FlexVPN:中心辐射型部署中的IPv6配置示例

目录

简介

本文档介绍在IPv6环境中使用Cisco IOS® FlexVPN分支和中心部署的常见配置。它扩展了FlexVPN中讨论的概念：IPv6基本LAN到LAN配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IOS FlexVPN
- 路由协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 第2代思科集成多业务路由器(ISR G2)
- Cisco IOS软件版本15.3（或版本15.4T，用于使用IPv6的动态分支到分支隧道）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

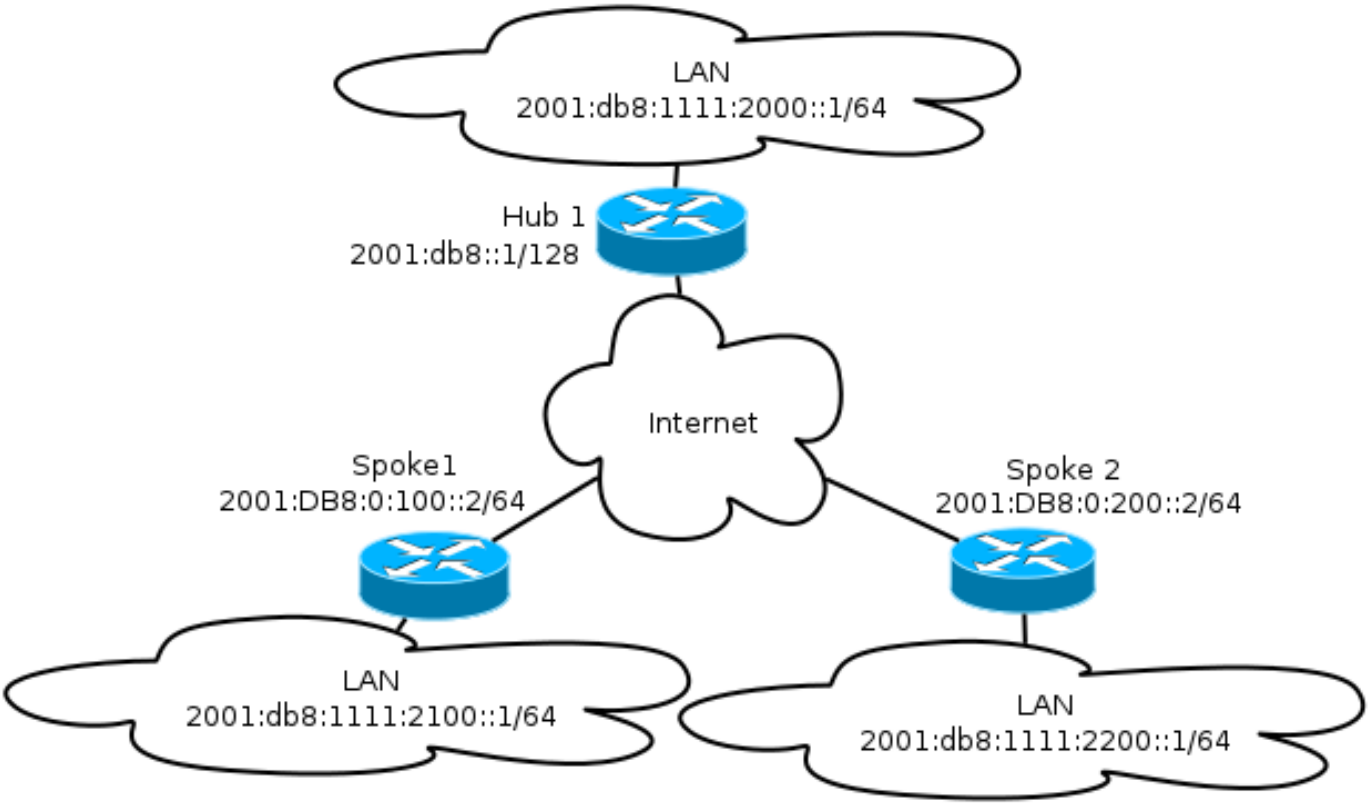
注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

虽然此配置示例和网络图使用IPv6作为传输网络，但FlexVPN部署中通常使用通用路由封装(GRE)。使用GRE而非IPsec，管理员可以通过相同隧道运行IPv4或IPv6或两者，而不管传输网络如何。

网络图

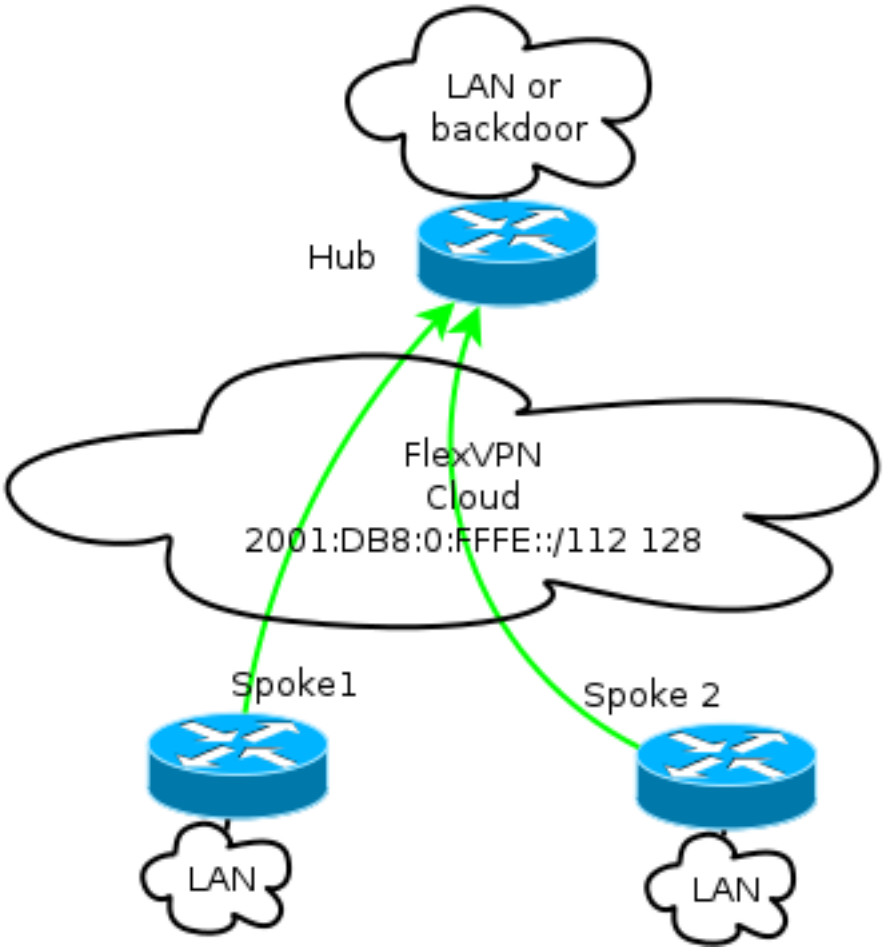
传输网络

以下是本示例中使用的传输网络图：



重叠网络

以下是本示例中使用的基本重叠网络拓扑图：



每个分支都从地址池/112分配，但会收到地址/128。因此，在集线器的IPv6池配置中使用记法“/112 128”。

配置

此配置显示通过IPv6主干工作的IPv4和IPv6重叠。

与使用IPv4作为主干的示例相比，请注意，应使用**tunnel mode**命令来更改节点并适应IPv6传输。

IPv6上的分支到分支隧道功能将在Cisco IOS软件版本15.4T中引入，该版本目前尚不可用。

路由协议

思科建议您使用内部边界网关协议(iBGP)在分支和集线器之间对等进行大型部署，因为iBGP是最可扩展的路由协议。

边界网关协议(BGP)侦听范围不支持IPv6范围，但它通过IPv4传输简化了使用。虽然在这种环境中使用BGP是可行的，但此配置说明了一个基本示例，因此选择了增强型内部网关路由协议(EIGRP)。

中心配置

与较早的示例相比，此配置包括使用新的传输协议。

要配置集线器，管理员需要：

- 启用单播路由。
- 调配传输路由。
- 调配要动态分配的新IPv6地址池。池为2001:DB8:0:FFFE::/112;16位可为65,535台设备寻址。
- 为下一跳解析协议(NHRP)配置启用IPv6，以便在重叠中允许IPv6。
- 在密钥环和加密配置中说明IPv6编址。

在本例中，集线器会向所有分支通告EIGRP摘要。

思科不建议在FlexVPN部署中使用虚拟模板接口上的汇总地址；但是，在动态多点VPN(DMVPN)中，这不仅很常见，而且被视为最佳实践。请参阅FlexVPN迁移：在同一设备上从DMVPN硬性移动到FlexVPN:已更新中心配置以了解详细信息。

```
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

与集线器配置一样，管理员需要调配IPv6编址、启用IPv6路由，并添加NHRP和加密配置。

使用EIGRP和其他路由协议进行分支对分支对等是可行的。但是，在典型场景中，不需要这些协议，可能会影响可扩展性和稳定性。

在本例中，路由配置仅保留分支和中心之间的EIGRP邻接关系，唯一非被动接口是Tunnel1接口：

```
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
```

在辐条上创建路由协议条目时，请遵循以下建议：

1. 允许路由协议通过连接（本例中为Tunnel1接口）与集线器建立关系。一般不希望在辐条之间建立路由邻接关系，因为这在大多数情况下会显着增加复杂性。

2. 仅通告本地LAN子网，并在集线器分配的IP地址上启用路由协议。请小心不要通告大型子网，因为它可能会影响分支到分支通信。

本示例反映了Spoke1上EIGRP的两个建议：

```
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
```

验证

使用本部分可确认配置能否正常运行。

注意：[命令输出解释程序工具（仅限注册用户）支持某些](#) **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

分支到中心会话

在分支设备和中心设备之间正确配置的会话具有已启用的互联网密钥交换版本2(IKEv2)会话，并具有可建立邻接关系的路由协议。在本例中，路由协议是EIGRP，因此有两个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使用分配的IP地址对等；在上一个示例中，它是集线器IP地址10.1.1.1。

IPv6使用本地链路地址；在本例中，集线器是FE80::A8BB:CCFF:FE00:6600。使用ping命令以验证可以通过其本地链路IP到达集线器：

```
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
```

辐射到辐射会话

分支到分支会话按需动态启动。使用简单ping 命令以触发会话：

```
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
```

要确认直接分支到分支的连接，管理员需要：

- 验证动态分支到分支会话是否触发新的虚拟访问接口：

```
%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
```

- 验证IKEv2会话状态：

```
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
```

请注意，有两个会话可用：一个分支到中心，一个分支到分支。

- 验证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
```

输出显示，2001:DB8:1111:2200::/64（Spoke2的LAN）可通过2001:DB8:0:FFFE::获得，这是Spoke2的Tunnel1接口上协商的IPv6地址。Tunnel1接口可通过非广播多路访问(NBMA)获得)地址2001:db8:0:200::2，即静态分配给Spoke2的IPv6地址。

- 检验流量是否通过该接口传输：

```
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
(...)
```

- 检验路由路径和CEF设置：

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

> **注意**：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

以下debug命令可帮助您排除故障：

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

有关这些命令的详细信息，请参阅Cisco IOS主命令列表，所有版本。