採用雙雲方法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](#)
[設定](#)
[網路圖表](#)
[傳輸網路](#)
[重疊網路](#)
[分支配置](#)
[分支隧道介面配置](#)
[分支邊界網關協定(BGP)配置](#)
[集線器配置](#)
[本地池](#)
[中心BGP配置](#)
[驗證](#)
[疑難排解](#)

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。

設定

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。

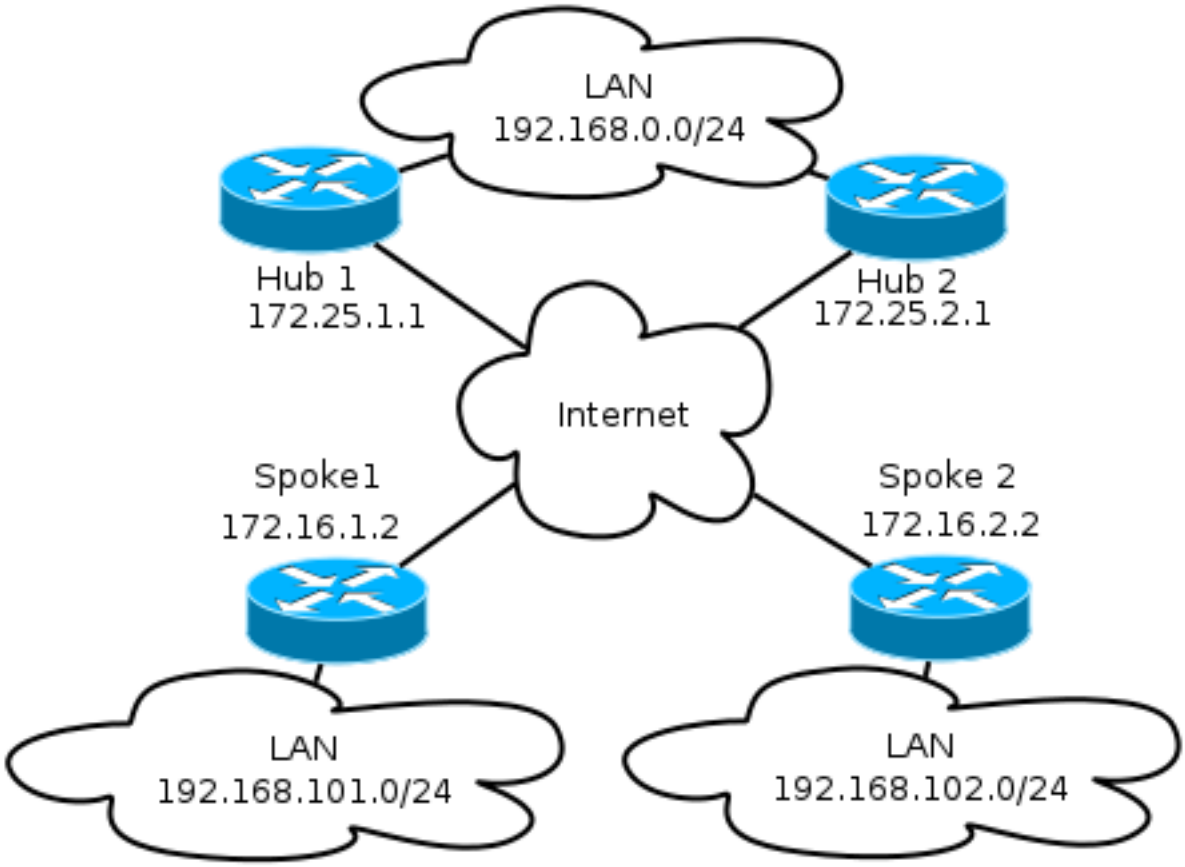
方針	優點	缺點
雙雲	• 基於路由協定計時器，在故障期間更快地恢復 • 由於與兩個集線器的連線均處於活動狀態，因此更有可能在集線器之間分配流量	• 輻條可同時資源
容錯移轉	• 輕鬆配置 — 內建於FlexVPN中 • 在出現故障時不依賴路由協定	• 恢復時間更 • 所有流量都

本文檔介紹第一種方法。此組態的方法類似於動態多點VPN(DMVPN)雙雲組態。中心輻射點的基本配置基於從DMVPN到FlexVPN的遷移文檔。請參閱FlexVPN遷移：「Hard Move from DMVPN to FlexVPN on Same Devices(在同一裝置上從DMVPN硬移到FlexVPN)」文章以瞭解此配置的說明。

網路圖表

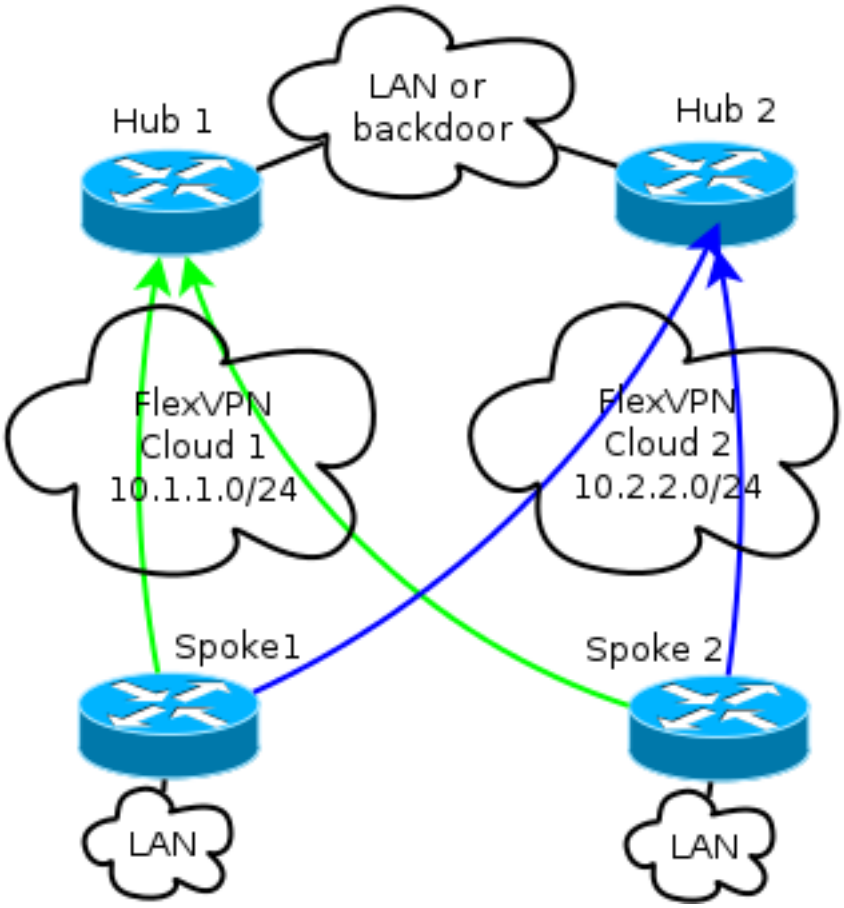
傳輸網路

此圖說明FlexVPN網路中通常使用的基本傳輸網路。



重疊網路

該圖說明了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。在正常運行期間，輻條1和輻條2與兩個中心保持關係。發生故障時，路由協定會從一個集線器切換到另一個集線器。



附註：在圖中，綠色線表示連線到集線器1的Internet金鑰交換版本2(IKEv2)/Flex會話的連線和方向，藍色線表示連線到集線器2。

兩個集線器在重疊雲中均保留單獨的IP編址。**/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。

分支配置

分支隧道介面配置

本示例中使用的典型配置只是兩個隧道介面，帶有兩個單獨的目的地址。

```
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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
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 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

為了正確形成輻條到輻條隧道，需要虛擬模板(VT)。

```
interface Virtual-Template1 type tunnel
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 path-mtu-discovery
tunnel protection ipsec profile default
```

分支使用未編號的介面，該介面表示虛擬路由和轉發(VRF)中的LAN介面，在本例中為全域性。但是，最好參考環回介面。這是因為環回介面在幾乎所有情況下都保持聯機。

分支邊界網關協定(BGP)配置

由於Cisco建議將iBGP用作重疊網路中的路由協定，因此本文檔僅提到此配置。

附註：輻條必須保持到兩個集線器的BGP可達性。

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

此配置中的FlexVPN沒有主要或次要集線器概念。管理員決定路由協定是優先選擇一台集線器而不是另一台集線器，或在某些情況下執行負載均衡。

分支故障切換和融合注意事項

為了最小化輻條檢測故障所需的時間，請使用以下兩種典型方法。

- 縮短BGP計時器。預設保持時間會導致故障轉移。
- 設定BGP容錯移轉，這將在本文BGP支援快速對等作業階段停用中討論。
- 請勿使用雙向轉發檢測(BFD)，因為大多數FlexVPN部署都不建議使用。

分支到分支隧道和故障轉移

分支到分支隧道使用下一跳解析協定(NHRP)快捷方式交換。Cisco IOS指示這些快捷方式是NHRP路由，例如：

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

BGP連線到期時，這些路由不會過期；相反，他們被扣押在國家人權保護局的拘留時間，預設為兩小時。這意味著即使發生故障，活動的輻條到輻條隧道仍可正常運行。

集線器配置

本地池

如**網路圖表**一節所述，兩個集線器都保留單獨的IP定址。

集線器1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

集線器2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

中心BGP配置

集線器BGP配置與先前的示例類似。

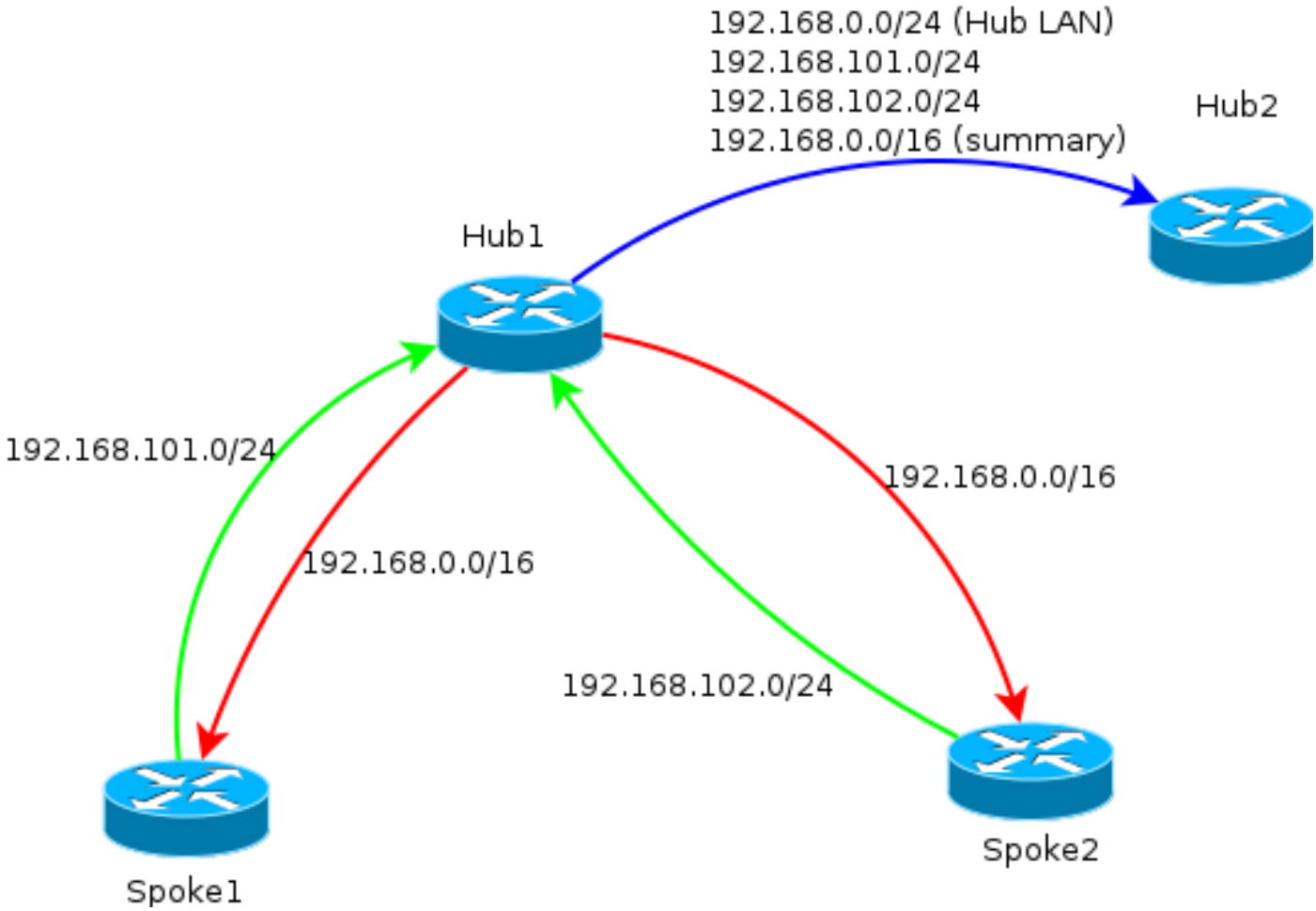
此輸出來自LAN IP地址為192.168.0.1的集線器1。

```
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
neighbor Spokes fall-over
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

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

本質上，這就是我們所做的：

- 本地FlexVPN地址池在BGP偵聽範圍內。
- 本地網路為192.168.0.0/24。
- 僅向輻條通告彙總。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。
- 所有特定字首都會通告給另一個集線器。因為它也是iBGP連線，因此需要路由反射器配置。

此圖表示一個FlexVPN雲中輻條和集線器之間的BGP字首交換。



附註：在圖中，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。

驗證

由於每個分支都保留與兩個集線器的關聯，因此使用**show crypto ikev2 sa**命令可看到兩個IKEv2會話。

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

要檢視路由協定資訊，請輸入以下命令：

```
show bgp ipv4 unicast

show bgp summary
```

在輻條上，您應該看到從集線器收到摘要首碼，並且到兩個集線器的連線都處於活動狀態。

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, 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
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

疑難排解

有兩個主要模組需要排除：

- 網際網路金鑰交換(IKE)
- 網際網路通訊協定安全(IPsec)

以下是相關的show命令：

```
show crypto ipsec sa

show crypto ikev2 sa
```

以下是相關的debug指令：

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

以下是相關的路由通訊協定：

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```