DMVPN到FlexVPN軟遷移配置示例

目錄

簡介

本文說明如何執行*軟遷移*，其中動態多點VPN(DMVPN)和FlexVPN可在裝置上同時工作，而無需權衡，並提供配置示例。

> **附註**：本文檔詳細介紹FlexVPN遷移：在同一裝置上從DMVPN硬遷移到FlexVPN並進行FlexVPN遷移：「Hard Move from DMVPN to FlexVPN on a Different Hub Cisco(在不同的中心思科上從DMVPN硬移到FlexVPN)」文章。這兩個文檔都描述了*硬*遷移，這些遷移在遷移期間會對流量造成一些中斷。這些文章中的侷限性是由於Cisco IOS®軟體中的缺陷引起的，現在已更正了該缺陷。

必要條件

需求

思科建議您瞭解以下主題：

- DMVPN
- FlexVPN

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合式服務路由器(ISR)版本15.3(3)M或更高版本
- Cisco 1000系列聚合服務路由器(ASR1K)版本3.10或更高版本

> **附註**：並非所有軟體和硬體都支援Internet金鑰交換版本2(IKEv2)。 請參閱思科功能導航器以瞭解資訊。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

較新的Cisco IOS平台和軟體的一個優勢就是能夠使用下一代加密技術。例如，在Galois/Counter Mode(GCM)中使用進階加密標準(AES)進行IPsec加密，如RFC 4106所述。AES GCM在某些硬體上允許更快的加密速度。

> **附註**：有關使用下一代加密並將其遷移至下一代加密的其他資訊，請參閱下一代加密思科文章。

設定

此配置示例重點介紹從DMVPN第3階段配置遷移到FlexVPN的過程，因為這兩種設計的工作方式相似。

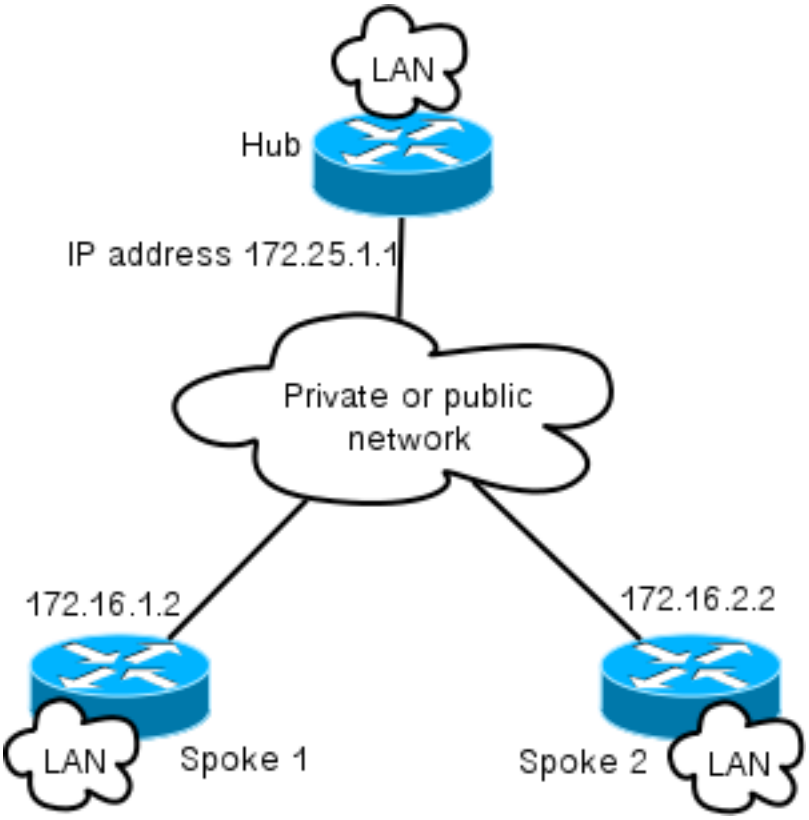
	DMVPN第2階段	DMVPN第3階段	FlexVPN
傳輸	使用IPsec的GRE	使用IPsec的GRE	使用IPsec的GRE、VTI
NHRP使用情況	註冊和解析	註冊和解析	解析
分支中的下一跳	其他輻條或集線器	中心摘要	中心摘要
NHRP快捷方式交換	否	是	是（可選）
NHRP重新導向	否	是	是
IKE和IPsec	IPsec可選，IKEv1典型	IPsec可選，IKEv1典型	IPsec、IKEv2

網路圖

本節提供傳輸和重疊網路圖。

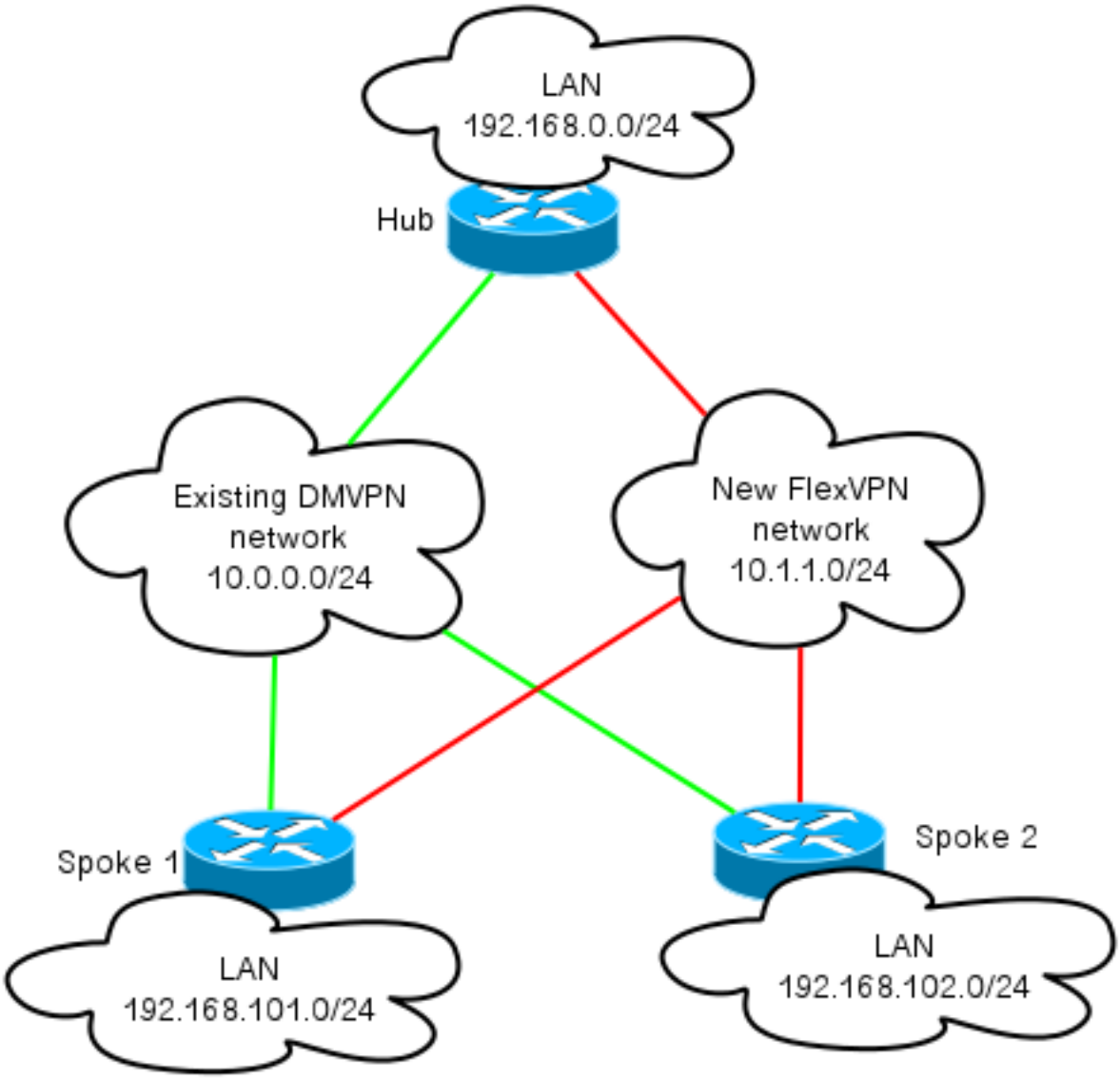
傳輸網路圖表

本示例中使用的傳輸網路包括連線的兩個輻條的單個集線器。所有裝置都通過模擬網際網路的網路連線。



重疊網路圖

本示例中使用的重疊網路包含連線了兩個分支的單個中心。請記住，DMVPN和FlexVPN同時處於活動狀態，但它們使用不同的IP地址空間。



組態

此組態會透過增強型內部閘道路由通訊協定(EIGRP)將最常見的DMVPN第3階段部署遷移到使用邊界閘道通訊協定(BGP)的FlexVPN。思科建議使用BGP和FlexVPN，因為這樣可讓部署更具擴展性。

> **附註**：集線器會終止同一IP位址上的IKEv1(DMVPN)和IKEv2(FlexVPN)作業階段。這只有在最近的Cisco IOS版本中才能實現。

分支配置

這是一個非常基本的配置，但有兩個明顯的例外情況，它們允許IKEv1和IKEv2進行互操作，以及兩個使用基於IPsec的通用路由封裝(GRE)進行傳輸以便共存的框架。

> **附註**：對Internet安全關聯和金鑰管理協定(ISAKMP)和IKEv2配置的相關更改以粗體突出顯示。

```
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_IKEv1

interface 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版本15.3允許您將IKEv2和ISAKMP配置檔案繫結到*隧道保護*配置中。除了對代碼進行一些內部更改外，這允許IKEv1和IKEv2在同一裝置上同時運行。

由於Cisco IOS在低於15.3的版本中選擇配置檔案（IKEv1或IKEv2）的方式，因此出現了一些警告，例如通過對等體向IKEv2啟動IKEv1。現在，IKE的分離基於配置檔案級別，而不是介面級別，後者通過新的CLI實現。

新Cisco IOS版本中的另一個升級是新增了*通道金鑰*。這是必需的，因為DMVPN和FlexVPN使用相同的源介面和相同的目標IP地址。如此一來，GRE通道便無法知道使用哪個通道介面來解除封裝流量。使用隧道金鑰可以區分**tunnel0**和**tunnel1**，但會增加少量（4位元組）開銷。可以在兩個介面上配置不同的金鑰，但通常只需要區分一個隧道。

附註：當DMVPN和FlexVPN共用同一介面時，不需要共用隧道保護選項。

因此，分支路由協定配置是基本的。EIGRP和BGP單獨工作。EIGRP僅通過隧道介面進行通告，以避免在分支到分支的隧道上進行對等，這限制了可擴充性。BGP僅維護與中心路由器(**10.1.1.1**)的關係，以便通告本地網路(**192.168.101.0/24**)。

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

集線器配置

您必須在中心端配置上進行與**分支配置**一節中所述類似的更改。

附註：對ISAKMP和IKEV2配置的相關更改以粗體突出顯示。

```
crypto ikev2 authorization policy default
```

```
pool FlexSpokes
route set interface

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 key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface 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_IKEv1

interface 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
```

在中心端，IKE配置檔案和IPsec配置檔案之間的繫結發生在配置檔案級別，與分支配置不同，分支配置是通過**tunnel protection**命令完成的。這兩種方法都是完成此繫結的可行方法。

必須注意的是，雲中DMVPN和FlexVPN的下一跳解析協定(NHRP)網路ID不同。在大多數情況下，當NHRP在兩個框架上建立單個域時，是不理想的。

通道金鑰區分了GRE級別的DMVPN和FlexVPN通道，以實現分支配置部分中提到的**相同目標。**

集線器上的路由配置非常基本。中心裝置與任何給定分支保持兩種關係，一個使用EIGRP，另一個使用BGP。BGP配置使用listen-range以避免每個分支的冗長配置。

總結地址介紹兩次。EIGRP配置使用**tunnel0配置(IP summary-address EIGRP 100)傳送一個摘**要，BGP使用聚合地址引入一個摘要。需要這些摘要以確保發生NHRP重定向，並簡化路由更新。您可以傳送NHRP重定向(非常類似於Internet控制消息協定(ICMP)重定向)，指示給定目標是否存在更佳的躍點，從而允許建立分支到分支隧道。這些摘要還用於最小化在中心之間傳送的路由更新量每個輻條，使設定可以更好地擴展。

```
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
```

驗證

此配置示例的驗證分為幾個部分。

遷移前檢查

由於DMVPN/EIGRP和FlexVPN/BGP同時運行，因此必須驗證分支是否通過IPsec與IKEv1和IKEv2保持關係，以及是否通過EIGRP和BGP獲取適當的字首。

在本例中，**Spoke1**顯示與中心路由器維護了兩個作業階段；一個使用IKEv1/**Tunnel**0，另一個使用IKEv2/**Tunnel1**。

> **附註**：為每個通道維護兩個IPsec安全關聯(SA)（一個入站和一個出站）。

```
Spoke1#show cry sess
Crypto session current status

Interface: 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 map

Interface: 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
```

在檢查路由協定時，必須驗證是否已形成鄰居關係，以及是否學習了正確的字首。首先使用EIGRP進行檢查。確認集線器作為鄰居可見，且從集線器得知192.168.0.0/16位址（摘要）：

```
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 Status

P 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
```

接下來，驗證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 found

Network 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
```

輸出顯示，集線器FlexVPN IP位址(10.1.1.1)是鄰居，輻條通過該鄰居接收一個字首(192.168.0.0/16)。 此外，BGP會通知管理員，192.168.0.0/16首碼發生路由資訊庫(RIB)故障。之所以會出現此故障，是因為路由表中已經存在該字首的更好路由。此路由由EIGRP產生，檢查路由表後可確認該路由。

```
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
```

移轉

上一節驗證了IPsec和路由協定均配置好，並且工作正常。在同一裝置上從DMVPN遷移到FlexVPN的最簡單方法之一是更改管理距離(AD)。在本示例中，內部BGP(iBGP)的AD為**200**，而EIGRP的AD為**90**。

為了讓流量正確通過FlexVPN，BGP必須具有更好的AD。在本例中，EIGRP AD對於內部路由和外部路由分別更改為**230**和**240**。這使得**200**的BGP AD對於**192.168.0.0/16**字首更可取。

實現這一點的另一種方法是降低BGP AD。但是，遷移後運行的協定具有非預設值，這可能會影響部署的其他部分。

在本示例中，使用**debug ip routing**命令驗證分支上的操作。

> **附註**：如果本部分中的資訊用於生產網路，請避免使用debug命令，並依靠下一部分中列出的show命令。此外，分支EIGRP進程必須與中心重新建立鄰接關係。

```
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 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

在此輸出中，需要注意三個重要操作：

- 分支注意到AD已更改，並禁用鄰接關係。
- 在路由表中，EIGRP字首被重新命名，並引入BGP。
- 通過EIGRP與集線器的鄰接關係恢復為聯機。

更改裝置上的AD時，只會影響從裝置到其它網路的路徑；不影響其它路由器的路由方式。例如，在**Spoke1**上增加EIGRP距離後（它在雲上使用FlexVPN來路由流量），集線器會維護已配置的（預設）AD。這表示它使用DMVPN將流量路由回**Spoke1**。

在某些情況下，這可能會導致問題，例如防火牆預期在同一介面上返回流量。因此，您應在集線器上更改所有分支上的AD。FlexVPN只有在完成此過程後才會完全遷移流量。

EIGRP到EIGRP遷移

本文檔不深入討論從DMVPN遷移至僅運行EIGRP的FlexVPN;但是，此處提及它只是為了完整。

可以將DMVPN和EIGRP新增到同一個EIGRP自治系統(AS)路由例項。這樣，就可以在兩種型別的雲上建立路由鄰接關係。這可能會導致負載均衡，通常不建議這樣做。

為了確保選擇FlexVPN或DMVPN，管理員可以基於每個介面分配不同的**Delay**值。但是，必須記住，當存在相應的虛擬訪問介面時，虛擬模板介面上不能發生更改。

遷移後檢查

與**遷移前檢查**部分中使用的過程相似，必須驗證IPsec和路由協定。

首先，驗證IPsec:

```
Spoke1#show crypto session
Crypto session current status

Interface: 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 map

Interface: 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
```

如前所述，可看到兩個作業階段，兩個作業階段都有兩個作用中IPsec SA。

在輻條上，聚合路由(**192.168.0.0/16**)從集線器指向，並通過BGP獲知。

```
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
```

同樣，中心上帶有字首的分支LAN必須通過EIGRP知道。在此示例中，選中**Spoke2** LAN子網：

```
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
```

在輸出中，轉發路徑會正確更新，並指向虛擬訪問介面。

其他考量事項

本節介紹與此組態範例相關的一些其他重要領域。

現有的輻射到輻射隧道

從EIGRP遷移到BGP時，分支到分支隧道不會受到影響，因為快捷方式交換仍在運行。分支上的快捷方式交換會插入更特定的NHRP路由，其AD為250。

以下是此類路由的範例：

```
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
```

已遷移和非遷移分支之間的通訊

如果FlexVPN/BGP上的分支希望與遷移過程尚未開始的裝置通訊，則流量始終會通過集線器傳輸。

發生以下過程：

1. 分支執行目標的路由查詢，目標指向中心通告的總結路由。
2. 將封包傳送到集線器。
3. 集線器接收資料包並執行目的地路由查詢，目的地從屬於不同NHRP域的另一個介面引出。

附註：對於FlexVPN和DMVPN，先前集線器配置中的NHRP網路ID不同。即使NHRP網路ID是統一的，遷移的分支也可能通過FlexVPN網路路由對象。其中包括用於配置快捷方式交換的指令。非遷移分支嘗試通過DMVPN網路運行對象，其特定目標是執行快捷方式交換。

疑難排解

本節介紹通常用於升級遷移的兩個類別。

嘗試建立通道時出現問題

如果IKE協商失敗，請完成以下步驟：

1. 使用以下命令驗證當前狀態：

   show crypto isakmp sa — 此命令顯示IKEv1會話的數量、源和目標。**show crypto ipsec sa** — 此命令顯示IPsec SA的活動。**附註**：與IKEv1不同，在此輸出中，完全向前保密(PFS)Diffie-hellman(DH)組的值顯示為**PFS(Y/N):否，DH組：無**在第一次通道交涉期間；但是，重新生成金鑰後，將顯示正確的值。這不是錯誤，即使CSCug67056中描述了該行為。IKEv1和IKEv2之間的區別在於，在後者中，子SA是作為**AUTH Exchange的一部分建立的。**在加密對映下配置的DH組僅在重新生成金鑰期間使用。因此，您會看**到PFS(Y/N):否，DH組：直到第一個重新生成金鑰為止。**使用IKEv1時，您會看到不同的行為，因為子SA建立發生在快速模式期間，而**CREATE_CHILD_SA**消息具有用於傳輸金鑰交換有效載荷的設定，該有效載荷指定DH引數以匯出新的共用金鑰。**show crypto ikev2 sa** — 此命令提供與ISAKMP類似的輸出，但特定於IKEv2。**show crypto session** — 此命令提供此裝置上加密會話的摘要輸出。**show crypto socket** — 此命令顯示加密套接字的狀態。**show crypto map** — 此命令顯示IKE和IPsec配置檔案到介面的對映。**show ip nhrp** — 此命令提供來自裝置的NHRP資訊。這對於FlexVPN設定中的分支到分支以及DMVPN設定中的分支到分支和分支到中心繫結都非常有用。
2. 使用以下命令對通道建立進行偵錯：

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

路由傳播問題

以下是可用於排除EIGRP和拓撲故障的一些有用命令：

- **show bgp summary** — 使用以下命令以驗證連線的鄰居及其狀態。
- **show ip eigrp neighbor** — 使用此命令以顯示通過EIGRP連線的鄰居。
- **show bgp** — 使用以下命令以驗證透過BGP得知的字首。
- **show ip eigrp topology** — 使用此命令以顯示通過EIGRP獲取的字首。

必須瞭解學習的字首不同於路由表中安裝的字首。有關此主題的詳細資訊，請參閱Cisco路由器中的路由選擇Cisco文章，或路由TCP/IP Cisco Press手冊。

已知警告

ASR1K上存在GRE隧道處理並行的限制。此問題在思科錯誤ID CSCue00443下跟蹤。目前，此限制在Cisco IOS XE軟體版本3.12中有一個計畫修復。

如果希望修復程式可用時收到通知，請監視此錯誤。