採用FlexVPN客戶端塊配置的冗餘中心設計中的FlexVPN分支配置示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[設定](#)
[網路圖](#)
[傳輸網路](#)
[重疊網路](#)
[分支和中心的基本配置](#)
[分支配置調整](#)
[分支配置 — 客戶端配置塊](#)
[完整分支配置 — 參考](#)
[集線器配置](#)
[分支地址](#)
[中心重疊地址](#)
[路由](#)
[網路摘要使用](#)
[輻射對輻射隧道](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

簡介

本文檔介紹如何在具有多個集線器的情況下使用FlexVPN客戶端配置塊在FlexVPN網路中配置分支。

必要條件

需求

思科建議您瞭解以下主題：

- FlexVPN
- 思科路由通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco G2系列整合式服務路由器(ISR)
- Cisco IOS®版本15.2M

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

出於冗餘目的，分支可能需要連線到多個集線器。分支端冗餘允許連續運行，而中心端無單點故障。

使用分支配置的兩種最常見的FlexVPN冗餘中心設計是：

- **雙雲方法，**其中輻條始終有兩個連線到兩個中心的獨立隧道。
- **故障切換方**法，其中輻條在任何給定時間點都具有一個中心點的活動隧道。

兩種方法都有各自的優缺點。

方針	優點	缺點
雙雲	• 根據路由協定計時器，在故障中更快地恢復 • 由於與兩個集線器的連線均處於活動狀態，因此更有可能在集線器之間分配流量	• 輻條可同時資源
容錯移轉	• 輕鬆配置 — 內建於FlexVPN中 • 在出現故障時不依賴路由協定	• 恢復時間更 • 所有流量都

本檔案介紹第二種方法。

設定

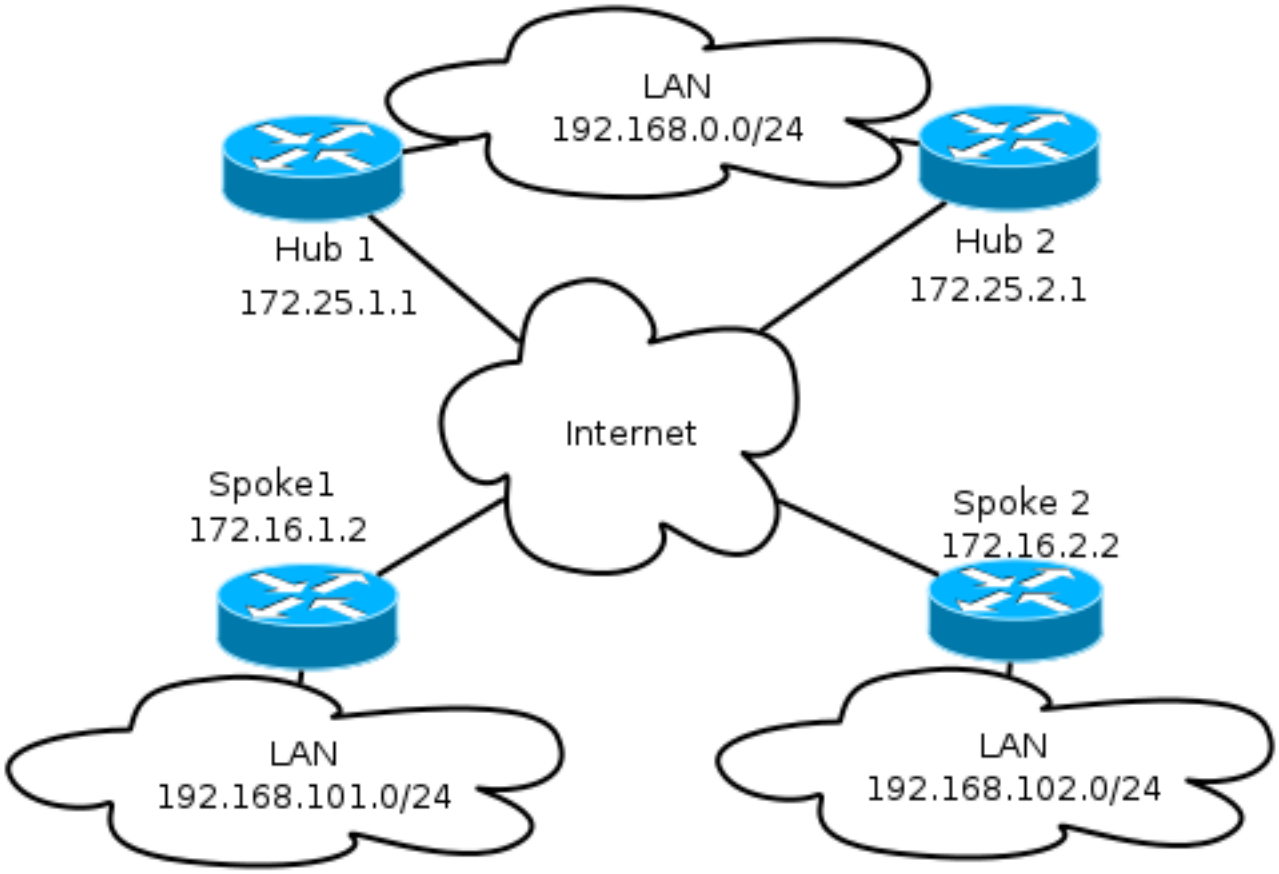
附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖

這些圖顯示了傳輸和重疊拓撲圖。

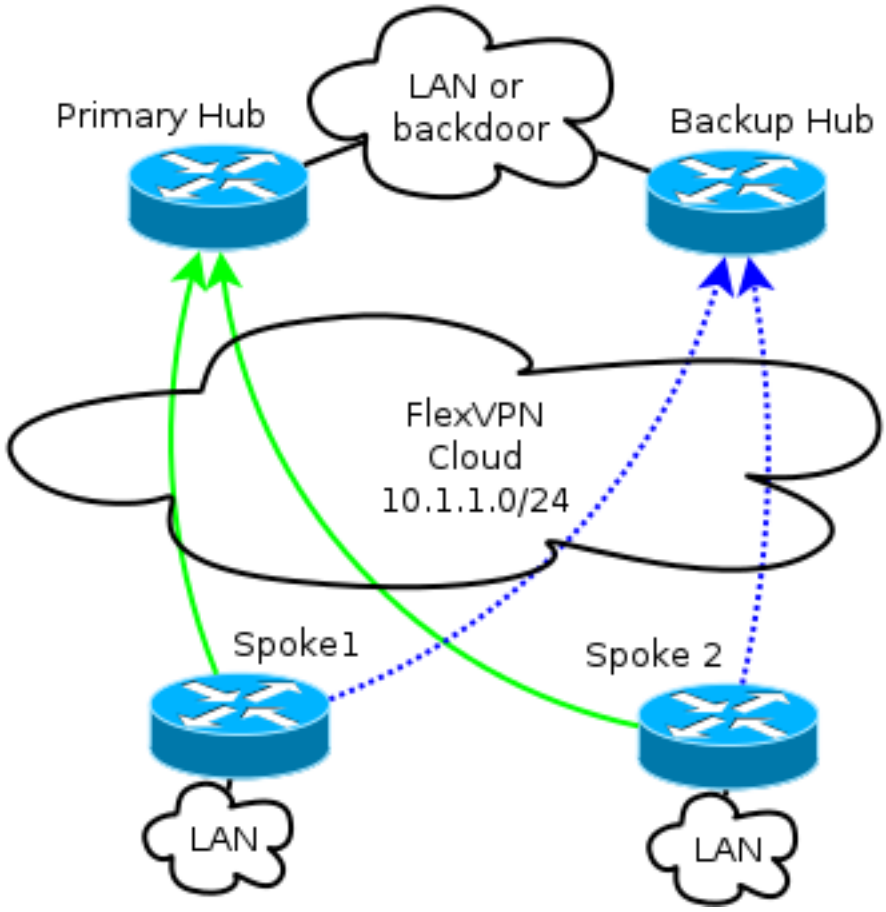
傳輸網路

此圖說明FlexVPN網路中通常使用的基本傳輸網路。



重疊網路

此圖說明具有邏輯連線的重疊網路，其中顯示了故障切換應如何工作。在正常操作期間，分支1和分支2僅與一個中心保持關係。



附註：在圖中，綠色的實線顯示主要Internet金鑰交換版本2(IKEv2)/Flex會話的連線和方向，藍色虛線表示如果與主要集線器的Internet金鑰交換(IKE)會話失敗時的備份連線。

/24編址表示為此雲分配的地址池，而不是實際介面編址。這是因為FlexVPN中心通常為分支介面分配動態IP地址，並且依賴於通過FlexVPN授權塊中的路由命令動態插入的路由。

分支和中心的基本配置

中心輻射點的基本配置基於從動態多點VPN(DMVPN)到FlexVPN的遷移文檔。FlexVPN遷移： 中介紹了此配置「Hard Move from DMVPN to FlexVPN on Same Devices（在同一裝置上從DMVPN硬移至FlexVPN）」文章。

分支配置調整

分支配置 — 客戶端配置塊

分支配置必須由客戶端配置塊擴展。

在基本配置中，指定了多個對等體。具有最高優先順序（最低編號）的對等體會先於其他對等體考慮。

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
```

```
peer 2 172.25.2.1
client connect Tunnel1
```
隧道配置必須更改，以允許根據FlexVPN客戶端配置塊動態選擇隧道目標。

```
interface Tunnel1
 tunnel destination dynamic
```
請務必記住，FlexVPN客戶端配置塊繫結到介面，而不是繫結到IKEv2或網際網路協定安全(IPsec)配置檔案。

客戶端配置塊提供多個選項以調整故障切換時間和操作，其中包括跟蹤對象使用情況、撥號備份和備份組功能。

在基本配置中，輻條依靠DPD來檢測輻條是否無響應，並且在對等體宣告失效後觸發更改。由於DPD的工作方式，使用DPD的選項不是快速選項。管理員可能需要通過對象跟蹤或類似增強功能來增強配置。

如需詳細資訊，請參閱Cisco IOS組態設定指南的**FlexVPN使用者端組態**一章，此章已連結在本檔案結尾的**相關資訊**一節中。

完整分支配置 — 參考

```
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 ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN 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
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

集線器配置

雖然大多數中心配置保持不變，但必須解決幾個方面。其中大多數都涉及一個或多個輻條連線到一個集線器，而其它輻條則保持與另一個集線器的關係。

分支地址

由於分支從集線器獲得IP地址，因此通常希望集線器從不同的子網或子網的不同部分分配地址。

例如：

集線器1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

集線器2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

即使地址不在FlexVPN雲外路由，這也可以防止重疊的建立，這可能會妨礙故障排除工作。

中心重疊地址

兩個集線器可以在虛擬模板介面上保留相同的IP地址；但是，在某些情況下，這可能會影響故障排除。這種設計選擇使部署和規劃更加容易，因為分支必須只有一個邊界網關協定(BGP)的對等地址。

在某些情況下，它可能是不希望或不需要的。

路由

集線器需要交換有關所連線輻條的資訊。

集線器必須能夠交換所連線裝置的特定路由，同時仍然為輻條提供總結。

由於思科建議您將iBGP與FlexVPN和DMVPN配合使用，因此只會顯示路由協定。

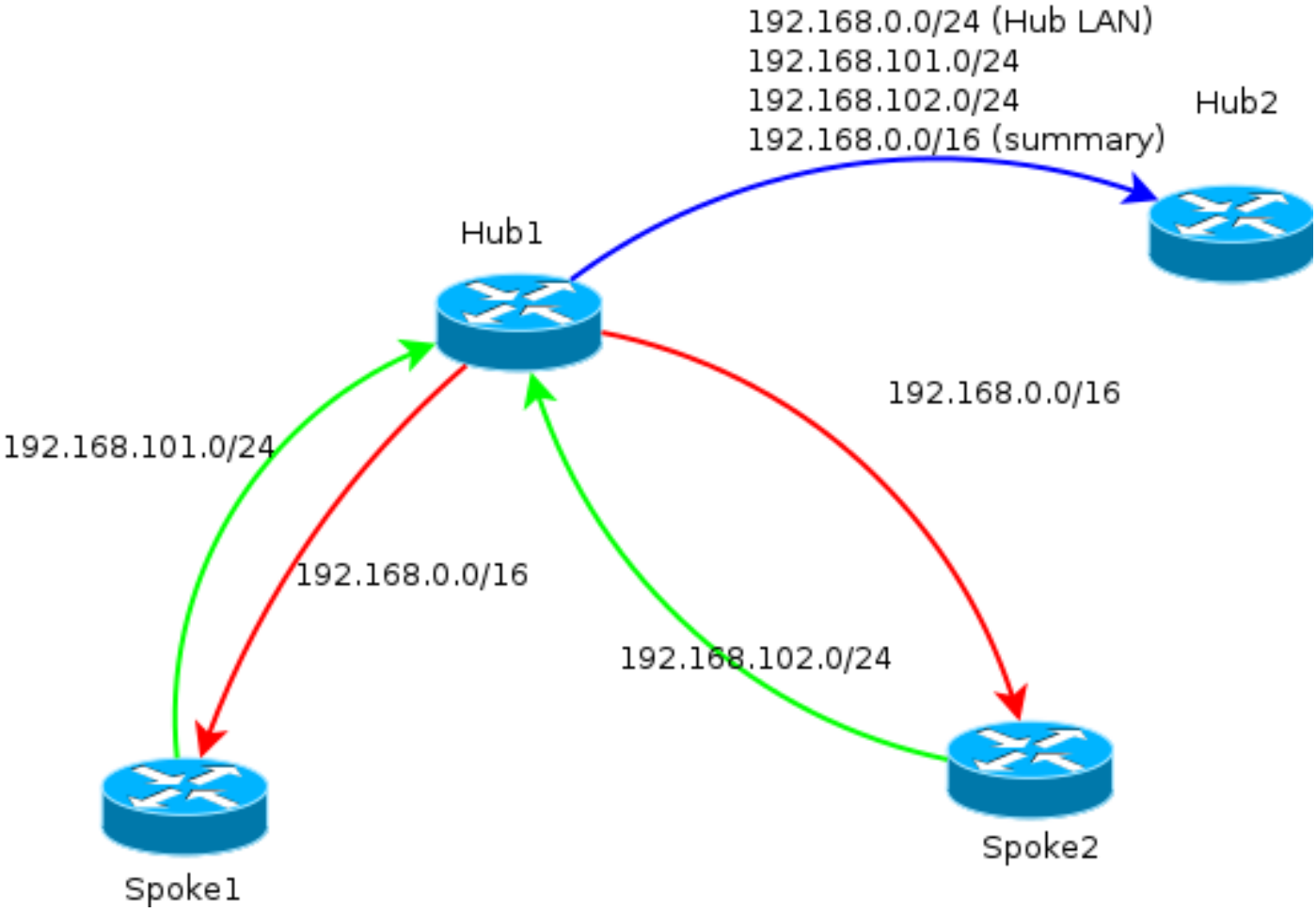
```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
```

```
neighbor Spokes remote-as 65001
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

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

此配置允許：

- 來自分配給分支的地址的動態偵聽程式
- 192.168.0.0/24的**廣告網路**
- 向所有輻條通告**192.168.0.0/16**的總結路由。aggregate-address配置通過null0介面為該字首建立靜態路由，該路由是用來防止路由環路的丟棄路由。
- 將特定字首轉發到另一個集線器
- 路由反射器使用者端，確保集線器之間交換從輻條獲取的資訊

此圖從其中一個集線器的角度呈現此設定中BGP中的首碼交換。



附註：在此圖中，綠線表示輻條向集線器提供的資訊，紅線表示每個集線器向輻條提供的資訊（僅限於彙總），藍線表示集線器之間交換的字首。

網路摘要使用

摘要在某些情況下可能不適用，或者不需要。在字首中指定目標IP時請謹慎小心，因為iBGP在預設情況下不會覆蓋下一跳。

對於經常更改狀態的網路，建議使用摘要。例如，不穩定的Internet連線可能需要摘要才能執行以下操作：避免刪除和新增字首，限制更新數量，並允許大多數設定正確擴展。

輻射對輻射隧道

在前一節提到的場景和配置中，不同集線器上的輻條無法建立直接的輻條到輻條隧道。連線到不同集線器的輻條之間的流量流經中央裝置。

對此有一個簡單的解決方法。但是，這要求在集線器之間啟用具有相同網路ID的下一跳解析協定(NHRP)。例如，如果您在集線器之間建立一個點對點通用路由封裝(GRE)通道，就可以達成此目的。則不需要使用IPsec。

驗證

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

show crypto ikev2 sa命令會通知您分支當前連線的位置。

show crypto ikev2 client flexvpn命令允許管理員瞭解FlexVPN客戶端操作的當前狀態。

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

使用**show logging**配置的成功故障切換將記錄分支裝置上的以下輸出：

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

在此輸出中，輻條從**hub 172.25.1.1**斷開，Flex_Client客戶端配置塊檢測到故障並強制連線到隧道出現處的**172.25.2.1**，並為輻條分配了**10.1.1.177**的IP。

疑難排解

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

> **附註**：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

以下是相關的debug指令：

- debug crypto ikev2
- debug radius

相關資訊

- FlexVPN和Internet金鑰交換版本2配置指南，Cisco IOS版本15 M&T
- 技術支援與文件 - Cisco Systems