8   -- rx prefetch threshold
register value
;rx_hthresh = 8             ;min: 0 max: 255 default: 8  -- rx host threshold register
value
;rx_wthresh = 4              ;min: 0 max: 255 default: 4  -- rx write-back threshold
register value
;tx_pthresh = 36              ;min: 0 max: 255 default: 36 -- tx prefetch threshold
register value
;tx_hthresh = 0             ;min: 0 max: 255 default: 0  -- tx host threshold register
value
;tx_wthresh = 0              ;min: 0 max: 255 default: 0  -- tx write-back threshold
register value

[MISC]
print_stats = yes          ;yes/no, default: yes -- print send/receive/drop statistics
stats_file = /tmp/pkt_stats.txt    ;name of file for print_stats
;stats_file_size = 10       ;min: 1 max: 100 default: 10 -- max size of statistics file
in megabytes. After rotate, previous instance saves as ".old"
;stats_period = 1              ;min: 1: max: 86400 default: 1 -- at this period (in
seconds) statistics is collected
;print_frames = no          ;yes/no, default: no -- print incoming/outgoing packets in
hex
;frames_file = /tmp/frames.txt      ;name of file for print_frames
;frames_file_size = 50      ;min: 1 max: 200 default: 50 -- max size of packet hexdump
file in megabytes. After roteate, previous instance saves as ".old"
;frames_time = no             ;yes/no, default: no -- print time for each packet in
print_frames
rte_log_file = /tmp/rte_log.txt    ;name of file for dpdk log messages
;rte_log_file_size = 10     ;min: 1 max: 100 default: 10 -- max size of rte_log file
in megabytes. After rotate, previous instance saves as ".old"
;pf_max_bytes = 42          ;min: 14 max: 1400 default: 42 -- print only N firs bytes
in print_frames
;natt_port = 4500           ;min: 1 max: 65535: default: 4500
;enable_pdump = no          ;yes/no, default: no -- enable packet dump with dpdk-pdump
utility
;macaddr_update_period = 200;min:1 max: 10000 default: 200 -- gateway mac address
update period in milliseconds
;kmod_name = igb_uio       ;igb_uio/vfio-pci/uio_pci_generic, default: igb_uio -- name
of kernel module for port binding


[PORT0]
pci_id = 0000:03:00.0
l3_ip = 172.16.100.2/24
gw_ip = 172.16.100.1
pair_port = 1
mtu = 9000
outer = yes ;yes/no, default: no -- consider port as looking to  outer network; outer
port can't be in l2-mode
;next_hop_mac = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv4
frames
```

```
;next_hop_mac6 = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv6
frames
;next_hop_mac_force = no ;yes/no, default no -- always set next_hop_mac as destination
mac address for outgoing IPv4 frames
;next_hop_mac6_force = no ;yes/no, default no -- always set next_hop_mac6 as destination
mac address for outgoing IPv6 frames
;dp_frag_ip = 0.0.0.0 ;default: disabled -- ip addresses (4 max, "," as divider) of
gate dp partners for this port
;dp_frag_ip6 =  ;disabled -- ipv6 addresses (4 max, "," as divider) of gate dp ipv6
partners for this port
;dp_frag_natt = no ;yes/no, default no -- enable fragmentation fix for natt
;frag_id_afterward = no ;yes/no, default no -- set frag id before send
;vlan_identifier = 0 ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier (VID)
;vlan_priority_code_point = 0 ;min: 0 max: 7 default: 0 -- Priority code point (PCP)
which refers to the 802.1p class of service
;allowed_ethertypes = none ;ethertypes in hex (32 max, "," as divider) -- pass this
ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = yes ;yes/no, default: yes (for l2-port port - no) -- disable promiscuous
mode on this port
;multicast_enable = yes ;yes/no, default: yes (for l2-port - no) -- enable receiving
all multicast ip packets mode on this port
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
;pmtud = 8000 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination
Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
;mssfix = 8000 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value

[PORT1]
pci_id = 0000:04:00.0
l2_src_ip = 172.16.100.2
l2_dst_ip = 172.16.1.2
pair_port = 0
mtu = 9000
thr_start = 0 ;min: 0 max: <threads - 1> -- first processing thread for this port
thr_count = 8 ;min: 1 max: <threads - thr_start> -- number of processing threads for
this port
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = no ;yes/no, default: no (for outer port - yes) -- disable promiscuous
mode on this port
;multicast_enable = no ;yes/no, default: no (for outer port - yes) -- enable receiving
all multicast ip packets mode on this port
;copy_tos = no ;yes/no, default: no -- copy ToS-field from orig ip header to l2-
encapsulation ip header
;df_handling = clear ;copy/set/clear, default clear -- DF bit: copy from orig ip header
to l2-encapsulation ip header
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value
```

```
[PORT2]
pci_id = 0000:0b:00.0
l3_ip = 172.16.101.2/24
gw_ip = 172.16.101.1
pair_port = 3
mtu = 9000
outer = yes ;yes/no, default: no -- consider port as looking to  outer network; outer
port can't be in l2-mode
;next_hop_mac = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv4
frames
;next_hop_mac6 = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv6
frames
;next_hop_mac_force = no ;yes/no, default no -- always set next_hop_mac as destination
mac address for outgoing IPv4 frames
;next_hop_mac6_force = no ;yes/no, default no -- always set next_hop_mac6 as destination
mac address for outgoing IPv6 frames
;dp_frag_ip = 0.0.0.0 ;default: disabled -- ip addresses (4 max, "," as divider) of
gate dp partners for this port
;dp_frag_ip6 =  ;disabled -- ipv6 addresses (4 max, "," as divider) of gate dp ipv6
partners for this port
;dp_frag_natt = no ;yes/no, default no -- enable fragmentation fix for natt
;frag_id_afterward = no ;yes/no, default no -- set frag id before send
;vlan_identifier = 0 ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier (VID)
;vlan_priority_code_point = 0 ;min: 0 max: 7 default: 0 -- Priority code point (PCP)
which refers to the 802.1p class of service
;allowed_ethertypes = none ;ethertypes in hex (32 max, "," as divider) -- pass this
ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = yes ;yes/no, default: yes (for l2-port port - no) -- disable promiscuous
mode on this port
;multicast_enable = yes ;yes/no, default: yes (for l2-port - no) -- enable receiving
all multicast ip packets mode on this port
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
;pmtud = 8000 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination
Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
;mssfix = 8000 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value

[PORT3]
pci_id = 0000:0c:00.0
l2_src_ip = 172.16.101.2
l2_dst_ip = 172.16.2.2
pair_port = 2
mtu = 9000
thr_start = 8 ;min: 0 max: <threads - 1> -- first processing thread for this port
thr_count = 8 ;min: 1 max: <threads - thr_start> -- number of processing threads for
this port
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = no ;yes/no, default: no (for outer port - yes) -- disable promiscuous
mode on this port
;multicast_enable = no ;yes/no, default: no (for outer port - yes) -- enable receiving
all multicast ip packets mode on this port
;copy_tos = no ;yes/no, default: no -- copy ToS-field from orig ip header to l2-
encapsulation ip header
```

```
;df_handling = clear ;copy/set/clear, default clear -- DF bit: copy from orig ip header
to l2-encapsulation ip header
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$y$j9T$MGcpBCo8IRC6KHuiByNOq.$lT.4iLqROWthotvJZKSymLrRg4inTH6jjXwbD1yZhKD
aaa new-model
!
!
hostname Spoke1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
ip local pool ADMIN_ADDRESS 192.168.255.2
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT esp-magma-mgm
 mode transport
!
```

```
object-group network SELF
 remark WAN IP
 host 172.16.1.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.1.2 host 172.16.100.2
!
ip access-list extended ADMIN_ACL
 remark MGMT IP
 permit ip host 192.168.254.1 host 192.168.255.2
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FW_INPUT_DP
 permit udp any object-group SELF eq non500-isakmp
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map MGMT 1
 match address ADMIN_ACL
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool ADMIN_ADDRESS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN_HUB1_AND_SPOKE1 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set local-address 172.16.1.2
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
!
interface TenGigabitEthernet0/1
 ip address 192.168.254.1 255.255.255.0
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1000
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1001
```

```
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE1
 crypto ipsec stream-id 1007
!
interface vEthernet0
 description WAN
 ip address 172.16.1.2 255.255.255.0
 mtu 9000
 ip access-group FW_INPUT_WAN in
 crypto map L3VPN
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
 no ip address
 mtu 9000
!
!
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:   Thu Dec 25 12:03:32 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Dec 25 12:03:32 2025 (user: root)"
    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_TRANSPORT:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

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

```
    )
)

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

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 1
```

```
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

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

AddressPool ADMIN_ADDRESS
(
    IPAddresses = 192.168.255.2
)

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

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

```
IKERule IKERule:L2VPN_HUB1_AND_SPOKE1:1
(
    IKEPeerIPFilter = 172.16.100.2
    IKELocalIPFilter = 172.16.1.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:L3VPN:1:MGMT:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    IKECFGPool          = ADMIN_ADDRESS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

IPsecAction IPsecAction:L2VPN_HUB1_AND_SPOKE1:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN_HUB1_AND_SPOKE1:1
)

IPsecAction IPsecAction:L3VPN:1:MGMT:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:L3VPN:1:MGMT:1
)

const IPsecPolicy:L2VPN_HUB1_AND_SPOKE1 = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.1.2
        DestinationIP = 172.16.100.2
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN_HUB1_AND_SPOKE1:1 >
        LogEventID                                                                  =
"IPsec:Protect:L2VPN_HUB1_AND_SPOKE1:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)
```

```
FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1000 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1001 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1002 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1003 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1004 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1005 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1006 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1007 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE1
    StreamID = 1007
)

FilterChain IPsecPolicy:L3VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.254.1
        DestinationIP = 192.168.255.2
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L3VPN:1:MGMT:1 >
        LogEventID = "IPsec:Protect:L3VPN:1:MGMT:1:ADMIN_ACL"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1001
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1005
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE1:1007
)
```

```
NetworkInterface (
    LogicalName = "vEthernet0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:L3VPN
)

NetworkInterface (
    LogicalName = "vEthernet1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

3. Конфигурация L2 (data plane)

Файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`

```
[PERFORMANCE]
threads = 8                          ;maximum: (cpu core num (maximum:254, including
HyperThreading) - 2 - 3 * ports_num) -- processing (encrypt/decrypt/filter) threads
number
no_max_freq = yes
;sendqueue_size = 64000     ;min: 1000 max: 200000 default: 64000 -- size of re-order
fixing queue
;disable_sendqueue = no     ;yes/no, default: no -- disable re-order fixing queue
;tx_retries = 10           ;min: 0 max: 1000 default: 10 -- retries count for outgoing
packets before drop
;tx_delay = 20                ;min: 0 max: 200 default: 20 -- delay in microseconds
before another retry of sending packet burst
;rx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of rx descriptors
in network adapter configuration
;tx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of tx descriptors
in network adapter configuration
;no_max_freq = no             ;yes/no, default: no -- disable setting max possible
frequency for our processor cores
;sendq_burst_threshold = 0   ;min: 100 max: 100000 default: 0 (disabled) -- make a
delay, if sending N packets from sendqueue in a row
;sendq_burst_delay = 10     ;min: 1 max: 200 default: 10 -- delay in microseconds when
sendq_burst_threshold activated
;pcap_mpool_size = 262143   ;min: 6736: max 4194303: default: auto -- number of buffers
in single memory pool, 1 pool per port
;rx_queue_len = 16           ;min: 1 max: 32 default: 16 -- size of thread queue (in
bursts)
;rx_sleep = 50              ;min: 0 max: 10000 default: 50 -- pause in microseconds on
rx thread if there are no packets incoming
;tx_sleep = 50              ;min: 0 max: 10000 default: 50 -- pause in microseconds on
tx thread if there are no packets to send
;wrk_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
wrk thread if there are no packets incoming
;kni_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
kni thread if there are no packets incoming or outgoing
;cb_wait = 50               ;min: 0 max: 10000 default: 50 -- wait in microseconds on
wrk thread if corresponding tx thread is busy
;rx_cache_size = 64000     ;min: 2000: max 200000: default: 64000 -- size of rx thread
packet cache
;wrk_overload_thresh = 90   ;min: 1: max 100: default: 90 -- threshold (in %) of wrk
thread queue fill when it counts as "overloaded"

[EAL]
corelist = 0-43
;coremask = 0x1              ;mask of cpu cores to run on, including HyperThreading
;corelist = 0-1             ;list of cpu cores to run on, including HyperThreading
```

```
;channels = 1               ;min: 1 max: 8 default: 1    -- memory channels number
;cpuset    =    (0-2,4)@(0-1)                    ;map    threads    to    cpu    cores:
<threads[@cpus]>[<,threads[@cpus]>...]
;eal_log_level = 4          ;min: 1 max: 8 default: 4    -- log level of dpdk messages
;rx_pthresh = 8               ;min: 0 max: 255 default: 8  -- rx prefetch threshold
register value
;rx_hthresh = 8             ;min: 0 max: 255 default: 8  -- rx host threshold register
value
;rx_wthresh = 4              ;min: 0 max: 255 default: 4  -- rx write-back threshold
register value
;tx_pthresh = 36             ;min: 0 max: 255 default: 36 -- tx prefetch threshold
register value
;tx_hthresh = 0             ;min: 0 max: 255 default: 0  -- tx host threshold register
value
;tx_wthresh = 0              ;min: 0 max: 255 default: 0  -- tx write-back threshold
register value

[MISC]
print_stats = yes          ;yes/no, default: yes -- print send/receive/drop statistics
stats_file = /tmp/pkt_stats.txt    ;name of file for print_stats
;stats_file_size = 10       ;min: 1 max: 100 default: 10 -- max size of statistics file
in megabytes. After rotate, previous instance saves as ".old"
;stats_period = 1             ;min: 1: max: 86400 default: 1 -- at this period (in
seconds) statistics is collected
;print_frames = no          ;yes/no, default: no -- print incoming/outgoing packets in
hex
;frames_file = /tmp/frames.txt      ;name of file for print_frames
;frames_file_size = 50      ;min: 1 max: 200 default: 50 -- max size of packet hexdump
file in megabytes. After roteate, previous instance saves as ".old"
;frames_time = no             ;yes/no, default: no -- print time for each packet in
print_frames
rte_log_file = /tmp/rte_log.txt    ;name of file for dpdk log messages
;rte_log_file_size = 10     ;min: 1 max: 100 default: 10 -- max size of rte_log file
in megabytes. After rotate, previous instance saves as ".old"
;pf_max_bytes = 42          ;min: 14 max: 1400 default: 42 -- print only N firs bytes
in print_frames
;natt_port = 4500           ;min: 1 max: 65535: default: 4500
;enable_pdump = no          ;yes/no, default: no -- enable packet dump with dpdk-pdump
utility
;macaddr_update_period = 200;min:1 max: 10000 default: 200 -- gateway mac address
update period in milliseconds
;kmod_name = igb_uio       ;igb_uio/vfio-pci/uio_pci_generic, default: igb_uio -- name
of kernel module for port binding


[PORT0]
pci_id = 0000:03:00.0
l3_ip = 172.16.1.2/24
gw_ip = 172.16.1.1
pair_port = 1
mtu = 9000
outer = yes ;yes/no, default: no -- consider port as looking to  outer network; outer
port can't be in l2-mode
;next_hop_mac = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv4
frames
;next_hop_mac6 = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv6
frames
;next_hop_mac_force = no ;yes/no, default no -- always set next_hop_mac as destination
mac address for outgoing IPv4 frames
;next_hop_mac6_force = no ;yes/no, default no -- always set next_hop_mac6 as destination
mac address for outgoing IPv6 frames
```

```
;dp_frag_ip = 0.0.0.0 ;default: disabled -- ip addresses (4 max, "," as divider) of
gate dp partners for this port
;dp_frag_ip6 =  ;disabled -- ipv6 addresses (4 max, "," as divider) of gate dp ipv6
partners for this port
;dp_frag_natt = no ;yes/no, default no -- enable fragmentation fix for natt
;frag_id_afterward = no ;yes/no, default no -- set frag id before send
;vlan_identifier = 0 ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier (VID)
;vlan_priority_code_point = 0 ;min: 0 max: 7 default: 0 -- Priority code point (PCP)
which refers to the 802.1p class of service
;allowed_ethertypes = none ;ethertypes in hex (32 max, "," as divider) -- pass this
ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = yes ;yes/no, default: yes (for l2-port port - no) -- disable promiscuous
mode on this port
;multicast_enable = yes ;yes/no, default: yes (for l2-port - no) -- enable receiving
all multicast ip packets mode on this port
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
;pmtud = 8000 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination
Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
;mssfix = 8000 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value

[PORT1]
pci_id = 0000:0b:00.0
l2_src_ip = 172.16.1.2
l2_dst_ip = 172.16.100.2
pair_port = 0
mtu = 9000
;thr_start = 0 ;min: 0 max: <threads - 1> -- first processing thread for this port
;thr_count = <threads> ;min: 1 max: <threads - thr_start> -- number of processing
threads for this port
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = no ;yes/no, default: no (for outer port - yes) -- disable promiscuous
mode on this port
;multicast_enable = no ;yes/no, default: no (for outer port - yes) -- enable receiving
all multicast ip packets mode on this port
;copy_tos = no ;yes/no, default: no -- copy ToS-field from orig ip header to l2-
encapsulation ip header
;df_handling = clear ;copy/set/clear, default clear -- DF bit: copy from orig ip header
to l2-encapsulation ip header
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value
```

Конфигурации криптошлюза Spoke2

1. Консоль cisco-like

```
!
```

```
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$y$j9T$PcZ2YxzlYzXiog0cqX4.W/$FFxhjAvLEQKCsUGsYJ4yZkPHXFshhKhZqMPYyFvsvx1
aaa new-model
!
!
hostname Spoke2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
ip local pool ADMIN_ADDRESS 192.168.255.3
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT esp-magma-mgm
 mode transport
!
object-group network SELF
 remark WAN IP
 host 172.16.2.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE2
 remark EtherIP L2 tunnel
 permit etherip host 172.16.2.2 host 172.16.101.2
!
ip access-list extended ADMIN_ACL
 remark MGMT IP
 permit ip host 192.168.254.2 host 192.168.255.3
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
```

```
ip access-list extended FW_INPUT_DP
 permit udp any object-group SELF eq non500-isakmp
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map MGMT 1
 match address ADMIN_ACL
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool ADMIN_ADDRESS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN_HUB1_AND_SPOKE2 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE2
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set local-address 172.16.2.2
 set peer 172.16.101.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
!
interface TenGigabitEthernet0/1
 ip address 192.168.254.2 255.255.255.0
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1008
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1009
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1010
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1011
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1012
!
interface DP5
 ip access-group FW_INPUT_DP in
```

```
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1013
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1014
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN_HUB1_AND_SPOKE2
 crypto ipsec stream-id 1015
!
interface vEthernet0
 description WAN
 ip address 172.16.2.2 255.255.255.0
 mtu 9000
 ip access-group FW_INPUT_WAN in
 crypto map L3VPN
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
 no ip address
 mtu 9000
!
!
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:   Thu Dec 25 12:04:40 2025

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Thu Dec 25 12:04:40 2025 (user: root)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

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

```
)

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

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

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

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

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

FilterChain FilterChain:FW_INPUT_DP (
    Filters = Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 17
        DestinationPort = 4500
```

```
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.2.2
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        DestinationIP = ::/0
        Action = DROP
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

AddressPool ADMIN_ADDRESS
(
    IPAddresses = 192.168.255.3
)

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

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

IKERule IKERule:L2VPN_HUB1_AND_SPOKE2:1
(
    IKEPeerIPFilter = 172.16.101.2
    IKELocalIPFilter = 172.16.2.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IKERule IKERule:L3VPN:1:MGMT:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
```

```
    IKECFGPool          = ADMIN_ADDRESS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

IPsecAction IPsecAction:L2VPN_HUB1_AND_SPOKE2:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN_HUB1_AND_SPOKE2:1
)

IPsecAction IPsecAction:L3VPN:1:MGMT:1
(
    TunnelingParameters = TunnelEntry(
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:L3VPN:1:MGMT:1
)

const IPsecPolicy:L2VPN_HUB1_AND_SPOKE2 = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.2.2
        DestinationIP = 172.16.101.2
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN_HUB1_AND_SPOKE2:1 >
        LogEventID                                                                    =
"IPsec:Protect:L2VPN_HUB1_AND_SPOKE2:1:IPSEC_ACL_HUB1_AND_SPOKE2"
    )
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1008 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1009 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1010 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1011 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
```

```
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1012 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1013 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1014 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1015 (
    +IPsecPolicy:L2VPN_HUB1_AND_SPOKE2
    StreamID = 1015
)

FilterChain IPsecPolicy:L3VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.254.2
        DestinationIP = 192.168.255.3
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L3VPN:1:MGMT:1 >
        LogEventID = "IPsec:Protect:L3VPN:1:MGMT:1:ADMIN_ACL"
    )
)

NetworkInterface (
    LogicalName = "TenGigabitEthernet0/0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1008
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
```

```
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1009
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1010
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1011
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1012
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1013
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1014
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN_HUB1_AND_SPOKE2:1015
)

NetworkInterface (
    LogicalName = "vEthernet0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:L3VPN
)

NetworkInterface (
    LogicalName = "vEthernet1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

3. Конфигурация L2 (data plane)

   Файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`

```
[PERFORMANCE]
```

```
threads = 8                          ;maximum: (cpu core num (maximum:254, including
HyperThreading) - 2 - 3 * ports_num) -- processing (encrypt/decrypt/filter) threads
number
no_max_freq = yes
;sendqueue_size = 64000     ;min: 1000 max: 200000 default: 64000 -- size of re-order
fixing queue
;disable_sendqueue = no     ;yes/no, default: no -- disable re-order fixing queue
;tx_retries = 10           ;min: 0 max: 1000 default: 10 -- retries count for outgoing
packets before drop
;tx_delay = 20                ;min: 0 max: 200 default: 20 -- delay in microseconds
before another retry of sending packet burst
;rx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of rx descriptors
in network adapter configuration
;tx_desc = 4096           ;min: 32 max: 4096 default: 4096 -- number of tx descriptors
in network adapter configuration
;no_max_freq = no             ;yes/no, default: no -- disable setting max possible
frequency for our processor cores
;sendq_burst_threshold = 0   ;min: 100 max: 100000 default: 0 (disabled) -- make a
delay, if sending N packets from sendqueue in a row
;sendq_burst_delay = 10     ;min: 1 max: 200 default: 10 -- delay in microseconds when
sendq_burst_threshold activated
;pcap_mpool_size = 262143   ;min: 6736: max 4194303: default: auto -- number of buffers
in single memory pool, 1 pool per port
;rx_queue_len = 16           ;min: 1 max: 32 default: 16 -- size of thread queue (in
bursts)
;rx_sleep = 50              ;min: 0 max: 10000 default: 50 -- pause in microseconds on
rx thread if there are no packets incoming
;tx_sleep = 50              ;min: 0 max: 10000 default: 50 -- pause in microseconds on
tx thread if there are no packets to send
;wrk_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
wrk thread if there are no packets incoming
;kni_sleep = 50             ;min: 0 max: 10000 default: 50 -- pause in microseconds on
kni thread if there are no packets incoming or outgoing
;cb_wait = 50               ;min: 0 max: 10000 default: 50 -- wait in microseconds on
wrk thread if corresponding tx thread is busy
;rx_cache_size = 64000     ;min: 2000: max 200000: default: 64000 -- size of rx thread
packet cache
;wrk_overload_thresh = 90   ;min: 1: max 100: default: 90 -- threshold (in %) of wrk
thread queue fill when it counts as "overloaded"

[EAL]
corelist = 0-43
;coremask = 0x1              ;mask of cpu cores to run on, including HyperThreading
;corelist = 0-1             ;list of cpu cores to run on, including HyperThreading
;channels = 1               ;min: 1 max: 8 default: 1    -- memory channels number
;cpuset    =    (0-2,4)@(0-1)                    ;map    threads    to    cpu    cores:
<threads[@cpus]>[<,threads[@cpus]>...]
;eal_log_level = 4          ;min: 1 max: 8 default: 4    -- log level of dpdk messages
;rx_pthresh = 8               ;min: 0 max: 255 default: 8  -- rx prefetch threshold
register value
;rx_hthresh = 8             ;min: 0 max: 255 default: 8  -- rx host threshold register
value
;rx_wthresh = 4              ;min: 0 max: 255 default: 4  -- rx write-back threshold
register value
;tx_pthresh = 36              ;min: 0 max: 255 default: 36 -- tx prefetch threshold
register value
;tx_hthresh = 0             ;min: 0 max: 255 default: 0  -- tx host threshold register
value
;tx_wthresh = 0              ;min: 0 max: 255 default: 0  -- tx write-back threshold
register value

[MISC]
```

```
print_stats = yes          ;yes/no, default: yes -- print send/receive/drop statistics
stats_file = /tmp/pkt_stats.txt    ;name of file for print_stats
;stats_file_size = 10      ;min: 1 max: 100 default: 10 -- max size of statistics file
in megabytes. After rotate, previous instance saves as ".old"
;stats_period = 1             ;min: 1: max: 86400 default: 1 -- at this period (in
seconds) statistics is collected
;print_frames = no          ;yes/no, default: no -- print incoming/outgoing packets in
hex
;frames_file = /tmp/frames.txt      ;name of file for print_frames
;frames_file_size = 50      ;min: 1 max: 200 default: 50 -- max size of packet hexdump
file in megabytes. After roteate, previous instance saves as ".old"
;frames_time = no             ;yes/no, default: no -- print time for each packet in
print_frames
rte_log_file = /tmp/rte_log.txt    ;name of file for dpdk log messages
;rte_log_file_size = 10     ;min: 1 max: 100 default: 10 -- max size of rte_log file
in megabytes. After rotate, previous instance saves as ".old"
;pf_max_bytes = 42          ;min: 14 max: 1400 default: 42 -- print only N firs bytes
in print_frames
;natt_port = 4500           ;min: 1 max: 65535: default: 4500
;enable_pdump = no          ;yes/no, default: no -- enable packet dump with dpdk-pdump
utility
;macaddr_update_period = 200;min:1 max: 10000 default: 200 -- gateway mac address
update period in milliseconds
;kmod_name = igb_uio       ;igb_uio/vfio-pci/uio_pci_generic, default: igb_uio -- name
of kernel module for port binding


[PORT0]
pci_id = 0000:03:00.0
l3_ip = 172.16.2.2/24
gw_ip = 172.16.2.1
pair_port = 1
mtu = 9000
outer = yes ;yes/no, default: no -- consider port as looking to  outer network; outer
port can't be in l2-mode
;next_hop_mac = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv4
frames
;next_hop_mac6 = 00:00:00:00:00:00 ;default destination mac-address for outgoing IPv6
frames
;next_hop_mac_force = no ;yes/no, default no -- always set next_hop_mac as destination
mac address for outgoing IPv4 frames
;next_hop_mac6_force = no ;yes/no, default no -- always set next_hop_mac6 as destination
mac address for outgoing IPv6 frames
;dp_frag_ip = 0.0.0.0 ;default: disabled -- ip addresses (4 max, "," as divider) of
gate dp partners for this port
;dp_frag_ip6 =  ;disabled -- ipv6 addresses (4 max, "," as divider) of gate dp ipv6
partners for this port
;dp_frag_natt = no ;yes/no, default no -- enable fragmentation fix for natt
;frag_id_afterward = no ;yes/no, default no -- set frag id before send
;vlan_identifier = 0 ;min: 0 max: 4094 default: 0 -- 802.1Q VLAN identifier (VID)
;vlan_priority_code_point = 0 ;min: 0 max: 7 default: 0 -- Priority code point (PCP)
which refers to the 802.1p class of service
;allowed_ethertypes = none ;ethertypes in hex (32 max, "," as divider) -- pass this
ethertypes to/from corresponding vEth. IPv4(0x0800) and ARP(0x0806) always passed,
others dropped by default
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = yes ;yes/no, default: yes (for l2-port port - no) -- disable promiscuous
mode on this port
;multicast_enable = yes ;yes/no, default: yes (for l2-port - no) -- enable receiving
all multicast ip packets mode on this port
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
```

```
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
;pmtud = 8000 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination
Unreachable -- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
;mssfix = 8000 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value

[PORT1]
pci_id = 0000:0b:00.0
l2_src_ip = 172.16.2.2
l2_dst_ip = 172.16.101.2
pair_port = 0
mtu = 9000
;thr_start = 0 ;min: 0 max: <threads - 1> -- first processing thread for this port
;thr_count = <threads> ;min: 1 max: <threads - thr_start> -- number of processing
threads for this port
;no_fc = no ;yes/no, default no  -- disable flow control on this port
;no_promisc = no ;yes/no, default: no (for outer port - yes) -- disable promiscuous
mode on this port
;multicast_enable = no ;yes/no, default: no (for outer port - yes) -- enable receiving
all multicast ip packets mode on this port
;copy_tos = no ;yes/no, default: no -- copy ToS-field from orig ip header to l2-
encapsulation ip header
;df_handling = clear ;copy/set/clear, default clear -- DF bit: copy from orig ip header
to l2-encapsulation ip header
;hw_ip_checksum = yes ;yes/no, default: yes -- enable additional stats about l3/l4
checksum errors and oversized packets
;hw_vlan_extend = no ;yes/no, default: no -- enable double-vlan. Disables Vector-RX on
i40e
pmtud = 8900 ;min: 68 max: 65535 default: disabled -- send "ICMP Destination Unreachable
-- Fragmentation Needed" for ip packets with DF bit, greater than N bytes
mssfix = 8860 ;min: 536 max: 9670 default: disabled  -- change MSS field in forwarded
tcp syn packets if it greater than N
;mssfix_force = no ;yes/no, default: no -- always change MSS field in forwarded tcp
syn packets, even if it's lesser than mssfix value
```