Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля при наличии NAT

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 криптошлюзов «С-Терра Шлюз» для обеспечения безопасного взаимодействия между центральным офисом и двумя филиалами в условиях, когда криптошлюзы с обеих сторон находятся за различными типами NAT.

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

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

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

Предварительные требования

Требования к материально-техническому обеспечению

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

Требования к квалификации администратора

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

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

Требования к инфраструктуре

1. Требования к устройствам.

   1.1. «С-Терра Шлюз».

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

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

   1.2. Центр выпуска сертификатов.

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

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

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

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

   1.3. HTTP сервер для распространения списка отозванных сертификатов.

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

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

2. Требования к сетевому взаимодействию.

   2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

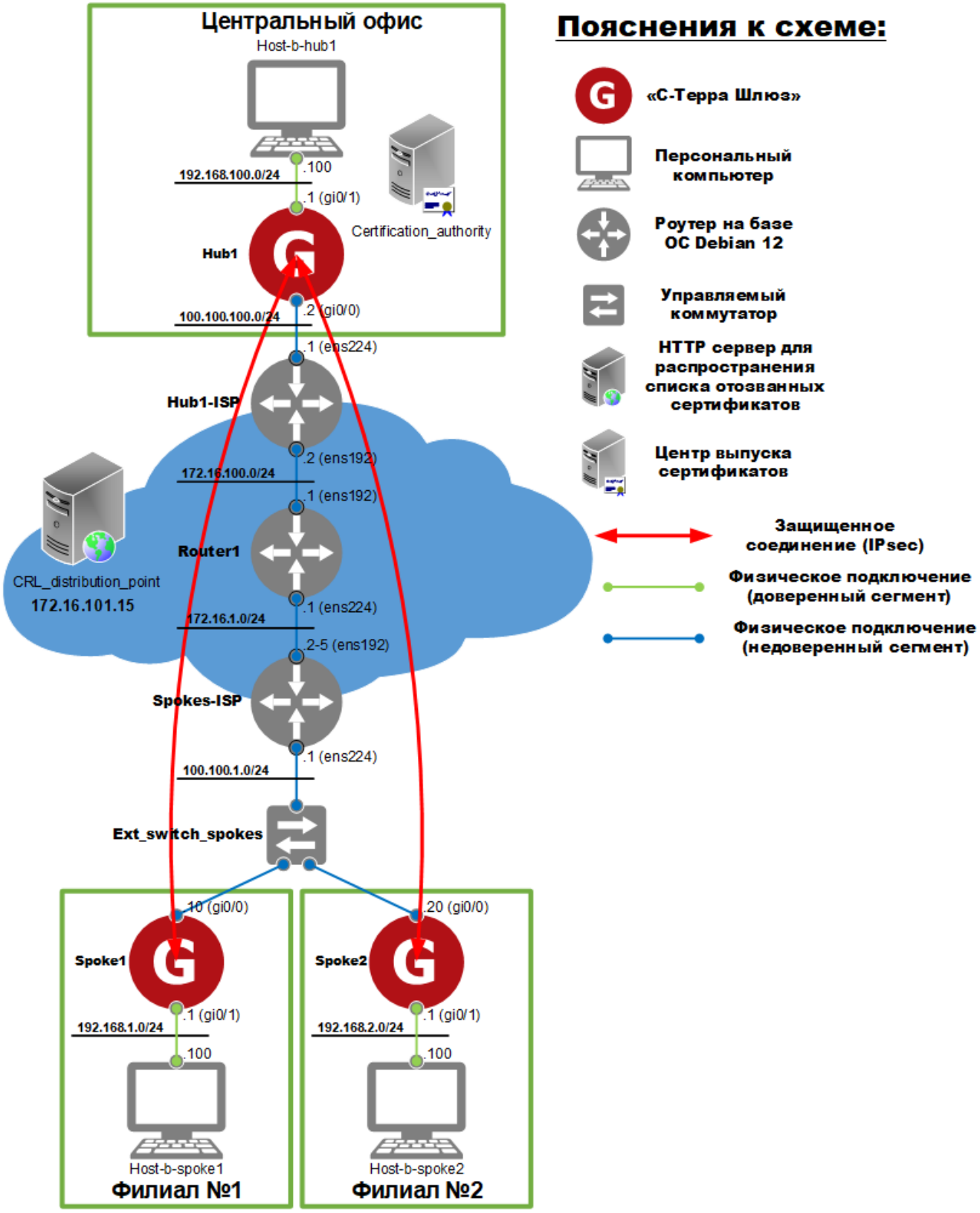


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюз «С-Терра Шлюз» (Hub1) и персональный компьютер (Host-b-hub1):

   1.2. В филиале №1 размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) и персональный компьютер (Host-b-spoke1).

   1.3. В филиале №2 размещаются: криптошлюз «С-Терра Шлюз» (Spoke2) и персональный компьютер (Host-b-spoke2).

   1.4. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизаторы (Router1, Hub1-ISP, Spokes-ISP) и управляемый коммутатор (Ext_switch_spokes).

2. Подключение к сети Интернет.

   В данном сценарии для эмуляции сети Интернет используются маршрутизаторы Router1, Hub1-ISP и Spokes-ISP.

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

   2.1. Криптошлюз Hub1 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Hub1-ISP).

   2.2. Криптошлюзы Spoke1 и Spoke2 подключаются к сети Интернет с помощью статической маршрутизации (маршрут по умолчанию через маршрутизатор Spokes-ISP).

3. Параметры NAT.

   На маршрутизаторе Hub1-ISP, за которым находится криптошлюз центрального офиса, настроен DNAT (Destination NAT) таким образом, что на его внешнем интерфейсе destination IP-адреса всех входящих пакетов транслируются в адрес WAN интерфейса криптошлюза Hub1 (100.100.100.2). На маршрутизаторе Hub1-ISP также настроен SNAT (Source NAT), транслирующий source IP-адреса всех исходящих пакетов из сети за маршрутизатором (100.100.100.0/24) в адрес внешнего интерфейса (172.16.100.2).

   На маршрутизаторе Spokes-ISP, за которым находятся криптошлюзы филиалов, настроен динамический SNAT таким образом, что source IP-адреса всех исходящих пакетов из сети за маршрутизатором (100.100.1.0/24) транслируются в случайно выбираемый адрес из пула адресов внешнего интерфейса (172.16.1.2 – 172.16.1.5).

4. Параметры межсетевого экранирования.

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

   4.1. На LAN интерфейсах IPv4 трафик не контролируется.

   4.2. На LAN интерфейсах IPv6 трафик заблокирован.

   4.3. На WAN интерфейсах разрешен входящий IPv4 трафик:

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

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

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

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

   4.4. На WAN интерфейсах IPv6 трафик заблокирован.

4.5. На WAN интерфейсах 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).

5. Параметры шифрования IPsec.

   Весь IPv4 трафик между подсетью центрального офиса (192.168.100.0/24) и филиалами (192.168.1.0/24 и 192.168.2.0/24) защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном IPv4 режиме.

   Инициировать защищенное соединение между криптошлюзами центрального офиса и филиалов может только трафик, идущий из филиалов в центр.

   5.1. Параметры протокола IKE:

   - Аутентификация при помощи цифровых сертификатов, алгоритм подписи – GOST R 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 GOST R 34.10-2012 (ключ 256 бит).

   5.2. Параметры протокола ESP:

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

Настройка стенда

Настройка устройства Router1

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

Настройка устройства Hub1-ISP

1. Настройте IP адрес – 172.16.100.2 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 100.100.100.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Задайте маршрут по умолчанию через 172.16.100.1.
4. Настройте Source NAT на сетевом интерфейсе ens192. Пример команды для iptables:

   ```
   iptables -t nat -A POSTROUTING -s 100.100.100.2/32 -o ens192 -j SNAT --to-source 172.16.100.2
   ```

5. Настройте Destination NAT на сетевом интерфейсе ens192. Пример команды для iptables:

   ```
   iptables -t nat -A PREROUTING -d 172.16.100.2/32 -i ens192 -j DNAT --to-destination 100.100.100.2
   ```

6. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Spokes-ISP

1. Настройте IP адреса – 172.16.1.2, 172.16.1.3, 172.16.1.4, 172.16.1.5 и маску – 255.255.255.0 на сетевом интерфейсе ens192.
2. Настройте IP адрес – 100.100.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.
3. Задайте маршрут по умолчанию через 172.16.1.1.
4. Настройте динамический Source NAT на сетевом интерфейсе ens192 для трафика из подсети 100.100.1.0/24. Пример команды для iptables:

```
iptables -t nat -A POSTROUTING -s 100.100.1.0/24 -o ens192 -j SNAT --to-source
172.16.1.2-172.16.1.5
```

5. Разрешите прохождение IP трафика (если заблокировано).

Настройка устройства Host-b-hub1

1. Настройте IP адрес – 192.168.100.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.100.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke1

1. Настройте IP адрес – 192.168.1.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.1.1.
3. Разрешите прием и отправку ICMP пакетов.

Настройка устройства Host-b-spoke2

1. Настройте IP адрес – 192.168.2.100 и маску – 255.255.255.0 на сетевом интерфейсе.
2. Задайте маршрут по умолчанию через 192.168.2.1.
3. 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

Войдите в CLI разграничения доступа (пользователь и пароль по умолчанию: `administrator`, `s-terra`) установите правильный тип терминала и требуемую ширину, смените пароль для пользователя `administrator`.

Перейдите в linux bash консоль, установите пароль для пользователя `root`, правильное время и временную зону.

Подробная настройка с описанием команд приведена в разделе «Начальные настройки» базового сценария.

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, доставьте его 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 разделе «Настройки PKI (запросы и сертификаты)» базового сценария.

Настройка сетевых параметров

1. Войдите в cisco-like консоль из CLI разграничения доступа:

```
administrator@sterragate] configure
sterragate login: cscons
```

```
Password:
S-Terra Gate 5.0.XXXXX (amd64)
sterragate#
```

2. Войдите в режим конфигурации:

```
sterragate#configure terminal
```

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

3. Задайте имя устройства:

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

4. Включите внешний (`GigabitEthernet0/0`) и внутренний (`GigabitEthernet0/1`) интерфейсы:

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

5. Убедитесь, что интерфейсы административно включены и line protocol (способность интерфейса передавать пакеты в данный момент) находится в состоянии up:

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

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 0050.569e.94c4
  MTU 1500 bytes
GigabitEthernet0/1 is up, line protocol is up
  Hardware address is 0050.569e.7f79
  MTU 1500 bytes
```

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

6. Настройте IP адреса на внешнем и внутренних интерфейсах в соответствии со схемой стенда:

```
Hub1(config)#interface gigabitEthernet 0/0
Hub1(config-if)#ip address 100.100.100.2 255.255.255.0
Hub1(config-if)#exit
Hub1(config)#interface gigabitEthernet 0/1
Hub1(config-if)#ip address 192.168.100.1 255.255.255.0
Hub1(config-if)#exit
```

7. Задайте маршрут по умолчанию через устройство Hub1-ISP:

```
Hub1(config)#ip route 0.0.0.0 0.0.0.0 100.100.100.1
```

8. Проверьте доступность устройства Hub1-ISP:

```
Hub1(config)#do ping 100.100.100.1
```

```
PING 100.100.100.1 (100.100.100.1) 100(128) bytes of data.
108 bytes from 100.100.100.1: icmp_seq=1 ttl=64 time=0.400 ms
108 bytes from 100.100.100.1: icmp_seq=2 ttl=64 time=0.394 ms
108 bytes from 100.100.100.1: icmp_seq=3 ttl=64 time=0.389 ms
108 bytes from 100.100.100.1: icmp_seq=4 ttl=64 time=0.397 ms
108 bytes from 100.100.100.1: icmp_seq=5 ttl=64 time=0.537 ms

--- 100.100.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.389/0.423/0.537/0.056 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
```

2. Настройте параметры IPsec.

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

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

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

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

   2.3. Создайте список доступа (ACL) для трафика, который нужно защищать между подсетью центрального офиса и подсетями филиалов:

```
Hub1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKES
Hub1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
Hub1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.2.0 0.0.0.255
Hub1(config-ext-nacl)#exit
```

   2.4. Создайте динамическую крипто-карту (имя DMAP, раздел 1) для построения IPsec туннеля между криптошлюзом центрального офиса и криптошлюзами филиалов:

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

   2.4.1 Укажите список доступа для защищаемого трафика:

```
Hub1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKES
```

   2.4.2 Укажите при помощи какого набора алгоритмов нужно защищать трафик:

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

   2.4.3 Прикрепите ISAKMP профиль `NEW_ALGS` к криптокарте:

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

   2.4.4 Включите префрагментацию:

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

2.4.5 Включите автоматическую и интеллектуальную корректировку значения MSS:

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

2.4.6 Обязательно отключите историю удаленных туннелей:

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

2.5. Создайте крипто-карту (имя VPN, раздел 1) и добавьте туда динамическую крипто-карту DMAP:

```
Hub1(config)#crypto map VPN 1 ipsec-isakmp dynamic DMAP
Hub1(config-crypto-map)#exit
```

2.6. Прикрепите крипто-карту `VPN` к внешнему интерфейсу `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#crypto map VPN
Hub1(config-if)#exit
```

2.7. Примените настройки:

```
Hub1(config)#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 100.100.100.2
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 500
Hub1(config-ext-nacl)#permit udp any object-group SELF eq 4500
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 правила инспектирования всего TCP и UDP трафика и задайте необходимое максимальное количество сессий:

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

4. Прикрепите правила межсетевого экранирования на WAN интерфейс `GigabitEthernet0/0`:

```
Hub1(config)#interface GigabitEthernet0/0
Hub1(config-if)#ip access-group FW_INPUT_WAN in
```

```
Hub1(config-if)#ip inspect INSPECT out
Hub1(config-if)#exit
```

5. Примените настройки:

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

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст конфигурации консоли cisco-like;
- текст LSP;

Дополнительно: настройка криптошлюза для подключения удаленных VPN клиентов

В данном сценарии показана настройка криптошлюзов для построения защищенного соединения между подсетями центрального офиса и филиалов. В случае необходимости добавления в схему стенда удаленных VPN клиентов для обеспечения им защищенного доступа в подсеть центрального офиса, на криптошлюзе Hub1 потребуется выполнить дополнительные настройки.

Так как центральный криптошлюз при подключении к нему как филиальных криптошлюзов, так и удаленных VPN клиентов во всех случаях выступает в качестве ответчика (респондера), и, соответственно, будет использовать динамическую криптокарту с двумя разделами (один раздел для криптошлюзов, другой раздел для VPN клиентов с выдачей IKECFG адресов), необходимо каким-либо образом различать подключаемых партнеров и корректно распределять их в соответствующий раздел криптокарты. В данном разделе описывается два метода для разделения партнеров:

- Метод с разделением партнеров по IP адресу.

  В данном методе на WAN интерфейсе центрального криптошлюза Hub1 настраивается два IP адреса. Филиальные криптошлюзы будут строить защищенное соединение на первый IP адрес, удаленные VPN клиенты – на второй.

- Метод с разделением партнеров по ISAKMP профилю.

  В данном методе на центральном криптошлюзе Hub1 распределение выполняется на основании содержимого полей DN сертификатов партнеров. Для использования этого метода нужно, чтобы, например, в DN в сертификатах удаленных VPN клиентов присутствовало поле, которое было бы одинаковое для всех сертификатов VPN клиентов и при этом не встречается в сертификатах криптошлюзов. В данном примере будет считаться, что все сертификаты удаленных VPN клиентов содержат поле `OU=Remote VPN Clients`.

Общие настройки

1. Войдите в режим конфигурации:

```
Hub1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Создайте IKECFG пул адресов, из которого будут назначаться IKECFG адреса для удаленных VPN клиентов:

```
Hub1(config)#ip local pool IKECFG_POOL 192.168.255.1 192.168.255.254
```

3. Создайте список доступа (ACL) для трафика, который нужно защищать между подсетью центрального офиса и удаленными VPN клиентами:

```
Hub1(config)#ip access-list extended IPSEC_ACL_HUB1_CLIENTS
Hub1(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.255.0 0.0.0.255
Hub1(config-ext-nacl)#exit
```

Далее выполните настройку с использованием одного из методов.

Метод с разделением по IP адресу

1. Задайте на внешнем интерфейсе `gigabitEthernet0/0` второй адрес (в данном примере 100.100.100.3):

```
Hub1(config)#interface gigabitEthernet 0/0
Hub1(config-if)#ip address 100.100.100.3 255.255.255.0 secondary
Hub1(config-if)#exit
```

2. Создайте динамическую криптокарту (имя DMAP, раздел 2) для построения IPsec туннеля между криптошлюзом центрального офиса и удаленными VPN клиентами, в качестве local-address укажите IP адрес 100.100.100.3:

```
Hub1(config)#crypto dynamic-map DMAP 2
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_CLIENTS
Hub1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)#set isakmp-profile NEW_ALGS
Hub1(config-crypto-map)#set pool IKECFG_POOL
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#set local-address 100.100.100.3
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

3. В динамической криптокарте (имя DMAP, раздел 1) для построения IPsec туннеля между криптошлюзом центрального офиса и криптошлюзами филиалов укажите IP адрес 100.100.100.2 в параметре local-address:

```
Hub1(config)#crypto dynamic-map DMAP 1
Hub1(config-crypto-map)#set local-address 100.100.100.2
Hub1(config-crypto-map)#exit
```

4. В сетевой `object-group` с именем `SELF` добавьте второй IP адрес WAN интерфейса:

```
Hub1(config)#object-group network SELF
Hub1(config-network-group)#host 100.100.100.3
Hub1(config-network-group)#exit
```

Настройка криптошлюза Hub1 завершена.

На устройстве Hub1-ISP на интерфейсе ens192 следует добавить второй IP адрес – 172.16.100.3 и маску – 255.255.255.0, и настроить правила NAT следующим образом:

```
iptables -t nat -A PREROUTING -d 172.16.100.2/32 -i ens192 -j DNAT --to-destination
100.100.100.2
iptables -t nat -A PREROUTING -d 172.16.100.3/32 -i ens192 -j DNAT --to-destination
100.100.100.3
iptables -t nat -A POSTROUTING -s 100.100.100.2/32 -o ens192 -j SNAT --to-source
172.16.100.2
iptables -t nat -A POSTROUTING -s 100.100.100.3/32 -o ens192 -j SNAT --to-source
172.16.100.3
```

Метод с разделением по ISAKMP профилю

1. Создайте раздел с описанием сертификата удаленных VPN клиентов:

```
Hub1(config)#crypto pki certificate map CLIENTS_CERT 1
Hub1(ca-certificate-map)#subject-name co OU=Remote VPN Clients
Hub1(ca-certificate-map)#exit
```

2. Создайте профиль настроек ISAKMP для удаленных VPN клиентов:

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

3. Создайте динамическую криптокарту (имя DMAP, раздел 2) для построения IPsec туннеля между криптошлюзом центрального офиса и удаленными VPN клиентами:

```
Hub1(config)#crypto dynamic-map DMAP 2
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_CLIENTS
Hub1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)#set isakmp-profile CLIENTS_IKE_PROFILE
Hub1(config-crypto-map)#set pool IKECFG_POOL
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#exit
```

4. Разделы динамической криптокарты DMAP следует упорядочить таким образом, чтобы раздел с настройками построения защищенного соединения между криптошлюзами находился **после** раздела с настройками построения защищенного соединения для удаленных VPN клиентов. Для этого можно, например, содержимое раздела 1 скопировать в раздел 3, а затем удалить раздел 1.

Настройка криптошлюза Hub1 завершена.

Настройка криптошлюза Spoke1

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

Войдите в CLI разграничения доступа (пользователь и пароль по умолчанию: `administrator`, `s-terra`) установите правильный тип терминала и требуемую ширину, смените пароль для пользователя `administrator`.

Перейдите в linux bash консоль, установите пароль для пользователя `root`, правильное время и временную зону.

Подробная настройка с описанием команд приведена в разделе «Начальные настройки» базового сценария.

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, доставьте его 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 разделе «Настройки PKI (запросы и сертификаты)» базового сценария.

Настройка сетевых параметров

1. Войдите в cisco-like консоль из CLI разграничения доступа:

```
administrator@sterragate] configure
sterragate login: cscons
```

```
Password:
S-Terra Gate 5.0.XXXXX (amd64)
sterragate#
```

2. Войдите в режим конфигурации:

```
sterragate#configure terminal
```

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

3. Задайте имя устройства:

```
sterragate(config)#hostname Spoke1
```

4. Включите внешний (`GigabitEthernet0/0`) и внутренний (`GigabitEthernet0/1`) интерфейсы:

```
Spoke1(config)#interface range gigabitEthernet 0/0 - 1
Spoke1(config-if-range)#no shutdown
Spoke1(config-if-range)#exit
```

5. Убедитесь, что интерфейсы административно включены и line protocol (способность интерфейса передавать пакеты в данный момент) находится в состоянии up:

```
Spoke1(config)#do show interfaces
```

```
GigabitEthernet0/0 is up, line protocol is up
  Hardware address is 0050.569e.94c4
  MTU 1500 bytes
GigabitEthernet0/1 is up, line protocol is up
  Hardware address is 0050.569e.7f79
  MTU 1500 bytes
```

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

6. Настройте IP адреса на внешнем и внутренних интерфейсах в соответствии со схемой стенда:

```
Spoke1(config)#interface gigabitEthernet 0/0
Spoke1(config-if)#ip address 100.100.1.10 255.255.255.0
Spoke1(config-if)#exit
Spoke1(config)#interface gigabitEthernet 0/1
Spoke1(config-if)#ip address 192.168.1.1 255.255.255.0
Spoke1(config-if)#exit
```

7. Задайте маршрут по умолчанию через устройство Spokes-ISP:

```
Spoke1(config)#ip route 0.0.0.0 0.0.0.0 100.100.1.1
```

8. Проверьте доступность устройства Spokes-ISP:

```
Spoke1(config)#do ping 100.100.1.1
```

```
PING 100.100.1.1 (100.100.1.1) 100(128) bytes of data.
108 bytes from 100.100.1.1: icmp_seq=1 ttl=64 time=0.518 ms
108 bytes from 100.100.1.1: icmp_seq=2 ttl=64 time=0.194 ms
108 bytes from 100.100.1.1: icmp_seq=3 ttl=64 time=0.412 ms
108 bytes from 100.100.1.1: icmp_seq=4 ttl=64 time=0.453 ms
108 bytes from 100.100.1.1: icmp_seq=5 ttl=64 time=0.447 ms

--- 100.100.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 0.194/0.404/0.518/0.110 ms
```

Настройка шифрования

1. Настройте параметры IKE.

   1.1. Задайте общие параметры IKE:

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

   1.2. Создайте политику, описывающую параметры IKE туннеля:

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

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

```
Spoke1(config)#crypto isakmp profile NEW_ALGS
Spoke1(conf-isa-prof)#match identity dn
```

```
Spoke1(conf-isa-prof)#set identity mapping
Spoke1(conf-isa-prof)#set policy 1
```

2. Настройте параметры IPsec.

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

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

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

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

   2.3. Создайте список доступа (ACL) для трафика, который нужно защищать между подсетью филиала №1 и подсетью центрального офиса:

   ```
   Spoke1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
   Spoke1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
   Spoke1(config-ext-nacl)#exit
   ```

   2.4. Создайте крипто-карту (имя VPN, раздел 1) для построения IPsec туннеля между криптошлюзом Spoke1 и криптошлюзом Hub1 (в качестве адреса партнера по IPsec укажите IP адрес внешнего интерфейса маршрутизатора Hub1-ISP):

   ```
   Spoke1(config)#crypto map VPN 1 ipsec-isakmp
   Spoke1(config-crypto-map)#match address IPSEC_ACl_HUB1_AND_SPOKE1
   Spoke1(config-crypto-map)#set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
   Spoke1(config-crypto-map)#set isakmp-profile NEW_ALGS
   Spoke1(config-crypto-map)#set security-association mss-fix out
   Spoke1(config-crypto-map)#set peer 172.16.100.2
   Spoke1(config-crypto-map)#set pre-fragmentation
   Spoke1(config-crypto-map)#set dead-connection history off
   Spoke1(config-crypto-map)#exit
   ```

   2.5. Прикрепите крипто-карту `VPN` к внешнему интерфейсу `GigabitEthernet0/0`:

   ```
   Spoke1(config)#interface GigabitEthernet0/0
   Spoke1(config-if)#crypto map VPN
   Spoke1(config-if)#exit
   ```

   2.6. Примените настройки:

   ```
   Spoke1(config)#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:

   ```
   Spoke1#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   Spoke1(config)#object-group network SELF
   Spoke1(config-network-group)#remark WAN IP
   ```

```
Spoke1(config-network-group)#host 100.100.1.10
Spoke1(config-network-group)#exit
```

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

```
Spoke1(config)#ip access-list extended FW_INPUT_WAN
Spoke1(config-ext-nacl)#permit udp any object-group SELF eq 500
Spoke1(config-ext-nacl)#permit udp any object-group SELF eq 4500
Spoke1(config-ext-nacl)#permit icmp any object-group SELF
Spoke1(config-ext-nacl)#permit esp any object-group SELF
Spoke1(config-ext-nacl)#exit
```

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

```
Spoke1(config)#ip inspect name INSPECT tcp
Spoke1(config)#ip inspect name INSPECT udp
Spoke1(config)#ip inspect tcp sessions-max 256000
Spoke1(config)#ip inspect udp sessions-max 65536
```

4. Прикрепите правила межсетевого экранирования на WAN интерфейс `GigabitEthernet0/0`:

```
Spoke1(config)#interface GigabitEthernet0/0
Spoke1(config-if)#ip access-group FW_INPUT_WAN in
Spoke1(config-if)#ip inspect INSPECT out
Spoke1(config-if)#exit
```

5. Примените настройки:

```
Spoke1(config)#end
```

Настройка криптошлюза Spoke1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст конфигурации консоли cisco-like;
- текст LSP;

Настройка криптошлюза Spoke2

Настройка криптошлюза происходит аналогично настройке Spoke1.

В Приложении представлены тексты конфигураций для криптошлюза Spoke2:

- текст консоли cisco-like;
- текст LSP;

Проверка работоспособности стенда

Проверка IP связности

1. Проверьте, что с криптошлюзов Hub1, Spoke1 и Spoke2 доступен маршрутизатор 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=63 time=0.729 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=63 time=0.805 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=63 time=0.491 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=63 time=0.328 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=63 time=0.648 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.328/0.600/0.805/0.171 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=63 time=0.624 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=63 time=0.716 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=63 time=0.709 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=63 time=0.606 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=63 time=0.905 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 0.606/0.712/0.905/0.106 ms
```

```
Spoke2#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=63 time=0.594 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=63 time=0.441 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=63 time=0.474 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=63 time=0.599 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=63 time=0.708 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4086ms
rtt min/avg/max/mdev = 0.441/0.563/0.708/0.096 ms
```

2. Проверьте, что с криптошлюзов Spoke1 и Spoke2 доступен криптошлюз Hub1. Для этого выполните команду ping из cisco-like консоли криптошлюзов:

```
Spoke1#ping 172.16.100.2
```

```
PING 172.16.100.2 (172.16.100.2) 100(128) bytes of data.
108 bytes from 172.16.100.2: icmp_seq=1 ttl=61 time=1.05 ms
108 bytes from 172.16.100.2: icmp_seq=2 ttl=61 time=1.25 ms
108 bytes from 172.16.100.2: icmp_seq=3 ttl=61 time=1.10 ms
108 bytes from 172.16.100.2: icmp_seq=4 ttl=61 time=1.14 ms
108 bytes from 172.16.100.2: icmp_seq=5 ttl=61 time=1.38 ms

--- 172.16.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.051/1.182/1.375/0.116 ms
```

```
Spoke2#ping 172.16.100.2
```

```
PING 172.16.100.2 (172.16.100.2) 100(128) bytes of data.
108 bytes from 172.16.100.2: icmp_seq=1 ttl=61 time=1.02 ms
```

```
108 bytes from 172.16.100.2: icmp_seq=2 ttl=61 time=1.00 ms
108 bytes from 172.16.100.2: icmp_seq=3 ttl=61 time=1.00 ms
108 bytes from 172.16.100.2: icmp_seq=4 ttl=61 time=1.25 ms
108 bytes from 172.16.100.2: icmp_seq=5 ttl=61 time=1.05 ms

--- 172.16.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.000/1.064/1.252/0.095 ms
```

3. Проверьте, что со всех защищаемых устройств доступен их соответствующий шлюз по умолчанию. Для этого выполните команду ping из консоли защищаемых устройств:

```
root@Host-b-hub1:~# ping 192.168.100.1 -c 4
```

```
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.551 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.723 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.569 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.384 ms

--- 192.168.100.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.384/0.556/0.723/0.120 ms
```

```
root@Host-b-spoke1:~# ping 192.168.1.1 -c 4
```

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.368 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.620 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.560 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.431 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3037ms
rtt min/avg/max/mdev = 0.368/0.494/0.620/0.100 ms
```

```
root@Host-b-spoke2:~# ping 192.168.2.1 -c 4
```

```
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.497 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.593 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.446 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.618 ms

--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.446/0.538/0.618/0.069 ms
```

Проверка PKI

1. Проверьте, что на всех криптошлюзах присутствуют локальный и доверенный сертификаты, а также CRL (если загрузка списка отозванных сертификатов была настроена). Для этого выполните следующие команды из cisco-like консоли криптошлюзов:

```
Hub1#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
2 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
3 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
Hub1#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Hub1
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
Spoke1#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1
3 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
Spoke1#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke1
```

```
Spoke2#run cert_mgr show
```

```
Found 2 certificates. Found 1 CRL.
1 Status: trusted C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 Status: local   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2
3 CRL: C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
```

```
Spoke2#run cert_mgr check
```

```
1 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=S-Terra CSP Test Root CA
2 State: Active   C=RU,L=Zelenograd,O=S-Terra CSP,OU=RnD,CN=Spoke2
```

Проверка построения защищенного соединения

1. Инициируйте построение защищенного соединения между криптошлюзом Hub1 и криптошлюзом Spoke1. Для этого отправьте ICMP запросы с устройства Host-b-spoke1 на устройство Host-b-hub1. Аналогичным образом инициируйте построение защищенного соединения между криптошлюзом Hub1 и криптошлюзом Spoke2 за счет отправки ICMP запросов с устройства Host-b-spoke2 на устройство Host-b-hub1.

   Для просмотра установленных соединений выполните следующую команду 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 1 (100.100.100.2,4500)-(172.16.1.5,4500) active 1928 1960
2 2 (100.100.100.2,4500)-(172.16.1.2,4500) active 1928 1960

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (192.168.100.0-192.168.100.255,*)-(192.168.1.0-192.168.1.255,*) * ESP nat-t-tunn
3608 3608
2 2 (192.168.100.0-192.168.100.255,*)-(192.168.2.0-192.168.2.255,*) * ESP nat-t-tunn
3432 3432
```

```
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 1 (100.100.1.10,4500)-(172.16.100.2,4500) active 1960 1928

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (192.168.1.0-192.168.1.255,*)-(192.168.100.0-192.168.100.255,*) * ESP nat-t-tunn
2464 2464
```

```
Spoke2#run sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
```

```
1 1 (100.100.1.20,4500)-(172.16.100.2,4500) active 1960 1928

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (192.168.2.0-192.168.2.255,*)-(192.168.100.0-192.168.100.255,*) * ESP nat-t-tunn
2816 2816
```

Если защищенные соединения не построились, проверьте файл журнала `/var/log/cspvpngate.log` (при необходимости увеличьте уровень логирования командой `logging trap debugging` в cisco-like консоли).

Приложение

Конфигурации криптошлюза Hub1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username           cscons           privilege           15           secret           5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Hub1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 100.100.100.2
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKES
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
 permit ip 192.168.100.0 0.0.0.255 192.168.2.0 0.0.0.255
!
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
!
ipv6 default filtering deny
!
!
ip inspect tcp sessions-max 256000
```

```
ip inspect udp sessions-max 65536
ip inspect name INSPECT tcp
ip inspect name INSPECT udp
!
crypto dynamic-map DMAP 1
 match address IPSEC_ACl_HUB1_AND_SPOKES
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 100.100.100.2 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.100.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 100.100.100.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Mar 29 10:11:24 2024

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Fri Mar 29 10:11:24 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 100.100.100.1
        )

)

FirewallParameters(
    TCPSynSentTimeout = 30
```

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

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

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 100.100.100.2
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.100.2
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.100.2
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.100.2
        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
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

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

```
)

IKERule IKERule:VPN:1:DMAP:1
(
    Transform = crypto:isakmp:policy:1
    AggrModeAuthMethod  = GOST:Sign:NEW_ALGS
    MainModeAuthMethod  = GOST:Sign:NEW_ALGS
    DPDIdleDuration     = 3
    DPDResponseDuration = 2
    DPDRetries          = 5
    Priority            = 100
)

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

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.1.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_ACl_HUB1_AND_SPOKES"
    ),
    Filter (
        SourceIP = 192.168.100.0/24
        DestinationIP = 192.168.2.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1:DMAP:1 >
        LogEventID = "IPsec:Protect:VPN:1:DMAP:1:IPSEC_ACl_HUB1_AND_SPOKES"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурации криптошлюза Spoke1

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke1
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 100.100.1.10
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
!
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
!
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 map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE1
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 100.100.1.10 255.255.255.0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 100.100.1.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Mar 29 10:12:51 2024

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Fri Mar 29 10:12:51 2024 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 100.100.1.1
        )

)

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

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

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

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 100.100.1.10
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.10
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.10
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.10
        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
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

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

IKERule IKERule:VPN:1
(
    IKEPeerIPFilter = 172.16.100.2
```

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

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

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.1.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACl_HUB1_AND_SPOKE1"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурации криптошлюза Spoke2

1. Консоль cisco-like:

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
crypto isakmp fragmentation
crypto isakmp security-association lifetime delta 50
```

```
crypto isakmp initiator-sessions-max 100
crypto isakmp responder-sessions-max 100
crypto ipsec security-association lifetime kilobytes unlimited
crypto isakmp keepalive 3
crypto isakmp keepalive retry-count 5
username          cscons          privilege          15          secret          5
$6$RiWz4IVm$qMp6sbpYnTfSUxuaJPZ9UCq4yy8/xheIEbSmbTfMzmbQqepMD6R1b18vHTdFQt949xNXzpRXW
A9dZ/gCK70z./
aaa new-model
!
!
hostname Spoke2
enable secret 5 HGJcyG+CRmCjINGFkW48VQ==
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto ipsec transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 100.100.1.20
!
ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE2
 permit ip 192.168.2.0 0.0.0.255 192.168.100.0 0.0.0.255
!
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
!
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 map VPN 1 ipsec-isakmp
 match address IPSEC_ACl_HUB1_AND_SPOKE2
 set transform-set MAGMA_GOST_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 set peer 172.16.100.2
 set pre-fragmentation
 set dead-connection history off
!
interface GigabitEthernet0/0
 ip address 100.100.1.20 255.255.255.0
 ip access-group FW_INPUT_WAN in
```

```
 crypto map VPN
 ip inspect INSPECT out
!
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
!
!
ip route 0.0.0.0 0.0.0.0 100.100.1.1
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Fri Mar 29 10:14:12 2024

GlobalParameters(
    Title                              = "This LSP was automatically generated by CSP
Converter at Fri Mar 29 10:14:12 2024 (user: cscons)"
    Version                     = LSP_5_0
    CRLHandlingMode             = ENABLE
    PreserveIPsecSA             = FALSE
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 100.100.1.1
        )

)

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

IKETransform crypto:isakmp:policy:1
```

```
(
    CipherAlg   = "GR341215M-K256-CFB-65526"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        DestinationIP = 100.100.1.20
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.20
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.20
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        DestinationIP = 100.100.1.20
        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
    ))

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

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

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

IPsecAction IPsecAction:VPN:1
(
```

```
    TunnelingParameters = TunnelEntry(
        PeerAddress = 172.16.100.2
        Prefragmentation = ENABLE
    )
    ContainedProposals = ( MAGMA_GOST_ENCRYPT_AND_INTEGRITY:ESP )
    NoDeadConnectionHistory = TRUE
    MSSFixOutgoing = TRUE
    DFHandling = COPY
    IKERule = IKERule:VPN:1
)

FilterChain IPsecPolicy:VPN (
    Filters = Filter (
        ProtocolID = 17
        SourcePort = 500, 4500
        Action = PASS
        PacketType = LOCAL_UNICAST, LOCAL_MISDIRECTED
    ),
    Filter (
        SourceIP = 192.168.2.0/24
        DestinationIP = 192.168.100.0/24
        Action = PASS
        ExtendedAction = ipsec< sa = IPsecAction:VPN:1 >
        LogEventID = "IPsec:Protect:VPN:1:IPSEC_ACl_HUB1_AND_SPOKE2"
    )
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)

NetworkInterface (
    LogicalName = "GigabitEthernet0/1"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```