Построение VPN туннеля с PPPoE/PPTP соединением между двумя подсетями, защищаемыми шлюзами безопасности «С-Терра Шлюз»

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

Введение

Данный сценарий описывает настройку безопасного взаимодействия между защищаемыми подсетями центрального офиса и филиала. Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec, при этом филиал подключается к интернету с использованием протоколов PPPoE/PPTP.

Все остальные соединения разрешены, но защищаться при помощи IPsec и PPPoE/PPTP они не будут.

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» 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, PPPoE, PPTP, 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 http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз <версия> -> «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 R2 (или новее).

1.2.3. Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp), либо утилиту ca-tool, входящую в состав пакета auxiliary-tools (пакет auxiliary-tools предназначен для установки на «С-Терра Шлюз» 5.0, документация на ca-tool приведена в инструкции «Центр выпуска тестовых ГОСТ сертификатов для IPsec», документацию и пакет можно загрузить на портале https://doc.s-terra.ru).

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

1.3. HTTP сервер для распространения списка отозванных сертификатов.

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

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

2. Требования к сетевому взаимодействию.

2.1. Между устройствами стенда должна быть обеспечена IP связность.

Схема взаимодействия

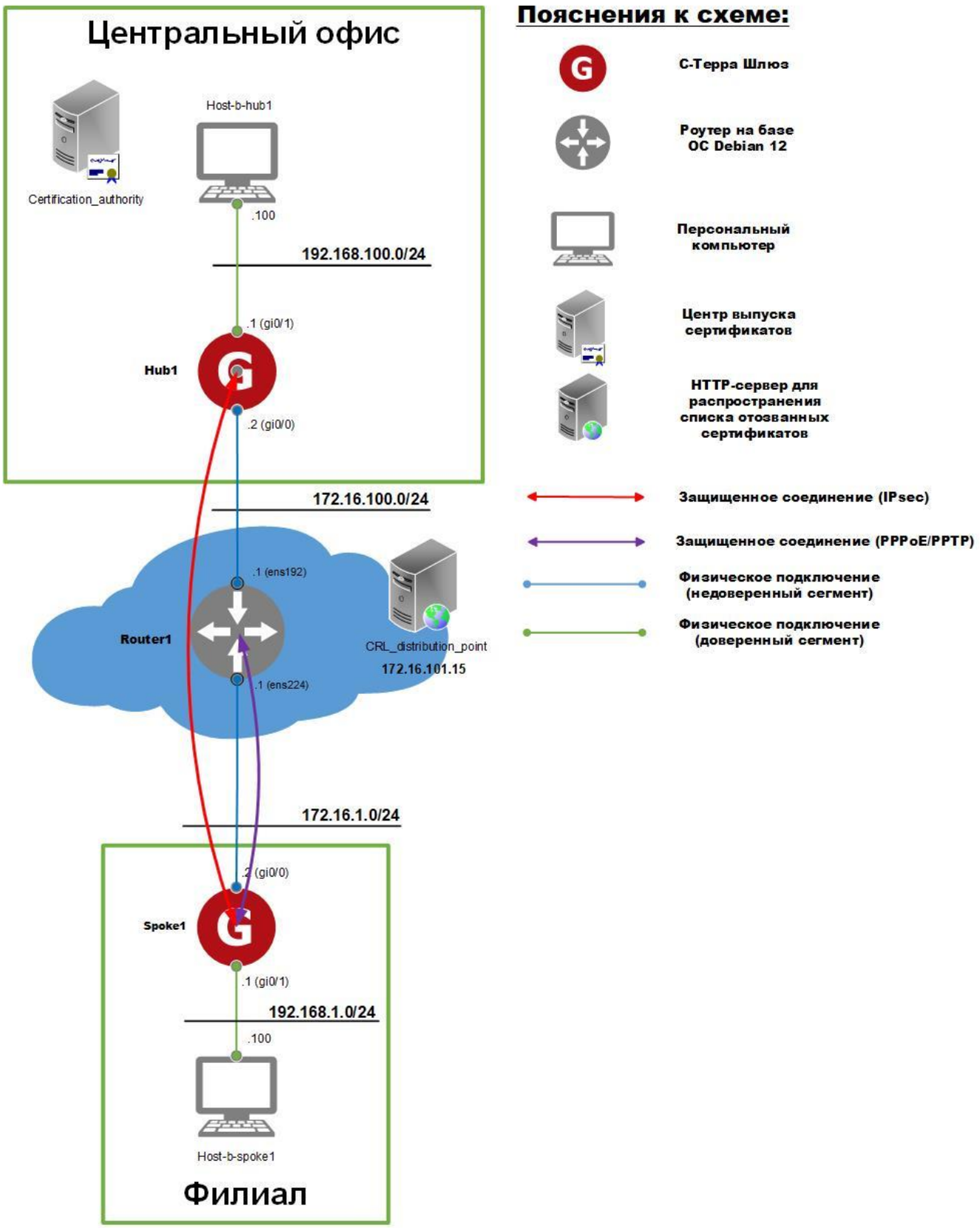


Рисунок 1. Схема взаимодействия

Общая логика работы

1. Размещение устройств.

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

   1.2. В филиале размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) и персональный компьютер (Host-b-spoke1).

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

2. Подключение к сети Интернет.

   В данном сценарии для эмуляции сети Интернет используются маршрутизатор Router1.

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

   2.1. 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 протокола PPPoE/PPTP (маршрут по умолчанию через маршрутизатор Router1).

Протоколы PPPoE и PPTP применяются по отдельности. Для PPTP обязательно нужна IP связность. Проявляйте внимательность при настройке, следуя соответствующим разделам инструкции для выбранного вами протокола.

3. Параметры шифрования IPsec.

   Весь IP-трафик между подсетями центрального офиса (192.168.100.0/24) и филиала (192.168.1.0/24) защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном режиме.

   Инициировать защищенное соединение может только трафик из подсети 192.168.1.0/24 в 192.168.100.0/24 (из филиала в центр), так как криптошлюз филиала имеет динамический IP-адрес.

   3.1. Параметры протокола IKE

      3.1.1. Параметры протокола IKE для версии 5.0:

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

      3.1.2. Параметры протокола IKE для совместимости с версией 4.3:

   - Аутентификация при помощи цифровых сертификатов, алгоритм подписи – ГОСТ Р 34.10-2012 (ключ 256 бит);
   - Алгоритм шифрования – ГОСТ 28147-89 (ключ 256 бит);
   - Алгоритм вычисления хеш-функции – ГОСТ Р 34.11-2012 ТК26 (ключ 256 бит);
   - Алгоритм выработки общего ключа (аналог алгоритма Диффи-Хеллмана) – VKO_GOSTR3410_2012_256 (ключ 256 бит).

   3.2. Параметры протокола ESP:

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

3.3. Параметры протокола PPPoE:

- Аутентификация по логину и паролю, протокол CHAP (также поддерживаются протоколы PAP, EAP, MSCHAP-V2).

3.4. Параметры протокола PPTP:

- Аутентификация по логину и паролю, протокол MSCHAP-V2 (также поддерживаются протоколы PAP, EAP, CHAP).
- Протокол шифрования данных MPPE с 128-разрядным ключом.

4. Параметры межсетевого экранирования.

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

4.1. Для «С-Терра Шлюз» версии 5.0:

4.1.1. На LAN интерфейсах IPv4 трафик не контролируется.

4.1.2. На LAN интерфейсах IPv6 трафик заблокирован.

4.1.3. На WAN интерфейсах разрешен входящий IPv4 трафик:

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

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

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

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

4.1.4. На WAN интерфейсах IPv6 трафик заблокирован.

4.1.5. 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).

4.2. Для «С-Терра Шлюз» версии 4.3:

Использование stateful фильтрации для версии 4.3 нежелательно, рекомендуется использовать статические правила (ACL).

4.2.1. На LAN и WAN интерфейсах IPv4 трафик не контролируется.

4.2.2. На LAN и WAN интерфейсах IPv6 трафик заблокирован (протокол IPv6 отключен в ядре операционной системы).

Настройка стенда

Настройка устройства Router1

Настройка сетевых параметров

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

2.1. Для этого откройте файл утилиты sysctl и измените соответствующий параметр с 0 на 1:

```
root@Router1:~# vim /etc/sysctl.conf
```

```
net.ipv4.ip_forward=1
```

2.2. Примените изменения:

```
root@Router1:~# sysctl -p
```

Настройка для PPPoE

1. Переведите сетевой интерфейс ens224 в состояние UP.

Настройка PPPoE сервера

1. Установите пакет pppoe:

```
root@Router1:~# apt-get install pppoe
```

2. Сконфигурируйте PPPoE сервер. Для этого приведите файл `/etc/ppp/pppoe-server-options` к следующему виду:

```
auth
require-chap
lcp-echo-interval 10
lcp-echo-failure 2
ms-dns 8.8.8.8
ms-dns 8.8.4.4
noipdefault
noipx
nodefaultroute
noproxyarp
netmask 255.255.255.255
logfile /var/log/log.pppoe
```

где:

- `auth` – требование аутентификации партнера;
- `require-chap` – требование использования протокола CHAP для аутентификации;
- `lcp-echo-interval 10` – установка интервала отправки LCP эхо-запросов – 10 секунд;
- `lcp-echo-failure 2` – определение разрыва соединения после 2 неотвеченных запросов;
- `ms-dns 8.8.8.8` и `ms-dns 8.8.4.4` – назначение DNS-серверов (в данном случае Google) для клиентов;
- `noipdefault` – требование к партнеру предоставить локальный IP-адрес во время согласования IPCP;
- `noipx` – отключение протокола IPXCP и IPX;
- `nodefaultroute` – отключение автоматического установления интерфейса `ppp0` (созданного автоматически при PPPoE подключении) в качестве маршрута по умолчанию;
- `noproxyarp` – запрещает серверу отвечать на ARP-запросы от имени клиентов локальной сети;
- `netmask 255.255.255.255` – установка маски подсети;
- `logfile /var/log/log.pppoe` – определение файла для записи логов.

3. Отредактируйте файл учетных записей PPPoE-сервера `/etc/ppp/chap-secrets`. В конец файла допишите следующую строку:

```
pppoelogin * pppoepass 172.16.1.100
```

где `pppoelogin` - имя пользователя, `pppoepass` – пароль, `172.16.1.100` – IP адрес, присвоенный этому пользователю.

4. Запустите pppoe-сервер:

```
root@Router1:~# pppoe-server -I ens224 -L 172.16.1.10
```

где `-L 172.16.1.10` – адрес сервера.

Настройка для PPTP

1. Настройте IP адрес – 172.16.1.1 и маску – 255.255.255.0 на сетевом интерфейсе ens224.

Настройка PPTP сервера

1. Установите пакет `pptpd`:

```
root@Router1:~# apt-get install pptpd
```

2. Откройте файл параметров PPTP сервера и в конце добавьте:

```
root@Router1:~# vim /etc/pptpd.conf
```

```
option /etc/ppp/pptpd-options
logwtmp
bcrelay ens224
localip 172.16.1.10
remoteip 172.16.1.100
```

где:

- `option /etc/ppp/pptpd-options` – указание на файл с дополнительными настройками для сервера PPTP;
- `logwtmp` – включение в системный журнал (wtmp) записи информации о пользователях, подключающихся через PPTP;
- `bcrelay ens224` – указание на интерфейс, через который будет проходить туннель;
- `localip 172.16.1.10` – установка локального IP-адреса для PPTP сервера;
- `remoteip 172.16.1.100` – установка IP-адресоа, который будет предоставлен удаленному клиенту при установлении туннеля.

3. Файл с дополнительными параметрами `/etc/ppp/pptpd-options` оставьте без изменений, будут использоваться настройки по умолчанию:

```
name pptpd
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe-128
proxyarp
nodefaultroute
lock
nobsdcomp
novj
novjccomp
nologfd
```

где:

- `name pptpd` – имя для PPTP сервера;
- `refuse-pap, refuse-chap, refuse-mschap` – отказ от использования протоколов авторизации PAP, CHAP, MS-CHAP;
- `require-mschap-v2` – требование использования протокола авторизации MS-CHAP v2;
- `require-mppe-128` – требование использования протокола шифрования MPPE-128;
- `proxyarp` параметр, необходимый для трансляции ARP-ответов из одного сегмента сети в другой;
- `nodefaultroute` – запрет устанавливать маршрут по умолчанию на сервер при установлении pptp соединения;
- `lock` – предотвращает использование одних и тех же учетных данных для одновременного подключения нескольких клиентов
- `nobsdcomp` – отключение BSD Compression для улучшения совместимости (используется на не BSD системах);
- `novj и novjccomp` – отключение Van Jacobson TCP/IP Header Compression для улучшения совместимости с некоторыми клиентскими устройствами (она используется только клиентами Windows 9x/ME/XP);
- `nologfd` – запрет записи отладочной информации в файл /var/log/ppp.log.

4. Теперь отредактируйте файл учетных записей PPTP-сервера:

```
root@Router1:~# vim /etc/ppp/chap-secrets
```

В конце файла допишите:

```
pptplogin * pptppass 172.16.1.100
```

где `pptplogin` - имя пользователя, `pptppass` - пароль, а `172.16.1.100` - IP-адрес, назначенный этому пользователю.

5. Запустите pptp-сервер:

```
root@Router1:~# service pptpd start
```

В Приложении представлены тексты конфигураций для Router1:

- текст конфигурации PPPoE сервера:
  - текст файла `/etc/ppp/pppoe-server-options`;
  - текст файла `/etc/ppp/chap-secrets`;
- текст конфигурации PPTP сервера:
  - текст файла `/etc/pptpd.conf`;
  - текст файла `/etc/ppp/pptpd-options`;
  - текст файла `/etc/ppp/chap-secrets`.

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 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 (в нашем примере это подсеть 192.168.100.0/24 для центрального офиса и подсеть 192.168.1.0/24 для филиала). Доверенным каналом связи также считается канал, защищенный при помощи протокола IPsec (например, после настройки шифрования между подсетями 192.168.1.0/24 и 192.168.100.0/24 разрешается выполнять настройку критошлюза Spoke1 из подсети 192.168.100.0/24 центрального офиса).

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.

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 базовом сценарии.

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

Изменение состояния интерфейсов и назначение IP адресов применяются сразу после ввода соответствующих команд. Политика безопасности применяются после выхода из режима конфигурирования.

1. Задайте имя устройства:

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

2. 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
```

3. Задайте IP адреса в соответствии со схемой стенда на внешнем `GigabitEthernet0/0` и внутреннем `GigabitEthernet0/1` интерфейсах:

```
Hub1(config)#interface GigabitEthernet 0/0
Hub1(config-if)#ip address 172.16.100.2 255.255.255.0
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
```

4. Задайте маршрут по умолчанию через устройство Router1:

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

Подробная настройка с описанием команд находится в базовом сценарии.

Настройка шифрования

1. 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 1, описывающую параметры IKE туннеля для совместимости с версией 5.0:

```
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. Опционально: создайте политику 2, описывающую параметры IKE туннеля для совместимости с версией 4.3:

```
Hub1(config)#crypto isakmp policy 2
Hub1(config-isakmp)#encryption gost
Hub1(config-isakmp)#hash gost341112-256-tc26
Hub1(config-isakmp)#authentication gost-sig
Hub1(config-isakmp)#group vko2
Hub1(config-isakmp)#exit
```

1.4. Создайте профиль настроек ISAKMP под именем `NEW_ALGS` для совместимости с версией 5.0:

```
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
```

1.5. Опционально: создайте профиль настроек ISAKMP под именем `OLD_ALGS` для совместимости с версией 4.3:

```
Hub1(config)#crypto isakmp profile OLD_ALGS
Hub1(conf-isa-prof)#match identity dn
Hub1(conf-isa-prof)#set identity mapping
Hub1(conf-isa-prof)#set policy 2
Hub1(conf-isa-prof)#exit
```

2. 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. Создайте IPsec трансформ, задающий комбинированный алгоритм шифрования и имитозащиты ГОСТ 34.12-2015 Магма в режиме MGM для трафика (для версий 5.0):

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

2.3. Опционально: для совместимости с версий 4.3 создайте IPsec трансформ, задающий комбинированный алгоритм шифрования и имитозащиты на базе ГОСТ 28147-89 для трафика:

```
Hub1(config)#crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-
imit
Hub1(cfg-crypto-trans)#exit
```

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

```
Hub1(config)#ip access-list extended IPSEC_ACl_HUB1_AND_SPOKE1
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)#exit
```

2.5. Создайте динамическую-карту (имя DMAP, раздел 1):

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

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 GOST_MAGMA_ENCRYPT_AND_INTEGRITY
```

2.5.3. Поскольку IP адрес партнера по IPsec в данном сценарии однозначно не определен, включите RRI:

```
Hub1(config-crypto-map)#reverse-route
```

2.5.4. Прикрепите настройки ISAKMP (протокол IKE):

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

2.5.5. Обязательно отключите историю удаленных туннелей, включите префрагментацию, включите автоматическую и интеллектуальную корректировку значения MSS для исходящего TCP трафика:

```
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#exit
```

2.6. Опционально: для совместимости с 4.3 используйте крипто-карту со следующими параметрами:

```
Hub1(config)#crypto dynamic-map DMAP 1
Hub1(config-crypto-map)#match address IPSEC_ACL_HUB1_AND_SPOKE1
Hub1(config-crypto-map)#set transform-set GOST_ENCRYPT_AND_INTEGRITY
Hub1(config-crypto-map)#reverse-route
Hub1(config-crypto-map)#set isakmp-profile OLD_ALGS
Hub1(config-crypto-map)#set dead-connection history off
Hub1(config-crypto-map)#set pre-fragmentation
Hub1(config-crypto-map)#set security-association mss-fix out
Hub1(config-crypto-map)#exit
```

2.7. Создайте крипто-карту с прикрепленной к ней динамической картой (имя VPN, раздел 1):

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

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

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

2.9. Примените настройки:

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

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка политики обработки COC (CRL)

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

Включите проверку COC и настройте автоматическую загрузку и импортирование в базу Продукта списка отозванных сертификатов с HTTP сервера CRL_distribution_point.

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка межсетевого экрана

1. Создайте сетевой `object-group` с именем `SELF` для хранения в нем WAN адресов криптошлюза:

```
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 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
```

Подробная настройка с описанием команд приведена в базовом сценарии.

Настройка криптошлюза Hub1 завершена.

В Приложении представлены тексты конфигураций для криптошлюза Hub1:

- текст консоли cisco-like;
- текст LSP.

Настройка криптошлюза Spoke1

Настройка криптошлюза Spoke1 происходит аналогично настройке Hub1, за исключением настройки сетевых параметров и настроек IKE/IPsec для совместимости с версией 4.3.

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP.

Настройка сетевых параметров

1. Задайте имя устройства:

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

2. 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
```

3. Задайте IP адрес на внутреннем `GigabitEthernet0/1` интерфейсе:

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

Настройка сетевых параметров для PPPoE

1. Добавьте интерфейс `PPPOE0` в карту интерфейсов. Для этого добавьте перед последней строкой файла `/etc/ifaliases.cf` следующую строку:

```
interface (name=”PPPOE0” pattern=”ppp0”)
```

   В итоге файл `/etc/ifaliases.cf` должен выглядеть следующим образом:

```
root@Spoke1:~# cat /etc/ifaliases.cf
```

```
interface (name="GigabitEthernet0/0" pattern="eth0")
interface (name="GigabitEthernet0/1" pattern="eth1")
interface (name="GigabitEthernet0/2" pattern="eth2")
interface (name="PPPOE0" pattern="ppp0")
interface (name="default" pattern="*")
```

2. После изменения файла нужно пересчитать его хеш:

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

3. Проверьте добавление интерфейса:

```
root@Spoke1:~# su cscons
Spoke1# show int
```

```
...
PPPOE0 is down, line protocol is down
  Hardware is absent (pattern "ppp0")
```

```
Spoke1#exit
```

4. Сконфигурируйте PPPoE соединение (название `test-pppoe`). Для этого создайте и отредактируйте файл `/etc/ppp/peers/test-pppoe` к следующему виду:

```
noipdefault
usepeerdns
defaultroute

hide-password
lcp-echo-interval 20
lcp-echo-failure 3
connect /bin/true
```

```
noauth
persist
mtu 1492
noaccomp
default-asyncmap

plugin rp-pppoe.so eth0
ifname ppp0
user "pppoelogin"
```

где:

- `noipdefault` – получение IP-адреса от PPPoE сервера;
- `usepeerdns` – получение DNS серверов от PPPoE сервера;
- `defaultroute` – установление маршрута по умолчанию через PPPoE соединение;
- `hide-password` – сокрытие паролей аутентификации из логов;
- `lcp-echo-interval 20` – установка интервала отправки LCP эхо-запросов – 20 секунд;
- `lcp-echo-failure 3` – определение разрыва соединения после 3 неотвеченных запросов;
- `connect /bin/true` – указание pppd команды, которую нужно запустить в оболочке перед попыткой начать согласование PPP (/bin/true возвращает 0);
- `noauth` – запрет требования аутентификации у партнера;
- `persist` – повторная попытка установления соединения после его разрыва, вместо немедленного завершения работы;
- `mtu 1492` – установление MTU = 1492 (стандарт для PPPoE соединения);
- `noaccomp` – отключение сжатия адресного/управляющего поля в заголовках ppp пакетов в обоих направлениях;
- `default-asyncmap` – запуск принудительного экранирования всех управляющих символов в направлениях передачи и приема;
- `plugin rp-pppoe.so eth0` – использование плагина для установления PPPoE на интерфейсе eth0;
- `ifname ppp0` – принудительная установка имени ppp0;
- `user "pppoelogin"` – использование пользователя testlogin для аутентификации.

5. Добавьте логин и пароль в файл аутентификации. Для этого добавьте в файл `/etc/ppp/chap-secrets` следующую строку:

```
pppoelogin * pppoepass
```

6. Настройте поведение интерфейса (авто включение при старте системы). Для этого в конец файла `/etc/network/interfaces` добавьте строки:

```
auto test-pppoe
iface test-pppoe inet ppp
provider test-pppoe
```

Обратите внимание, что строки между маркерами: ###netifcfg-*### содержат автосгенерированную информацию. Вносить все изменения в конфигурацию нужно за пределами этих маркеров.

7. Запустите соединение с помощью команды `pon test-pppoe`.:

```
root@Spoke1:~# pon test-pppoe
```

Для прекращения работы конфигурации используйте команду `poff test-pppoe`.

8. Проверить установление соединения можно с помощью команды `plog`:

```
root@Spoke1:~# plog
```

```
2025-11-21T10:52:30.684691+03:00 Spoke1 pppd[2981]: rcvd [IPCP ConfAck id=0x2 <addr
172.16.1.100> <ms-dns1 8.8.8.8> <ms-dns2 8.8.4.4>]
2025-11-21T10:52:30.685156+03:00 Spoke1 pppd[2981]: Script /etc/ppp/ip-pre-up started
(pid 2986)
```

```
2025-11-21T10:52:30.692109+03:00 Spoke1 pppd[2981]: Script /etc/ppp/ip-pre-up finished
(pid 2986), status = 0x0
2025-11-21T10:52:30.692284+03:00 Spoke1 pppd[2981]: local  IP address 172.16.1.100
2025-11-21T10:52:30.692319+03:00 Spoke1 pppd[2981]: remote IP address 172.16.1.10
2025-11-21T10:52:30.692337+03:00 Spoke1 pppd[2981]: primary   DNS address 8.8.8.8
2025-11-21T10:52:30.692354+03:00 Spoke1 pppd[2981]: secondary DNS address 8.8.4.4
2025-11-21T10:52:30.692699+03:00 Spoke1 pppd[2981]: Script /etc/ppp/ip-up started (pid
2994)
2025-11-21T10:52:30.692743+03:00 Spoke1 pppd[2981]: Script /etc/ppp/ipv6-up finished
(pid 2984), status = 0x0
2025-11-21T10:52:30.715201+03:00 Spoke1 pppd[2981]: Script /etc/ppp/ip-up finished
(pid 2994), status = 0x0
```

Настройка сетевых параметров для PPTP

1. Задайте IP адрес в соответствии со схемой стенда на внешнем `GigabitEthernet0/0` интерфейсе:

```
Spoke1(config)#interface GigabitEthernet 0/0
Spoke1(config-if)#ip address 172.16.1.2 255.255.255.0
Spoke1(config-if)#exit
```

2. Добавьте интерфейс `PPPOE0` в карту интерфейсов в точности так же, как это было сделано для PPPoE и пересчитайте хэш. В результате карта интерфейсов должна иметь следующий вид:

```
root@Spoke1:~# cat /etc/ifaliases.cf
```

```
interface (name="GigabitEthernet0/0" pattern="eth0")
interface (name="GigabitEthernet0/1" pattern="eth1")
interface (name="GigabitEthernet0/2" pattern="eth2")
interface (name="PPPOE0" pattern="ppp0")
interface (name="default" pattern="*")
```

3. Проверьте добавление интерфейса:

```
root@Spoke1:~# su cscons
Spoke1# show int
```

```
...
PPPOE0 is down, line protocol is down
  Hardware is absent (pattern "ppp0")
```

```
Spoke1#exit
```

4. Настройте поведение интерфейса (авто включение при старте системы). Для этого за пределами маркеров ###netifcfg-*### добавьте следующие строки:

```
auto test-pptp
iface test-pptp inet ppp
provider test-pptp
```

Обратите внимание, что строки между маркерами: ###netifcfg-*### содержат автосгенерированную информацию. Вносить все изменения в конфигурацию нужно за пределами этих маркеров.

5. Сконфигурируйте PPTP соединение (название `test-pptp`). Для этого создайте и отредактируйте файл `/etc/ppp/peers/test-pptp` к следующему виду:

```
pty "pptp 172.16.1.1 --nolaunchpppd"
name pptplogin
remotename pptpd
require-mppe-128
file /etc/ppp/options.pptp
defaultroute
replacedefaultroute
ipparam pptpcon1
```

где:

- `pty "pptp 172.16.1.1 --nolaunchpppd"` – подключение по PPTP к серверу по IP-адресу 172.16.1.1
- `name pptplogin` – установка имени пользователя, используемое при аутентификации на PPTP сервере;
- `remotename pptpd` – указание имени для идентификации удаленного сервера;
- `require-mppe-128` – использование протокола MPPE с 128-битным ключом для шифрования;
- `file /etc/ppp/options.pptp` – файл с дополнительными опциями для соединения;
- `defaultroute` – установление маршрута по умолчанию через PPTP соединение;
- `replacedefaultroute` – замена существующего маршрута по умолчанию новым, установленным через PPTP-соединение;
- `ipparam pptpcon1` – идентификация соединения в скриптах pppd, эта строка передает дополнительный параметр pptpcon1 в скрипты pppd.

6. Добавьте логин и пароль в файл аутентификации. Для этого добавтье в файл `/etc/ppp/chap-secrets` следующую строку:

```
pptplogin * pptppass
```

7. Запустите соединение с помощью команды `pon test-pptp`:

```
root@Spoke1:~# pon test-pptp
```

Для прекращения работы конфигурации используйте команду `poff test-pptp`.

8. Проверить установление соединения можно с помощью команды `plog`:

```
root@Spoke1:~# plog
2025-11-26T11:55:53.397542+03:00 Spoke1 pppd[12518]: CHAP authentication succeeded
2025-11-26T11:55:53.397991+03:00 Spoke1 pppd[12518]: MPPE 128-bit stateless
compression enabled
2025-11-26T11:55:53.398642+03:00 Spoke1 pppd[12518]: local LL address
fe80::a904:e194:94c9:9c19
2025-11-26T11:55:53.398683+03:00 Spoke1 pppd[12518]: remote LL address
fe80::6584:adb0:5d25:6ef6
2025-11-26T11:55:53.404978+03:00 Spoke1 pppd[12518]: local IP address 172.16.1.100
2025-11-26T11:55:53.405048+03:00 Spoke1 pppd[12518]: remote IP address 172.16.1.10
```

В Приложении представлены тексты конфигураций для криптошлюза Spoke1:

- текст консоли cisco-like;
- текст LSP;
- текст конфигурации карты сетевых интерефейсов `/etc/ifaliases.cf`;
- текст конфигурации PPPoE соединения:
  - текст файла `/etc/ppp/peers/test-pppoe`;
  - текст файла `/etc/ppp/chap-secrets`;
- текст конфигурации PPTP соединения:
  - текст файла `/etc/ppp/peers/test-pptp`;
  - текст файла `/etc/ppp/chap-secrets`.

Проверка работоспособности стенда

Проверку работоспособности нужно выполнять после завершения настройки всех устройств стенда.

Проверка соединения между Spoke1 и Router1 с помощью PPPoE

1. Убедитесь, что PPPoE концентратор доступен. Для этого введите команду `pppoe` с опцией `-A`. В результате выполнения данной команды будут отправлены PADI пакеты и согласно полученным ответным пакетам выведен список доступных концентраторов:

   ```
   root@Spoke1:~# pppoe -A
   ```

   ```
   Access-Concentrator: Router1
   Got a cookie: e2 98 29 77 75 8e 46 78 72 95 05 ad 04 fc a9 08 ac 03 00 00
   AC-Ethernet-Address: 00:50:56:9e:00:a7
   ------------------------------------------------
   ```

2. Если ранее соединение не было запущено, запустите его с помощью следующей команды:

   ```
   root@Spoke1:~# pon test-pppoe
   ```

   ```
   Plugin rp-pppoe.so loaded.
   ```

   Если соединение было запущено на этапе настройки, пропустите этот шаг.

3. Проверить ход построения соединения можно при помощи команды `plog`:

   ```
   root@Spoke1:~# plog
   ```

   ```
   2025-11-19T10:30:33.245203+03:00 Spoke1 pppd[4055]: Script /etc/ppp/ip-pre-up finished
   (pid 4059), status = 0x0
   2025-11-19T10:30:33.245288+03:00 Spoke1 pppd[4055]: local  IP address 172.16.1.100
   2025-11-19T10:30:33.245311+03:00 Spoke1 pppd[4055]: remote IP address 172.16.1.10
   2025-11-19T10:30:33.245327+03:00 Spoke1 pppd[4055]: primary   DNS address 8.8.8.8
   2025-11-19T10:30:33.245343+03:00 Spoke1 pppd[4055]: secondary DNS address 8.8.4.4
   2025-11-19T10:30:33.245797+03:00 Spoke1 pppd[4055]: Script /etc/ppp/ip-up started (pid
   4068)
   2025-11-19T10:30:33.245847+03:00 Spoke1 pppd[4055]: Script /etc/ppp/ipv6-up finished
   (pid 4058), status = 0x0
   2025-11-19T10:30:33.277050+03:00 Spoke1 pppd[4055]: Script /etc/ppp/ip-up finished
   (pid 4068), status = 0x0
   ```

   Для расширенной диагностики добавьте в файл конфигурации соединения `/etc/ppp/peers/test-pppoe` следующие строки:

   ```
   debug
   logfile /var/log/pppd.log
   ```

   Все сообщения, касающиеся построения соединения будут записываться в файл `/var/log/pppd.log`. Содержание данного файла можно посмотреть с помощью утилиты `cat`:

   ```
   root@Spoke1:~# cat /var/log/pppd.log
   ```

   ```
   Send PPPOE Discovery V1T1 PADI session 0x0 length 12
    dst ff:ff:ff:ff:ff:ff  src 00:50:56:9e:a3:ef
    [service-name] [host-uniq  d7 0f 00 00]
   Recv PPPOE Discovery V1T1 PADO session 0x0 length 47
    dst 00:50:56:9e:a3:ef  src 00:50:56:9e:00:a7
    [AC-name Router1] [service-name] [AC-cookie  e2 98 29 77 75 8e 46 78 72 95 05 ad 04
   fc a9 08 ac 03 00 00] [host-uniq  d7 0f 00 00]
   Send PPPOE Discovery V1T1 PADR session 0x0 length 36
    dst 00:50:56:9e:00:a7  src 00:50:56:9e:a3:ef
    [service-name] [host-uniq  d7 0f 00 00] [AC-cookie  e2 98 29 77 75 8e 46 78 72 95 05
   ad 04 fc a9 08 ac 03 00 00]
   Recv PPPOE Discovery V1T1 PADS session 0x21 length 12
    dst 00:50:56:9e:a3:ef  src 00:50:56:9e:00:a7
    [service-name] [host-uniq  d7 0f 00 00]
   PADS: Service-Name: ''
   ```

```
PPP session is 33
Connected to 00:50:56:9e:00:a7 via interface eth0
using channel 33
Renamed interface ppp0 to ppp0
Using interface ppp0
Connect: ppp0 <--> eth0
sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xf9f66320>]
rcvd [LCP ConfReq id=0x1 <mru 1492> <auth chap MD5> <magic 0x12412b4c>]
sent [LCP ConfAck id=0x1 <mru 1492> <auth chap MD5> <magic 0x12412b4c>]
rcvd [LCP ConfAck id=0x1 <mru 1492> <magic 0xf9f66320>]
sent [LCP EchoReq id=0x0 magic=0xf9f66320]
rcvd [LCP EchoReq id=0x0 magic=0x12412b4c]
sent [LCP EchoRep id=0x0 magic=0xf9f66320]
rcvd [CHAP Challenge id=0x6a <159de2713c7254a8de620928b07b56f1>, name = "Router1"]
sent [CHAP Response id=0x6a <99890683e18d510fcba594c2afead64f>, name = "testlogin"]
rcvd [LCP EchoRep id=0x0 magic=0x12412b4c]
rcvd [CHAP Success id=0x6a "Access granted"]
CHAP authentication succeeded: Access granted
CHAP authentication succeeded
peer from calling number 00:50:56:9E:00:A7 authorized
sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
sent [IPV6CP ConfReq id=0x1 <addr fe80::c560:5a31:13c3:253c>]
rcvd [CCP ConfReq id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
sent [CCP ConfReq id=0x1]
sent [CCP ConfRej id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 172.16.1.1>]
sent [IPCP ConfRej id=0x1 <compress VJ 0f 01>]
rcvd [IPV6CP ConfReq id=0x1 <addr fe80::8532:1b9d:4584:5e25>]
sent [IPV6CP ConfAck id=0x1 <addr fe80::8532:1b9d:4584:5e25>]
rcvd [IPCP ConfNak id=0x1 <addr 172.16.1.2> <ms-dns1 8.8.8.8> <ms-dns2 8.8.4.4>]
sent [IPCP ConfReq id=0x2 <addr 172.16.1.2> <ms-dns1 8.8.8.8> <ms-dns2 8.8.4.4>]
rcvd [IPV6CP ConfAck id=0x1 <addr fe80::c560:5a31:13c3:253c>]
local  LL address fe80::c560:5a31:13c3:253c
remote LL address fe80::8532:1b9d:4584:5e25
Script /etc/ppp/ipv6-up started (pid 4058)
rcvd [CCP ConfAck id=0x1]
rcvd [CCP ConfReq id=0x2]
sent [CCP ConfAck id=0x2]
rcvd [IPCP ConfReq id=0x2 <addr 172.16.1.1>]
sent [IPCP ConfAck id=0x2 <addr 172.16.1.1>]
rcvd [IPCP ConfAck id=0x2 <addr 172.16.1.2> <ms-dns1 8.8.8.8> <ms-dns2 8.8.4.4>]
Script /etc/ppp/ip-pre-up started (pid 4059)
Script /etc/ppp/ip-pre-up finished (pid 4059), status = 0x0
local  IP address 172.16.1.2
remote IP address 172.16.1.1
primary   DNS address 8.8.8.8
secondary DNS address 8.8.4.4
Script /etc/ppp/ip-up started (pid 4068)
Script /etc/ppp/ipv6-up finished (pid 4058), status = 0x0
Script /etc/ppp/ip-up finished (pid 4068), status = 0x0
```

4. Проверьте получение маршрутов через интерфейс PPPOE с помощью команды `ip a`:

```
root@Spoke1:~# ip r show dev ppp0
```

```
default scope link
172.16.1.1 proto kernel scope link src 172.16.1.100
```

5. Убедитесь, что в системе появился интерфейс ppp0 и на нем настроен соответствующий адрес:

```
root@Spoke1:~# ip a show dev ppp0
```

```
7: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1492 qdisc fq_codel state
UNKNOWN group default qlen 3
    link/ppp
```

```
    inet 172.16.1.100 peer 172.16.1.10/32 scope global ppp0
       valid_lft forever preferred_lft forever
    inet6 fe80::106e:3a7d:2ce:a021 peer fe80::1072:1a24:fa71:e33/128 scope link
       valid_lft forever preferred_lft forever
```

6. Проверьте, что с криптошлюза Spoke1 по ICMP доступен Router1. Для этого выполните команду `ping` из cisco-like консоли криптошлюза:

```
Spoke1#ping 172.16.1.1
```

```
PING 172.16.1.1 (172.16.1.1) 100(128) bytes of data.
108 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.495 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.547 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.344 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=0.327 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=0.356 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4085ms
rtt min/avg/max/mdev = 0.327/0.413/0.547/0.089 ms
```

Проверка соединения между Spoke1 и Router1 с помощью PPTP

1. Проверьте, что с криптошлюза Spoke1 по ICMP доступен шлюз по умолчанию (Router1). Для этого выполните команду `ping`:

```
Spoke1#ping 172.16.1.1
```

```
PING 172.16.1.1 (172.16.1.1) 100(128) bytes of data.
108 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.771 ms
108 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.282 ms
108 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=0.276 ms
108 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=0.268 ms
108 bytes from 172.16.1.1: icmp_seq=5 ttl=64 time=0.244 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4096ms
rtt min/avg/max/mdev = 0.244/0.368/0.771/0.202 ms
```

2. Вернитесь в linux bash. Если ранее соединение не было запущено, запустите его с помощью следующей команды:

```
root@Spoke1:~# pon test-pptp
```

Если соединение было запущено на этапе настройки, пропустите этот шаг

3. Проверить ход построения соединения можно при помощи команды `plog`:

```
root@Spoke1:~# plog
```

```
2025-11-20T16:10:20.222998+03:00 Spoke1 pppd[1136]: CHAP authentication succeeded
2025-11-20T16:10:20.223705+03:00 Spoke1 pppd[1136]: MPPE 128-bit stateless compression
enabled
2025-11-20T16:10:20.226205+03:00    Spoke1    pppd[1136]:    local       LL    address
fe80::3946:abb9:e413:62cb
2025-11-20T16:10:20.226252+03:00    Spoke1    pppd[1136]:    remote    LL    address
fe80::4d4d:b588:ffec:f813
2025-11-20T16:10:20.233057+03:00 Spoke1 pppd[1136]: local  IP address 172.16.1.100
2025-11-20T16:10:20.233107+03:00 Spoke1 pppd[1136]: remote IP address 172.16.1.10
```

4. Убедитесь, что в системе появился интерфейс ppp0 и на нем настроен соответствующий адрес:

```
root@Spoke1:~# ip a show dev ppp0
```

```
9: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1496 qdisc fq_codel state
UNKNOWN group default qlen 3
    link/ppp
```

```
    inet 172.16.1.100 peer 172.16.1.10/32 scope global ppp0
       valid_lft forever preferred_lft forever
    inet6 fe80::3ca5:cb34:2b3a:4b7e peer fe80::d5ff:c076:e720:ba76/128 scope link
       valid_lft forever preferred_lft forever
```

Проверка IP связности

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

```
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=0.781 ms
108 bytes from 172.16.100.1: icmp_seq=2 ttl=64 time=0.280 ms
108 bytes from 172.16.100.1: icmp_seq=3 ttl=64 time=0.311 ms
108 bytes from 172.16.100.1: icmp_seq=4 ttl=64 time=0.230 ms
108 bytes from 172.16.100.1: icmp_seq=5 ttl=64 time=0.351 ms

--- 172.16.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.230/0.390/0.781/0.199 ms
```

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

```
Spoke1#ping 172.16.100.2 -c 5
```

```
PING 172.16.100.2 (172.16.100.2) 56(84) bytes of data.
64 bytes from 172.16.100.2: icmp_seq=1 ttl=63 time=1.13 ms
64 bytes from 172.16.100.2: icmp_seq=2 ttl=63 time=1.11 ms
64 bytes from 172.16.100.2: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 172.16.100.2: icmp_seq=4 ttl=63 time=1.10 ms
64 bytes from 172.16.100.2: icmp_seq=5 ttl=63 time=1.30 ms

--- 172.16.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4014ms
rtt min/avg/max/mdev = 1.090/1.144/1.296/0.077 ms
```

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

3. Проверьте, что с защищаемых устройств Host-b-spoke1 и Host-b-hub1 доступен по ICMP соответствующий криптошлюз, который является шлюзом по умолчанию. Для этого выполните команду `ping` из linux bash консоли защищаемых устройств.

```
root@Host-b-hub1:~# ping 192.168.100.1 -c 5
```

```
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=0.211 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.235 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.223 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.254 ms
64 bytes from 192.168.100.1: icmp_seq=5 ttl=64 time=0.233 ms

--- 192.168.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4088ms
rtt min/avg/max/mdev = 0.211/0.231/0.254/0.017 ms
```

```
root@Host-b-spoke1:~# ping 192.168.1.1 -c 5
```

```
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=0.214 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.223 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.189 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.210 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.212 ms
```

```
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.189/0.209/0.223/0.019 ms
```

Видно, что с защищаемых устройств Host-b-spoke1 и Host-b-hub1 соответствующие криптошлюзы доступны по ICMP.

Проверка PKI

1. Проверьте, что на криптошлюзах Hub1 и Spoke1 СОС импортирован в базу Продукта. Для этого выполните команду `run cert_mgr show` 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
```

```
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
```

Видно, что на криптошлюзах Hub1 и Spoke1 СОС импортирован в базу Продукта. Если этого не произошло, то проверьте файл журнала (команда `run grep getcrls_daemon /var/log/cspvpngate.log`) и, при необходимости, перезапустите сервис автоматической загрузки СОС (команда `run systemctl restart getcrls.service`).

2. Проверьте, что на криптошлюзах Hub1 и Spoke1 статус всех сертификатов Active. Для этого выполните команду `run cert_mgr check` из cisco-like консоли криптошлюзов.

```
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 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
```

Видно, что на криптошлюзах Hub1 и Spoke1 статус всех сертификатов Active. Если статус Inactive, то проверьте загружен ли СОС в базу Продукта и правильность установки даты и времени.

Проверка построения защищенного соединения между подсетями Hub1 и Spoke1

1. Инициируйте построение защищенного соединения между криптошлюзами Hub1 и Spoke1 при помощи ICMP трафика, посылаемого с устройства Host-b-spoke1 на Host-b-hub1. Для этого выполните команду `ping` из linux bash консоли защищаемого устройства Host-b-spoke1.

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

```
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=62 time=884 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=62 time=0.721 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=62 time=0.880 ms
64 bytes from 192.168.100.100: icmp_seq=4 ttl=62 time=0.819 ms
64 bytes from 192.168.100.100: icmp_seq=5 ttl=62 time=0.781 ms

--- 192.168.100.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4068ms
rtt min/avg/max/mdev = 0.721/177.445/884.027/353.291 ms
```

2. Проверьте, что на криптошлюзах Hub1 и Spoke1 установлено защищенное IPsec соединение. 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 1 (172.16.100.2,500)-(172.16.1.100,500) 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 tunn 4576
4576
```

```
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 (172.16.1.100,500)-(172.16.100.2,500) 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 tunn 1056
1056
```

Видно, что на криптошлюзах Hub1 и Spoke1 установлено защищенное IPsec соединение. 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.

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 password 0 csp
aaa new-model
!
!
hostname Hub1
enable password csp
!
!
!
!
!
!
!
crypto isakmp policy 1
 encr magma
 hash stribog-256
 authentication gost-sig
 group vko2
!
crypto isakmp policy 2
 encr gost
 hash gost341112-256-tc26
 authentication gost-sig
 group vko2
!
crypto isakmp profile NEW_ALGS
 match identity dn
 set identity mapping
 set policy 1
!
crypto isakmp profile OLD_ALGS
 match identity dn
 set identity mapping
 set policy 2
!
crypto ipsec transform-set GOST_MAGMA_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
crypto ipsec transform-set GOST_ENCRYPT_AND_INTEGRITY esp-gost28147-4m-imit
!
object-group network SELF
 remark WAN IP
 host 172.16.100.2
```

```
!
ip access-list extended IPSEC_ACL_HUB1_AND_SPOKE1
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 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_SPOKE1
 set transform-set GOST_MAGMA_ENCRYPT_AND_INTEGRITY
 set isakmp-profile NEW_ALGS
 set security-association mss-fix out
 reverse-route
 set pre-fragmentation
 set dead-connection history off
!
crypto map VPN 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 172.16.100.2 255.255.255.0
 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
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
!
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
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
quit
!
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Wed Nov 26 15:57:31 2025
```

```
GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Wed Nov 26 15:57:31 2025 (user: cscons)"
    Version                      = LSP_5_0
    CRLHandlingMode              = ENABLE
    PreserveIPsecSA              = FALSE
)

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

)

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

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

IKETransform crypto:isakmp:policy:2
(
    CipherAlg   = "G2814789CPRO1-K256-CBC-65534"
    HashAlg     = "GR341112_256TC26-65128"
    GroupID     = VKO2_1B
    RestrictAuthenticationTo = GOST_SIGN
    LifetimeSeconds = 86400
)

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

FilterChain FilterChain:FW_INPUT_WAN (
```

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

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

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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

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

AuthMethodGOSTSign GOST:Sign: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 = ( GOST_MAGMA_ENCRYPT_AND_INTEGRITY:ESP )
    ReverseRoute = TRUE
    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_SPOKE1"
    )
)

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

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

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)
```

Конфигурации криптошлюза Spoke1

При использовании PPPoE

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 password 0 csp
aaa new-model
!
!
```

```
hostname Spoke1
enable password csp
!
!
!
!
!
!
!
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 GOST_MAGMA_ENCRYPT_AND_INTEGRITY esp-magma-mgm
!
object-group network SELF
 remark WAN IP
 host 172.16.1.100
!
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 GOST_MAGMA_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
 no ip address
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 no ip address
 shutdown
!
```

```
interface PPPOE0
 ip access-group FW_INPUT_WAN in
 crypto map VPN
 ip inspect INSPECT out
!
!
!
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check crl
 crl download group ROOTCA http://172.16.101.15/certcrl.crl
 crl download time 60
crypto pki certificate chain s-terra_technological_trustpoint
certificate 58E026BFD6D625BE4582C16C6189C183
30820227308201D4A003020102021058E026BFD6D625BE4582C16C6189C18330
...
AD4F8901771632E0A0AF83

quit
!
end
```

2. Конфигурация LSP:

```
#   This is automatically generated LSP
#
#   Conversion Date/Time:   Thu Nov 27 12:09:58 2025

GlobalParameters(
    Title                      = "This LSP was automatically generated by CSP Converter
at Thu Nov 27 12:09:58 2025 (user: cscons)"
    Version                       = LSP_5_0
    CRLHandlingMode               = ENABLE
    PreserveIPsecSA               = FALSE
)

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 GOST_MAGMA_ENCRYPT_AND_INTEGRITY:ESP
```

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

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

FilterChain FilterChain:FW_INPUT_WAN (
    Filters = Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.100
        ProtocolID = 17
        DestinationPort = 500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.100
        ProtocolID = 17
        DestinationPort = 4500
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.100
        ProtocolID = 1
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 172.16.1.100
        ProtocolID = 50
        Action = PASS
        LogEventID = "FW_INPUT_WAN"
    ),
    Filter (
        SourceIP = 0.0.0.0/0
        DestinationIP = 0.0.0.0/0
        Action = DROP
    )
    IPv6Filters = Filter (
        SourceIP = ::/0
        DestinationIP = ::/0
        Action = DROP
    ))
```

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

IdentityEntry Remote:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

IdentityEntry Local:Cert:NEW_ALGS(
    DistinguishedName = USER_SPECIFIC_DATA
)

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 = ( GOST_MAGMA_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 = IPv6Default
    OutputFilter = IPv6Default
)

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

NetworkInterface (
    LogicalName = "GigabitEthernet0/2"
    InputFilter = IPv6Default
    OutputFilter = IPv6Default
)

NetworkInterface (
    LogicalName = "PPPOE0"
    InputFilter = FilterChain:FW_INPUT_WAN
    OutputFilter = InspectChain:INSPECT
    IPsecPolicy = IPsecPolicy:VPN
)
```

3. Конфигурация карты сетевых интерфейсов `/etc/ifaliases.cf`:

```
interface (name="GigabitEthernet0/0" pattern="eth0")
interface (name="GigabitEthernet0/1" pattern="eth1")
interface (name="GigabitEthernet0/2" pattern="eth2")
interface (name="PPPOE0" pattern="ppp0")
interface (name="default" pattern="*")
```

4. Конфигурация PPPoE:

   4.1. Содержимое файла `/etc/ppp/peers/test-pppoe`

```
noipdefault
usepeerdns
defaultroute

hide-password
lcp-echo-interval 20
lcp-echo-failure 3
connect /bin/true
noauth
persist
mtu 1492
noaccomp
default-asyncmap

plugin rp-pppoe.so eth0
ifname ppp0
user "pppoelogin"
```

   4.2. Содержимое файла `/etc/ppp/chap-secrets`

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses

pppoelogin * pppoepass
```

При использовании PPTP

Разница между конфигурацией cisco-like для PPPoE и PPTP состоит в наличии для PPTP адреса на интерфейсе `GigabitEthernet0/0` адреса.

1. Конфигурация PPTP:

   1.1. Содержимое файла `/etc/ppp/peers/test-pptp`

```
pty "pptp 172.16.1.1 --nolaunchpppd"
name pptplogin
require-mppe-128
file /etc/ppp/options.pptp
defaultroute
replacedefaultroute
ipparam pptpcon1
```

   1.2. Содержимое файла `/etc/ppp/chap-secrets`

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses

pptplogin * pptppass
```

Конфигурация Router1

1. Конфигурация PPPOE сервера:

   1.1. Содержимое файла `/etc/ppp/pppoe-server-options`

```
auth
require-chap
lcp-echo-interval 10
lcp-echo-failure 2
ms-dns 8.8.8.8
ms-dns 8.8.4.4
noipdefault
```

```
noipx
nodefaultroute
noproxyarp
# netmask for clietns
netmask 255.255.255.255
# path to logs
logfile /var/log/log.pppoe
```

1.2. Содержимое файла `/etc/ppp/chap-secrets`

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
pppoelogin * pppoepass 172.16.1.100
```

2. Конфигурация PPTP сервера:

2.1. Содержимое файла `/etc/pptpd.conf`

```
option /etc/ppp/pptpd-options
logwtmp
bcrelay ens224
localip 172.16.1.10
remoteip 172.16.1.100
```

2.2. Содержимое файла `/etc/ppp/pptpd-options`

```
name pptpd
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe-128
proxyarp
nodefaultroute
lock
nobsdcomp
novj
novjccomp
nologfd
```

2.3. Содержимое файла `/etc/ppp/chap-secrets`

```
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
pptplogin * pptppass 172.16.1.100
```