在不同的中心從DMVPN硬遷移到FlexVPN

目錄

簡介

本文提供如何從目前存在的動態多點VPN(DMVPN)網路遷移到不同集線器裝置上的FlexVPN的相關資訊。這兩個框架的配置在裝置上共存。在本文檔中，僅顯示最常見的情況 — 使用預共用金鑰進行身份驗證的DMVPN以及增強型內部網關路由協定(EIGRP)作為路由協定。本文檔展示了遷移到邊界網關協定(BGP)（推薦的路由協定）和不太理想的EIGRP的示例。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- DMVPN
- FlexVPN

採用元件

> **附註**：並非所有軟體和硬體都支援Internet金鑰交換版本2(IKEv2)。 如需詳細資訊，請參閱思科功能導覽器。

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15.2(4)M1或更新版本
- 思科聚合服務路由器1000系列(ASR1K)3.6.2版本15.2(2)S2或更新版本

較新的平台和軟體的優勢之一是可以使用下一代加密技術，例如進階加密標準(AES)花旗/計數器模式(GCM)在網際網路通訊協定安全(IPsec)中加密，如要求建議(RFC)4106中所述。AES GCM允許您在某些硬體上實現更快的加密速度。要檢視思科關於下一代加密技術的使用和遷移的建議，請參閱下一代加密文章。

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。

移轉程式

目前，推薦的從DMVPN遷移到FlexVPN的方法是使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，此限制已計畫刪除，該功能在思科端的多個增強請求(包括思科錯誤ID CSCuc0806)下跟蹤。這些功能應在2013年6月下旬提供。

當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**，它表示一個框架到另一個框架的影響最小，且故障轉移平穩。兩個框架的配置同時存在，但不同時運行的遷移稱為硬**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。

兩個不同中心之間的硬遷移

本檔案將討論從目前使用的DMVPN集線器遷移到新的FlexVPN集線器的問題。此遷移允許已遷移到

FlexVPN的輻條與仍在DMVPN上運行且可在多個階段中在每個輻條上分別執行的輻條之間的互通。

如果路由資訊已正確填充，遷移和非遷移輻條之間的通訊應該仍可進行。但是，由於遷移和非遷移的輻條不會在彼此之間構建分支到分支隧道，因此可以觀察到額外的延遲。同時，遷移的輻條應該能夠在它們之間建立直接的輻條到輻條隧道。這同樣適用於非遷移輻條。

在此新的遷移功能可用之前，請完成以下步驟，以便使用來自DMVPN和FlexVPN的不同集線器執行遷移：

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。
3. （在維護時段內）在每個分支上，逐個關閉DMVPN隧道。
4. 在與步驟3相同的分支上，取消關閉FlexVPN隧道介面。
5. 驗證分支到中心點的連線。
6. 在FlexVPN中驗證分支到分支連線。
7. 通過FlexVPN的DMVPN驗證分支到分支連線。
8. 分別對每個分支重複步驟3至7。
9. 如果在步驟5、6或7中描述的驗證過程中遇到任何問題，請關閉FlexVPN介面，然後取消關閉DMVPN介面以恢復到DMVPN。
10. 驗證通過備份的DMVPN的分支與中心之間的通訊。
11. 通過備份的DMVPN驗證分支到分支的通訊。

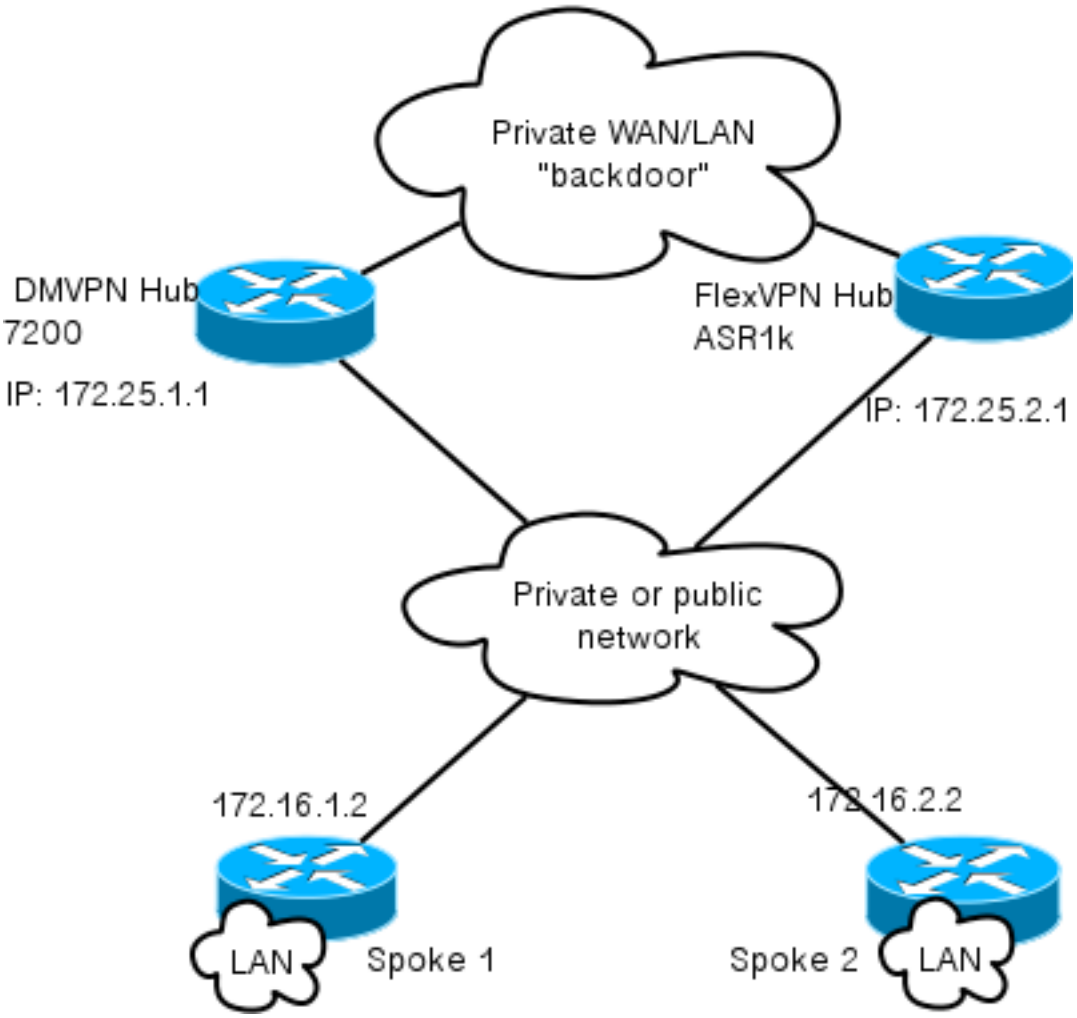
定製方法

如果由於您的網路或路由複雜性，上述方法可能不是您的最佳解決方案，請在遷移之前與您的思科代表展開討論。討論自定義遷移流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

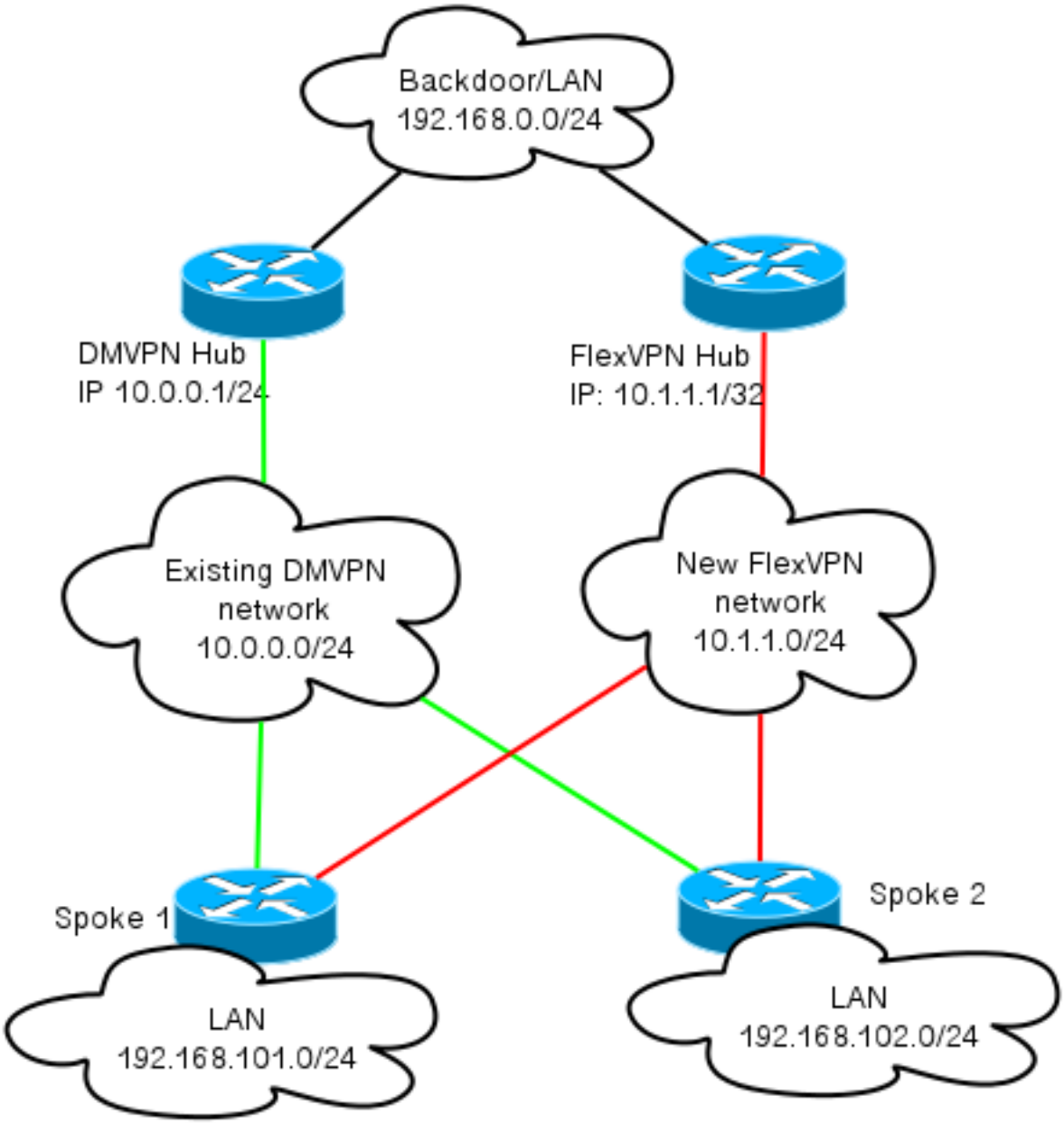
此圖顯示Internet上主機的典型連線拓撲。集線器的IP地址**loopback0**(**172.25.1.1**)用於終止DMVPN IPsec會話。新集線器上的IP地址**(172.25.2.1**)用於FlexVPN。



注意兩個集線器之間的鏈路。在遷移過程中，此連結對於實現FlexVPN和DMVPN雲之間的連線至關重要。它允許已遷移到FlexVPN的輻條與DMVPN網路通訊，反之亦然。

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（紅色連線）。顯示了相應站點的LAN字首。**10.1.1.0/24**子網在介面編址方面不代表實際子網，但代表專用於FlexVPN雲的IP空間塊。其基本原理稍後將在**FlexVPN配置**部分討論。



組態

本節介紹DMVPN和FlexVPN配置。

DMVPN配置

本節介紹DMVPN中心和分支的基本配置。

預共用金鑰(PSK)用於IKEv1身份驗證。建立IPsec後，會執行從輻射點到中心點的下一個躍點解析協定(NHRP)註冊，以便中心點可以動態得知輻射點的非廣播多路訪問(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，並且可以交換路由。在本示例中，EIGRP用作重疊網路的基本路由協定。

分支DMVPN配置

您可以在此處找到將PSK身份驗證和EIGRP用作路由協定的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**，其IP地址為**172.25.1.1**。其餘部分是以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中的預設值不同，使用IKEv2而不是IKEv1來協商IPsec安全關聯(SA)。IKEv2提供比IKEv1更好的效能，例如恢復能力和建立受保護的資料通道所需的消息數量。

- **GRE :**與DMVPN不同的是，使用靜態和動態點對點介面，而不僅僅是一個靜態多點GRE介面。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。輻條不會註冊到集線器。

- **路由**:由於輻條不執行到集線器的NHRP註冊，您必須依靠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。預設設定為在隧道另一端引入IP地址的as **/32**路由，該路由允許分支到集線器的直接通訊。

在從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）。
- 虛擬路由和轉送(VRF)- VRF分離允許更大的靈活性，此處不作討論（可選）。

分支FlexVPN配置

與DMVPN相比，FlexVPN中的分支配置的一個區別在於，您可能有兩個介面。分支到中心通訊有所需的隧道，分支到分支隧道有可選隧道。如果選擇不採用動態輻條到輻條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。

請注意，靜態通道介面會收到基於交涉的IP位址。這樣，集線器便可以動態地將隧道介面IP地址提供給分支，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
local identity fqdn spoke.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
```

> **附註**：預設情況下，本地身份設定為使用IP地址。因此，對等體上的相應match語句也必須基於地址匹配。如果要求根據憑證中的可分辨名稱(DN)進行配對，則必須使用憑證映像來完成配對。

思科建議您將AES GCM與支援它的硬體結合使用。

```
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 172.25.2.1
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
```

公開金鑰基礎架構(PKI)是在IKEv2中執行大規模身份驗證的推薦方法。但是，只要您知道其限制，仍然可以使用PSK。

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
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

FlexVPN中心配置

通常，集線器只終止動態輻條到集線器隧道。這就是在集線器配置中找不到FlexVPN的靜態隧道介面的原因。而是使用虛擬模板介面。

附註：在集線器端，必須指定要分配給輻條的池地址。

來自此地址池的地址稍後會作為每個分支的**/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
local identity fqdn hub.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
```

思科建議您將AES GCM與支援它的硬體結合使用。

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

附註：在此配置中，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 172.25.2.1 255.255.255.255
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
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，中心點和分支點上應用相同的原則。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。

> **附註**：IKEv2在身份驗證方面提供了靈活性。一端可以通過PSK進行身份驗證，而另一端使用Rivest-Shamir-Adleman簽名(RSA-SIG)。

如果要求使用預共用金鑰進行身份驗證，則配置更改類似於此處針對分支路由器所描述的更改。

集線器間BGP連線

確保集線器知道特定字首的位置。這一點變得日益重要，因為某些輻條已遷移到FlexVPN，而另一些輻條仍保留在DMVPN上。

以下是基於DMVPN集線器配置的集線器間BGP連線：

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

流量遷移

作為重疊路由協定遷移到BGP [推薦]

BGP是一種基於單播交換的路由協定。由於其特性，它是DMVPN網路中最佳擴展協定。

在此範例中，使用內部BGP(iBGP)。

分支BGP配置

輻條遷移由兩部分組成。首先，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（請參閱下一部分），瞭解BGP上的新字首後，您可以將流量從當前DMVPN雲切換到新的FlexVPN雲。

中心BGP配置

FlexVPN中心 — 完整BGP配置

在集線器上，為了避免單獨保留每個分支的鄰居關係配置，請配置動態偵聽器。在此設定中，BGP不啟動新連線，但接受來自所提供的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。

需要注意兩點：

- FlexVPN中心向DMVPN中心通告特定字首；因此，使用的是不緊壓的地圖。
- 將**10.1.1.0/24**的FlexVPN子網通告給路由表，或確保DMVPN中心將FlexVPN中心視為下一跳。

本檔案介紹後一種方法。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

DMVPN中心 — 完整BGP和EIGRP配置

DMVPN中心上的配置是基本的，因為它只從FlexVPN中心接收特定字首並通告它從EIGRP獲取的字首。

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

將流量遷移到BGP/FlexVPN

如前所述，您必須關閉DMVPN功能並啟動FlexVPN才能執行遷移。

此過程保證最小影響：

1. 在每個分支上，分別輸入以下內容：

   ```
   interface tunnel 0
    shut
   ```

   此時，請確保沒有為此分支建立IKEv1會話。如果您檢查**show crypto isakmp sa**命令的輸出，並監控由**crypto logging session**命令生成的系統日誌消息，則可以**驗證此**情況。確認此情況

後，您可以繼續啟用FlexVPN。

2. 在同一分支上，輸入以下內容：

```
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使用**crypto logging session**配置命令監控系統日誌。如果您看到會話的開啟和關閉，這可能表明IKEv2/FlexVPN級別上存在問題，必須在遷移開始之前更正此問題。

已填充BGP資訊

如果IPsec是穩定的，請確保BGP表中填充有來自分支（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，可以使用以下命令來檢視：

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

以下是FlexVPN中心正確資訊的示例：

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

輸出顯示，集線器已從每個輻條獲知一個字首，並且兩個輻條都是動態的，並用星號(*)標籤。它還顯示從集線器間連線總共收到四個字首。

以下是來自分支的類似資訊的示例：

```
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 120 109 57 0 0 01:33:23 2
```

輻條已從集線器收到兩個字首。在此設定的情況下，一個字首應該是在FlexVPN中心上通告的摘要。另一個是DMVPN **10.0.0.0/24**網路，該網路在DMVPN分支上重新分發到BGP。

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，它的擴展性比BGP差，並且沒有提供許多高級機制供BGP直接使用。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

通過單獨的EIGRP進程新增新的自治系統(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
```

> **附註**：最好不要通過分支到分支隧道建立路由協定鄰接關係。因此，只能使**tunnel1**（輻條到集線器）的介面不是被動介面。

更新的FlexVPN中心配置

同樣，對於FlexVPN中心，請在適當的AS中準備路由協定，與輻條上配置的路由協定匹配。

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

有兩種方法可用於向輻條提供彙總。

- 重新分發指向**null**0(首選**選項**)的靜態路由。

  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip route 10.1.1.0 255.255.255.0 null 0

  ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
  ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

  route-map EIGRP_SUMMARY permit 20
  match ip address prefix-list EIGRP_SUMMARY_ONLY

  router eigrp 200
  distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
  redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
  ```

  此選項允許控制摘要和重新分發，而無需修改集線器的虛擬化技術(VT)配置。這一點非常重要，因為如果存在關聯的活動虛擬訪問，則無法修改集線器的VT配置。

- 在虛擬模板上設定DMVPN樣式的摘要地址。

  建議不要使*用此配置*，因為會進行內部處理，並將所述摘要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 200 192.168.0.0 255.255.0.0
  ```

要考慮的另一方面是中心間路由交換。如果將EIGRP例項重分發到iBGP，就可以完成此操作。

DMVPN中心 — 更新的BGP配置

配置仍是基本配置。您必須將特定字首從EIGRP重新分發到BGP:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

FlexVPN中心 — 更新的BGP配置

與DMVPN中心類似，在FlexVPN中，您必須將新EIGRP進程的字首重新分發到BGP:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

將流量遷移到FlexVPN

必須關閉DMVPN功能並在每個分支上逐個啟動FlexVPN，才能執行遷移。此過程可保證最小影響：

1. 在每個分支上，分別輸入以下內容：

   ```
   interface tunnel 0
    shut
   ```

   此時，請確保此分支上未建立IKEv1會話。如果您檢查**show crypto isakmp sa**命令的輸出，並監控由**crypto logging session**命令生成的系統日誌消息，則可以**驗證此**情況。確認此情況後，您可以繼續啟用FlexVPN。
2. 在同一分支上，輸入以下內容：

   ```
   interface tunnel 1
     no shut
   ```

驗證步驟

IPsec穩定性

與BGP的情況一樣，您必須評估IPsec是否穩定。這樣做的最佳方式是啟用**crypto logging session**配置命令後監控系統日誌。如果您看到會話的開啟和關閉，這可能表明IKEv2/FlexVPN級別上存在問題，必須在遷移開始之前更正此問題。

拓撲表中的EIGRP資訊

確保EIGRP拓撲表中填充了中心點上的分支LAN條目和分支點上的摘要。如果在中心和分支上輸入以下命令，可以驗證這一點：

show ip eigrp [AS_NUMBER] topology

以下是輻條輸出的範例：

```
Spoke1#show ip eigrp 200 topology
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)
via 10.1.1.1 (26240000/128256), Tunnel1

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 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

輸出顯示，輻條知道其LAN子網(斜體*)和*這些子網的總結(**粗體**)。

以下是集線器輸出的範例：

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
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, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

輸出顯示，集線器知道輻條的LAN子網(以*斜體*表示)、所通告的摘要字首(以**粗體**)以及通過協商為每個輻條分配的IP地址。

其他考量事項

已存在的分支到分支隧道

由於DMVPN隧道介面的關閉導致NHRP條目被刪除，因此已經存在的分支到分支隧道將被關閉。

清除NHRP條目

FlexVPN中心不依賴來自分支的NHRP註冊過程以便瞭解如何路由回流量。但是，動態輻條到輻條隧道依賴於NHRP條目。

在DMVPN中，如果清除集線器上的NHRP，可能會導致連線問題持續時間較短。在FlexVPN中，清除分支上的NHRP將導致與分支到分支隧道相關的FlexVPN IPsec會話被關閉。清除集線器上的NHRP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

輻射到輻射流量可能受Cisco錯誤ID CSCub07382影響。

相關資訊

- **DMVPN到FlexVPN軟遷移配置示例**
- **技術支援與文件 - Cisco Systems**