FlexVPN говорил в избыточном дизайне концентратора с примером конфигурации блока клиента FlexVPN

Содержание

Введение

Этот документ описывает, как настроить луч в сети FlexVPN с использованием блока конфигурации клиента FlexVPN в сценарии, где несколько концентраторов доступны.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- FlexVPN
- Протоколы маршрутизации Cisco

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор с интеграцией служб (ISR) Cisco G2 Series
- Cisco IOS® Version 15.2M

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Для обеспечений резервирования луч, возможно, должен был бы соединиться с несколькими концентраторов. Резервирование на стороне оконечного устройства позволяет непрерывную операцию без единственного уязвимого звена на стороне концентратора.

Два наиболее распространенных FlexVPN избыточные дизайны концентратора, которые используют конфигурацию оконечного устройства:

- **Двойной облачный подход**, где луч имеет два отдельных туннеля, активные к обоим концентраторам в любом случае.
- **Подход аварийного переключения**, где луч имеет активный туннель с одним концентратором в любой данный момент времени.

Оба подхода имеют уникальный набор за и против.

Подход	Плюсы	Недостатки
Двойное облако	• Более быстрое восстановление в сбое, на основе таймеров протокола маршрутизации • Большие возможности распределить трафик среди концентраторов, так как соединения с обоими концентраторами активны	• Луч поддерживает сеанс к обоим концентраторам в то же время, который использует ресурсы на обои концентраторах
Failover	• Простота конфигурации - встроенный в FlexVPN • Не полагается на протокол маршрутизации в сбое	• Более медленное время восстановления - на основе Dead Pe Detection (DPD) или (дополнительно) отслеживания объектов • Весь трафик вынужден переместить в один концентратор за один раз

Этот документ описывает второй подход.

Настройка

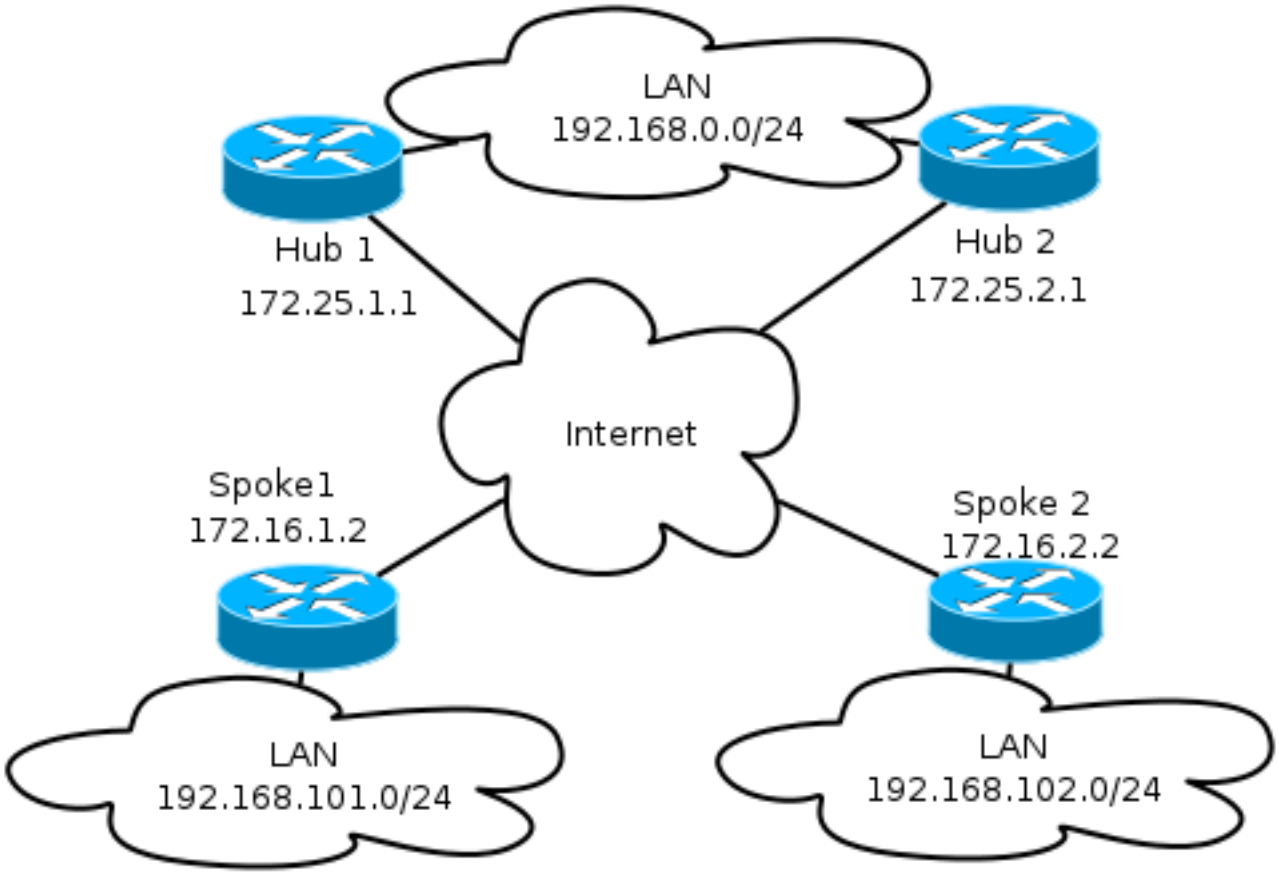
> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Сетевые графики

Эти схемы показывают обоим транспорт и накладывают схемы топологии.

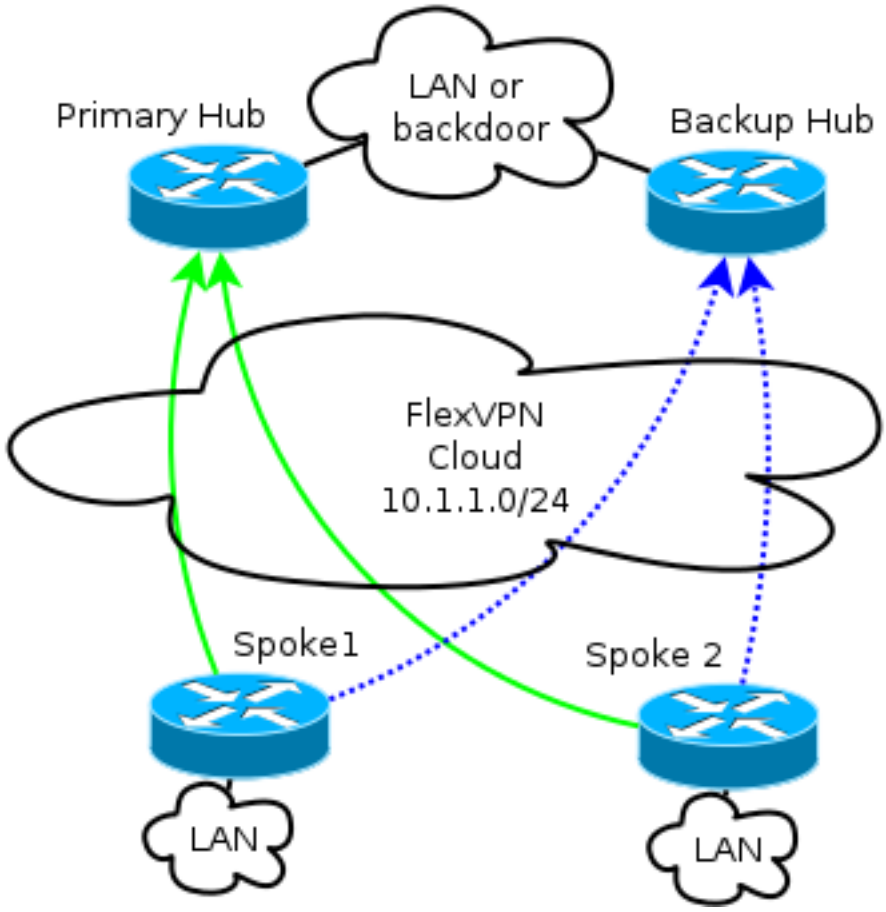
Транспортная сеть

Эта схема иллюстрирует основную транспортную сеть, которая, как правило, используется в сетях FlexVPN.



Оверлейная сеть

Эта схема иллюстрирует оверлейную сеть с логическим подключением, которое показывает, как должно работать аварийное переключение. Во время нормальной работы, Луч 1 и Говорил 2, поддерживают отношения с одним концентратором только.



Примечание: В схеме существенные зеленые линии показывают соединение и направление основной второй версии протокола Internet Key Exchange (IKEv2) / сеансы Flex, и точечные голубые линии указывают, что резервное подключение должно сеанс Протокола IKE к сбою первичного концентратора.

Адресация**/24** представляет пул адресов, выделенных для этого облака, а не фактической интерфейсной адресации. Это вызвано тем, что концентратор FlexVPN, как правило, выделяет динамический IP - адрес для лучевого интерфейса и полагается на маршруты, вставленные динамично через команды маршрута в блоке авторизации FlexVPN.

Базовая конфигурация луча и концентратора

Базовая конфигурация концентратора и луча основывается на документах миграции от Динамической многоточечной VPN (DMVPN) до FlexVPN. Эта конфигурация описана в Миграции FlexVPN: Твердое Перемещение от DMVPN до FlexVPN на статье Same Devices.

Корректировка конфигурации оконечного устройства

Конфигурация оконечного устройства - блок конфигурации клиента

Конфигурация оконечного устройства должна быть расширена блоком конфигурации клиента.

В базовой конфигурации заданы множественные одноранговые телефонные соединения. Узел с наивысшим приоритетом (самый низкий номер) рассматривают перед другими.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

Конфигурация туннеля должна измениться, чтобы позволить назначению туннеля быть выбранным динамично, на основе блока конфигурации клиента FlexVPN.

```
interface Tunnel1
 tunnel destination dynamic
```

Крайне важно помнить, что блок конфигурации клиента FlexVPN связан к интерфейсу, а не к IKEv2 или протоколу IPSEC (Internet Protocol Security) (IPsec) профиль.

Блок конфигурации клиента предоставляет составные опции для регулировки времени аварийного переключения и операций, которые включают использование объектов отслеживания, резервирование коммутируемыми каналами и функциональность групп резервного копирования.

С базовой конфигурацией луч полагается на DPD, чтобы обнаружить, безразличен ли луч, и это инициирует изменение, как только узел объявлен мертвый. Опция для использования DPD не является быстрой, из-за того, как работают DPD. Администратор мог бы хотеть улучшить конфигурацию с отслеживанием объектов или подобными усовершенствованиями.

Для получения дополнительной информации обратитесь к главе **Конфигурации клиента FlexVPN** руководства Конфигурации Cisco IOS, которое связано в **Разделе связанных сведений** в конце этого документа.

Полная конфигурация оконечного устройства - ссылка

```
interface Tunnel1
 tunnel destination dynamic
```

Конфигурация концентратора

В то время как большинство конфигурации концентратора остается тем же, несколько аспектов должны быть обращены. Большинство из них принадлежит ситуации, в которой или больше лучей связаны с одним концентратором, в то время как другие остаются в отношении к другому концентратору.

Лучевые адреса

Так как лучи получают IP-адреса из концентраторов, обычно желательно, чтобы концентраторы назначили адреса от других подсетей или другой части подсети.

Пример:

Hub1

```
interface Tunnel1
 tunnel destination dynamic
```
Hub2

```
interface Tunnel1
 tunnel destination dynamic
```
Это предотвращает создание наложения, даже если адреса не маршрутизируются за пределами облака FlexVPN, которое могло бы повредить устранение проблем.

Адрес наложения концентратора

Оба концентратора могут сохранить тот же IP-адрес на виртуальном интерфейсе; однако, это может повлиять на устранение проблем в некоторых случаях. Это проектное решение упрощает развертываться и планировать, так как луч должен иметь только один адрес партнера (peer) для Протокола BGP.

В некоторых случаях это не могло бы быть желаемо или нуждалось.

Маршрутизация

Необходимо для концентраторов обмениваться информацией о лучах, которые связаны.

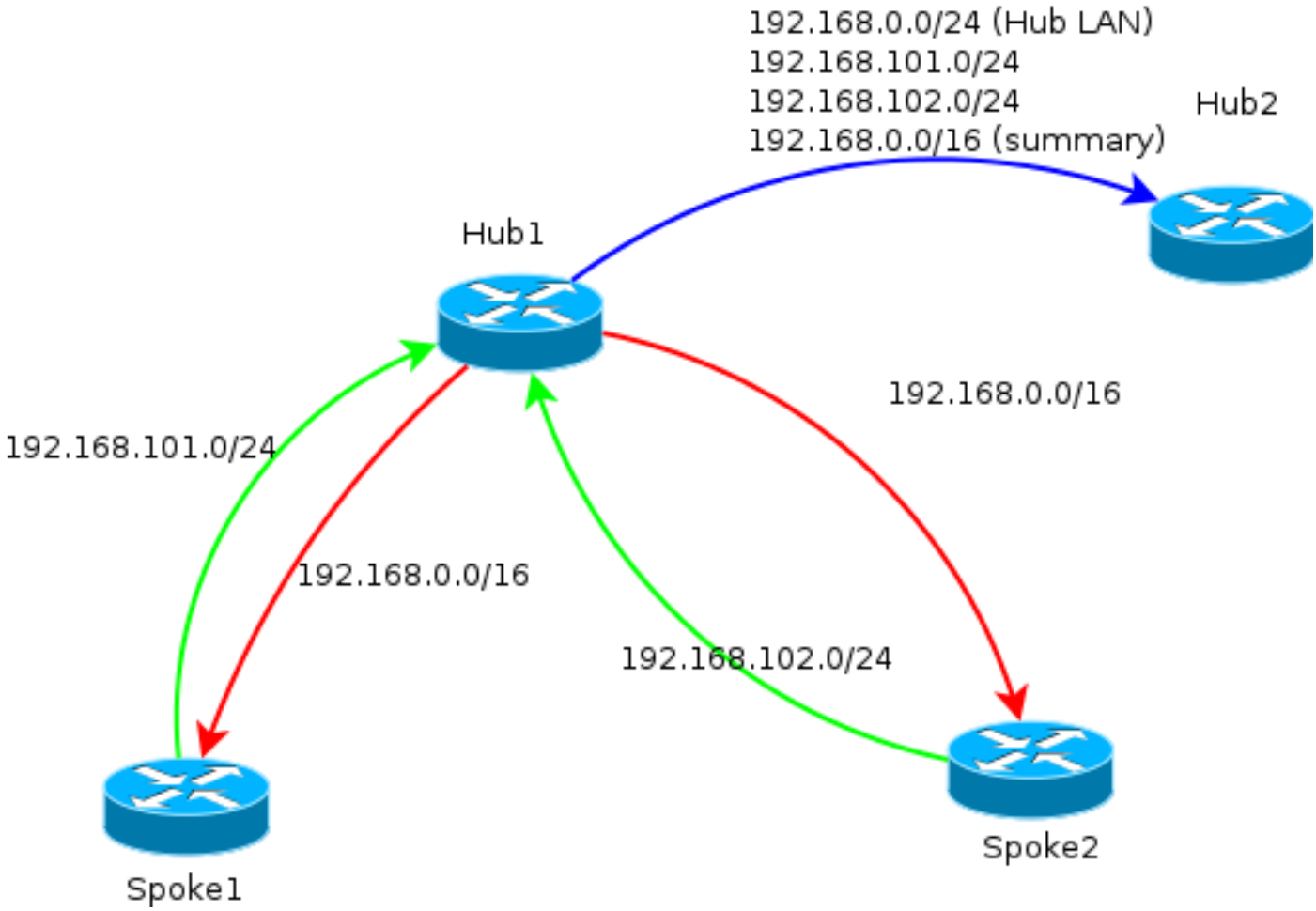
Концентраторы должны быть в состоянии обмениваться определенными маршрутами устройств, которые они подключили, и все еще предоставляют сводку лучам.

Так как Cisco рекомендует использовать iBGP с FlexVPN и DMVPN, только тот протокол маршрутизации показывают.

```
interface Tunnel1
 tunnel destination dynamicinterface Tunnel1
 tunnel destination dynamic
```
Эта конфигурация позволяет:

- Динамический слушатель от адресов, назначенных на лучи
- Рекламная сеть 192.168.0.0/24
- Рекламный объединенный маршрут 192.168.0.0/16 ко всем лучам. Конфигурация агрегаторного адреса создает статический маршрут для того префикса через интерфейс null0, который является маршрутом сброса, который используется для предотвращения циклов маршрутизации.
- Передача определенных префиксов к другому концентратору
- Клиент отражателя маршрута, чтобы удостовериться, что концентраторы обмениваются информацией, изученной из лучей друг между другом

Эта схема представляет префиксный обмен в BGP в этой настройке, с точки зрения одного из концентраторов.



Примечание: В этой схеме зеленая линия представляет информацию, предоставленную лучами концентратору, красная линия представляет информацию, предоставленную каждым концентратором лучам (только сводка), и голубая линия представляет префиксы, которыми обмениваются между концентраторами.

Сетевое использование сводок

Сводки не могли бы быть применимы или не желаемы в некоторых сценариях. Проявите осмотрительность при обозначении IP - адреса назначения в префиксах потому что iBGP не отвергает следующий переход по умолчанию.

Сводки часто рекомендуются в сетях то состояние изменения. Например, нестабильные Интернет-соединения могли бы потребовать сводок чтобы к: избегите удаления и добавления префиксов, ограничьте количество обновлений и позвольте большинству настроек масштабироваться должным образом.

Туннели конечного маршрутизатор - конечного маршрутизатора

В сценарии и конфигурации, упомянутой в предыдущем разделе, лучи на других концентраторах не в состоянии установить прямые туннели конечного маршрутизатор - конечного маршрутизатора. Трафик между лучами соединился с другими потоками концентраторов по центральным устройствам.

Существует легкий обходной путь для этого. Однако это требует, чтобы Протокол NHRP с тем же network-ID был включен между концентраторами. Это может быть достигнуто, например при создании Туннеля универсальной инкапсуляции маршрутизации (GRE) "точка-точка" между концентраторами. Затем IPsec не требуется.

Проверка

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Команда show crypto ikev2 sa сообщает вам о том, где в настоящее время связывается луч.

Показ крипто-ikev2 клиентская flexvpn команда позволяет администратору понимать текущее состояние операции клиента FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpnSpoke2# show crypto ikev2 client flexvpn
```

Успешное аварийное переключение с конфигурацией **show logging** регистрирует эти выходные данные на лучевом устройстве:

```
Spoke2# show crypto ikev2 client flexvpn
```

В этих выходных данных, лучевых разъединениях от **концентратора 172.25.1.1**, блок конфигурации клиента Flex_Client обнаруживает сбой и вызывает соединение с **172.25.2.1**, где туннель подходит, и лучу назначают IP **10.1.1.177**.

Устранение неполадок

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Вот соответствующие команды отладки:

- **debug crypto ikev2**
- **debug radius**

Дополнительные сведения

- FlexVPN и руководство по конфигурации версии 2 обмена ключами между сетями, Cisco IOS Выпуск 15 M&T
- Cisco Systems – техническая поддержка и документация