Построение L2 VPN туннелей средствами «С-Терра Шлюз DP». Отказоустойчивое решение с балансировкой нагрузки при помощи протокола LACP

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

Введение

Данный сценарий описывает настройку безопасного взаимодействия между основным и резервным ЦОДами на уровне 2 модели OSI (L2 VPN) средствами Продукта «С-Терра Шлюз DP». Трафик, поступающий на коммутаторы Int-switch1-Hub1 и Int-switch1-Spoke1, балансируется с использованием протокола LACP между криптошлюзами Hub1-1, Hub1-2 и Spoke1-1, Spoke1-2 соответственно. В случае отказа одного из криптошлюзов, средствами протокола LACP будет осуществлена балансировка трафика на работающий криптошлюз.

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

Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты. В качестве криптопровайдера будет использована криптографическая библиотека, разработанная компанией «С-Терра СиЭсПи». Шлюзы безопасности (или 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, NAT, Firewall, routing, switching.

Администратор должен быть ознакомлен со сценарием «Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (протокол IPv4)». Далее по тексту он будет называться базовым сценарием. И 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 в заводском состоянии.
   1.2. Центр выпуска сертификатов.
      1.2.1 Должен быть настроен центр выпуска сертификатов (удостоверяющий центр, далее УЦ) для IPsec. Устройство с именем Certification_authority на схеме.
      1.2.2 Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2016 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 5.0 R2 (или новее).
      1.2.3 Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp), либо утилиту ca-tool, входящую в состав пакета auxiliary-tools (пакет auxiliary-tools предназначен для установки на «С-Терра Шлюз» 5.0, документация на ca-tool приведена в инструкции «Центр выпуска тестовых ГОСТ сертификатов для IPsec», документацию и пакет можно загрузить на портале https://doc.s-terra.ru).

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

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

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

2. Требования к сетевому взаимодействию.
   2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

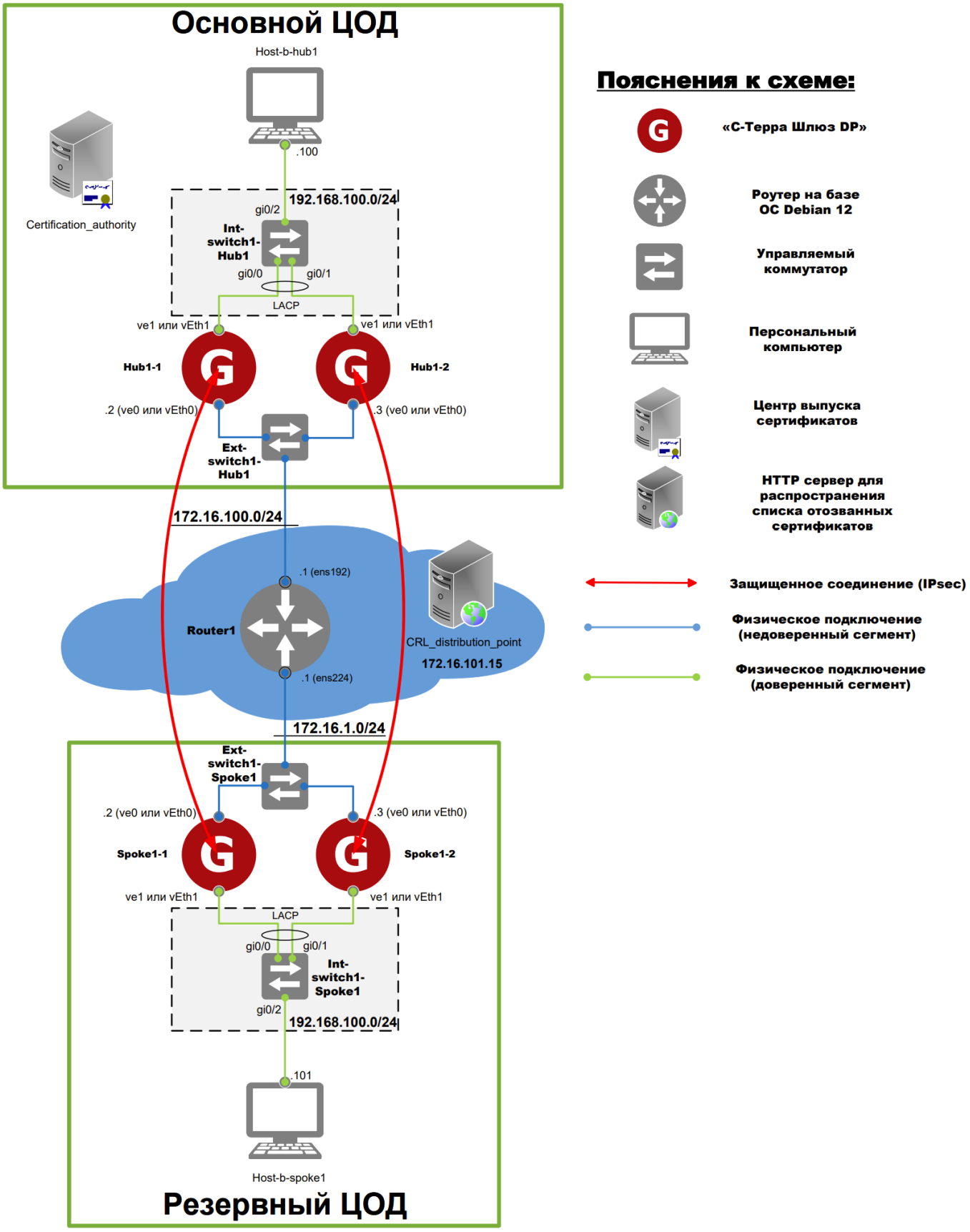


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В основном ЦОДе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюзы «С-Терра Шлюз DP» (Hub1-1 и Hub1-2), коммутаторы (Int-switch1-Hub1 и Ext-switch1-Hub1) и персональный компьютер (Host-b-hub1).

   1.2. В резервном ЦОДе размещаются: криптошлюзы «С-Терра Шлюз DP» (Spoke1-1 и Spoke1-2), коммутаторы (Int-switch1-Spoke1 и Ext-switch1-Spoke1) и персональный компьютер (Host-b-spoke1).

   1.3. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизатор (Router1).

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

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

   2.1. Криптошлюзы Hub1-1 и Hub1-2 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

   2.2. Криптошлюзы Spoke1-1 и Spoke1-2 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

3. Параметры безопасного взаимодействия.

   Весь трафик на втором уровне модели OSI подсети 192.168.100.0/24, который передается между основным и резервным ЦОДами, а также трафик управления на третьем уровне модели OSI, защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном режиме.

   Инициировать защищенное соединение может как трафик из резервного ЦОДа в основной, так и наоборот – из основного ЦОДа в резервный.

   3.1. Параметры протокола IKE:

   - Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
   - Алгоритм шифрования – ГОСТ Р 34.12-2015 Магма (ключ 256 бит);
   - Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 Стрибог (ключ 256 бит);
   - Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

   3.2. Параметры протокола ESP для L2 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 – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
2. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
3. Разрешите прохождение транзитного IP трафика (если он заблокирован).

Настройка устройства Int-switch1-Hub1

1. На интерфейсах `gi0/0` и `gi0/1` должно быть настроено агрегирование LACP.

Настройка устройства Int-switch1-Spoke1

1. На интерфейсах `gi0/0` и `gi0/1` должно быть настроено агрегирование LACP.

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 криптошлюза Hub1-1

Настройка будет происходить локально при помощи консольного подключения.

Настройка может осуществляться и удаленно (по SSH), но исключительно по доверенному каналу связи. Доверенным каналом связи может считаться канал в пределах контролируемой зоны в случае отсутствия в нем нарушителя. 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 12:32:30 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 "0000:0b:00.0" is already bound to driver "vmxnet3". Skipping
INFO: Device "0000:13:00.0" is already bound to driver "vmxnet3". Skipping
```

В зависимости от аппаратной платформы драйвер сетевой карты 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] : 2
```

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 linux-консоли шлюза или рассчитать, исходя из спецификации установленных в конкретную платформу процессоров), `ports_num` – количество портов (интерфейсов) для L2, заданное на предыдущем шаге. В зависимости от ситуации, это число можно изменять (только **в меньшую** сторону).

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

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

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

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 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 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):

Данный адрес может не присутствовать в системе и быть любым, но должен совпадать с `l2_dst_ip` на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke1-1.

```
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):

Данный адрес должен совпадать с `l2_src_ip` на криптошлюзе, с которым будет настраиваться L2 VPN. В данном сценарии – это Spoke1-1.

```
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) [8900] : 9000
```

6.4.12 Нажмите Enter, если все параметры введены верно:

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

```
+---+--------------+---------------+---------+
|   |    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

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

6.5. 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 (data plane)

В данном разделе будут описаны:

- настройка фрагментации;
- настройка механизма Path MTU Discovery;
- настройка механизма изменения MSS в TCP пакетах;
- настройка политики копирования DF бита;
- настройка политики копирования ToS байта.

1. Перейдите в linux bash:

```
administrator@sterragate] 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 редактирование конфигурационного файла `/opt/VPNagent/etc/ipsm_dpdk.cfg`:

   3.1. Включите механизм Path MTU Discovery и изменение MSS в TCP пакетах на LAN порту (PORT1). Для этого на LAN порту (PORT1) 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 = 0000:0b:00.0
l2_src_ip = 172.16.100.2
l2_dst_ip = 172.16.1.2
pair_port = 0
mtu = 9000
...
pmtud = 8900
mssfix = 8860
...
```

   3.2. Установите желаемое значение для параметра `df_handling` на LAN порту (PORT1). Этот параметр определяет политику копирования DF бита из исходных пакетов при инкапсуляции в EtherIP. Допустимые значения:

   - clear – обнулять DF бит (значение по умолчанию);
   - set – выставлять DF бит;
   - copy – копировать значение DF бита из исходного пакета.

   3.3. Установите желаемое значение для параметра copy_tos на LAN порту (PORT1). Этот параметр определяет политику копирования ToS байта из исходных пакетов при инкапсуляции в EtherIP. Допустимые значения:

   - no – не копировать ToS байт (значение по умолчанию);
   - yes – копировать ToS байт.

   3.4. 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.

Настройка 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

Выведите список всех интерфейсов, доступных в cisco-like консоли:

```
sterragate#show interfaces
```

```
TenGigabitEthernet0/0 is down, line protocol is down
  Hardware address is 0050.569e.d457
  MTU 1500 bytes
DP0
  Virtual data plane interface (pattern "10G_000")
DP1
  Virtual data plane interface (pattern "10G_001")
DP2
...
DP35
  Virtual data plane interface (pattern "10G_035")
vEthernet0 is up, line protocol is up
  Hardware address is 0050.569e.c11d
  Internet address is 172.16.100.2/24
  MTU 9000 bytes
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.ad40
  MTU 9000 bytes
```

Видно, что интерфейс `TenGigabitEthernet0/0` не задействован в L2. Интерфейсы `vEthernetN` задействованы в L2, `vEthernet0` соответствует WAN интерфейсу, а `vEthernet1` – LAN-интерфейсу.

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 Hub1-1
   ```

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:

   ```
   Hub1-1(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
```

```
Hub1-1(config)#do show interfaces vEthernet1
```

```
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.26ec
  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`):

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

4. Проверьте доступность устройства Router1:

```
Hub1-1(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
```

Настройка шифрования

1. Настройте параметры IKE.

   1.1. Задайте общие параметры IKE:

```
Hub1-1(config)#crypto isakmp identity dn
Hub1-1(config)#crypto isakmp keepalive 3 2
Hub1-1(config)#crypto isakmp keepalive retry-count 5
Hub1-1(config)#crypto isakmp fragmentation
Hub1-1(config)#crypto isakmp security-association lifetime delta 50
Hub1-1(config)#crypto isakmp initiator-sessions-max 100
Hub1-1(config)#crypto isakmp responder-sessions-max 100
```

   1.2. Создайте политику, описывающую параметры IKE туннеля:

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

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

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

2. Параметры IPsec для защиты транзитного L2 трафика.

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

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

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

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

2.3. Создайте список доступа (ACL) для транзитного инкапсулированного в EtherIP пользовательского трафика, который нужно защищать между основным и резервным ЦОДами:

```
Hub1-1(config)#ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
Hub1-1(config-ext-nACL)#remark EtherIP L2 tunnel
Hub1-1(config-ext-nACL)#permit etherip host 172.16.100.2 host 172.16.1.2
Hub1-1(config-ext-nACL)#exit
```

2.4. Создайте криптокарту (имя L2VPN, раздел 1):

```
Hub1-1(config)#crypto map L2VPN 1 ipsec-isakmp
```

2.4.1 Укажите список доступа для защищаемого трафика:

```
Hub1-1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_SPOKE1
```

2.4.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

```
Hub1-1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
```

2.4.3 Укажите IP адрес партнера по IPsec, в данном сценарии это внешний IP адрес устройства Spoke1:

```
Hub1-1(config-crypto-map)#set peer 172.16.1.2
```

2.4.4 Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

```
Hub1-1(config-crypto-map)#set isakmp-profile NEW_ALGS
```

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

```
Hub1-1(config-crypto-map)#set dead-connection history off
```

2.4.6 Включите префрагментацию:

```
Hub1-1(config-crypto-map)#set pre-fragmentation
Hub1-1(config-crypto-map)#exit
```

2.5. Прикрепите созданную криптокарту `L2VPN` ко **всем DP интерфейсам** (количество DP интерфейсов может отличаться в зависимости от аппаратной платформы):

```
Hub1-1(config)# interface range DP 0 - 35
Hub1-1(config-if-range)#crypto map L2VPN
Hub1-1(config-if-range)#exit
```

2.6. Примените настройки:

```
Hub1-1(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:

```
Hub1-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hub1-1(config)#object-group network SELF
Hub1-1(config-network-group)#remark WAN IP
Hub1-1(config-network-group)#host 172.16.100.2
Hub1-1(config-network-group)#exit
```

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

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

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

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

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

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

5. Прикрепите правила межсетевого экранирования на WAN интерфейс `vEthernet0`:

```
Hub1-1(config)#interface vEthernet0
Hub1-1(config-if)#ip access-group FW_INPUT_WAN in
Hub1-1(config-if)#ip inspect INSPECT out
Hub1-1(config-if)#exit
```

6. Прикрепите правила межсетевого экранирования на все DP интерфейсы:

```
Hub1-1(config)#interface range DP 0 - 36
Hub1-1(config-if-range)#ip access-group FW_INPUT_DP in
Hub1-1(config-if-range)#exit
```

7. Примените настройки:

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

Настройка криптошлюза Hub1-1 завершена.
В главе «

Приложение» представлены тексты конфигураций для криптошлюза Hub1-1:

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

Настройка криптошлюза Hub1-2

Настройка криптошлюза Hub1-2 происходит аналогично настройке Hub1-1.
В главе «

Приложение» представлены тексты конфигураций для криптошлюза Hub1-2:

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

Настройка криптошлюза Spoke1-1

Настройка криптошлюза Spoke1-1 происходит аналогично настройке Spoke1-1.
В главе «

Приложение» представлены тексты конфигураций для криптошлюза Spoke1-1:

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

Настройка криптошлюза Spoke1-2

Настройка криптошлюза Spoke1-2 происходит аналогично настройке Spoke1-1.
В главе «

Приложение» представлены тексты конфигураций для криптошлюза Spoke1-2:

- 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 Hub1-1, Hub1-2, Spoke1-1 и Spoke1-2 по ICMP доступен шлюз по умолчанию (Router1). Для этого выполните команду `ping` из cisco-like консоли криптошлюзов.

```
Hub1-1#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=5.07 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=3.62 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=6.55 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=4.68 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=2.86 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.867/4.562/6.552/1.263 ms
```

```
Hub1-2#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=3.62 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=5.81 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=6.01 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=3.74 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=4.12 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 4.224/6.456/12.704/2.235 ms
```

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

```
PING 172.16.1.1 (172.16.1.1) 100(128) bytes of data.
108 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=14.7 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=9.22 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=7.03 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=5.25 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=8.15 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 5.259/8.876/14.704/3.195 ms
```

```
Spoke1-2#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=7.17 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=4.54 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=9.25 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=1.82 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=3.73 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 4.567/4.326/6.723/4.125 ms
```

   Видно, что устройство Router1 доступно по ICMP с Hub1-1, Hub1-2, Spoke1-1 и Spoke1-2.

2. Проверьте, что с криптошлюза Hub1-1 доступен по ICMP криптошлюз Spoke1-1 (по внешним интерфейсам) и с криптошлюза Hub1-2 доступен по ICMP криптошлюз Spoke1-2 (также по внешним интерфейсам). Для этого выполните команду `ping` из cisco-like консоли криптошлюзов.

```
Hub1-1#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
```

Видно, что с криптошлюза Hub1-1 доступен по ICMP криптошлюз Spoke1-1.

```
Hub1-2#ping 172.16.1.3
```

```
PING 172.16.1.3 (172.16.1.3) 100(128) bytes of data.
108 bytes from 172.16.1.3: icmp_seq=1 ttl=63 time=19.1 ms
108 bytes from 172.16.1.3: icmp_seq=2 ttl=63 time=14.7 ms
108 bytes from 172.16.1.3: icmp_seq=3 ttl=63 time=15.3 ms
108 bytes from 172.16.1.3: icmp_seq=4 ttl=63 time=7.32 ms
108 bytes from 172.16.1.3: icmp_seq=5 ttl=63 time=10.4 ms

--- 172.16.1.3 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
```

Видно, что с криптошлюза Hub1-2 доступен по ICMP криптошлюз Spoke1-2.

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 ЦОДами

В силу того, что протокол LACP обменивается служебными пакетами, защищённые IPsec-соединения должны быть предварительно построены на между парами криптошлюзов Hub1-1, Spoke1-1 и Hub1-2, Spoke1-2. Для того, чтобы в этом убедиться, необходимо воспользоваться командой `sa_mgr show`.

1. Убедитесь в том, что между криптошлюзами Hub1-1 и Spoke1-1 построены IPsec-соединения. Для этого выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

```
Hub1-1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 17 (172.16.100.2,500)-(172.16.1.2,500) active 13220 13480

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3452 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
2 3453 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 480
3 3455 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 480 384
4 3456 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
5 3458 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 768 512
6 3459 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 384
7 3460 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 484 384
8 3461 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 768 384
9 3462 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 640
10 3463 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 1152
11 3464 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
12 3465 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 640 512
13 3466 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 864 384
14 3467 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
```

```
15 3468 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 512
16 3469 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
17 3470 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
18 3471 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
19 3472 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 472 384
20 3473 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 472
21 3474 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 728
22 3475 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 472 640
23 3476 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
24 3477 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 768 384
25 3478 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
26 3479 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 768
27 3480 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
28 3481 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 1024
29 3482 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 480
30 3483 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 768 384
31 3484 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 480
32 3485 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 512 384
33 3486 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 384
34 3487 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 640 384
35 3488 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 384
36 3489 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP tunn 384 512
```

```
Spoke1-1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 13 (172.16.1.2,500)-(172.16.100.2,500) active 13480 13220

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 3452 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
2 3453 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 480 512
3 3455 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 480
4 3456 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
5 3458 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 768
6 3459 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 384
7 3460 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 484
8 3461 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 768
9 3462 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 640 384
10 3463 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 1152 512
11 3464 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
12 3465 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 640
13 3466 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 864
14 3467 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
15 3468 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 512
16 3469 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
17 3470 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
18 3471 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
19 3472 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 472
20 3473 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 472 512
21 3474 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 728 384
22 3475 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 640 472
23 3476 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
24 3477 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 768
25 3478 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
26 3479 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 768 384
27 3480 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
28 3481 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 1024 384
29 3482 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 384
30 3483 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 768
31 3484 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 384
32 3485 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 512
33 3486 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 384
34 3487 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 640
```

```
35 3488 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 384 384
36 3489 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP tunn 512 384
```

Видно, что между криптошлюзами Hub1-1 и Spoke1-1 установлено защищенное IPsec-соединение (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. Аналогичным образом проверьте, что защищённое IPsec-соединение установлено между криптошлюзами Hub1-2 и Spoke1-2

Проверка отказоустойчивости

1. Посылайте с устройства Host-b-spoke1 на Host-b-hub1 ICMP-трафик, который далее будет защищаться криптошлюзами:

   ```
   root@host-b-spoke1:~# ping 192.168.100.100
   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=3.54 ms
   64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=2.33 ms
   64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=2.49 ms
   64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=2.26 ms
   64 bytes from 192.168.100.100: icmp_seq=5 ttl=64 time=2.32 ms
   ...
   ```

2. Смоделируйте отказ канала связи, например, отключив сетевой кабель внешнего интерфейса, на том криптошлюзе из резервного ЦОДа, через который в данный момент идет защищаемый ICMP трафик (в данном случае это Spoke1-1) от 192.168.100.101 к 192.168.100.100.

3. При помощи диагностических команд, выполняемых на коммутаторах Int-switch1-Spoke1, Int-switch1-Hub1, убедитесь в том, что сетевые интерфейсы, которые были подключены к криптошлюзам, через которые шел защищаемый ICMP трафик от 192.168.100.101 к 192.168.100.100, переведены в неактивное состояние (с точки зрения протокола LACP).

4. Подождите некоторое время пока протокол LACP перебалансирует трафик на рабочую пару криптошлюзов.

5. Как только произошла перебалансировка трафика, убедитесь в том, что в IPsec-туннелях рабочей пары криптошлюзов симметрично увеличиваются счетчики `Sent` и `Rcvd`. Для просмотра счетчиков выполните команду `run sa_mgr show` из cisco-like консоли криптошлюзов.

   При наличии отклонений проанализируйте журналы на криптошлюзах.

Приложение

Конфигурации криптошлюза Hub1-1

1. Конфигурация 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 Hub1-1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
!
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 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 inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
```

```
ip inspect name INSPECT udp
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
!
interface TenGigabitEthernet0/0
 no ip address
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1000
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1001
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1007
!
interface DP8
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1008
!
interface DP9
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1009
!
interface DP10
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
```

```
 crypto ipsec stream-id 1010
!
interface DP11
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1011
!
interface DP12
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1012
!
interface DP13
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1013
!
interface DP14
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1014
!
interface DP15
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1015
!
interface DP16
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1016
!
interface DP17
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1017
!
interface DP18
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1018
!
interface DP19
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1019
!
interface DP20
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1020
!
interface DP21
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1021
!
interface DP22
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1022
!
interface DP23
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1023
```

```
!
interface DP24
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1024
!
interface DP25
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1025
!
interface DP26
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1026
!
interface DP27
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1027
!
interface DP28
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1028
!
interface DP29
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1029
!
interface DP30
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1030
!
interface DP31
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1031
!
interface DP32
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1032
!
interface DP33
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1033
!
interface DP34
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1034
!
interface DP35
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1035
!
interface vEthernet0
 description WAN
 ip access-group FW_INPUT_WAN in
 ip inspect INSPECT out
!
```

```
interface vEthernet1
 description LAN
!
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
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon Dec  2 14:58:44 2024

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Mon Dec  2 14:58:44 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

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

)

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

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

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

FilterChain 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 = 172.16.100.2
        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 = 172.16.100.2
        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 = 172.16.100.2
        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
    ))

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:1
(
    IKEPeerIPFilter = 172.16.1.2
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
```

```
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:L2VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.1.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
)

const IPsecPolicy:L2VPN = 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:1 >
        LogEventID = "IPsec:Protect:L2VPN:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)

FilterChain IPsecPolicy:L2VPN:1000 (
    +IPsecPolicy:L2VPN
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN:1001 (
    +IPsecPolicy:L2VPN
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN:1002 (
    +IPsecPolicy:L2VPN
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN:1003 (
    +IPsecPolicy:L2VPN
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN:1004 (
    +IPsecPolicy:L2VPN
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN:1005 (
    +IPsecPolicy:L2VPN
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN:1006 (
    +IPsecPolicy:L2VPN
```

```
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN:1007 (
    +IPsecPolicy:L2VPN
    StreamID = 1007
)

FilterChain IPsecPolicy:L2VPN:1008 (
    +IPsecPolicy:L2VPN
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN:1009 (
    +IPsecPolicy:L2VPN
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN:1010 (
    +IPsecPolicy:L2VPN
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN:1011 (
    +IPsecPolicy:L2VPN
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN:1012 (
    +IPsecPolicy:L2VPN
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN:1013 (
    +IPsecPolicy:L2VPN
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN:1014 (
    +IPsecPolicy:L2VPN
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN:1015 (
    +IPsecPolicy:L2VPN
    StreamID = 1015
)

FilterChain IPsecPolicy:L2VPN:1016 (
    +IPsecPolicy:L2VPN
    StreamID = 1016
)

FilterChain IPsecPolicy:L2VPN:1017 (
    +IPsecPolicy:L2VPN
    StreamID = 1017
)

FilterChain IPsecPolicy:L2VPN:1018 (
    +IPsecPolicy:L2VPN
    StreamID = 1018
)

FilterChain IPsecPolicy:L2VPN:1019 (
    +IPsecPolicy:L2VPN
    StreamID = 1019
```

```
)

FilterChain IPsecPolicy:L2VPN:1020 (
    +IPsecPolicy:L2VPN
    StreamID = 1020
)

FilterChain IPsecPolicy:L2VPN:1021 (
    +IPsecPolicy:L2VPN
    StreamID = 1021
)

FilterChain IPsecPolicy:L2VPN:1022 (
    +IPsecPolicy:L2VPN
    StreamID = 1022
)

FilterChain IPsecPolicy:L2VPN:1023 (
    +IPsecPolicy:L2VPN
    StreamID = 1023
)

FilterChain IPsecPolicy:L2VPN:1024 (
    +IPsecPolicy:L2VPN
    StreamID = 1024
)

FilterChain IPsecPolicy:L2VPN:1025 (
    +IPsecPolicy:L2VPN
    StreamID = 1025
)

FilterChain IPsecPolicy:L2VPN:1026 (
    +IPsecPolicy:L2VPN
    StreamID = 1026
)

FilterChain IPsecPolicy:L2VPN:1027 (
    +IPsecPolicy:L2VPN
    StreamID = 1027
)

FilterChain IPsecPolicy:L2VPN:1028 (
    +IPsecPolicy:L2VPN
    StreamID = 1028
)

FilterChain IPsecPolicy:L2VPN:1029 (
    +IPsecPolicy:L2VPN
    StreamID = 1029
)

FilterChain IPsecPolicy:L2VPN:1030 (
    +IPsecPolicy:L2VPN
    StreamID = 1030
)

FilterChain IPsecPolicy:L2VPN:1031 (
    +IPsecPolicy:L2VPN
    StreamID = 1031
)

FilterChain IPsecPolicy:L2VPN:1032 (
    +IPsecPolicy:L2VPN
    StreamID = 1032
)
```

```
FilterChain IPsecPolicy:L2VPN:1033 (
    +IPsecPolicy:L2VPN
    StreamID = 1033
)

FilterChain IPsecPolicy:L2VPN:1034 (
    +IPsecPolicy:L2VPN
    StreamID = 1034
)

FilterChain IPsecPolicy:L2VPN:1035 (
    +IPsecPolicy:L2VPN
    StreamID = 1035
)

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1001
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1005
)

NetworkInterface (
    LogicalName = "DP6"
```

```
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1007
)

NetworkInterface (
    LogicalName = "DP8"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1008
)

NetworkInterface (
    LogicalName = "DP9"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1009
)

NetworkInterface (
    LogicalName = "DP10"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1010
)

NetworkInterface (
    LogicalName = "DP11"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1011
)

NetworkInterface (
    LogicalName = "DP12"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1012
)

NetworkInterface (
    LogicalName = "DP13"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1013
)

NetworkInterface (
    LogicalName = "DP14"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1014
)

NetworkInterface (
    LogicalName = "DP15"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1015
```

```
)

NetworkInterface (
    LogicalName = "DP16"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1016
)

NetworkInterface (
    LogicalName = "DP17"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1017
)

NetworkInterface (
    LogicalName = "DP18"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1018
)

NetworkInterface (
    LogicalName = "DP19"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1019
)

NetworkInterface (
    LogicalName = "DP20"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1020
)

NetworkInterface (
    LogicalName = "DP21"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1021
)

NetworkInterface (
    LogicalName = "DP22"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1022
)

NetworkInterface (
    LogicalName = "DP23"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1023
)

NetworkInterface (
    LogicalName = "DP24"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1024
)

NetworkInterface (
```

```
    LogicalName = "DP25"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1025
)

NetworkInterface (
    LogicalName = "DP26"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1026
)

NetworkInterface (
    LogicalName = "DP27"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1027
)

NetworkInterface (
    LogicalName = "DP28"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1028
)

NetworkInterface (
    LogicalName = "DP29"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1029
)

NetworkInterface (
    LogicalName = "DP30"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1030
)

NetworkInterface (
    LogicalName = "DP31"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1031
)

NetworkInterface (
    LogicalName = "DP32"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1032
)

NetworkInterface (
    LogicalName = "DP33"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1033
)

NetworkInterface (
    LogicalName = "DP34"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
```

```
    IPsecPolicy = IPsecPolicy:L2VPN:1034
)

NetworkInterface (
    LogicalName = "DP35"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1035
)

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

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

3. Конфигурация L2 (data plane)

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

```
[PERFORMANCE]
threads = 36                        ;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 = 0000:0b: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 = <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 Hub1-2

1. Конфигурация cisco-like

```
!
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
username          cscons          privilege          15          secret          5
$6$lQHk46/t$MDufPsXck4QGNohEy/CS8Qf/U9SF7LZfA/1RC9RBjLwOIP5vIjiDE7bYGKfodQwUcopzFDVLf
1v.6m9CV.Zan0
aaa new-model
!
!
hostname Hub1-2
enable secret 5 vIWbAnRJu0Afqhm/xJTTXg==
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.100.3
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.100.3 host 172.16.1.3
!
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
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set peer 172.16.1.3
 set pre-fragmentation
 set dead-connection history off
!
interface TenGigabitEthernet0/0
 no ip address
!
interface DP0
 ip access-group FW_INPUT_DP in
```

```
 crypto map L2VPN
 crypto ipsec stream-id 1000
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1001
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1007
!
interface DP8
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1008
!
interface DP9
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1009
!
interface DP10
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1010
!
interface DP11
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1011
!
interface DP12
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1012
!
interface DP13
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
```

```
 crypto ipsec stream-id 1013
!
interface DP14
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1014
!
interface DP15
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1015
!
interface DP16
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1016
!
interface DP17
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1017
!
interface DP18
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1018
!
interface DP19
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1019
!
interface DP20
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1020
!
interface DP21
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1021
!
interface DP22
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1022
!
interface DP23
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1023
!
interface DP24
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1024
!
interface DP25
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1025
!
interface DP26
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1026
```

```
!
interface DP27
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1027
!
interface DP28
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1028
!
interface DP29
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1029
!
interface DP30
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1030
!
interface DP31
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1031
!
interface DP32
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1032
!
interface DP33
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1033
!
interface DP34
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1034
!
interface DP35
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1035
!
interface vEthernet0
 description WAN
 ip access-group FW_INPUT_WAN in
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
!
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
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
```

```
!
end
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon Dec  2 15:00:59 2024

GlobalParameters(
    Title                       = "This LSP was automatically generated by CSP Converter
at Mon Dec  2 15:00:59 2024 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

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

)

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

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

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

FilterChain 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 = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        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 = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.100.3
        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
    ))

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:1
(
    IKEPeerIPFilter = 172.16.1.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:L2VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.1.3
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
```

```
)

const IPsecPolicy:L2VPN = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.100.3
        DestinationIP = 172.16.1.3
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN:1 >
        LogEventID = "IPsec:Protect:L2VPN:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)

FilterChain IPsecPolicy:L2VPN:1000 (
    +IPsecPolicy:L2VPN
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN:1001 (
    +IPsecPolicy:L2VPN
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN:1002 (
    +IPsecPolicy:L2VPN
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN:1003 (
    +IPsecPolicy:L2VPN
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN:1004 (
    +IPsecPolicy:L2VPN
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN:1005 (
    +IPsecPolicy:L2VPN
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN:1006 (
    +IPsecPolicy:L2VPN
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN:1007 (
    +IPsecPolicy:L2VPN
    StreamID = 1007
)

FilterChain IPsecPolicy:L2VPN:1008 (
    +IPsecPolicy:L2VPN
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN:1009 (
    +IPsecPolicy:L2VPN
```

```
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN:1010 (
    +IPsecPolicy:L2VPN
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN:1011 (
    +IPsecPolicy:L2VPN
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN:1012 (
    +IPsecPolicy:L2VPN
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN:1013 (
    +IPsecPolicy:L2VPN
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN:1014 (
    +IPsecPolicy:L2VPN
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN:1015 (
    +IPsecPolicy:L2VPN
    StreamID = 1015
)

FilterChain IPsecPolicy:L2VPN:1016 (
    +IPsecPolicy:L2VPN
    StreamID = 1016
)

FilterChain IPsecPolicy:L2VPN:1017 (
    +IPsecPolicy:L2VPN
    StreamID = 1017
)

FilterChain IPsecPolicy:L2VPN:1018 (
    +IPsecPolicy:L2VPN
    StreamID = 1018
)

FilterChain IPsecPolicy:L2VPN:1019 (
    +IPsecPolicy:L2VPN
    StreamID = 1019
)

FilterChain IPsecPolicy:L2VPN:1020 (
    +IPsecPolicy:L2VPN
    StreamID = 1020
)

FilterChain IPsecPolicy:L2VPN:1021 (
    +IPsecPolicy:L2VPN
    StreamID = 1021
)

FilterChain IPsecPolicy:L2VPN:1022 (
    +IPsecPolicy:L2VPN
    StreamID = 1022
```

```
)

FilterChain IPsecPolicy:L2VPN:1023 (
    +IPsecPolicy:L2VPN
    StreamID = 1023
)

FilterChain IPsecPolicy:L2VPN:1024 (
    +IPsecPolicy:L2VPN
    StreamID = 1024
)

FilterChain IPsecPolicy:L2VPN:1025 (
    +IPsecPolicy:L2VPN
    StreamID = 1025
)

FilterChain IPsecPolicy:L2VPN:1026 (
    +IPsecPolicy:L2VPN
    StreamID = 1026
)

FilterChain IPsecPolicy:L2VPN:1027 (
    +IPsecPolicy:L2VPN
    StreamID = 1027
)

FilterChain IPsecPolicy:L2VPN:1028 (
    +IPsecPolicy:L2VPN
    StreamID = 1028
)

FilterChain IPsecPolicy:L2VPN:1029 (
    +IPsecPolicy:L2VPN
    StreamID = 1029
)

FilterChain IPsecPolicy:L2VPN:1030 (
    +IPsecPolicy:L2VPN
    StreamID = 1030
)

FilterChain IPsecPolicy:L2VPN:1031 (
    +IPsecPolicy:L2VPN
    StreamID = 1031
)

FilterChain IPsecPolicy:L2VPN:1032 (
    +IPsecPolicy:L2VPN
    StreamID = 1032
)

FilterChain IPsecPolicy:L2VPN:1033 (
    +IPsecPolicy:L2VPN
    StreamID = 1033
)

FilterChain IPsecPolicy:L2VPN:1034 (
    +IPsecPolicy:L2VPN
    StreamID = 1034
)

FilterChain IPsecPolicy:L2VPN:1035 (
    +IPsecPolicy:L2VPN
    StreamID = 1035
)
```

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1001
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1005
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1007
)

NetworkInterface (
    LogicalName = "DP8"
    InputFilter = FilterChain:FW_INPUT_DP
```

```
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1008
)

NetworkInterface (
    LogicalName = "DP9"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1009
)

NetworkInterface (
    LogicalName = "DP10"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1010
)

NetworkInterface (
    LogicalName = "DP11"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1011
)

NetworkInterface (
    LogicalName = "DP12"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1012
)

NetworkInterface (
    LogicalName = "DP13"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1013
)

NetworkInterface (
    LogicalName = "DP14"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1014
)

NetworkInterface (
    LogicalName = "DP15"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1015
)

NetworkInterface (
    LogicalName = "DP16"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1016
)

NetworkInterface (
    LogicalName = "DP17"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1017
)
```

```
NetworkInterface (
    LogicalName = "DP18"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1018
)

NetworkInterface (
    LogicalName = "DP19"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1019
)

NetworkInterface (
    LogicalName = "DP20"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1020
)

NetworkInterface (
    LogicalName = "DP21"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1021
)

NetworkInterface (
    LogicalName = "DP22"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1022
)

NetworkInterface (
    LogicalName = "DP23"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1023
)

NetworkInterface (
    LogicalName = "DP24"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1024
)

NetworkInterface (
    LogicalName = "DP25"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1025
)

NetworkInterface (
    LogicalName = "DP26"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1026
)

NetworkInterface (
    LogicalName = "DP27"
```

```
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1027
)

NetworkInterface (
    LogicalName = "DP28"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1028
)

NetworkInterface (
    LogicalName = "DP29"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1029
)

NetworkInterface (
    LogicalName = "DP30"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1030
)

NetworkInterface (
    LogicalName = "DP31"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1031
)

NetworkInterface (
    LogicalName = "DP32"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1032
)

NetworkInterface (
    LogicalName = "DP33"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1033
)

NetworkInterface (
    LogicalName = "DP34"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1034
)

NetworkInterface (
    LogicalName = "DP35"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1035
)

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

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

3. Конфигурация L2 (data plane)

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

```
[PERFORMANCE]
threads = 36                        ;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 = 172.16.100.3/24
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 = 0000:0b:00.0
l2_src_ip = 172.16.100.3
l2_dst_ip = 172.16.1.3
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 Spoke1-1

1. Конфигурация 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
username          cscons          privilege          15          secret          5
$6$lQHk46/t$MDufPsXck4QGNohEy/CS8Qf/U9SF7LZfA/1RC9RBjLwOIP5vIjiDE7bYGKfodQwUcopzFDVLf
1v.6m9CV.Zan0
aaa new-model
!
!
```

```
hostname Spoke1-1
enable secret 5 vIWbAnRJu0Afqhm/xJTTXg==
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.1.2
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.1.2 host 172.16.100.2
!
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 inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
interface TenGigabitEthernet0/0
 no ip address
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1000
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1001
!
interface DP2
 ip access-group FW_INPUT_DP in
```

```
 crypto map L2VPN
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1007
!
interface DP8
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1008
!
interface DP9
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1009
!
interface DP10
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1010
!
interface DP11
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1011
!
interface DP12
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1012
!
interface DP13
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1013
!
interface DP14
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1014
!
interface DP15
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
```

```
 crypto ipsec stream-id 1015
!
interface DP16
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1016
!
interface DP17
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1017
!
interface DP18
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1018
!
interface DP19
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1019
!
interface DP20
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1020
!
interface DP21
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1021
!
interface DP22
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1022
!
interface DP23
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1023
!
interface DP24
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1024
!
interface DP25
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1025
!
interface DP26
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1026
!
interface DP27
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1027
!
interface DP28
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1028
```

```
!
interface DP29
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1029
!
interface DP30
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1030
!
interface DP31
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1031
!
interface DP32
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1032
!
interface DP33
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1033
!
interface DP34
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1034
!
interface DP35
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1035
!
interface vEthernet0
 description WAN
 ip access-group FW_INPUT_WAN in
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
!
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
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon Dec  2 15:03:26 2024

GlobalParameters(
```

```
    Title                       = "This LSP was automatically generated by CSP Converter
at Mon Dec  2 15:03:26 2024 (user: cscons)"
    Version                       = LSP_5_0
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

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

)

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

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

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

FilterChain 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
    ))

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

IPsecAction IPsecAction:L2VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
)

const IPsecPolicy:L2VPN = 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:1 >
        LogEventID = "IPsec:Protect:L2VPN:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)

FilterChain IPsecPolicy:L2VPN:1000 (
    +IPsecPolicy:L2VPN
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN:1001 (
    +IPsecPolicy:L2VPN
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN:1002 (
    +IPsecPolicy:L2VPN
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN:1003 (
    +IPsecPolicy:L2VPN
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN:1004 (
    +IPsecPolicy:L2VPN
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN:1005 (
    +IPsecPolicy:L2VPN
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN:1006 (
    +IPsecPolicy:L2VPN
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN:1007 (
    +IPsecPolicy:L2VPN
    StreamID = 1007
)

FilterChain IPsecPolicy:L2VPN:1008 (
    +IPsecPolicy:L2VPN
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN:1009 (
    +IPsecPolicy:L2VPN
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN:1010 (
    +IPsecPolicy:L2VPN
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN:1011 (
```

```
    +IPsecPolicy:L2VPN
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN:1012 (
    +IPsecPolicy:L2VPN
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN:1013 (
    +IPsecPolicy:L2VPN
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN:1014 (
    +IPsecPolicy:L2VPN
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN:1015 (
    +IPsecPolicy:L2VPN
    StreamID = 1015
)

FilterChain IPsecPolicy:L2VPN:1016 (
    +IPsecPolicy:L2VPN
    StreamID = 1016
)

FilterChain IPsecPolicy:L2VPN:1017 (
    +IPsecPolicy:L2VPN
    StreamID = 1017
)

FilterChain IPsecPolicy:L2VPN:1018 (
    +IPsecPolicy:L2VPN
    StreamID = 1018
)

FilterChain IPsecPolicy:L2VPN:1019 (
    +IPsecPolicy:L2VPN
    StreamID = 1019
)

FilterChain IPsecPolicy:L2VPN:1020 (
    +IPsecPolicy:L2VPN
    StreamID = 1020
)

FilterChain IPsecPolicy:L2VPN:1021 (
    +IPsecPolicy:L2VPN
    StreamID = 1021
)

FilterChain IPsecPolicy:L2VPN:1022 (
    +IPsecPolicy:L2VPN
    StreamID = 1022
)

FilterChain IPsecPolicy:L2VPN:1023 (
    +IPsecPolicy:L2VPN
    StreamID = 1023
)

FilterChain IPsecPolicy:L2VPN:1024 (
    +IPsecPolicy:L2VPN
```

```
    StreamID = 1024
)

FilterChain IPsecPolicy:L2VPN:1025 (
    +IPsecPolicy:L2VPN
    StreamID = 1025
)

FilterChain IPsecPolicy:L2VPN:1026 (
    +IPsecPolicy:L2VPN
    StreamID = 1026
)

FilterChain IPsecPolicy:L2VPN:1027 (
    +IPsecPolicy:L2VPN
    StreamID = 1027
)

FilterChain IPsecPolicy:L2VPN:1028 (
    +IPsecPolicy:L2VPN
    StreamID = 1028
)

FilterChain IPsecPolicy:L2VPN:1029 (
    +IPsecPolicy:L2VPN
    StreamID = 1029
)

FilterChain IPsecPolicy:L2VPN:1030 (
    +IPsecPolicy:L2VPN
    StreamID = 1030
)

FilterChain IPsecPolicy:L2VPN:1031 (
    +IPsecPolicy:L2VPN
    StreamID = 1031
)

FilterChain IPsecPolicy:L2VPN:1032 (
    +IPsecPolicy:L2VPN
    StreamID = 1032
)

FilterChain IPsecPolicy:L2VPN:1033 (
    +IPsecPolicy:L2VPN
    StreamID = 1033
)

FilterChain IPsecPolicy:L2VPN:1034 (
    +IPsecPolicy:L2VPN
    StreamID = 1034
)

FilterChain IPsecPolicy:L2VPN:1035 (
    +IPsecPolicy:L2VPN
    StreamID = 1035
)

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

NetworkInterface (
    LogicalName = "DP0"
```

```
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1001
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1005
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1007
)

NetworkInterface (
    LogicalName = "DP8"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1008
)

NetworkInterface (
    LogicalName = "DP9"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1009
```

```
)

NetworkInterface (
    LogicalName = "DP10"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1010
)

NetworkInterface (
    LogicalName = "DP11"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1011
)

NetworkInterface (
    LogicalName = "DP12"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1012
)

NetworkInterface (
    LogicalName = "DP13"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1013
)

NetworkInterface (
    LogicalName = "DP14"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1014
)

NetworkInterface (
    LogicalName = "DP15"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1015
)

NetworkInterface (
    LogicalName = "DP16"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1016
)

NetworkInterface (
    LogicalName = "DP17"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1017
)

NetworkInterface (
    LogicalName = "DP18"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1018
)

NetworkInterface (
```

```
    LogicalName = "DP19"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1019
)

NetworkInterface (
    LogicalName = "DP20"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1020
)

NetworkInterface (
    LogicalName = "DP21"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1021
)

NetworkInterface (
    LogicalName = "DP22"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1022
)

NetworkInterface (
    LogicalName = "DP23"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1023
)

NetworkInterface (
    LogicalName = "DP24"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1024
)

NetworkInterface (
    LogicalName = "DP25"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1025
)

NetworkInterface (
    LogicalName = "DP26"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1026
)

NetworkInterface (
    LogicalName = "DP27"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1027
)

NetworkInterface (
    LogicalName = "DP28"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
```

```
    IPsecPolicy = IPsecPolicy:L2VPN:1028
)

NetworkInterface (
    LogicalName = "DP29"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1029
)

NetworkInterface (
    LogicalName = "DP30"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1030
)

NetworkInterface (
    LogicalName = "DP31"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1031
)

NetworkInterface (
    LogicalName = "DP32"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1032
)

NetworkInterface (
    LogicalName = "DP33"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1033
)

NetworkInterface (
    LogicalName = "DP34"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1034
)

NetworkInterface (
    LogicalName = "DP35"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1035
)

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

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

3. Конфигурация L2 (data plane)

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

```
[PERFORMANCE]
threads = 36                        ;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 Spoke1-2

1. Конфигурация 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
username          cscons          privilege          15          secret          5
$6$lQHk46/t$MDufPsXck4QGNohEy/CS8Qf/U9SF7LZfA/1RC9RBjLwOIP5vIjiDE7bYGKfodQwUcopzFDVLf
1v.6m9CV.Zan0
aaa new-model
!
!
hostname Spoke1-2
enable secret 5 vIWbAnRJu0Afqhm/xJTTXg==
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
```

```
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.1.3
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.1.3 host 172.16.100.3
!
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
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACL_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set peer 172.16.100.3
 set pre-fragmentation
 set dead-connection history off
!
interface TenGigabitEthernet0/0
 no ip address
!
interface DP0
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1000
!
interface DP1
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1001
!
interface DP2
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1002
!
interface DP3
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1003
!
interface DP4
 ip access-group FW_INPUT_DP in
```

```
 crypto map L2VPN
 crypto ipsec stream-id 1004
!
interface DP5
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1005
!
interface DP6
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1006
!
interface DP7
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1007
!
interface DP8
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1008
!
interface DP9
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1009
!
interface DP10
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1010
!
interface DP11
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1011
!
interface DP12
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1012
!
interface DP13
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1013
!
interface DP14
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1014
!
interface DP15
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1015
!
interface DP16
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1016
!
interface DP17
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
```

```
 crypto ipsec stream-id 1017
!
interface DP18
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1018
!
interface DP19
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1019
!
interface DP20
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1020
!
interface DP21
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1021
!
interface DP22
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1022
!
interface DP23
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1023
!
interface DP24
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1024
!
interface DP25
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1025
!
interface DP26
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1026
!
interface DP27
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1027
!
interface DP28
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1028
!
interface DP29
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1029
!
interface DP30
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1030
```

```
!
interface DP31
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1031
!
interface DP32
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1032
!
interface DP33
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1033
!
interface DP34
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1034
!
interface DP35
 ip access-group FW_INPUT_DP in
 crypto map L2VPN
 crypto ipsec stream-id 1035
!
interface vEthernet0
 description WAN
 ip access-group FW_INPUT_WAN in
 ip inspect INSPECT out
!
interface vEthernet1
 description LAN
!
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
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Mon Dec  2 15:05:44 2024

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Mon Dec  2 15:05:44 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
```

```
            Destination = 0.0.0.0/0
            Gateway = 172.16.1.1
        )

)

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

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

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

FilterChain 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 = 172.16.1.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.1.3
        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 = 172.16.1.3
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.3
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.3
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 172.16.1.3
        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
    ))

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:1
(
    IKEPeerIPFilter = 172.16.100.3
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 10
)

IPsecAction IPsecAction:L2VPN:1
(
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.3
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
)

const IPsecPolicy:L2VPN = FilterChain  (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 172.16.1.3
        DestinationIP = 172.16.100.3
        ProtocolID = 97
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:L2VPN:1 >
        LogEventID = "IPsec:Protect:L2VPN:1:IPSEC_ACL_HUB1_AND_SPOKE1"
    )
)
```

```
FilterChain IPsecPolicy:L2VPN:1000 (
    +IPsecPolicy:L2VPN
    StreamID = 1000
)

FilterChain IPsecPolicy:L2VPN:1001 (
    +IPsecPolicy:L2VPN
    StreamID = 1001
)

FilterChain IPsecPolicy:L2VPN:1002 (
    +IPsecPolicy:L2VPN
    StreamID = 1002
)

FilterChain IPsecPolicy:L2VPN:1003 (
    +IPsecPolicy:L2VPN
    StreamID = 1003
)

FilterChain IPsecPolicy:L2VPN:1004 (
    +IPsecPolicy:L2VPN
    StreamID = 1004
)

FilterChain IPsecPolicy:L2VPN:1005 (
    +IPsecPolicy:L2VPN
    StreamID = 1005
)

FilterChain IPsecPolicy:L2VPN:1006 (
    +IPsecPolicy:L2VPN
    StreamID = 1006
)

FilterChain IPsecPolicy:L2VPN:1007 (
    +IPsecPolicy:L2VPN
    StreamID = 1007
)

FilterChain IPsecPolicy:L2VPN:1008 (
    +IPsecPolicy:L2VPN
    StreamID = 1008
)

FilterChain IPsecPolicy:L2VPN:1009 (
    +IPsecPolicy:L2VPN
    StreamID = 1009
)

FilterChain IPsecPolicy:L2VPN:1010 (
    +IPsecPolicy:L2VPN
    StreamID = 1010
)

FilterChain IPsecPolicy:L2VPN:1011 (
    +IPsecPolicy:L2VPN
    StreamID = 1011
)

FilterChain IPsecPolicy:L2VPN:1012 (
    +IPsecPolicy:L2VPN
    StreamID = 1012
)

FilterChain IPsecPolicy:L2VPN:1013 (
```

```
    +IPsecPolicy:L2VPN
    StreamID = 1013
)

FilterChain IPsecPolicy:L2VPN:1014 (
    +IPsecPolicy:L2VPN
    StreamID = 1014
)

FilterChain IPsecPolicy:L2VPN:1015 (
    +IPsecPolicy:L2VPN
    StreamID = 1015
)

FilterChain IPsecPolicy:L2VPN:1016 (
    +IPsecPolicy:L2VPN
    StreamID = 1016
)

FilterChain IPsecPolicy:L2VPN:1017 (
    +IPsecPolicy:L2VPN
    StreamID = 1017
)

FilterChain IPsecPolicy:L2VPN:1018 (
    +IPsecPolicy:L2VPN
    StreamID = 1018
)

FilterChain IPsecPolicy:L2VPN:1019 (
    +IPsecPolicy:L2VPN
    StreamID = 1019
)

FilterChain IPsecPolicy:L2VPN:1020 (
    +IPsecPolicy:L2VPN
    StreamID = 1020
)

FilterChain IPsecPolicy:L2VPN:1021 (
    +IPsecPolicy:L2VPN
    StreamID = 1021
)

FilterChain IPsecPolicy:L2VPN:1022 (
    +IPsecPolicy:L2VPN
    StreamID = 1022
)

FilterChain IPsecPolicy:L2VPN:1023 (
    +IPsecPolicy:L2VPN
    StreamID = 1023
)

FilterChain IPsecPolicy:L2VPN:1024 (
    +IPsecPolicy:L2VPN
    StreamID = 1024
)

FilterChain IPsecPolicy:L2VPN:1025 (
    +IPsecPolicy:L2VPN
    StreamID = 1025
)

FilterChain IPsecPolicy:L2VPN:1026 (
    +IPsecPolicy:L2VPN
```

```
    StreamID = 1026
)

FilterChain IPsecPolicy:L2VPN:1027 (
    +IPsecPolicy:L2VPN
    StreamID = 1027
)

FilterChain IPsecPolicy:L2VPN:1028 (
    +IPsecPolicy:L2VPN
    StreamID = 1028
)

FilterChain IPsecPolicy:L2VPN:1029 (
    +IPsecPolicy:L2VPN
    StreamID = 1029
)

FilterChain IPsecPolicy:L2VPN:1030 (
    +IPsecPolicy:L2VPN
    StreamID = 1030
)

FilterChain IPsecPolicy:L2VPN:1031 (
    +IPsecPolicy:L2VPN
    StreamID = 1031
)

FilterChain IPsecPolicy:L2VPN:1032 (
    +IPsecPolicy:L2VPN
    StreamID = 1032
)

FilterChain IPsecPolicy:L2VPN:1033 (
    +IPsecPolicy:L2VPN
    StreamID = 1033
)

FilterChain IPsecPolicy:L2VPN:1034 (
    +IPsecPolicy:L2VPN
    StreamID = 1034
)

FilterChain IPsecPolicy:L2VPN:1035 (
    +IPsecPolicy:L2VPN
    StreamID = 1035
)

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

NetworkInterface (
    LogicalName = "DP0"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1000
)

NetworkInterface (
    LogicalName = "DP1"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1001
```

```
)

NetworkInterface (
    LogicalName = "DP2"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1002
)

NetworkInterface (
    LogicalName = "DP3"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1003
)

NetworkInterface (
    LogicalName = "DP4"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1004
)

NetworkInterface (
    LogicalName = "DP5"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1005
)

NetworkInterface (
    LogicalName = "DP6"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1006
)

NetworkInterface (
    LogicalName = "DP7"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1007
)

NetworkInterface (
    LogicalName = "DP8"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1008
)

NetworkInterface (
    LogicalName = "DP9"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1009
)

NetworkInterface (
    LogicalName = "DP10"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1010
)

NetworkInterface (
```

```
    LogicalName = "DP11"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1011
)

NetworkInterface (
    LogicalName = "DP12"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1012
)

NetworkInterface (
    LogicalName = "DP13"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1013
)

NetworkInterface (
    LogicalName = "DP14"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1014
)

NetworkInterface (
    LogicalName = "DP15"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1015
)

NetworkInterface (
    LogicalName = "DP16"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1016
)

NetworkInterface (
    LogicalName = "DP17"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1017
)

NetworkInterface (
    LogicalName = "DP18"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1018
)

NetworkInterface (
    LogicalName = "DP19"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1019
)

NetworkInterface (
    LogicalName = "DP20"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
```

```
    IPsecPolicy = IPsecPolicy:L2VPN:1020
)

NetworkInterface (
    LogicalName = "DP21"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1021
)

NetworkInterface (
    LogicalName = "DP22"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1022
)

NetworkInterface (
    LogicalName = "DP23"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1023
)

NetworkInterface (
    LogicalName = "DP24"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1024
)

NetworkInterface (
    LogicalName = "DP25"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1025
)

NetworkInterface (
    LogicalName = "DP26"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1026
)

NetworkInterface (
    LogicalName = "DP27"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1027
)

NetworkInterface (
    LogicalName = "DP28"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1028
)

NetworkInterface (
    LogicalName = "DP29"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1029
)
```

```
NetworkInterface (
    LogicalName = "DP30"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1030
)

NetworkInterface (
    LogicalName = "DP31"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1031
)

NetworkInterface (
    LogicalName = "DP32"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1032
)

NetworkInterface (
    LogicalName = "DP33"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1033
)

NetworkInterface (
    LogicalName = "DP34"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1034
)

NetworkInterface (
    LogicalName = "DP35"
    InputFilter = FilterChain:FW_INPUT_DP
    OutputFilter = IPv6Default
    IPsecPolicy = IPsecPolicy:L2VPN:1035
)

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

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

3. Конфигурация L2 (data plane)

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

```
[PERFORMANCE]
threads = 36                        ;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 = 172.16.1.3/24
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 = 172.16.1.3
l2_dst_ip = 172.16.100.3
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
```