在同一裝置上從DMVPN硬遷移到FlexVPN

目錄

簡介

本文提供有關如何在相同裝置上從現有DMVPN網路遷移到FlexVPN的資訊。

兩個框架的配置將共存於裝置上。

本檔案只會顯示最常見的情況：DMVPN使用預共用金鑰進行身份驗證，EIGRP作為路由協定。

本文檔演示了向BGP（推薦的路由協定）和不太理想的EIGRP的遷移。

必要條件

需求

本檔案假設讀者瞭解DMVPN和FlexVPN的基本概念。

採用元件

請注意，並非所有軟體和硬體都支援IKEv2。請參閱Cisco Feature Navigator瞭解資訊。理想情況下，要使用的軟體版本為：

- ISR - 15.2(4)M1或更高版本
- ASR1k - 3.6.2版本15.2(2)S2或更高版本

較新的平台和軟體的優勢之一是有可能使用下一代加密技術，例如AES GCM在IPsec中加密。RFC 4106中將對此進行討論。

AES GCM允許在某些硬體上達到更快的加密速度。

要檢視思科關於使用和遷移到下一代加密技術的建議，請參閱：

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

移轉程式

目前，建議從DMVPN遷移到FlexVPN的方法是讓兩個框架不能同時運行。

由於ASR 3.10版本中將引入新的遷移功能，此限制將被刪除。在思科方面(包括CSCuc08066)的多個增強請求下跟蹤這些功能。這些功能將於2013年6月下旬推出。

兩個框架共存並在相同裝置上同時運行的遷移稱為軟遷移，這表示一個框架到另一個框架的影響最小，故障轉移平穩。

如果兩個框架的配置共存但不同時運行，則這種遷移稱為硬遷移。這表示從一個框架切換到另一個框架意味著即使只有極少的通訊量，也缺乏通過VPN的通訊。

相同裝置上的硬遷移

本文檔討論了從現有DMVPN網路到相同裝置上的新FlexVPN網路的遷移。

此遷移要求兩個框架不會在裝置上同時運行，這實際上要求在啟用FlexVPN之前全面禁用DMVPN功能。

在新遷移功能可用之前，使用相同裝置執行遷移的方法是：

1. 驗證通過DMVPN的連線。
2. 新增FlexVPN配置並關閉屬於新配置的隧道和虛擬模板介面。
3. （在維護視窗期間）在進入步驟4之前，關閉所有分支和集線器上的所有DMVPN隧道介面。
4. 取消關閉FlexVPN隧道介面。
5. 檢驗與中心連通性。
6. 驗證分支到分支的連線。
7. *如果點5或6中的驗證未通過關閉FlexVPN介面和取消關閉DMVPN介面正確恢復到DMVPN。*
8. *驗證與中心通訊的輻條。*
9. *驗證分支到分支的通訊。*

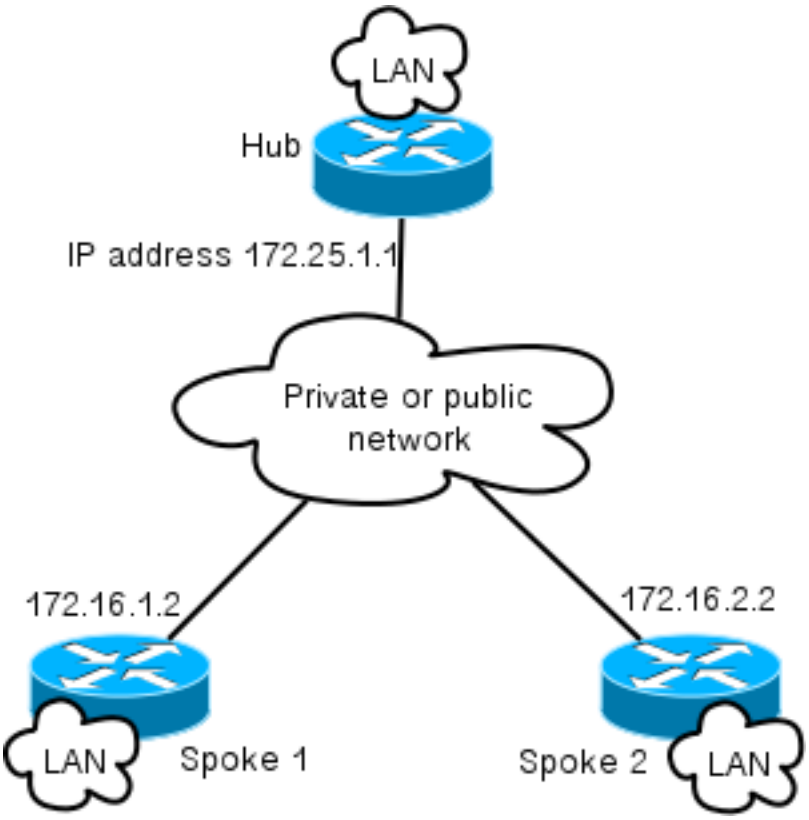
定製方法

如果由於您的網路或路由複雜性，這種方法可能不是您的最佳選擇，請在遷移之前與您的思科代表進行討論。討論自定義遷移過程的最佳人員是您的系統工程師或高級服務工程師。

網路拓撲

傳輸網路拓撲

此圖顯示Internet上主機的典型連線拓撲。在本文檔中，集線器的IP地址loopback0(172.25.1.1)用於終止IPsec會話。

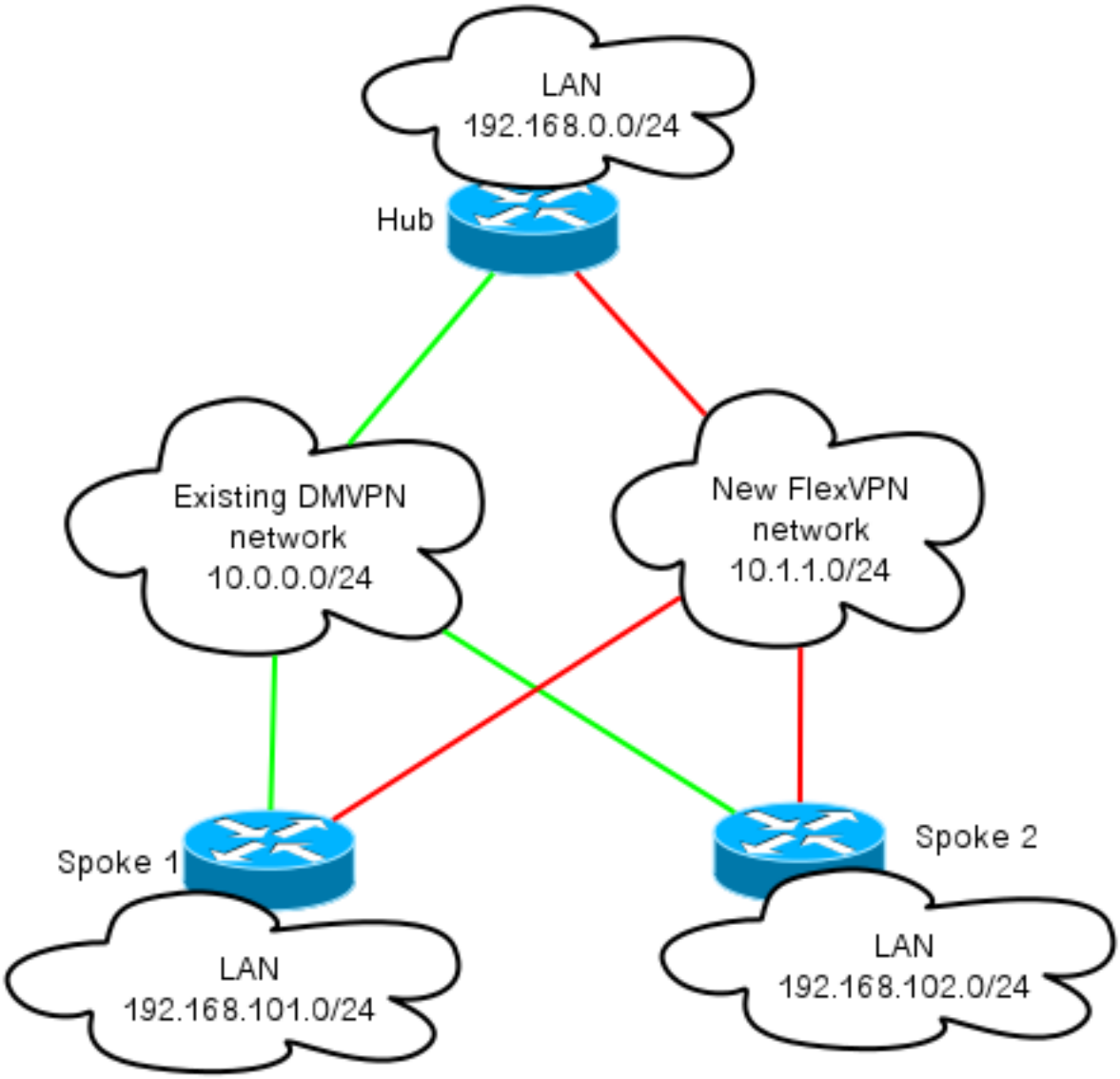


重疊網路拓撲

此拓撲圖顯示用於重疊的兩個單獨的雲：DMVPN（綠色連線）和FlexVPN連線。

為相應的端顯示區域網字首。

10.1.1.0/24子網在介面定址方面並不代表實際子網，而是代表FlexVPN雲專用的一塊IP空間。FlexVPN配置部分稍後將討論其基本原理。



組態

DMVPN配置

本節包含DMVPN中心輻射點的基本配置。

預共用金鑰(PSK)用於IKEv1身份驗證。

建立IPsec後，NHRP註冊從分支到中心，以便中心可以獲知動態分支的NBMA定址。

當NHRP在分支和中心上執行註冊時，可以建立路由鄰接關係並交換路由。在本示例中，EIGRP用作重疊網路的基本路由協定。

分支DMVPN配置

以下是使用預共用金鑰身份驗證和EIGRP作為路由協定的DMVPN基本配置示例。

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
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
interface Tunnel0
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 protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.102.0
 passive-interface default
 no passive-interface Tunnel0
```

中心DMVPN配置

在集線器配置中，隧道源自loopback0,IP地址為172.25.1.1。

其餘是將EIGRP作為路由協定的DMVPN集線器的標準部署。

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco 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
 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 protection ipsec profile DMVPN_IKEv1
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
```

FlexVPN配置

FlexVPN基於以下相同的基礎技術：

- IPsec:與DMVPN中的預設設定不同，使用IKEv2而不是IKEv1來協商IPsec SA。IKEv2提供了比IKEv1更好的功能，從恢復能力開始，到建立受保護的資料通道所需的消息數量結束。
- GRE :與DMVPN不同，使用靜態和動態點對點介面，而且不僅是在靜態多點GRE介面上。此配置可增加靈活性，尤其是針對每個分支/每個中心點的行為。
- NHRP:在FlexVPN中，NHRP主要用於建立分支到分支通訊。輻條未註冊到集線器。
- 路由：由於輻條不執行到集線器的NHRP註冊，因此需要依賴其他機制來確保集線器和輻條可以雙向通訊。與DMVPN類似，可以使用動態路由協定。但是，FlexVPN允許您使用IPsec來引入路由資訊。預設設定為隧道另一側的IP地址引入/32路由，這將允許分支到中心點的直接通訊。

從DMVPN硬遷移到FlexVPN時，兩個框架不能同時在同一裝置上工作。但是，建議將其分開。

從多個層面分離它們：

- NHRP — 使用不同的NHRP網路ID（推薦）。
- 路由 — 使用單獨的路由進程（推薦）。
- VRF - VRF分離可帶來更大的靈活性，但不會在此討論（可選）。

分支FlexVPN配置

與DMVPN相比，FlexVPN中的分支配置有一個差異，那就是您可能有兩個介面。

存在分支到中心通訊所需的隧道以及分支到分支隧道的可選隧道。如果您選擇不使用動態分支到分支隧道並且希望所有內容都通過中心裝置，則可以刪除虛擬模板介面，並從隧道介面刪除NHRP快捷方式交換。

您還會注意到，靜態隧道介面具有基於協商接收的IP地址。這樣，集線器便可以動態提供到分支的隧道介面IP，而無需在FlexVPN雲中建立靜態定址。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco建議在支援它的硬體中使用AES GCM。

```
crypto ipsec transform-set IKEv2 esp-gcm
    mode transport
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
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
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 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
```

PKI是在IKEv2中執行大規模身份驗證的推薦方法。

但是，只要您知道預共用金鑰的侷限性，您仍然可以使用它。

以下是使用「cisco」作為PSK的組態範例：

```
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
```

FlexVPN中心配置

通常，集線器只會終止動態輻條到集線器的通道。這就是在集線器的組態中，找不到適用於FlexVPN的靜態通道介面，而是使用虛擬範本介面的原因。這將為每個連線生成一個虛擬訪問介面。

請注意，在集線器端，您需要指出要分配給輻條的池地址。

此地址池中的地址稍後將作為每個分支的/32路由新增到路由表中。

```
aaa new-model
aaa authorization network default local
aaa session-id common
```

```
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco建議在支援它的硬體中使用AES GCM。

```
crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

請注意，在下面的配置中，AES GCM操作已被註釋掉。

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

在IKEv2中進行身份驗證時，中心點和分支點上使用相同的原則。

為獲得可擴充性和靈活性，請使用證書。但是，您可以為PSK重複使用與分支上相同的配置。

注意：IKEv2在身份驗證方面提供了靈活性。一端可以使用PSK進行身份驗證，而另一端的RSA-SIG進行身份驗證。

流量遷移

作為重疊路由協定遷移到BGP [推薦]

BGP是基於單播交換的路由協定。由於其自身的特點，它一直是DMVPN網路中最好的擴展協定。

本範例中使用的是iBGP。

分支BGP配置

輻條遷移由兩部分組成。啟用BGP作為動態路由。

```
router bgp 65001
```

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

在BGP鄰居啟動後（請參閱本遷移部分中的中心BGP配置），在BGP上學習新的字首後，您可以將流量從現有DMVPN雲切換到新的FlexVPN雲。

中心BGP配置

在集線器上，為避免單獨保留每個分支的鄰居關係配置，將配置動態監聽程式。

在此設定中，BGP不會啟動新連線，但會接受來自所提供的IP地址池的連線。在本例中，所述池為10.1.1.0/24，這是新FlexVPN雲中的所有地址。

```
router bgp 65001
 network 192.168.0.0
 bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
 neighbor Spokes peer-group
 neighbor Spokes remote-as 65001
```

將流量遷移到FlexVPN

如前所述，需要通過關閉DMVPN功能和啟動FlexVPN來完成遷移。

這個程式保證影響最小。

1. 在所有輻條上：
   ```
   interface tunnel 0
      shut
   ```
2. 在Hub上：
   ```
   interface tunnel 0
     shut
   ```
   此時，請確保沒有從輻條建立到此集線器的IKEv1會話。檢查**show crypto isakmp sa**命令的輸出，並監視加密日誌記錄會話生成的系統日誌消息，即可驗證這一點。確認此情況後，您可以繼續啟動FlexVPN。
3. 繼續使用集線器：
   ```
   interface Virtual-template 1
    no shut
   ```
4. 輪輻上：
   ```
   interface tunnel 1
      no shut
   ```

驗證步驟

IPsec穩定性

評估IPsec穩定性的最佳方法是啟用此配置命令後監控系統日誌：

```
crypto logging session
```

如果您看到會話的開啟和關閉，這可能表明在IKEv2/FlexVPN級別上存在問題，需要在開始遷移之前更正此問題。

已填充BGP資訊

如果IPsec是穩定的，請確保BGP表已填充來自分支（在集線器上）的條目和來自集線器的摘要（在分支上）。

在BGP的情況下，可通過執行以下操作檢視此情況：

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

來自集線器的正確資訊示例：

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1
*10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

您可以看到，集線器已從每個輻條獲得1個字首，並且兩個輻條都是動態的(標有星號(*))。

來自分支的類似資訊的示例：

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

分支已從中心收到一個字首。在此設定的情況下，此字首應該是在集線器上通告的摘要。

使用EIGRP遷移到新隧道

EIGRP因其相對簡單的部署和快速收斂而成為DMVPN網路中的常用選擇。

但是，它的擴展性會比BGP差，並且不能提供許多高級機制，BGP可以直接使用開箱即用。

下一節介紹使用新EIGRP進程遷移到FlexVPN的方法之一。

更新的分支配置

在本例中，新增了一個包含獨立EIGRP進程的新AS。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```

注意：您應避免在輻射分支到輻射分支隧道上建立路由協定鄰接關係，這樣只會使tunnel1（輻射分支到集線器）的介面不是被動介面。

已更新中心配置

類似地，在集線器上，DMVPN應該仍然是交換流量的首選方式。但是，FlexVPN應該通告並學習相同的字首。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```

有兩種方法可以向輻條提供摘要。

- 重新分配指向null0（首選選項）的靜態路由。
  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```
  此選項允許在不接觸集線器的VT配置的情況下控制摘要和重新分發。
- 或者，可以在虛擬模板上設定DMVPN樣式的摘要地址。建議不要進行此配置，因為會對這些摘要進行內部處理並將其複製到每個虛擬訪問。此處顯示以供參考：
  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 172.16.1.0 255.255.255.0
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   delay 2000
  ```

將流量遷移到FlexVPN

遷移需要通過關閉DMVPN功能和啟動FlexVPN來完成。

以下程式保證影響最小。

1. 在所有輻條上：
   ```
   interface tunnel 0
      shut
   ```
2. 在Hub上：
   ```
   interface tunnel 0
     shut
   ```
   此時，請確保沒有從輻條建立到此集線器的IKEv1會話。檢查**show crypto isakmp sa**命令的輸出，並監視加密日誌記錄會話生成的系統日誌消息，即可驗證這一點。確認此情況後，您可以繼續啟動FlexVPN。
3. 繼續使用集線器：
   ```
   interface Virtual-template 1
    no shut
   ```
4. 在所有輻條上：
   ```
   interface tunnel 1
      no shut
   ```

驗證步驟

IPsec穩定性

在BGP的情況下，您需要評估IPsec是否穩定。最佳方法是在啟用此組態指令的情況下監控系統日誌：

```
crypto logging session
```

如果您看到會話的開啟和關閉，這可能表明在IKEv2/FlexVPN級別上存在問題，需要在開始遷移之前更正此問題。

拓撲表中的EIGRP資訊

確保您的EIGRP拓撲表中填充了中心節點上的分支LAN條目和分支上的摘要。這可以通過在中心和分支上發出此命令來驗證。

```
show ip eigrp topology
```

輯條正確輸出的示例：

```
Spoke1#sh 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
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
 via Rstatic (26112000/0)


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 26114560
 via 10.1.1.1 (26114560/1709056), Tunnel1


P 10.1.1.107/32, 1 successors, FD is 26112000
 via Connected, Tunnel1
```

您會注意到spoke知道其LAN子網（斜體）以及這些子網的總結(**粗體**)。

集線器正確輸出的示例。

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100
```

```
P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 10.1.1.107/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 10.1.1.106/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 0.0.0.0/0, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

您會注意到，中心節點知道分支的LAN子網（斜體）、其通告的摘要字首（粗體）以及通過協商為每個分支分配的IP地址。

其他考量事項

現有分支到分支隧道

由於關閉DMVPN隧道介面會導致NHRP條目被刪除，因此現有分支到分支隧道將被關閉。

清除NHRP條目

如前所述，FlexVPN中心不會依賴來自分支的NHRP註冊流程來瞭解如何將流量路由回來。但是，動態輻條隧道依賴於NHRP條目。

在DMVPN中，清除集線器上的NHRP可能導致短暫的連線問題。

在FlexVPN清除中，分支上的NHRP將導致與分支到分支隧道相關的FlexVPN IPsec會話斷開。清除NHRP時，任何集線器都不會影響FlexVPN會話。

這是因為在FlexVPN中，預設情況下：

- 輻條不會註冊到集線器。
- 集線器僅作為NHRP重定向器工作，不安裝NHRP條目。
- NHRP快捷方式條目安裝在輻條到輻條隧道的輻條上，並且是動態的。

已知警告

CSCub07382可能會影響分支流量。

相關資訊

- 技術支援與文件 - Cisco Systems