Построение L2 VPN туннеля между двумя «С-Терра Шлюз DP»

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

Введение

Данный сценарий описывает настройку «С-Терра Шлюз DP» для безопасного взаимодействия между центральным офисом и филиалом на втором уровне модели OSI (L2 VPN). Также в документе показан пример настройки «С-Терра Шлюз DP» для защищенного удаленного доступа (L3 VPN) с целью управления.

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

Настройки «С-Терра Клиент» в данном сценарии не описываются, конфигурирование происходит по аналогии со сценарием «Организация защищенного взаимодействия между криптошлюзом «С-Терра Шлюз» и удаленным VPN клиентом «С-Терра Клиент».

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, «С-Терра Клиент» 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.

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

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

2. Требования к сетевому взаимодействию.

2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

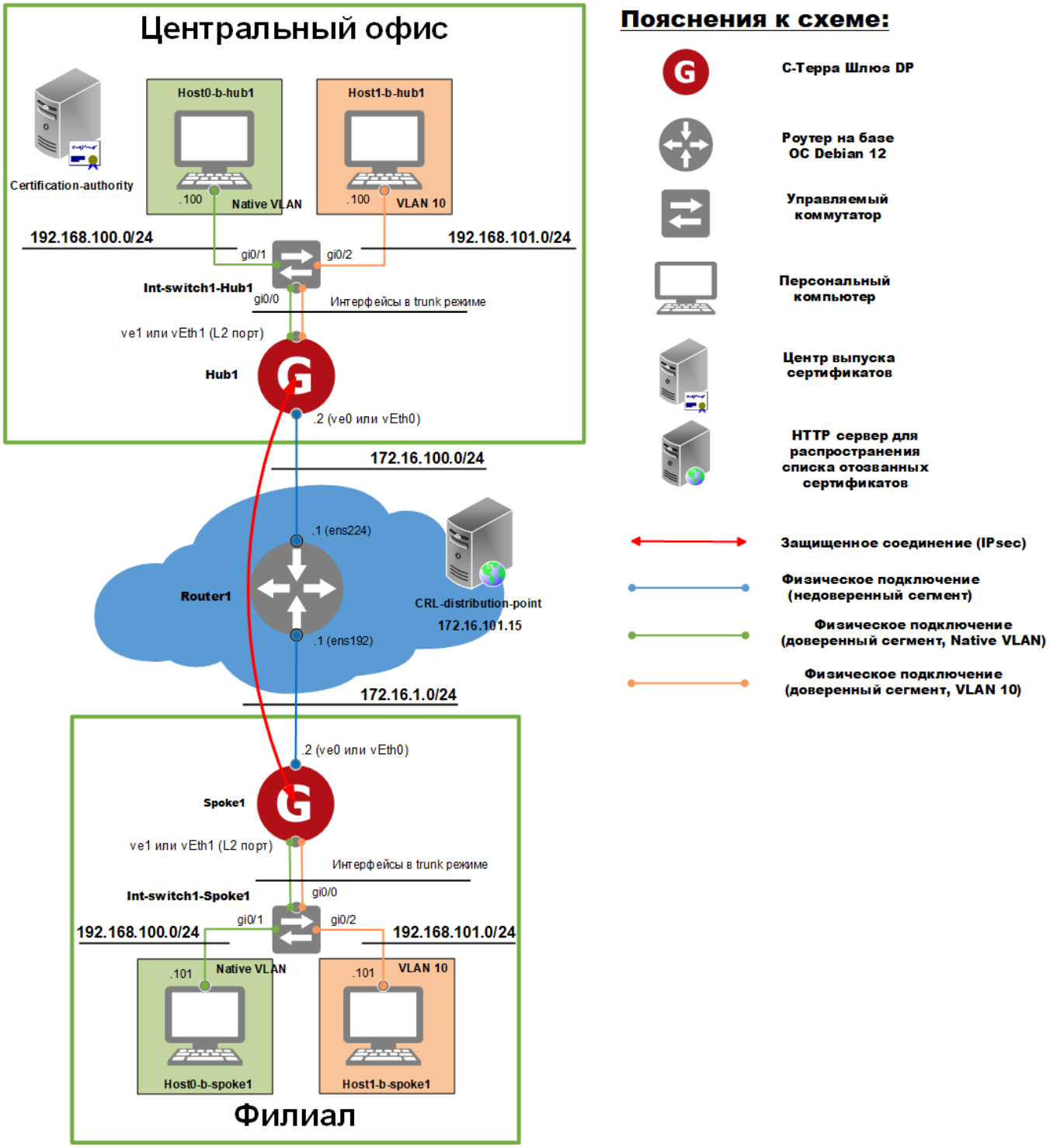


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification-authority), криптошлюз «С-Терра Шлюз DP» (Hub1), управляемый коммутатор (Int-switch1-Hub1) и персональные компьютеры (Host0-b-hub1 и Host1-b-hub1).

   1.2. В филиале размещаются: криптошлюз «С-Терра Шлюз DP» (Spoke1), управляемый коммутатор (Int-switch1-Spoke1) и персональные компьютеры (Host0-b-spoke1 и Host1-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 DP» будет считаться успешным, если по протоколу ICMP (или «ping») будет доступен HTTP сервер для распространения списка отозванных сертификатов (устройство CRL-distribution-point на схеме).

   2.1. Криптошлюз Hub1 подключается к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Router1).

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

3. L2 VPN/L3 VPN.

   Общие сведения

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

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

   Логика обработка фреймов/пакетов

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

   Логика настройки шифрования

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

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

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

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

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

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

Накладные расходы (overhead) L2 VPN

Так как оригинальный фрейм инкапсулируется в EtherIP (протокол 97), то накладные расходы инкапсуляции L2 – это 22 байта.

Накладные расходы инкапсуляции IPsec для туннельного режима могут составлять от 50 до 60 байт (зависит от алгоритма шифрования и наличия NAT).

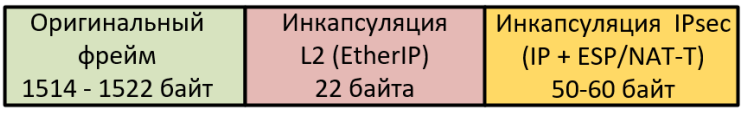


Рисунок 2. Накладные расходы (overhead) L2 + IPsec

Рисунок (см. рисунок 2) показывает минимальный и максимальный размер накладных расходов при организации L2 VPN для оригинального нетегированного, 802.1 Q и QinQ фрейма. Если шифруется MPLS, то размер оригинального фрейма может варьироваться в зависимости от количества меток в стеке, учитывайте это.

Для транспортного режима IPsec накладные расходы IPsec инкапсуляции будут на 20 байт меньше, по сравнению с туннельным режимом.

Из рисунка (см. рисунок 2) видно, что с учетом размера оригинального фрейма, а также L2 и IPsec инкапсуляций результирующий пакет может иметь размер от 1586 до 1604 байт. Если MTU на WAN интерфейсе «С-Терра Шлюз DP» имеет значение в 1500 байт, то инкапсулированные пакеты будут фрагментированы (фрагментация по умолчанию выключена), что в свою очередь приведет к снижению производительности (до 15 %). Соответственно, при наличии возможности, заказывайте нужный вам

MTU у вашего провайдера на каналообразующем оборудовании, чтобы избежать фрагментации и снижения производительности.

Фрагментация, MTU и DF бит

Фрагментация по умолчанию выключена. Чтобы ее включить нужно в файле `/opt/VPNagent/etc/ipsm_dpdk.cfg` для порта `[PORT<N>]`, который соответствует WAN интерфейсу, параметру `dp_frag_ip` в качестве значения задать IP адрес партнера, который также является «С-Терра Шлюз DP» версии 5.0 и выше. Если «С-Терра Шлюз DP» находится за статическим NAT (динамический не поддерживается), то параметру `dp_frag_natt` нужно выставить значение `yes`.

Пример:

```
[PORT0]
...
outer = yes
dp_frag_ip = 172.16.100.2
dp_frag_natt = yes
...
```

Фрагментация пакетов происходит после зашифрования. Статистику по зашифрованным пакетам можно посмотреть при помощи утилиты `kstat_show` (счетчик `frag ok`).

В случае, если в криптокарте на DP интерфейсах включена префрагментация, то включать фрагментацию в файле `/opt/VPNagent/etc/ipsm_dpdk.cfg` не требуется.

Чтобы уменьшить количество фрагментированных транзитных пакетов (L2 VPN) рекомендуется включать механизмы PMTUD и MSSFIX (параметры `pmtud` и `mssfix` в файле `/opt/VPNagent/etc/ipsm_dpdk.cfg`) для порта `[PORT<N>]`, который соответствует LAN интерфейсу. Данные механизмы работают только для IPv4 пакетов. Пример:

```
[PORT1]
...
mtu = 1500
pmtud = 1400
mssfix = 1360
...
```

Механизмы PMTUD и MSSFIX применимы для пакетов протокола IPv4, которые вкладываются в Ethernet/802.1Q/QinQ. Для MPLS не применимы.

MTU для LAN и WAN интерфейсов задается в процессе инициализации «С-Терра Шлюз DP» в мастере настроек (MTU также можно изменить через консоль cisco-like или же через файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`, параметр `mtu` для соответствующего порта `[PORT<N>]`).

По умолчанию DF (don't fragment) бит с исходных пакетов на инкапсулированные не переносится (можно включить перенос DF бита, но не рекомендуется).

Защита 802.1Q/QinQ/MPLS трафика

Для шифрования 802.1Q/QinQ/MPLS трафика никаких дополнительных настроек не требуется.

Управление «С-Терра Шлюз DP» через интерфейс захвата пакетов (LAN интерфейс)

Управление «С-Терра Шлюз DP» через интерфейс захвата пакетов (LAN интерфейс) невозможно.

Управление «С-Терра Шлюз DP» через выделенный сетевой интерфейс

Для управления «С-Терра Шлюз DP» из LAN сегмента используйте выделенный сетевой интерфейс. Данный интерфейс не должен быть добавлен в конфигурационный файл `/opt/VPNagent/etc/ipsm_dpdk.cfg`, а его настройку нужно производить через cisco-like консоль. Пример:

```
sterragate#show running-config
```

```
...
interface GigabitEthernet0/2
 ip address 192.168.253.1 255.255.255.0
...
```

Пропуск фреймов протоколов LACP/LLDP

По умолчанию фреймы протоколов LACP/LLDP пропускаются через «С-Терра Шлюз DP».

Копирование ToS байта из оригинального пакета в инкапсулированный

Копирование ToS байта из оригинального пакета в инкапсулированный EtherIP включается при помощи параметра `copy_tos` в конфигурационном файле `/opt/VPNagent/etc/ipsm_dpdk.cfg`. Копирование ToS байта из EtherIP в ESP/NAT-T пакеты происходит по умолчанию.

Применимо для пакетов протокола IPv4, которые вкладываются в Ethernet/802.1Q/QinQ. Для MPLS копирование не работает.

VLAN (802.1Q) на WAN интерфейсе

Чтобы пакеты, уходящие с WAN интерфейса, тегировались определенным VLAN ID нужно в конфигурационном файле `/opt/VPNagent/etc/ipsm_dpdk.cfg` для соответствующего порта параметру `vlan_identifier` выставить нужное значение. Пример:

```
[PORT0]
...
outer = yes
vlan_identifier = 42
...
```

В файле `/etc/network/interfaces` никаких настроек делать не нужно.

На соответствующему данному WAN порту интерфейсе `vEthernet<N>` в консоли cisco-like нужно, чтобы была прикреплена либо криптокарта (L3 VPN), либо список доступа (любой). Иначе тегирование работать не будет.

4. Параметры межсетевого экранирования.

   Для пакетов применяются следующие правила фильтрации:

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

   4.2. На WAN интерфейсах vEthernet0 разрешен входящий IPv4 трафик:

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

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

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

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

   4.3. На WAN интерфейсах vEthernet0 IPv6 трафик заблокирован.

   4.4. На WAN интерфейсах vEthernet0 инспектируются все исходящие локальные и транзитные IPv4 соединения для протоколов TCP и UDP. На основе результатов инспектирования осуществляется фильтрация входящего трафика с учетом состояния сессии (stateful).

   4.5. На DP интерфейсах разрешен входящий IPv4 трафик:

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

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

   4.6. На DP интерфейсах IPv6 трафик заблокирован.

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

5. Параметры безопасного взаимодействия.

   Весь трафик на втором уровне модели OSI подсетей 192.168.100.0/24 и 192.168.101.0/24, который передается между центральным офисом и филиалом защищается с использованием алгоритмов ГОСТ и протокола IPsec в транспортном режиме, трафик управления (L3 VPN) – в туннельном режиме.

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

   5.1. Параметры протокола IKE:

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

   5.2. Параметры протокола ESP для L2 VPN:

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

   5.3. Параметры протокола ESP для L3 VPN:

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

Настройка стенда

Настройка устройства Router1

1. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 172.16.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Разрешите прохождение IP трафика.

Настройка устройства Int-switch1-Hub1

1. Интерфейс `gi0/0` должен быть в trunk режиме. Должно быть разрешено прохождения фреймов с VLAN ID 10 и других.
2. Интерфейс `gi0/1` должен быть в access режиме (с VLAN тэгом или без него).
3. Интерфейс `gi0/2` должен быть в access режиме с VLAN ID 10.

Настройка устройства Int-switch1-Spoke1

1. Интерфейс `gi0/0` должен быть в trunk режиме. Должно быть разрешено прохождения фреймов с VLAN ID 10 и других.
2. Интерфейс `gi0/1` должен быть в access режиме (с VLAN тэгом или без него).
3. Интерфейс `gi0/2` должен быть в access режиме с VLAN ID 10.

Настройка устройства Host0-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 Host1-b-hub1

1. Настройте IP адрес – 192.168.101.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host0-b-spoke1

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

Настройка устройства Host1-b-spoke1

1. Настройте IP адрес – 192.168.101.101 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Разрешите прием и отправку ICMP пакетов.

Настройка криптошлюза Hub1

Настройка будет происходить локально при помощи консольного подключения.

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

Начальные настройки

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

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

   ```
   S-Terra administrative console
   ```

   введите логин и пароль для CLI разграничения доступа:

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

   ```
   login as: administrator
   ```

   ```
   administrator's password:

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

   administrator@sterragate]
   ```

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

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

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

   3.1. Войдите в linux bash.

   ```
   administrator@sterragate] system
   ```

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

   3.2. Установите нужную временную зону:

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

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

   ```
   root@sterragate:~# date -s "11/15/2024 12:30:00"
   ```

   ```
   Fri Nov 15 12:30:00 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:
GATEDP
```

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

В зависимости от аппаратной платформы драйвер может отличаться.
Варианты могут быть следующие: `ixgbe`, `i40e`, `vmxnet3`, `ice`.

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

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

6.4.2 Нажмите Enter на просьбу ввести количество потоков, чтобы было использовано значение по умолчанию (количество потоков соответствует количеству `DP<N>` интерфейсов):

Количество потоков (DP интерфейсов) может отличаться в зависимости от аппаратной платформы. Не изменяйте значение потоков по умолчанию без осознанной необходимости.

```
threads (1-36) [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 |
| 3 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+--------------+---------+
```

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

```
Enter device index to be configured as WAN interface "PORT0" (0-3): 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 WAN интерфейса (в данном сценарии - 24):

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

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

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

6.4.7 Нажмите Enter, если все параметры введены верно:

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

6.4.8 Выберите из вновь предложенного списка PCI адрес для 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 |
| 3 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+---------------+---------+
```

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

```
Enter device index to be configured as LAN interface "PORT1" and paired with "PORT0"
(0-3): 1
```

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

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

```
Enter source IP-address for l2-tunnel (l2_src_ip) (allowed_protocols: ipv4,ipv6):
172.16.100.2
```

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

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

```
Enter destination IP-address for l2-tunnel (l2_dst_ip) (allowed_protocols: ipv4):
172.16.1.2
```

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

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

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

6.4.12 Нажмите Enter, если все параметры введены верно:

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

Дождитесь окончания процедуры:

```
+---+--------------+---------------+---------+
|   |    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 |
| 3 | 0000:1b:00.0 |       -       | vmxnet3 |
+---+--------------+---------------+---------+
INFO: Operation completed successfully. Restart your system to apply the changes
INFO: OK

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

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

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

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

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

6.4.14 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/configure_dp.sh`

Настройка L2

В данном разделе будут описаны:

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

1. Перейдите в linux bash:

```
administrator@Hub1] system
```

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

2. Уменьшите время сборки фрагментированных пакетов:

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

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

3. Дальнейшие настройки осуществляются через 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.

Настройки PKI (запросы и сертификаты)

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

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

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка паролей доступа к консоли cisco-like

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка сетевых параметров

Настройка сетевых параметров проходит в два этапа. Первый – настройка Mgmt интерфейса (`GigabitEthernet0/2`) в cisco-like консоли (данный интерфейс не представлен на схеме). Второй – настройка маршрутизации в cisco-like консоли.

Первый этап.

1. Выведите список всех интерфейсов, доступных в cisco-like консоли и выберите незадействованный в L2. Незадействованные в L2 интерфейсы будут иметь имя `GigabitEthernet0/N`, а задействованные `vEthernetN`:

```
sterragate#show interfaces
```

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 0050.569e.9fd9
  MTU 1500 bytes
```

```
GigabitEthernet0/1 is down, line protocol is down
  Hardware address is 0050.569e.01ea
  MTU 1500 bytes
DP0
  Virtual data plane interface (pattern "10G_000")
DP1
  Virtual data plane interface (pattern "10G_001")
...
DP34
  Virtual data plane interface (pattern "10G_034")
DP35
  Virtual data plane interface (pattern "10G_035")
vEthernet0 is up, line protocol is up
  Hardware address is 0050.569e.1b91
  Description: WAN
  Internet address is 172.16.100.2/24
  MTU 9000 bytes
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.68bd
  MTU 9000 bytes
```

Видно, что интерфейс `GigabitEthernet0/1` не задействован в L2. Интерфейсы `vEthernetN` задействованы в L2, `vEthernet0` соответствует WAN, а `vEthernet1` – LAN.

2. Настройте интерфейс:

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

```
sterragate#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sterragate(config)#interface GigabitEthernet0/1
sterragate(config-if)#ip address 192.168.253.1 255.255.255.0
sterragate(config-if)#exit
```

Второй этап.

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

1. Задайте имя устройства:

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

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

```
Hub1(config)#do show interfaces vEthernet0
vEthernet0 is up, line protocol is up
  Hardware address is 0050.569e.1b91
  Description: WAN
  Internet address is 172.16.100.2/24
  MTU 9000 bytes
```

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

```
vEthernet1 is up, line protocol is up
  Hardware address is 0050.569e.68bd
  MTU 9000 bytes
```

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

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

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

4. Проверьте доступность устройства Router1:

```
Hub1(config)#do ping 172.16.100.1
```

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

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

Настройка шифрования

1. Настройте параметры IKE.

   1.1. Задайте общие параметры IKE:

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

   1.2. Создайте политику, описывающую параметры IKE туннеля:

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

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

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

2. Параметры IPsec для защиты транзитного L2 трафика.

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

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

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

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

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

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

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

```
Hub1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
Hub1(config-ext-nacl)#remark EtherIP L2 tunnel
Hub1(config-ext-nacl)#permit etherip host 172.16.100.2 host 172.16.1.2
Hub1(config-ext-nacl)#exit
```

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

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

2.5.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKE1
```

2.5.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

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

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

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

2.5.4 Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

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

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

2.5.6 Включите префрагментацию:

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

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

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

3. Параметры IPsec для защиты удаленного управления криптошлюзом.

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

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

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

```
Hub1(config)#ip access-list extended ADMIN_ACL
```

```
Hub1(config-ext-nacl)#remark MGMT IP
Hub1(config-ext-nacl)#permit ip host 192.168.253.1 host 192.168.255.1
Hub1(config-ext-nacl)#exit
Hub1(config)#
```

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

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

3.3.1 Укажите список доступа для защищаемого трафика:

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

3.3.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

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

3.3.3 Укажите IKECFG пул:

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

3.3.4 Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

3.3.5 Включите префрагментацию:

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

3.3.6 Включите автоматическую и интеллектуальную корректировку значения MSS:

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

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

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

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

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

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

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

3.6. Примените настройки:

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

Настройка политики обработки COC (CRL)

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

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка межсетевого экрана

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

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

```
Hub1(config-network-group)#host 172.16.100.2
Hub1(config-network-group)#exit
```

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

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

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

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

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

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

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

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

6. Прикрепите правила межсетевого экранирования на все DP интерфейсы:

```
Hub1(config)#interface range DP 0 - 35
Hub1(config-if-range)#ip access-group FW_INPUT_DP in
Hub1(config-if-range)#exit
```

7. Примените настройки:

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

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

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

Настройка криптошлюза Spoke1

Настройка криптошлюза Spoke1 происходит аналогично настройке Hub1.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

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

```
Hub1#ping 172.16.100.1
```

```
PING 172.16.100.1 (172.16.100.1) 100(128) bytes of data.
108 bytes from 172.16.100.1: icmp_seq=1 ttl=64 time=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
```

```
Spoke1#ping 172.16.1.1
```

```
PING 172.16.1.1 (172.16.1.1) 100(128) bytes of data.
108 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=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
```

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

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

```
Hub1#ping 172.16.1.2
```

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

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

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

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 Hub1 и Spoke1

1. Инициируйте построение защищенного L2 соединения между криптошлюзами Hub1 и Spoke1 с любого из защищаемых устройств. Для проверки выберем пары устройств Host0-b-spoke1 на Host0-b-hub1

(можно и наоборот) из **Native VLAN** и Host1-b-spoke1 на Host1-b-hub1 (можно и наоборот) из **VLAN ID 10**.

1.1. Выполните команду `ping` из linux bash консоли защищаемого устройства Host0-b-spoke1.

```
root@Host0-b-spoke1:~# ping 192.168.100.100 -c 5
```

```
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=64 time=3.48 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=64 time=3.25 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=64 time=3.03 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=64 time=2.71 ms
64 bytes from 192.168.100.100: icmp_seq=5 ttl=64 time=3.03 ms

--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 2.706/3.099/3.481/0.263 ms
```

1.2. Выполните команду `ping` из linux bash консоли защищаемого устройства Host1-b-spoke1.

```
root@Host1-b-spoke1:~# ping 192.168.101.100 -c 5
```

```
PING 192.168.101.100 (192.168.101.100) 56(84) bytes of data.
64 bytes from 192.168.101.100: icmp_seq=1 ttl=64 time=4.43 ms
64 bytes from 192.168.101.100: icmp_seq=2 ttl=64 time=3.70 ms
64 bytes from 192.168.101.100: icmp_seq=3 ttl=64 time=3.45 ms
64 bytes from 192.168.101.100: icmp_seq=4 ttl=64 time=2.47 ms
64 bytes from 192.168.101.100: icmp_seq=5 ttl=64 time=2.63 ms

--- 192.168.101.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 2.473/3.336/4.428/0.719 ms
```

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

```
Hub1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 2 (172.16.100.2,500)-(172.16.1.2,500) active 15676 15432

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 2 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 416 272
2 3 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 376 416
3 4 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 416 416
4 5 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 416 376
5 6 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 416 416
6 7 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 416
7 8 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 64 104
8 9 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 208 208
9 10 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 272 272
10 11 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
11 12 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 272 272
12 13 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
13 14 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
14 15 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
15 16 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 272 312
16 17 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 376 272
17 18 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
18 19 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
19 20 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
20 21 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
```

```
21 22 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
22 23 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
23 24 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
24 25 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 272 312
25 26 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 272
26 27 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 232 312
27 28 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 232
28 29 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
29 30 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
30 31 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 284
31 32 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
32 33 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
33 34 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
34 35 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
35 36 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 312 312
36 37 (172.16.100.2,*)-(172.16.1.2,*) 97 ESP trans 272 272
```

```
Spoke1#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 2 (172.16.1.2,500)-(172.16.100.2,500) active 15432 15676

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 2 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 584 728
2 3 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 688
3 4 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 728
4 5 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 688 728
5 6 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 728
6 7 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 728
7 8 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 104 0
8 9 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
9 10 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 688 688
10 11 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 728
11 12 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 688 688
12 13 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 624
13 14 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 728 624
14 15 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
15 16 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 584
16 17 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 584 688
17 18 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
18 19 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
19 20 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
20 21 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
21 22 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
22 23 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
23 24 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 584
24 25 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 584 544
25 26 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 544 624
26 27 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 608
27 28 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 544 584
28 29 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 584 584
29 30 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 688 624
30 31 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 556 624
31 32 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 584
32 33 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
33 34 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
34 35 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 544 544
35 36 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 624 624
36 37 (172.16.1.2,*)-(172.16.100.2,*) 97 ESP trans 584 584
```

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

Проверка Path MTU Discovery

Проверка выполняется с любого из защищаемых устройств, в данном примере с устройства Host1-b-hub1. Значение MTU на интерфейсе устройства Host1-b-hub1 должно быть больше, чем значение параметра `pmtud` на криптошлюзе.

1. Отправьте ICMP запрос на устройство Host1-b-spoke1 такого размера, чтобы результирующий размер IP пакета был равен 8900 байт (что соответствует значению параметра pmtud на криптошлюзах), установите DF-бит:

```
root@host1-b-hub1:~# ping 192.168.101.101 -s 8872 -M do -c 1
```

```
PING 192.168.101.101 (192.168.101.101) 8872(8900) bytes of data.
8880 bytes from 192.168.101.101: icmp_seq=1 ttl=64 time=4.31 ms

--- 192.168.101.101 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.311/4.311/4.311/0.000 ms
```

2. Увеличьте размер на 1 байт и снова отправьте ICMP запрос:

```
root@host1-b-hub1:~# ping 192.168.101.101 -s 8873 -M do -c 1
```

```
PING 192.168.101.101 (192.168.101.101) 8873(8901) bytes of data.
From 192.168.101.101 icmp_seq=1 Frag needed and DF set (mtu = 8900)

--- 192.168.101.101 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Видно, что, если размер пакета превысит заданное в параметре pmtud значение, в ответ на него будет сформирован пакет ICMP Destination Unreachable (Fragmentation Needed).

Проверка MSSfix

Проверка выполняется на любой из пар защищаемых устройств, в данном примере на устройствах Host1-b-hub1 и Host1-b-spoke1.

1. На устройстве Host1-b-hub1 запустите утилиту tcpdump для просмотра TCP трафика на сетевом интерфейсе:

```
root@host1-b-hub1:~# tcpdump -i ens192 -nvvv proto 6
```

2. На устройстве Host1-b-spoke1 запустите утилиту tcpdump для просмотра TCP трафика на сетевом интерфейсе:

```
root@host1-b-spoke1:~# tcpdump -i ens192 -nvvv proto 6
```

3. С устройства Host1-b-hub1 инициируйте TCP сессию на устройство Host1-b-spoke1, например, с помощью утилит curl или wget:

```
root@host1-b-hub1:~# curl 192.168.101.101
```

```
curl: (7) Failed to connect to 192.168.101.101 port 80: Connection refused
```

4. На устройстве Host1-b-hub1 в выводе утилиты tcpdump проверьте значение MSS в исходящем трафике:

```
17:27:42.410526 IP (tos 0x0, ttl 64, id 44614, offset 0, flags [DF], proto TCP (6),
length 60)
    192.168.101.100.33898 > 192.168.101.101.80: Flags [S], cksum 0x4c49 (incorrect ->
0xc9fd), seq 1536386096, win 62720, options [mss 8960,sackOK,TS val 3043304887 ecr
0,nop,wscale 7], length 0
```

```
17:27:42.762510 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length
40)
    192.168.101.101.80 > 192.168.101.100.33898: Flags [R.], cksum 0x1f37 (correct),
seq 0, ack 1536386097, win 0, length 0
```

5. На устройстве Host1-b-spoke1 в выводе утилиты tcpdump проверьте значение MSS во входящем трафике:

```
17:27:43.064355 IP (tos 0x0, ttl 64, id 44614, offset 0, flags [DF], proto TCP (6),
length 60)
    192.168.101.100.33898 > 192.168.101.101.80: Flags [S], cksum 0xca61 (correct), seq
1536386096, win 62720, options [mss 8860,sackOK,TS val 3043304887 ecr 0,nop,wscale 7],
length 0
17:27:43.064418 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length
40)
    192.168.101.101.80 > 192.168.101.100.33898: Flags [R.], cksum 0x1f37 (correct),
seq 0, ack 1536386097, win 0, length 0
```

Видно, что механизм mssfix на шлюзе заменил значение MSS в TCP пакете от устройства Host1-b-hub1 к устройству Host1-b-spoke1 на значение, заданное в параметре `mssfix`.

Проверка префрагментации

Для проверки работы префрагментации следует на криптошлюзах отключить механизм Path MTU Discovery (закомментировать параметр `pmtud`), установить одинаковое значение MTU на WAN и LAN интерфейсах (в данном примере – 9000), для параметра `df_handling` установить значение copy. MTU на интерфейсах всех остальных устройств – 9000.

1. На устройстве Router1 запустите утилиту tcpdump для просмотра IPsec (протокол ESP) трафика на сетевом интерфейсе ens224:

```
root@Router1:~# tcpdump -i ens224 -envvv proto 50
```

2. На устройстве Host1-b-hub1 запустите утилиту tcpdump для просмотра ICMP трафика на сетевом интерфейсе:

```
root@host1-b-hub1:~# tcpdump -i ens192 -envvv proto 1
```

3. С устройства Host1-b-hub1 отправьте ICMP запрос на устройство Host1-b-spoke1 такого размера, чтобы результирующий размер IP пакетов был равен значению MTU (9000), DF бит при этом следует обнулить:

```
root@host1-b-hub1:~# ping 192.168.101.101 -s 8972 -M dont -c 1
```

```
PING 192.168.101.101 (192.168.101.101) 8972(9000) bytes of data.
8980 bytes from 192.168.101.101: icmp_seq=1 ttl=64 time=10.6 ms

--- 192.168.101.101 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.562/10.562/10.562/0.000 ms
```

4. На устройстве Host1-b-hub1 в выводе утилиты tcpdump проверьте размер IP пакетов и отсутствие фрагментации:

```
14:20:19.793725 00:50:56:9e:1e:fd > 00:50:56:9e:be:a5, ethertype IPv4 (0x0800), length
9014: (tos 0x0, ttl 64, id 18210, offset 0, flags [none], proto ICMP (1), length 9000)
    192.168.101.100 > 192.168.101.101: ICMP echo request, id 10625, seq 1, length 8980
14:20:19.807393 00:50:56:9e:be:a5 > 00:50:56:9e:1e:fd, ethertype IPv4 (0x0800), length
9014: (tos 0x0, ttl 64, id 13724, offset 0, flags [none], proto ICMP (1), length 9000)
    192.168.101.101 > 192.168.101.100: ICMP echo reply, id 10625, seq 1, length 8980
```

5. На устройстве Router1 в выводе утилиты tcpdump проверьте размер ESP пакетов и отсутствие фрагментации:

```
07:20:25.143310 00:50:56:9e:b7:bc > 00:50:56:9e:b9:ff, ethertype IPv4 (0x0800), length
9010: (tos 0x0, ttl 255, id 29328, offset 0, flags [none], proto ESP (50), length 8996)
    172.16.100.2 > 172.16.1.2: ESP(spi=0x2a4f2463,seq=0x8), length 8976
```

```
07:20:25.143310 00:50:56:9e:b7:bc > 00:50:56:9e:b9:ff, ethertype IPv4 (0x0800), length
174: (tos 0x0, ttl 255, id 29329, offset 0, flags [none], proto ESP (50), length 160)
    172.16.100.2 > 172.16.1.2: ESP(spi=0x2a4f2463,seq=0x9), length 140
07:20:25.145023 00:50:56:9e:b9:ff > 00:50:56:9e:b7:bc, ethertype IPv4 (0x0800), length
9010: (tos 0x0, ttl 254, id 53464, offset 0, flags [none], proto ESP (50), length 8996)
    172.16.1.2 > 172.16.100.2: ESP(spi=0x65ff16ce,seq=0x8), length 8976
07:20:25.145031 00:50:56:9e:b9:ff > 00:50:56:9e:b7:bc, ethertype IPv4 (0x0800), length
174: (tos 0x0, ttl 254, id 53465, offset 0, flags [none], proto ESP (50), length 160)
    172.16.1.2 > 172.16.100.2: ESP(spi=0x65ff16ce,seq=0x9), length 140
```

Видно, что исходные ICMP пакеты не фрагментированы, фрагментация пакетов выполняется до шифрования, результирующий размер IPsec пакетов не превышает MTU на WAN интерфейсах криптошлюзов, IPsec пакеты не фрагментированы.

6. С устройства Host1-b-hub1 снова отправьте ICMP запрос на устройство Host1-b-spoke1 того же размера, но с выставленным DF битом:

```
root@host1-b-hub1:~# ping 192.168.101.101 -s 8972 -M do -c 1
```

```
PING 192.168.101.101 (192.168.101.101) 8972(9000) bytes of data.

--- 192.168.101.101 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

7. На устройстве Host1-b-hub1 в выводе утилиты tcpdump проверьте размер IP пакета и отсутствие фрагментации:

```
14:35:55.775096 00:50:56:9e:1e:fd > 00:50:56:9e:be:a5, ethertype IPv4 (0x0800), length
9014: (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1), length 9000)
    192.168.101.100 > 192.168.101.101: ICMP echo request, id 10634, seq 1, length 8980
```

8. На устройстве Router1 в выводе утилиты tcpdump проверьте, что ESP пакеты отсутствуют совсем, или присутствуют только ESP пакеты малого размера (ARP трафик):

```
07:40:38.414228 00:50:56:9e:b7:bc > 00:50:56:9e:b9:ff, ethertype IPv4 (0x0800), length
146: (tos 0x0, ttl 255, id 53539, offset 0, flags [none], proto ESP (50), length 132)
    172.16.100.2 > 172.16.1.2: ESP(spi=0x5c5c0241,seq=0x56), length 112
07:40:38.474687 00:50:56:9e:b9:ff > 00:50:56:9e:b7:bc, ethertype IPv4 (0x0800), length
146: (tos 0x0, ttl 254, id 20782, offset 0, flags [none], proto ESP (50), length 132)
    172.16.1.2 > 172.16.100.2: ESP(spi=0xdd24bed4,seq=0x53), length 112
```

Видно, что теперь ICMP запрос не проходит, так как размер его пакета после зашифрования превысит MTU на WAN интерфейсе криптошлюза, и при этом выставленный DF бит не разрешает фрагментировать этот пакет.

Примечание: для того, чтобы префрагментация пакетов на криптошлюзе могла выполняться вне зависимости от значения DF бита в пакетах, следует на криптошлюзах в cisco-like консоли в криптокарте задать параметр `set pre-fragmentation force`. Также можно закомментировать параметр `df_handling` в конфигурационном файле ipsm_dpdk.cfg (таким образом значение DF бита будет обнуляться при инкапсулировании исходного пакета в EtherIP).

Диагностика

Телеметрия

Для получения текущих значений телеметрии можно воспользоваться утилитой `dpdk-telemetry.py`:

```
root@sterragate:~# dpdk-telemetry.py
```

```
Connecting to /var/run/dpdk/rte/dpdk_telemetry.v2
{
  "version": "DPDK 23.07.0",
  "pid": 814,
  "max_output_len": 16384
}
Connected to application: "ipsm-app"
```

Для просмотра статистики по портам выполните следующую команду:

```
--> /ipsm/port_stats,0
```

где 0 – это номер порта (в данном сценарии 0 – WAN интерфейс, 1 – LAN интерфейс)


```
{
  "/ipsm/port_stats": {
    "ipsm_port_id": 0,
    "pci_id": "0000:03:00.0",
    "sent_total": 768,
    "recv_total": 777,
    "drop_total": 16,
    "bytes_in": 142015,
    "bytes_out": 141053,
    "sendq_len": 0,
    "sq_ovf_cnt": 0,
    "tx_fail": 0,
    "rx_overflow": 0,
    "rx_pa_kill": 0,
    "rx_null_mbuf": 0,
    "kni_tx_fail": 0,
    "process_pktmbuf": 0,
    "free_pdata": 0,
    "free_priv": 0,
    "rx_forbidden_ethertype": 0,
    "kni_tx_to_l2": 0,
    "forbidden_vlan": 0,
    "bad_pkt_to_l2": 0,
    "bad_ipv6_exthdrs": 0,
    "rx_l4_cksum_bad": 0,
    "rx_ip_cksum_bad": 0,
    "rx_outer_l4_cksum_bad": 0
  }
}
```


Для получения информации о сетевых оптических трансиверах на портах выполните команду:

```
--> /ethdev/module_eeprom,0
```


```
{
  "/ethdev/module_eeprom": {
    "Identifier": "0x0d (QSFP+)",
    "Extended identifier": "0xd0",
    "Extended identifier description": "3.5W max. Power consumption; No CDR in TX; No
CDR in RX; High Power Class (> 3.5 W) not enabled",
    "Connector": "0x07 (LC)",
    "Transceiver codes": "0x02 0x00 0x00 0x00 0x10 0x10 0x01 0xd5",
    "Transceiver type": "40G Ethernet: 40G Base-LR4; FC: long distance (L); FC: Longwave
laser (LL); FC: Single Mode (SM); FC: 1200 MBytes/sec; FC: 800 ",
    "Encoding": "0x05 (64B/66B)",
    "BR, Nominal": "10300Mbps",
    "Rate identifier": "0x00",
    "Length (SMF,km)": "20km",
    "Length (OM3 50um)": "0m",
    "Length (OM2 50um)": "0m",
    "Length (OM1 62.5um)": "0m",
    "Length (Copper or Active cable)": "0m",
    "Transmitter technology": "0x40 (1310 nm DFB)",
    "Laser wavelength": "1271.000nm",
    "Laser wavelength tolerance": "50.000nm",
    "Vendor name": "OEM",
    "Vendor OUI": "00:1b:21",
    "Vendor PN": "QSFP+40G-LR4-20",
```

```
    "Vendor rev": "1A",
    "Vendor SN": "XTV2312050959",
    "Date code": "231205",
    "Revision Compliance": "SFF-8636 Rev 1.5",
    "Module temperature": "31.00 degrees C / 87.80 degrees F",
    "Module voltage": "3.2689 V",
    "Alarm/warning flags implemented": "Yes",
    "Laser tx bias current (Channel 1)": "29.212 mA",
    "Laser tx bias current (Channel 2)": "29.538 mA",
    "Laser tx bias current (Channel 3)": "28.798 mA",
    "Laser tx bias current (Channel 4)": "28.888 mA",
    "Transmit avg optical power (Channel 1)": "0.7406 mW / -1.30 dBm",
    "Transmit avg optical power (Channel 2)": "0.7178 mW / -1.44 dBm",
    "Transmit avg optical power (Channel 3)": "0.9179 mW / -0.37 dBm",
    "Transmit avg optical power (Channel 4)": "0.8381 mW / -0.77 dBm",
    "Rcvr signal avg optical power(Channel 1)": "0.0701 mW / -11.54 dBm",
    "Rcvr signal avg optical power(Channel 2)": "0.0424 mW / -13.73 dBm",
    "Rcvr signal avg optical power(Channel 3)": "0.0380 mW / -14.20 dBm",
    "Rcvr signal avg optical power(Channel 4)": "0.0406 mW / -13.91 dBm",
    "Laser bias current high alarm   (Chan 1)": "Off",
    "Laser bias current low alarm    (Chan 1)": "On",
    "Laser bias current high warning (Chan 1)": "Off",
    "Laser bias current low warning  (Chan 1)": "On",
    "Laser bias current high alarm   (Chan 2)": "Off",
    "Laser bias current low alarm    (Chan 2)": "On",
    "Laser bias current high warning (Chan 2)": "Off",
    "Laser bias current low warning  (Chan 2)": "On",
    "Laser bias current high alarm   (Chan 3)": "Off",
    "Laser bias current low alarm    (Chan 3)": "On",
    "Laser bias current high warning (Chan 3)": "Off",
    "Laser bias current low warning  (Chan 3)": "On",
    "Laser bias current high alarm   (Chan 4)": "Off",
    "Laser bias current low alarm    (Chan 4)": "On",
    "Laser bias current high warning (Chan 4)": "Off",
    "Laser bias current low warning  (Chan 4)": "On",
    "Module temperature high alarm": "Off",
    "Module temperature low alarm": "Off",
    "Module temperature high warning": "Off",
    "Module temperature low warning": "Off",
    "Module voltage high alarm": "Off",
    "Module voltage low alarm": "Off",
    "Module voltage high warning": "Off",
    "Module voltage low warning": "Off",
    "Laser tx power high alarm   (Channel 1)": "Off",
    "Laser tx power low alarm    (Channel 1)": "On",
    "Laser tx power high warning (Channel 1)": "Off",
    "Laser tx power low warning  (Channel 1)": "On",
    "Laser tx power high alarm   (Channel 2)": "Off",
    "Laser tx power low alarm    (Channel 2)": "On",
    "Laser tx power high warning (Channel 2)": "Off",
    "Laser tx power low warning  (Channel 2)": "On",
    "Laser tx power high alarm   (Channel 3)": "Off",
    "Laser tx power low alarm    (Channel 3)": "On",
    "Laser tx power high warning (Channel 3)": "Off",
    "Laser tx power low warning  (Channel 3)": "On",
    "Laser tx power high alarm   (Channel 4)": "Off",
    "Laser tx power low alarm    (Channel 4)": "On",
    "Laser tx power high warning (Channel 4)": "Off",
    "Laser tx power low warning  (Channel 4)": "On",
    "Laser rx power high alarm   (Channel 1)": "Off",
    "Laser rx power low alarm    (Channel 1)": "On",
    "Laser rx power high warning (Channel 1)": "Off",
```

```
    "Laser rx power low warning  (Channel 1)": "On",
    "Laser rx power high alarm   (Channel 2)": "Off",
    "Laser rx power low alarm    (Channel 2)": "On",
    "Laser rx power high warning (Channel 2)": "Off",
    "Laser rx power low warning  (Channel 2)": "On",
    "Laser rx power high alarm   (Channel 3)": "Off",
    "Laser rx power low alarm    (Channel 3)": "On",
    "Laser rx power high warning (Channel 3)": "Off",
    "Laser rx power low warning  (Channel 3)": "On",
    "Laser rx power high alarm   (Channel 4)": "Off",
    "Laser rx power low alarm    (Channel 4)": "On",
    "Laser rx power high warning (Channel 4)": "Off",
    "Laser rx power low warning  (Channel 4)": "On",
    "Laser bias current high alarm threshold": "75.000 mA",
    "Laser bias current low alarm threshold": "10.000 mA",
    "Laser bias current high warning threshold": "70.000 mA",
    "Laser bias current low warning threshold": "15.000 mA",
    "Laser output power high alarm threshold": "2.8184 mW / 4.50 dBm",
    "Laser output power low alarm threshold": "0.2239 mW / -6.50 dBm",
    "Laser output power high warning threshold": "2.5119 mW / 4.00 dBm",
    "Laser output power low warning threshold": "0.2512 mW / -6.00 dBm",
    "Module temperature high alarm threshold": "80.00 degrees C / 176.00 degrees F",
    "Module temperature low alarm threshold": "-10.00 degrees C / 14.00 degrees F",
    "Module temperature high warning threshold": "75.00 degrees C / 167.00 degrees F",
    "Module temperature low warning threshold": "-5.00 degrees C / 23.00 degrees F",
    "Module voltage high alarm threshold": "3.8000 V",
    "Module voltage low alarm threshold": "2.8000 V",
    "Module voltage high warning threshold": "3.7000 V",
    "Laser rx power high alarm threshold": "2.8183 mW / 4.50 dBm",
    "Laser rx power low alarm threshold": "0.0223 mW / -16.52 dBm",
    "Laser rx power high warning threshold": "2.5118 mW / 4.00 dBm",
    "Laser rx power low warning threshold": "0.0446 mW / -13.51 dBm"
  }
}
```

Для выхода выполните команду `quit`:

```
--> quit
```

Описание всех доступных параметров можно посмотреть на портале документации.

Перехват сетевого трафика

Для того, чтобы включить поддержку записи сетевого трафика, следует в конфигурационном файле `/opt/VPNagent/etc/ipsm_dpdk.cfg` в разделе `[MISC]` раскомментировать параметр `enable_pdump` и выставить его значение в `yes`:

```
enable_pdump = yes
```

После этого требуется перезапустить сервис `ipsmapp`:

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

Для захвата трафика используется утилита dpdk-dumpcap. При вызове утилиты нужно указать номер порта, на котором будет захватываться трафик в параметре `-i`, например:

```
root@sterragate:~# dpdk-dumpcap -i 1
```

```
EAL: WARNING: Address Space Layout Randomization (ASLR) is enabled in the kernel.
EAL:    This may cause issues with mapping memory into secondary processes
File: /tmp/dpdk-dumpcap_1_0000:0b:00.0_20240322164806.pcap
Capturing on '0000:0b:00.0'
Packets captured: 25 ^C
Packets received/dropped on interface '0000:0b:00.0': 25/0 (100.0)
```

Завершить процесс сбора можно при помощи сочетания клавиш Ctrl + C.

По умолчанию, файл с дампом трафика пишется в /tmp, имя файла содержится в выводе утилиты (в примере выше это /tmp/dpdk-dumpcap_1_0000:0b:00.0_20240322164806.pcap). Если требуется, файл для записи трафика можно указать в параметре `-w` (например, `dpdk-dumpcap -i 1 -w /home/dump.pcap`).

В зависимости от объема трафика, размер файла с дампом трафика может увеличиваться очень быстро. В связи с этим не рекомендуется указывать какие-либо другие директории для файла, кроме /tmp. Также не рекомендуется записывать в уже существующий файл, это может привести к порче содержимого файла.

Параметр `-s` позволяет задать ограничение по размеру в байтах записываемых в дамп фреймов. Например, если установить значение `-s 1000`, то в дамп будут записываться только первые 1000 байт каждого захваченного фрейма (если размер фрейма 1000 или меньше, то фрейм будет записан целиком). Минимальное значение параметра – 109, максимальное – 65384. Значение по умолчанию – 10240.

Полный список поддерживаемых параметров можно посмотреть в выводе `dpdk-dumpcap --help`.

Логи, специфичные для «С-Терра Шлюз DP»

Кроме файла `/var/log/cspvpngate.log`, используемого продуктом для логирования основной информации (см. базовый сценарий), продукт «С-Терра Шлюз DP» тоже имеет возможность собирать дополнительную статистику.

Информация об ошибках IPSM собирается в файл `/tmp/stvpn_93242D85-AC20-4A8A-8F02-6725EF08D82D/ipsm-app/error.log`.

Также по умолчанию включён сбор статистики по пакетам, проходящим через IPSM порты. Статистика записывается в файл `/tmp/pkt_stats.txt` с периодом в 1 секунду. Ротация происходит после достижения файлом размера в 10 МБ.

Изменить настройки сбора статистики по пакетам и, при необходимости, включить другие инструменты диагностики можно в `/opt/VPNagent/etc/ipsm_dpdk.cfg`. Настройки описаны в документации.

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
username          cscons          privilege          15          secret          5
$6$lQHk46/t$MDufPsXck4QGNohEy/CS8Qf/U9SF7LZfA/1RC9RBjLwOIP5vIjiDE7bYGKfodQwUcopzFDVLf
1v.6m9CV.Zan0
aaa new-model
!
!
hostname Hub1
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
!
ip local pool ADMIN_ADDRESS 192.168.255.1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT esp-magma-mgm
 mode transport
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
!
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 ADMIN_ACL
 remark MGMT IP
 permit ip host 192.168.253.1 host 192.168.255.1
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
```

```
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FW_INPUT_DP
 permit udp any object-group SELF eq non500-isakmp
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map MGMT 1
 match address ADMIN_ACL
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool ADMIN_ADDRESS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set peer 172.16.1.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
!
interface GigabitEthernet0/0
 ip address 192.168.253.1 255.255.255.0
!
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 address 172.16.100.2 255.255.255.0
 mtu 8000
 ip access-group FW_INPUT_WAN in
 crypto map L3VPN
 ip inspect INSPECT out
!
interface vEthernet1
 no ip address
 mtu 9000
!
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Nov 18 23:08:36 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Tue Nov 18 23:08:36 2025 (user: root)"
    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_TRANSPORT:ESP
(
    Transform* = ESPTransform
    (
        CipherAlg*          = "GR341215M-K288-MGM-33"
        LifetimeSeconds     = 3600
    )
)

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

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

FilterChain FilterChain:FW_INPUT_DP (
    Filters = Filter (
        DestinationIP = 172.16.100.2
```

```
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_DP"
    ),
    Filter (
        DestinationIP = 172.16.100.2
        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
    ))

AddressPool ADMIN_ADDRESS
(
    IPAddresses = 192.168.255.1
)

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

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

IKERule IKERule:L2VPN: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
)

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

```
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    IKECFGPool          = ADMIN_ADDRESS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

IPsecAction IPsecAction:L2VPN:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
)

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

const IPsecPolicy:L2VPN = 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
)

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

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
```

```
    LogicalName = "GigabitEthernet0/1"
    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
    IPsecPolicy = IPsecPolicy:L3VPN
)

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
;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_mac_force6 = no ;yes/no, default no -- always set next_hop_mac 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 Spoke1

1. Консоль cisco-like

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
username          cscons          privilege          15          secret          5
$6$4SGBmgmh$bLy4I.E4SSgwM8kSHldWJwC6GvoKUcE7uUogvpwwk4iGcd78.GSlhH.x.NGYJMTvTEdqF9Yy2
7fBbLs5OT4Aq/
aaa new-model
!
!
hostname Spoke1
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
!
ip local pool ADMIN_ADDRESS 192.168.255.2
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT esp-magma-mgm
 mode transport
!
object-group network SELF
 remark WAN IP
 host 172.16.1.2
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
 remark EtherIP L2 tunnel
 permit etherip host 172.16.1.2 host 172.16.100.2
!
ip access-list extended ADMIN_ACL
 remark MGMT IP
 permit ip host 192.168.254.1 host 192.168.255.2
!
ip access-list extended FW_INPUT_WAN
 permit udp any object-group SELF eq isakmp
```

```
 permit udp any object-group SELF eq non500-isakmp
 permit icmp any object-group SELF
 permit esp any object-group SELF
!
ip access-list extended FW_INPUT_DP
 permit udp any object-group SELF eq non500-isakmp
 permit esp any object-group SELF
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map MGMT 1
 match address ADMIN_ACL
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set pool ADMIN_ADDRESS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map L2VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT
 set isakmp-profile NEW_ALGS
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
crypto map L3VPN 1 ipsec-isakmp dynamic MGMT
!
interface GigabitEthernet0/0
 ip address 192.168.254.1 255.255.255.0
!
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 address 172.16.1.2 255.255.255.0
 mtu 8000
 ip access-group FW_INPUT_WAN in
 crypto map L3VPN
 ip inspect INSPECT out
!
interface vEthernet1
 no ip address
 mtu 9000
!
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Tue Nov 18 21:54:32 2025

GlobalParameters(
    Title                     = "This LSP was automatically generated by CSP Converter
at Tue Nov 18 21:54:32 2025 (user: root)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    Routes =
```

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

)

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

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

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

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

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

FilterChain FilterChain:FW_INPUT_DP (
```

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

```
        DestinationIP = ::/0
        Action = DROP
    ))

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

AddressPool ADMIN_ADDRESS
(
    IPAddresses = 192.168.255.2
)

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

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

IKERule IKERule:L2VPN: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
)

IKERule IKERule:L3VPN:1:MGMT:1
(
```

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

IPsecAction IPsecAction:L2VPN:1
(
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY_TRANSPORT:ESP )
    NoDeadConnectionHistory = TRUE
    DFHandling = COPY
    IKERule = IKERule:L2VPN:1
)

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

const IPsecPolicy:L2VPN = 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
)

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

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

```
NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    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
    IPsecPolicy = IPsecPolicy:L3VPN
)

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
;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_mac_force6 = no ;yes/no, default no -- always set next_hop_mac 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
```