FlexVPN:集中星型部署中的IPv6配置示例

目錄

簡介

本文檔介紹在IPv6環境中使用Cisco IOS® FlexVPN分支和中心部署的常見配置。它擴展了FlexVPN中討論的概念：IPv6基本LAN到LAN配置。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS FlexVPN
- 路由協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科第二代整合多業務路由器(ISR G2)
- Cisco IOS軟體版本15.3（或版本15.4T，用於使用IPv6的動態輻射點到輻射點隧道）

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

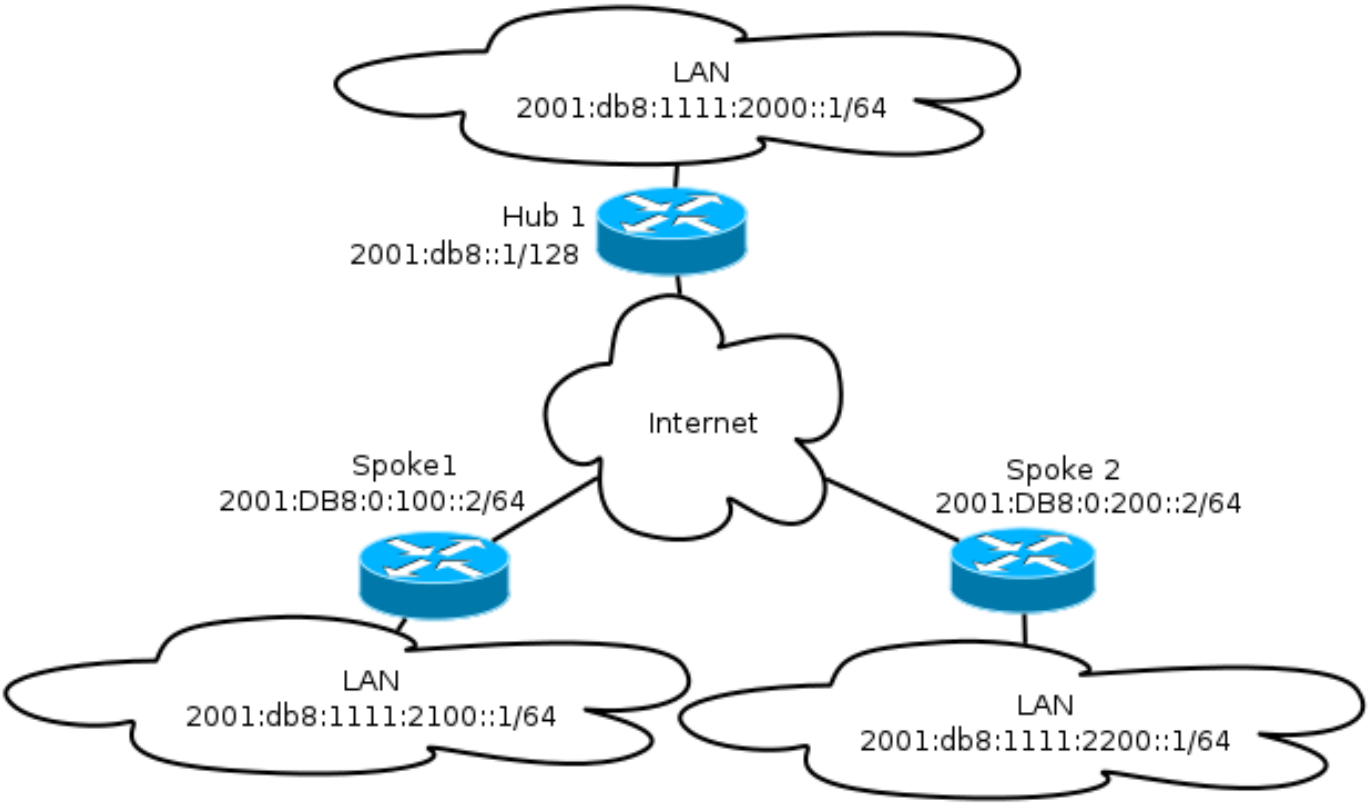
附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

雖然此組態範例和網路圖使用IPv6作為傳輸網路，但FlexVPN部署中通常使用通用路由封裝(GRE)。使用GRE而不是IPsec使管理員能夠通過相同的隧道運行IPv4或IPv6或同時運行IPv6和/或IPv6，而不管傳輸網路如何。

網路圖表

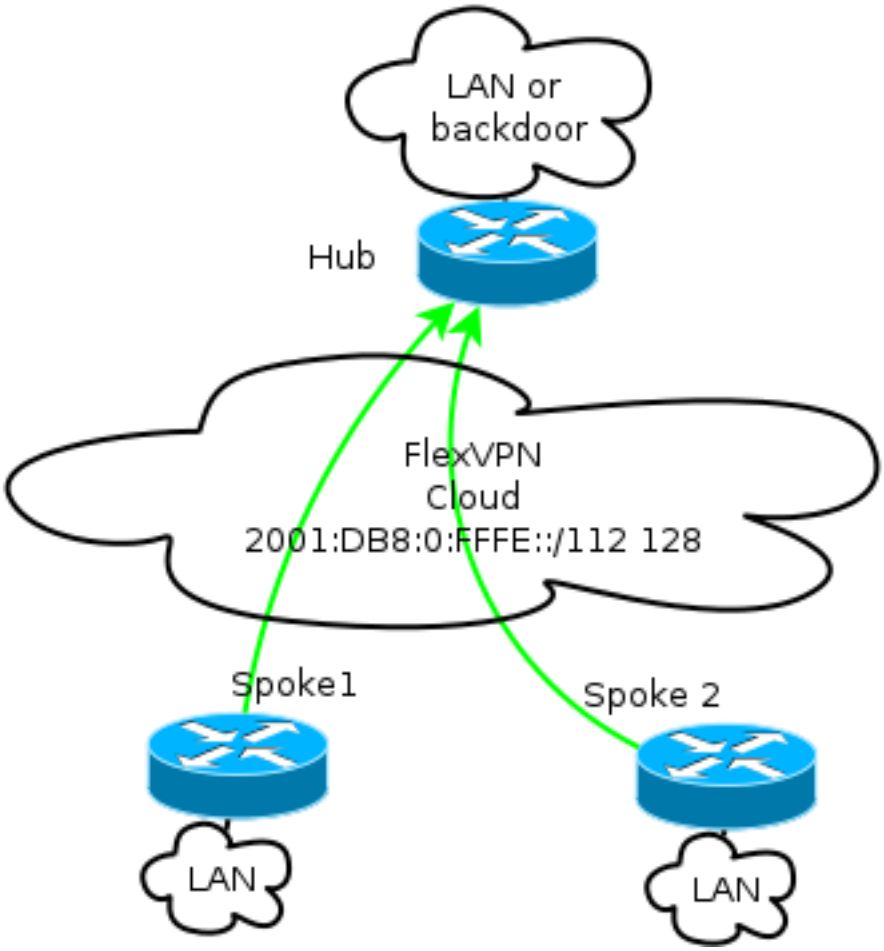
傳輸網路

以下是此範例中使用的傳輸網路圖表：



重疊網路

以下是此範例中使用的基本重疊網路拓撲圖：



每個分支都從/112地址池中分配，但接收到/128地址。因此，符號「/112 128」用於集線器的IPv6池配置。

組態

此配置顯示了通過IPv6主幹運行的IPv4和IPv6重疊。

與使用IPv4作為骨幹網的示例相比，請注意，應使用**tunnel mode**命令來更改節點並適應IPv6傳輸。

Cisco IOS軟體版本15.4T將引入通過IPv6的分支到分支隧道功能，該版本尚未提供。

路由通訊協定

對於大型部署，思科建議使用內部邊界閘道通訊協定(iBGP)在分支和集線器之間進行對等，因為iBGP是最具擴充性的路由通訊協定。

邊界網關協定(BGP)偵聽範圍不支援IPv6範圍，但它確實簡化了IPv4傳輸的使用過程。雖然在這種環境中使用BGP是可行的，但此配置說明了一個基本示例，因此選擇了增強型內部網關路由協定(EIGRP)。

集線器配置

與早期的示例相比，此配置包括使用新的傳輸協定。

為了配置集線器，管理員需要：

- 啟用單播路由。
- 設定傳輸路由。
- 調配要動態分配的新IPv6地址池。池為2001:DB8:0:FFFE::/112;16位允許65,535台裝置定址。
- 為下一跳解析協定(NHRP)配置啟用IPv6，以便在重疊中允許IPv6。
- 考慮金鑰環中的IPv6編址以及加密配置中的配置檔案。

在本示例中，集線器向所有分支通告EIGRP摘要。

思科建議不要在FlexVPN部署中的虛擬模板介面上使用摘要地址；但是，在動態多點VPN(DMVPN)中，這不僅很常見，而且被認為是最佳實踐。請參閱FlexVPN遷移：在同一裝置上從DMVPN硬移動到FlexVPN:已更新中心配置以瞭解詳細資訊。

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
```

```
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
 distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
 network 10.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
 distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```

分支配置

與hub配置一樣，管理員需要調配IPv6定址、啟用IPv6路由並新增NHRP和加密配置。

將EIGRP和其他路由協定用於分支到分支對等是可行的。但是，在典型場景中，不需要使用協定，這可能會影響可擴充性和穩定性。

在本示例中，路由配置僅保持分支和集線器之間的EIGRP鄰接關係，唯一非被動介面是Tunnel1介面：

```
ipv6 unicast-routing
ipv6 cef

crypto logging session

crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

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 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

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
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

在分支上建立路由協定條目時，請遵循以下建議：

1. 允許路由通訊協定透過與集線器的連線（在本案例中為Tunnel1介面）建立關係。通常不需要在分支之間建立路由鄰接關係，因為在大多數情況下這會顯著增加複雜性。

2. 僅通告本地LAN子網，並在集線器分配的IP地址上啟用路由協定。請注意不要通告大型子網，因為它可能會影響輻射到輻射點的通訊。

此示例反映了Spoke1上對EIGRP的兩種建議：

```
router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel1

ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

驗證

使用本節內容，確認您的組態是否正常運作。

附註：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。

分支到中心會話

在分支裝置和中心裝置之間正確配置的會話有一個Internet金鑰交換版本2(IKEv2)會話，該會話處於開啟狀態，並且有一個可以建立鄰接關係的路由協定。在本示例中，路由協定是EIGRP，因此有兩個EIGRP命令：

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/1945 sec

Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                  14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                  11 00:21:05   11  1398  0  26
```

在IPv4中，EIGRP使用分配給對等體的IP地址；在上一個示例中，它是集線器IP地址10.1.1.1。

IPv6使用本地鏈路地址；在本示例中，中心是FE80::A8BB:CCFF:FE00:6600。使用**ping**命令驗證集線器是否可通過其本地連結IP連線：

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

分支到分支會話

分支到分支會話按需動態啟動。使用簡單的ping命令可觸發作業階段：

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

要確認直接的輻射到輻射連線，管理員需要：

- 驗證動態分支到分支會話是否觸發新的虛擬訪問介面：

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
```

- 驗證IKEv2會話狀態：

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/3275 sec

Tunnel-id    fvrf/ivrf              Status
2          none/none             READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8:0:200::2/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/665 sec
```

請注意，有兩個作業階段可用：一個輻條到中心點，一個輻條到輻條。

- 驗證NHRP:

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

輸出顯示，2001:DB8:1111:2200::/64（Spoke2的LAN）可通過2001:DB8:0:FFFE::（即Spoke2的Tunnel1介面上的協商IPv6地址）獲得。Tunnel1介面可通過非廣播多路訪問(NBMA)地址2001:db8:0:200::2獲得，該地址是靜態分配給Spoke2的IPv6地址。

- 驗證流量是否通過該介面：

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
  remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
  current_peer 2001:DB8:0:200::2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
   #pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- 驗證路由路徑和CEF設定：

```
Spoke1#show ipv6 route
(...)
D   2001:DB8:1111:2200::/64 [90/27161600]
    via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
    via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

> **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debug命令可協助您進行疑難排解：

- FlexVPN/IKEv2和IPsec: **debug crypto ipsecdebug crypto ikev2 [packet|internal]**
- NHRP（輻射對輻射）：
  - **debug nhrp pack**
  - **debug nhrp extension**
  - **debug nhrp cache**
  - **debug nhrp route**

如需這些命令的詳細資訊，請參閱Cisco IOS主機命令清單、所有版本。