FlexVPN говорил в избыточном дизайне концентратора с двойным облачным примером конфигурации подхода

Содержание

Введение

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

Настройка

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.

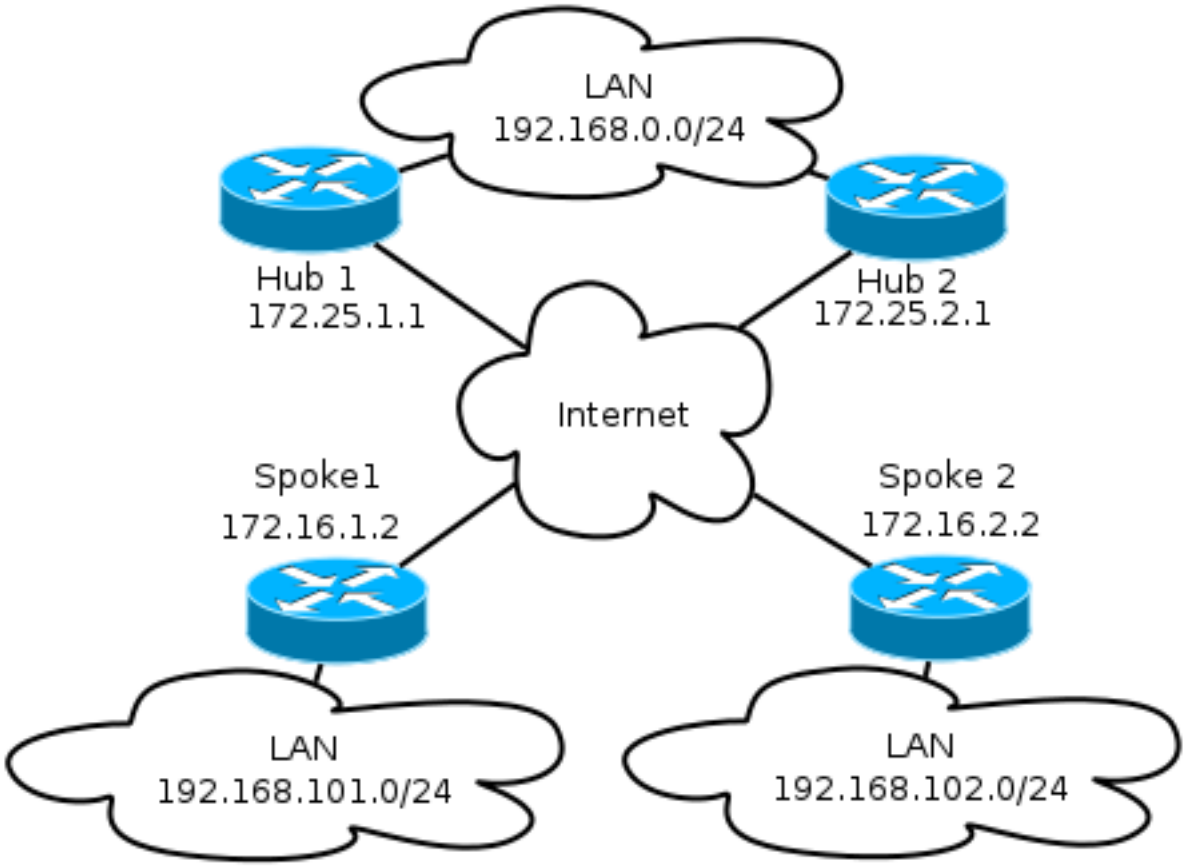
Подход	Плюсы	Недостатки
Двойное облако	• Более быстрое восстановление во время сбоя, на основе таймеров протокола маршрутизации • Большие возможности распределить трафик среди концентраторов, начиная с соединения с обоими концентраторами активны	• Луч поддерживает сеанс к обоим концентраторам в то же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

Этот документ описывает первый подход. Подход к этой конфигурации подобен Динамической многоточечной VPN (DMVPN) двойная облачная конфигурация. Базовая конфигурация концентратора и луча основывается на документах миграции от DMVPN до FlexVPN. См. Миграцию FlexVPN: Твердое Перемещение от DMVPN до FlexVPN на статье Same Devices для описания этой конфигурации.

Схема сети

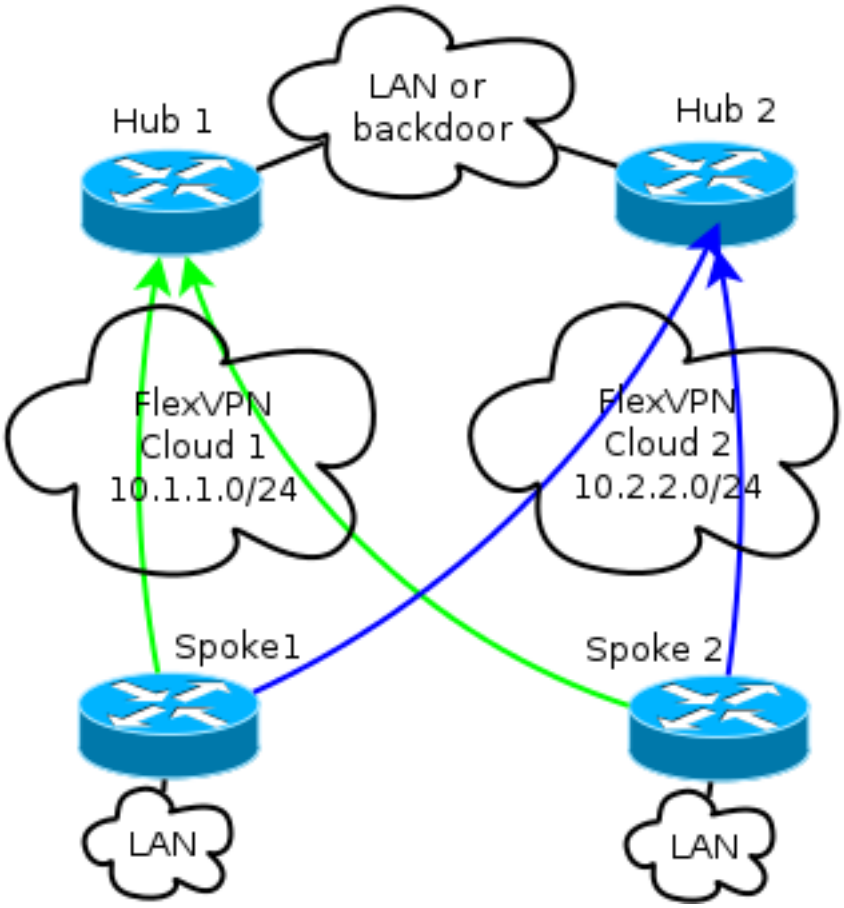
Транспортная сеть

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



Оверлейная сеть

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 обоими концентраторами. После сбоя протокол маршрутизации переключается от одного концентратора до другого.



Примечание: В схеме зеленые линии показывают соединение и направление второй версии протокола Internet Key Exchange (IKEv2) / сеансы Flex для Концентрации 1, и голубые линии указывают на соединение для Концентрации 2.

Оба концентратора сохраняют отдельную IP-адресацию в облаках наложения. Адресация**/24** представляет пул адресов, выделенных для этого облака, 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.

Конфигурации оконечного устройства

Лучевая конфигурация туннельного интерфейса

Типичная конфигурация, используемая в данном примере, является просто двумя туннельными интерфейсами с двумя отдельными адресами назначения (DA).

```
interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
```

```
tunnel protection ipsec profile default

interface Tunnel2
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Чтобы позволить туннелям конечного маршрутизатор - конечного маршрутизатора формироваться должным образом, Виртуальный шаблон (VT) необходим.

```
interface Virtual-Template1 type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Луч использует ненумерованный интерфейс, который указывает на интерфейс LAN (локальной сети) в Виртуальной маршрутизации и Передаче (VRF), который является глобальным в этом случае. Однако могло бы быть лучше сослаться на интерфейс обратной связи. Это вызвано тем, что интерфейсы обратной связи остаются онлайновыми при почти всех условиях.

Лучевая конфигурация протокола BGP

Так как Cisco рекомендует iBGP как протокол маршрутизации использоваться в оверлейной сети, этот документ упоминает только эту конфигурацию.

Примечание: Спицы должны сохранить достижимость BGP к обоим концентраторам.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

FlexVPN в этой конфигурации не имеет основного понятия или понятия вспомогательного концентратора. Администратор решает, предпочитает ли протокол маршрутизации один концентратор по другому или, в некоторых сценариях, выполняет распределение нагрузки.

Лучевые факторы аварийного переключения и конвергенции

Для уменьшения времени, оно берет для луча, чтобы обнаружить сбой, использовать эти два типичных метода.

- Сократите таймеры BGP. Время удержания по умолчанию вызывает аварийное

переключение.
- Настройте BGP, падают, который обсужден в этой статье, Поддержке BGP для Быстрой Деактивации Сеанса с равноправным участием.
- Не используйте обнаружение двунаправленной передачи данных (BFD), потому что оно не рекомендуется в большинстве развертываний FlexVPN.

Туннели конечного маршрутизатор - конечного маршрутизатора и аварийное переключение

Туннели конечного маршрутизатор - конечного маршрутизатора используют коммутацию ярлыка Протокола NHRP. Cisco IOS указывает, что те ярлыки являются маршрутами NHRP, например:

```
Spoke1#show ip route nhrp
(...) 192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Когда соединение BGP истекает, те маршруты не истекают; вместо этого, они проводятся для времени удержания NHRP, которое составляет два часа по умолчанию. Это означает, что активные туннели конечного маршрутизатор - конечного маршрутизатора остаются в операции даже в сбое.

Конфигурации концентратора

Локальные пулы

Как обсуждено в разделе **Диаграммы сети**, оба концентратора сохраняют отдельную IP-адресацию.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

BGP - конфигурация концентратора

BGP - конфигурация концентратора остается подобным предыдущим примерам.

Эти выходные данные прибывают из Концентратора 1 с IP-адресом LAN **192.168.0.1**.

```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL route-map ALL permit 10
```

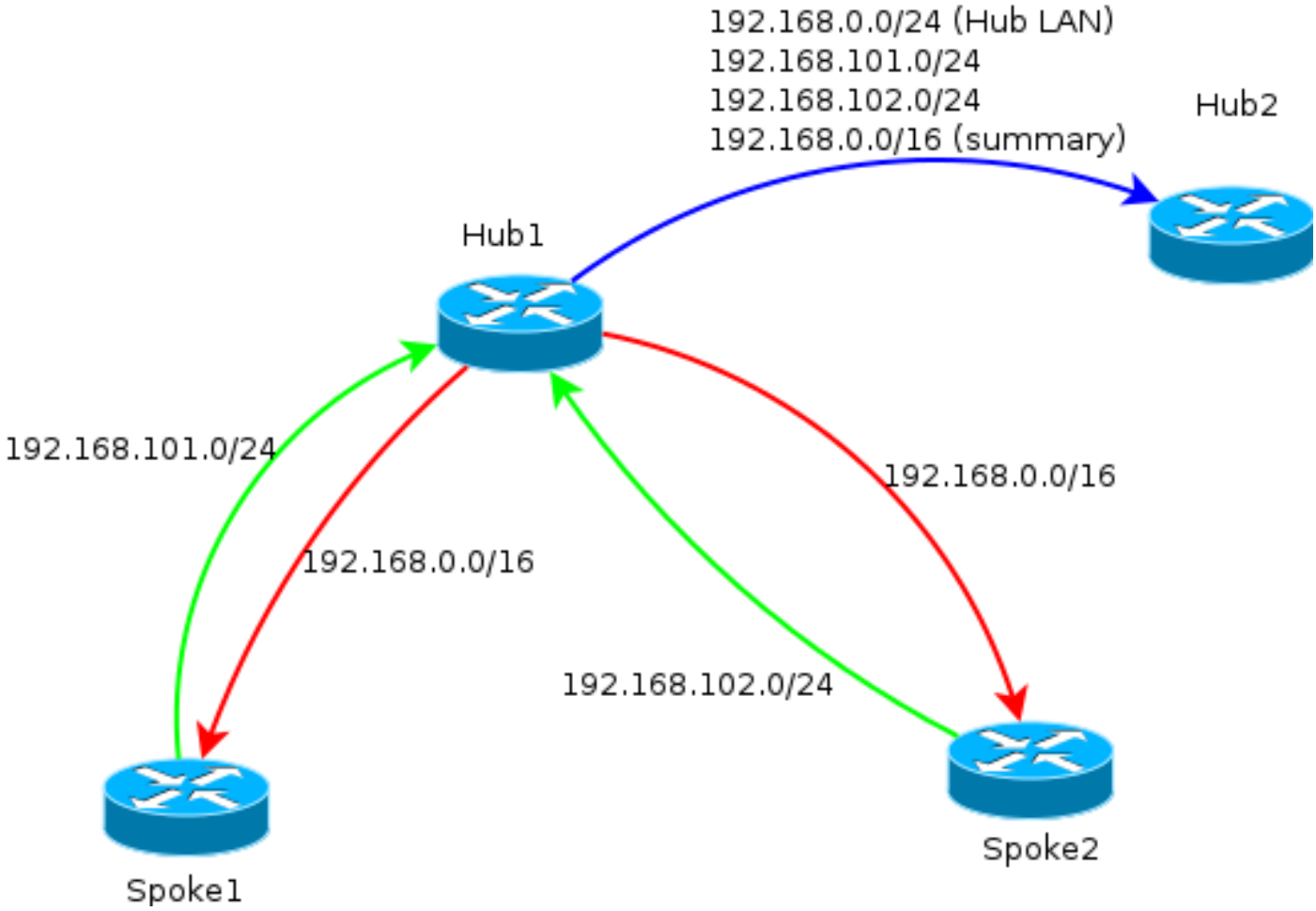
```
match ip address 1

ip access-list standard 1
permit any
```

В сущности это - то, что сделано:

- Локальный пул адресов FlexVPN находится в диапазоне BGP listen.
- Локальная сеть является 192.168.0.0/24.
- Сводка объявлена только к лучам. Конфигурация агрегаторного адреса создает статический маршрут для того префикса через интерфейс null0, который является маршрутом сброса, который используется для предотвращения циклов маршрутизации.
- Все определенные префиксы объявлены к другому концентратору. Так как это - также соединение iBGP, это требует конфигурации рефлектора маршрута.

Эта схема представляет обмен префиксами BGP между лучами и концентраторами в одном облаке FlexVPN.



Примечание: В 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.

Проверка

Так как каждый луч сохраняет ассоциацию с обоими концентраторами, два сеанса IKEv2

замечены с командой show crypto ikev2 sa.

```
IPv4 Crypto IKEv2 SATunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Для просмотра информации о протоколе маршрутизации введите эти команды:

```
show bgp ipv4 unicast

show bgp summary
```

На лучах необходимо видеть, что итоговый префикс получен от концентраторов, и что соединения с обоими концентраторами активны.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found Network Next Hop Metric LocPrf Weight Path
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer
InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Устранение неполадок

Существует два главных блока для устранения проблем:

- Протокол IKE
- Протокол IPSEC (Internet Protocol Security) (IPsec)

Вот соответствующие команды показа:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Вот соответствующие команды отладки:

```
debug crypto ikev2 [internal|packet]
```

debug crypto ipsec

debug vtemplate event

Вот соответствующий протокол маршрутизации:

show bgp ipv4 unicast (or show ip bgp)

show bgp summary