DMVPN к FlexVPN мягкий пример конфигурации миграции

Содержание

Введение

Этот документ описывает, как выполнить *мягкую* миграцию, где и Динамическая многоточечная VPN (DMVPN) и FlexVPN работают на устройство одновременно без потребности в обходном пути, и предоставляет пример конфигурации.

> **Примечание:** Этот документ подробно останавливается на понятиях, описанных в Миграции FlexVPN: Твердое Перемещение от DMVPN до FlexVPN на Тех же Устройствах и Миграции FlexVPN: Твердое Перемещение от DMVPN до FlexVPN на Different Hub Cisco статьи. Оба из этих документов описывают *трудные* миграции, которые вызывают некоторое разрушение к трафику во время миграции. Ограничения

в этих статьях происходят из-за дефицита в программном обеспечении Cisco IOS, которое теперь исправлено.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- DMVPN
- FlexVPN

Используемые компоненты

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

- Версии маршрутизатора с интеграцией служб (ISR) Cisco 15.3 (3) M или позже
- Серия Cisco 1000 объединенный маршрутизатор услуг (ASR1K) освобождает 3.10 или позже

Примечание: Не вся вторая версия протокола Internet Key Exchange (IKEv2) поддержек программных и аппаратных средств. См. Cisco Feature Navigator для получения информации.

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

Одно из преимуществ более новой платформы Cisco IOS и программного обеспечения является способностью использовать Криптографию Следующего поколения. Примером является использование Расширенного стандарта шифрования (AES) в Режиме Галуа/Счетчика (GCM) для шифрования в IPsec, как обсуждено в RFC 4106. AES GCM позволяет намного более быстрые скорости шифрования на некоторых аппаратных средствах.

Примечание: Для дополнительных сведений об использовании и миграции к Криптографии Следующего поколения, обратитесь к статье Next Generation Encryption Cisco.

Настройка

Этот пример конфигурации фокусируется на миграции от конфигурации Фазы 3 DMVPN до FlexVPN, потому что оба дизайна работают так же.

	Фаза 2 DMVPN	Фаза 3 DMVPN	FlexVPN
Транспорт	GRE по IPsec	GRE по IPsec	GRE по IPsec,
Использование NHRP	Регистрация и разрешение	Регистрация и разрешение	Разрешение
Следующий переход от луча	Другие спицы или концентратор	Сводка от концентратора	Сводка от концентратора
Коммутация ярлыка NHRP	Нет	Да	Да (Необязатель
Перенаправление NHRP	Нет	Да	Да
IKE и IPsec	Дополнительный IPsec, типичный IKEv1	Дополнительный IPsec, типичный IKEv1	IPsec, IKEv2

Сетевые графики

Этот раздел предоставляет и схемы транспортной и оверлейной сети.

Схема транспортной сети

Транспортная сеть, используемая в данном примере, включает один концентратор с двумя связанными лучами. Все устройства связаны через сеть, которая моделирует Интернет.

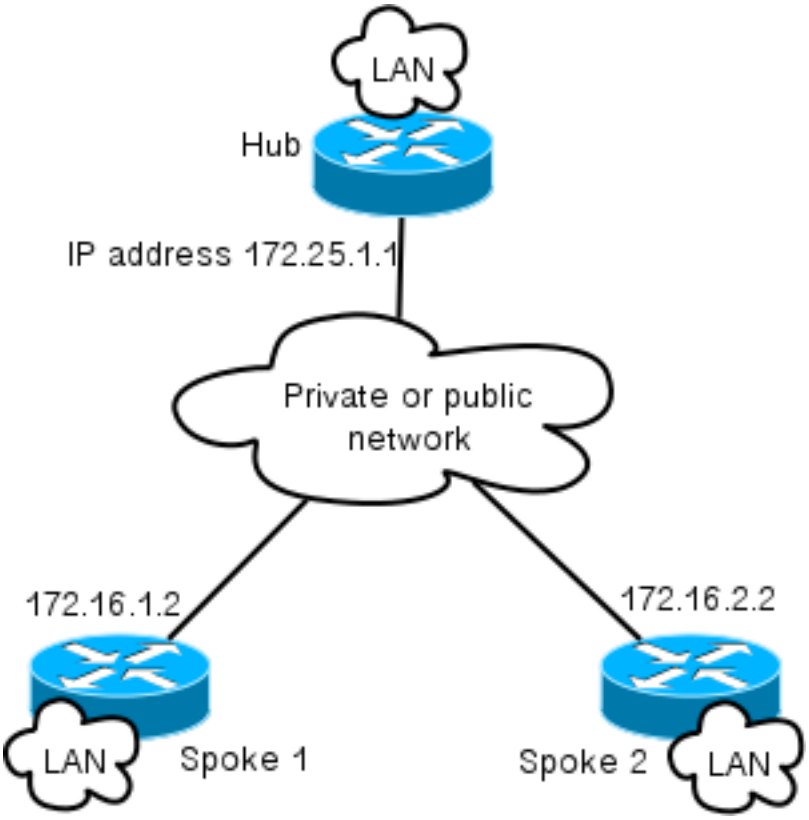
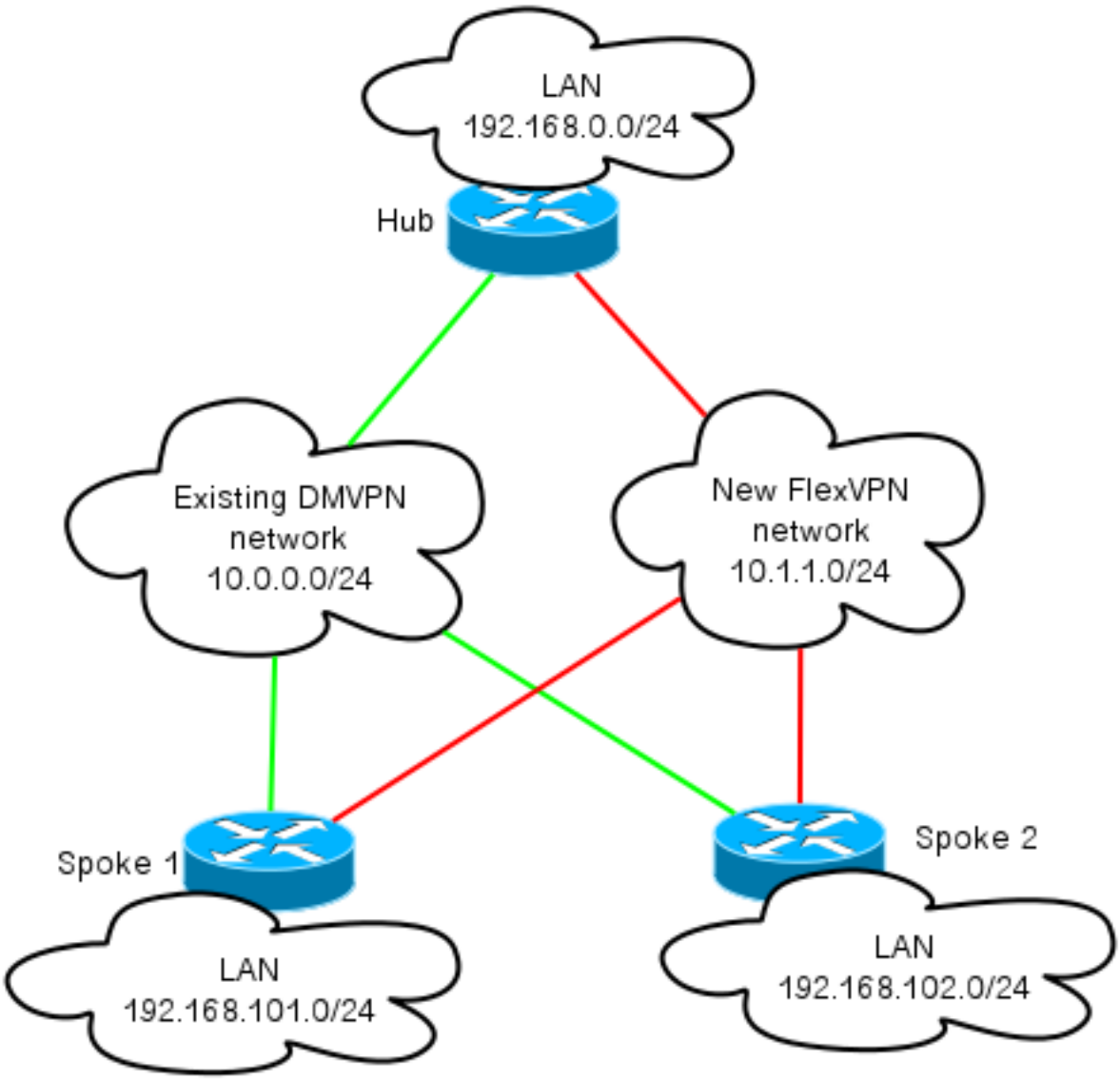


Схема оверлейной сети

Оверлейная сеть, используемая в данном примере, включает один концентратор с двумя

связанными лучами. Помните, что и DMVPN и FlexVPN активны одновременно, но они используют пробелы другого IP-адреса.



Конфигурации

Эта конфигурация перемещает самые популярные развертывания Фазы 3 DMVPN через Протокол EIGRP к FlexVPN с Протоколом BGP. Cisco рекомендует использование BGP с FlexVPN, потому что это позволяет развертываниям масштабироваться лучше.

> **Примечание:** Концентратор завершает IKEv1 (DMVPN) и IKEv2 (FlexVPN) сеансы на том же IP-адресе. Это возможно только с недавними Cisco IOS Release.

Конфигурация оконечного устройства

Это - очень простая конфигурация с двумя исключениями, которые позволяют взаимодействие и IKEv1 и IKEv2, а также двух платформ, которые используют Универсальную инкапсуляцию маршрутизации (GRE) по IPsec для транспорта для сосуществования.

Примечание: Соответствующие изменения к Протоколу ISAKMP и конфигурации IKEv2 выделены полужирным.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

crypto logging session

crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2 interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1interface Tunnel1
description FlexVPN spoke-to-hub tunnel
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 protection ipsec profile default ikev2-profile Flex_IKEv2
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS Release 15.3 позволяет вам связывать и IKEv2 и профили ISAKMP вместе в конфигурации *tunnel protection*. Наряду с некоторыми внутренними изменениями к коду, это позволяет IKEv1 и IKEv2 воздействовать на то же устройство одновременно.

Из-за пути Cisco IOS выбирает профили (IKEv1 или IKEv2) в версиях ранее, чем 15.3, это привело к некоторым предупреждениям, таким как ситуации, где IKEv1 инициируется к IKEv2 через узел. Разделение IKE теперь на основе уровня профиля, не интерфейсного, который достигнут через новый CLI.

Другое обновление в новом ПО Cisco IOS выпуске является добавлением *ключа туннеля*. Это необходимо, потому что и DMVPN и FlexVPN используют тот же исходный интерфейс и тот же IP - адрес назначения. С этим на месте, нет никакого пути к Туннелю GRE для знания, какой туннельный интерфейс используется для декапсуляции трафика. Ключ туннеля позволяет вам дифференцировать **tunnel0** и **tunnel1** с добавлением маленьких (4-байтовых) издержек. Другой ключ может быть настроен на обоих интерфейсах, но, как правило, только необходимо дифференцировать один туннель.

> **Примечание:** Когда DMVPN и FlexVPN совместно используют тот же интерфейс, совместно используемая опция tunnel protection не требуется.

Таким образом лучевая конфигурация протокола маршрутизации является основной. EIGRP и BGP работают отдельно. EIGRP дает объявление только по туннельному интерфейсу во избежание смотрения на туннели конечного маршрутизатор - конечного маршрутизатора, который ограничивает масштабируемость. BGP поддерживает отношения только с маршрутизатором концентратора **(10.1.1.1)** для объявления локальной сети **(192.168.101.0/24)**.

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Конфигурация концентратора

Необходимо внести подобные изменения на конфигурации стороны концентратора как описанные в разделе **Конфигурации оконечного устройства**.

Примечание: Соответствующие изменения к ISAKMP и конфигурации IKEV2 выделены полужирным.

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

На стороне концентратора, привязке между профилем IKE и Профилем IPSEC происходит на уровне профиля, в отличие от конфигурации оконечного устройства, где это завершено через **команду tunnel protection**. Оба подхода являются жизнеспособными методами для завершения этой привязки.

Следует отметить, что обнаружение несанкционированного доступа к сети Протокола NHRP является другим для DMVPN и FlexVPN в облаке. В большинстве случаев, когда NHRP создает одиночный домен по обеим платформам, это - нежелательный.

Ключ туннеля дифференцирует DMVPN и туннели FlexVPN на уровне GRE для достижения той же цели, которая упомянута в разделе **Конфигурации оконечного устройства**.

Настройка маршрутизации на концентраторе является довольно основной. Устройство концентратора поддерживает два отношений с любым данным лучом, тот, который использует EIGRP и тот, который использует BGP. BGP - конфигурация использует слушать-диапазон во избежание длинного на конфигурацию оконечного устройства.

Сводные адреса представлены дважды. Конфигурация протокола EIGRP передает сводку с использованием конфигурации **tunnel0** (IP summary-address EIGRP 100), и BGP начинает сводку с использования агрегаторного адреса. Сводки требуются, чтобы гарантировать, что перенаправление NHRP происходит, и для упрощения обновлений маршрута. Можно передать перенаправление NHRP (во многом как перенаправление Протокола ICMP),

который указывает, существует ли лучший переход для заданного получателя, который позволяет туннелю конечного маршрутизатор - конечного маршрутизатора быть установленным. Эти сводки также используются для уменьшения суммы обновлений маршрута, которые передаются между концентратором и каждым лучом, который позволяет настройкам масштабироваться лучше.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

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
```

Проверка

Проверка для этого примера конфигурации разделена на несколько разделов.

Проверки перед миграцией

И начиная с DMVPN/EIGRP и начиная с FlexVPN/BGP работают одновременно, необходимо проверить, что луч поддерживает отношения по IPsec и с IKEv1 и с IKEv2, и что соответствующие префиксы изучены по EIGRP и BGP.

В данном примере Spoke1 показывает, что два сеанса поддержаны с маршрутизатором концентратора; каждый использует IKEv1/Tunnel0, и каждый использует IKEv2/Tunnel1.

> **Примечание:** Два Сопоставления безопасности IPSec (SA) (одно входящее и одно исходящее) поддержаны для каждого из туннелей.

```
Spoke1#show cry sess
Crypto session current statusInterface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto mapInterface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

При проверке протоколов маршрутизации необходимо проверить, что соседство

сформировано, и что изучены корректные префиксы. Это сначала проверено с EIGRP. Проверьте, что концентратор видим как соседний узел, и что 192.168.0.0/16 обращаются (сводка) изучен из концентратора:

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia StatusP 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

Затем, проверьте BGP:

```
Spoke1#show bgp summary
(...)Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, 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 foundNetwork Next Hop Metric LocPrf Weight Path
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

Выходные данные показывают, что концентратор, IP-адрес FlexVPN (10.1.1.1) является соседним узлом, через который луч получает один префикс (192.168.0.0/16). Кроме того, BGP сообщает администратору, что сбой Routing Information Base (RIB) произошел для префикса 192.168.0.0/16. Этот сбой происходит, потому что существует лучший маршрут для того префикса, который уже существует в таблице маршрутизации. Этот маршрут инициируется EIGRP и может быть подтвержден при проверке таблицы маршрутизации.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

Миграция

Предыдущий раздел проверил, что и IPsec и протоколы маршрутизации настроены и работают как ожидалось. Один из самых легких способов мигрировать от DMVPN до FlexVPN на том же устройстве состоит в том, чтобы изменить Административное расстояние (AD). В данном примере Внутренний BGP (iBGP) имеет AD 200, и EIGRP имеет AD 90.

Для трафика для течения через FlexVPN должным образом BGP должен иметь лучший AD. В данном примере AD EIGRP изменен на **230** и **240** для внутренних и внешних маршрутизаций, соответственно. Это делает AD BGP (**200**) более предпочтительным для префикса **192.168.0.0/16**.

Другой метод, который используется для достигания этого должен уменьшить AD BGP. Однако протокол, который бежит за миграцией, имеет нестандартные значения, которые могут повлиять на другие части развертываний.

В данном примере команда **debug ip routing** используется для проверки операции на луче.

> **Примечание:** Если информация в этом разделе используется на рабочей сети, избегите использования команд отладки и полагайтесь на команды показа, перечисленные в следующем разделе. Кроме того, лучевой процесс EIGRP должен восстановить смежность с концентратором.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1
```

Существует три важных действия для замечания в этих выходных данных:

- Луч замечает, что AD, измененный, и, отключает смежность.
- В таблице маршрутизации повторно связан префикс EIGRP, и BGP представлен.
- Смежность с концентратором по EIGRP возвращается онлайн.

При изменении AD на устройстве он только влияет на путь от устройства до других сетей; это не влияет, как другие маршрутизаторы выполняют маршрутизацию. Например, после того, как расстояние EIGRP увеличено на **Spoke1** (и это использует FlexVPN на облаке для маршрутизации трафика), концентратор поддерживает настроенные AD (по умолчанию).

Это означает, что использует DMVPN для маршрутизации трафика назад к **Spoke1**.

В определенных сценариях это может вызвать проблемы, такой как тогда, когда межсетевые экраны ожидают ответный трафик на том же интерфейсе. Поэтому необходимо изменить AD на всех лучах перед изменением его на концентраторе. Трафик полностью перемещен FlexVPN только, как только это завершено.

Миграция ОТ EIGRP К EIGRP

Миграция от DMVPN до FlexVPN, который выполняет только EIGRP, не обсуждена всесторонняя в этом документе; однако, это упомянуто здесь для полноты.

Возможно добавить и DMVPN и EIGRP к той же Анонимной системе EIGRP (AS) экземпляр маршрутизации. С этим на месте, смежность маршрутизации установлена по обоим типам облаков. Это может заставить распределение нагрузки происходить, который, как правило, не рекомендуется.

Чтобы гарантировать, что или FlexVPN или DMVPN выбраны, администратор может назначить другие **Значения задержки** на поинтерфейсной основе. Однако важно помнить, что никакие изменения не возможны на виртуальных интерфейсах, в то время как присутствуют соответствующие интерфейсы виртуального доступа.

Проверки постмиграции

Подобный процессу, используемому в разделе **Проверок Перед миграцией**, IPsec и протокол маршрутизации должны быть проверены.

Во-первых, проверьте IPsec:

```
Spoke1#show crypto session
Crypto session current statusInterface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto mapInterface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Как прежде, два сеанса замечены, оба из которых имеют два SA активного IPSec.

На луче объединенный маршрут **(192.168.0.0/16)** указывает от концентратора и изучен по BGP.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
```

```
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

Точно так же лучевая LAN, которая снабжена префиксом на концентраторе, должна быть известна через EIGRP. В данном примере проверена подсеть LAN **Spoke2**:

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

В выходных данных путь переадресации обновлен должным образом и указывает из интерфейса виртуального доступа.

Дополнительные замечания

В этом разделе описываются некоторые важные дополнительные области, которые относятся к этому примеру конфигурации.

Существующие туннели конечного маршрутизатор - конечного маршрутизатора

С миграцией от EIGRP до BGP не влияют на туннели конечного маршрутизатор - конечного маршрутизатора, потому что коммутация ярлыка находится все еще в операции. Коммутация ярлыка на луче вставляет более определенный маршрут NHRP с AD 250.

Вот пример такого маршрута:

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

Связь между перемещенными и неперемещенными спицами

Если луч, который уже находится на FlexVPN/BGP, хочет связаться с устройством, для которого не начался процесс переноса, трафик всегда течет по концентратору.

Это - процесс, который происходит:

1. Луч выполняет поиск маршрута для назначения, которое указывает через объединенный маршрут, который объявлен концентратором.
2. Пакет передан к концентратору.
3. Концентратор получает пакет и выполняет поиск маршрута для назначения, которое указывает из другого интерфейса, который является частью другого домена NHRP.

   Примечание: ID сети NHRP в предыдущей конфигурации концентратора является другим и для FlexVPN и для DMVPN.

Даже если ID сети NHRP объединены, проблема могла бы произойти, где перемещенный луч направляет объекты по сети FlexVPN. Это включает директиву, используемую для настройки коммутации ярлыка. Неперемещенный луч пытается выполнить объекты по сети DMVPN с определенной целью выполнить коммутацию ярлыка.

Устранение неполадок

В этом разделе описываются эти две категории, как правило, используемые чтобы к toubleshoot миграция.

Проблемы с попытками установить туннели

Выполните эти шаги, если отказывает Ike согласование:

1. Проверьте текущее состояние с этими командами:

   show crypto isakmp sa- Эта команда показывает сумму, источник и назначение сеанса IKEv1.**show crypto ipsec sa-** Эта команда показывает действие контекстов безопасности IPSec.**Примечание:** В отличие от этого, в IKEv1, в этих выходных данных Групповое значение Diffie-Hellman (DH) безопасной пересылки (Perfect Forward Secrecy, PFS) появляется как **безопасная пересылка (PFS) (Y/N): N, группа DH: ни один** во время первого согласования туннеля; однако, после того, как повторно введение происходит, правильные значения появляются. Это не дефект, даже при том, что поведение описано в CSCug67056. Различие между IKEv1 и IKEv2 - то, что в последнем, Дочерние SA созданы как часть обмена **AUTH**. DH Group, которая настроена под криптокартой, используется только во время повторно введения. Поэтому вы видите **безопасную пересылку (PFS) (Y/N): N, группа DH: ни один** до первого не повторно вводит. С IKEv1 вы видите другое поведение, потому что создание Child SA происходит во время Быстрого режима, и сообщение **CREATE_CHILD_SA** имеет условия для переноса информационного наполнения Обмена ключами, которое задает параметры DH для получения нового общего секретного ключа.**show crypto ikev2 sa** - Эта команда предоставляет выходные данные, подобные ISAKMP, но является определенной для IKEv2.**show crypto session** - Эта команда предоставляет сводные выходные данные криптографических сеансов на этом устройстве.**show crypto socket** - Эта команда показывает статус крипто-сокетов.**show crypto map** - Эта команда показывает сопоставление IKE и Профилей IPSEC к интерфейсам.**show ip nhrp** - Эта команда предоставляет NHRP informtion от устройства. Это полезно для конечного маршрутизатор - конечного маршрутизатора в настройках FlexVPN, и и для конечного маршрутизатор - конечного маршрутизатора и для связываний оконечного устройства - концентратора в настройках DMVPN.
2. Используйте эти команды для отладки установки туннеля:

debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

Проблемы с распространением маршрутов

Вот некоторые полезные команды, которые можно использовать для устранения проблем EIGRP и топологии:

- **show bgp summary** - Используйте эту команду для проверки подключенных соседей и их состояний.
- **show ip eigrp neighbor** - Используйте эту команду, чтобы показать соседним узлам, которые связаны через EIGRP.
- **show bgp** - Используйте эту команду для проверки префиксов, изученных по BGP.
- **show ip eigrp topology-** Используйте эту команду для показа префиксов, изученных через EIGRP.

Важно знать, что изученный префикс является другим, чем префикс, который установлен в таблице маршрутизации. Для получения дополнительной информации об этом, сошлитесь на статью Route Selection in Cisco Routers Cisco или Книгу Cisco Press TCP/IP Маршрутизации.

Известные предупреждения

Ограничение, которое параллельно обработке Туннеля GRE, существует на ASR1K. Это отслежено под идентификатором ошибки Cisco CSCue00443. В это время ограничение имеет запланированное исправление в Выпуске 3.12 программного обеспечения Cisco IOS XE.

Контролируйте этот дефект, если вы желаете уведомления, как только исправление становится доступным.