采用双云方法的冗余中心设计中的FlexVPN分支配置示例

目录

简介

本文档介绍在多个集线器可用的情况下，如何使用FlexVPN客户端配置块在FlexVPN网络中配置辐条。

先决条件

要求

Cisco 建议您了解以下主题：

- FlexVPN
- 思科路由协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科G2系列集成多业务路由器(ISR)
- Cisco IOS®版本15.2M

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

为实现冗余，分支可能需要连接到多个集线器。辐射端的冗余允许在中心端进行连续操作，而无单点故障。

使用分支配置的两种最常见的FlexVPN冗余中心设计是：

- **双云方法**，辐射点始终有两个独立的通道可活动到两个中心。
- **故障切**换方法，其中分支在任意给定时间点具有一个活动隧道和一个中心。

这两种方法都有一组独特的优点和缺点。

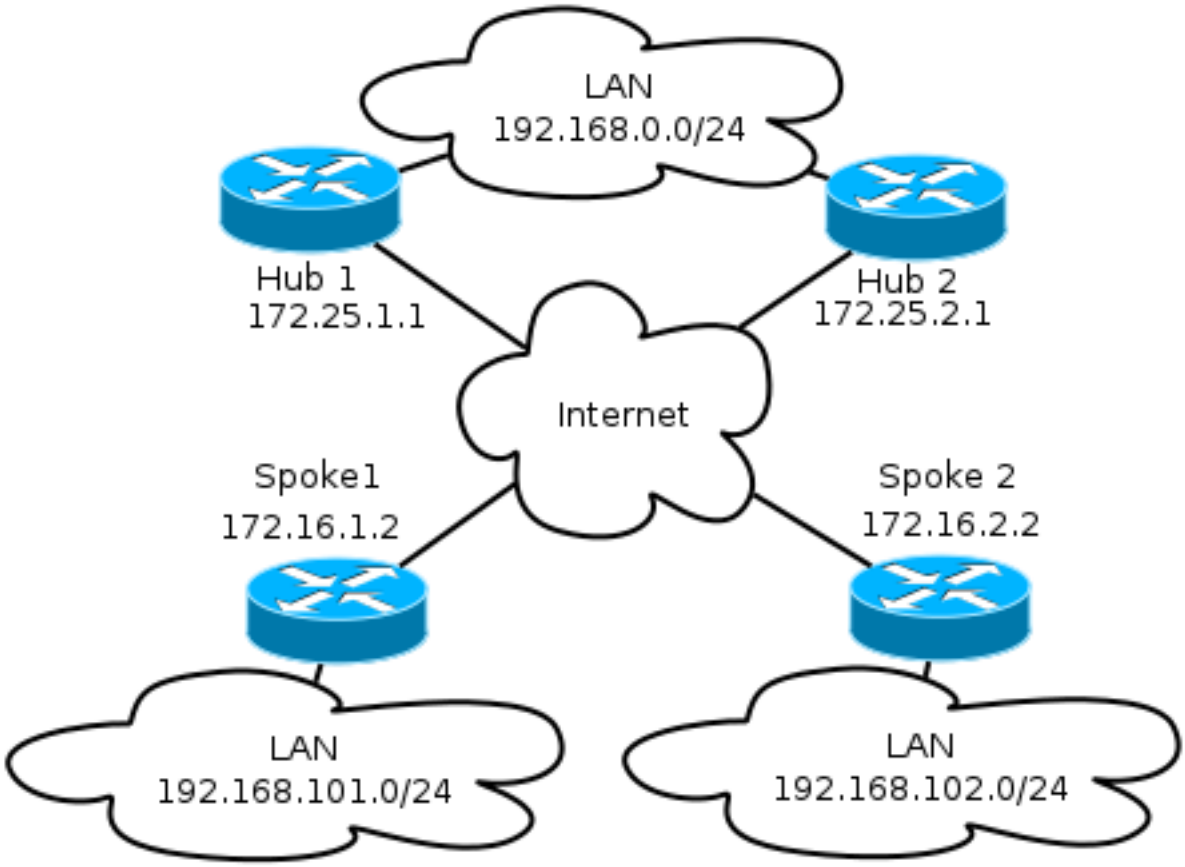
方法	优点	缺点
双云	• 基于路由协议计时器，在故障期间更快恢复 • 在集线器之间分配流量的可能性更大，因为与两个集线器的连接都处于活动状态	• 辐射型同时资源
故障转移	• 轻松配置 — 内置于FlexVPN • 在发生故障时不依赖路由协议	• 更慢的恢复）对象跟踪 • 所有流量都

本文档介绍第一种方法。此配置的方法类似于动态多点VPN(DMVPN)双云配置。中心辐射点的基本配置基于从DMVPN到FlexVPN的迁移文档。请参阅FlexVPN迁移：有关此配置的说明，请在同一设备上硬从DMVPN移动到FlexVPN文章。

网络图

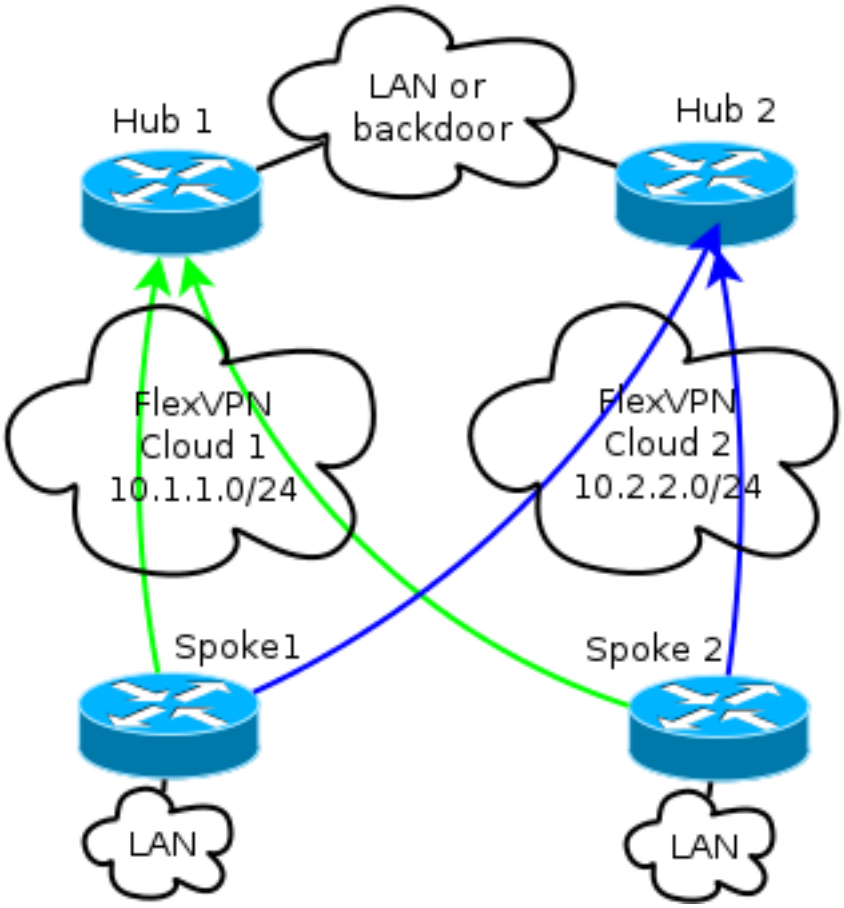
传输网络

此图说明了FlexVPN网络中通常使用的基本传输网络。



重叠网络

该图说明了具有逻辑连接的重叠网络，该网络显示了故障切换应如何工作。在正常操作期间，分支1和分支2与两个中心保持关系。发生故障时，路由协议会从一个集线器切换到另一个集线器。



注意：在图中，绿色线显示与集线器1的互联网密钥交换版本2(IKEv2)/Flex会话的连接和方向，蓝色线指示与集线器2的连接。

两个集线器在重叠云中保留单独的IP编址。/24编址表示为此云分配的地址池，而不是实际接口编址。这是因为FlexVPN中心通常为分支接口分配动态IP地址，并依赖于通过FlexVPN授权块中的路由命令动态插入的路由。

分支配置

分支隧道接口配置

本示例中使用的典型配置只是两个具有两个独立目标地址的隧道接口。

```
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
```

为了允许分支到分支隧道正确形成，需要虚拟模板(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
```

分支使用未编号接口，指示虚拟路由和转发(VRF)中的LAN接口，在本例中为全局接口。但是，最好参考环回接口。这是因为环回接口在几乎所有情况下都保持在线。

分支边界网关协议(BGP)配置

由于思科建议iBGP作为要在重叠网络中使用的路由协议，因此本文档仅提及此配置。

注意：分支必须保留到两个集线器的BGP可达性。

```
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没有主集线器或辅助集线器概念。管理员决定路由协议是首选一个集线器还是执行负载均衡。

辐射型故障转移和融合注意事项

为了将辐条检测故障所需的时间降至最低，请使用以下两种典型方法。

- 缩短BGP计时器。默认保持时间会导致故障切换。
- 配置BGP故障切换，本文将讨论BGP支持以快速对等会话停用。
- 请勿使用双向转发检测(BFD)，因为在大多数FlexVPN部署中不建议使用它。

分支到分支隧道和故障转移

分支到分支隧道使用下一跳解析协议(NHRP)快捷方式交换。Cisco IOS表示这些快捷方式是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
```

当BGP连接到期时，这些路由不会过期；相反，它们被保留为NHRP保持时间，默认为两小时。这意味着活动的分支到分支隧道即使在发生故障时仍保持运行。

集线器配置

本机地址池

如网络图部**分所**述，两个集线器都保留单独的IP编址。

集线器1

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

集线器2

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

集线器BGP配置

集线器BGP配置与以前的示例相似。

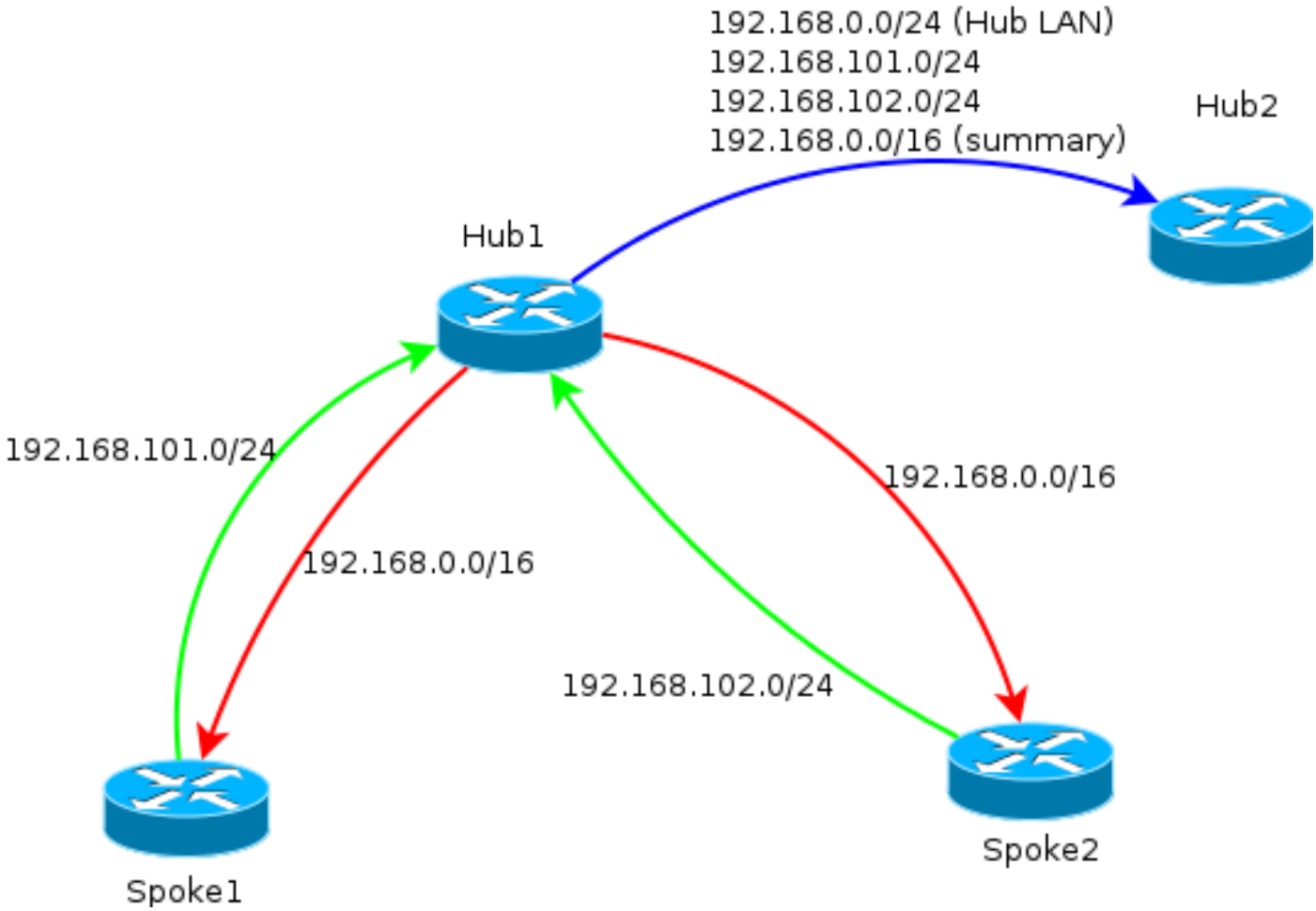
此输出来自LAN IP地址为192.168.0.1**的集线器1**。

```
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
```

从本质上讲，这就是所做的：

- 本地FlexVPN地址池在BGP侦听范围内。
- 本地网络为192.168.0.0/24。
- 汇总仅通告给辐条。聚合地址配置通过null0接口为该前缀创建静态路由，该接口是用于防止路由环路的丢弃路由。
- 所有特定前缀都通告给其他集线器。由于它也是iBGP连接，因此需要配置路由反射器。

此图表示一个FlexVPN云中的分支和集线器之间的BGP前缀交换。



注意：在图中，绿线表示辐条向集线器提供的信息，红线表示每个集线器向辐条提供的信息（仅摘要），蓝线表示集线器之间交换的前缀。

验证

由于每个分支都保留与两个集线器的关联，因此使用show crypto ikev2 sa命令可**以看到两个IKEv2**会话。

```
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
```

要查看路由协议信息，请输入以下命令：

```
show bgp ipv4 unicast

show bgp summary
```

在辐条上，您应该看到从集线器收到汇总前缀，并且到两个集线器的连接处于活动状态。

```
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
```

故障排除

有两个主要块要进行故障排除：

- Internet 密钥交换 (IKE)
- 互联网协议安全(IPsec)

以下是相关的show命令：

```
show crypto ipsec sa

show crypto ikev2 sa
```

以下是相关的debug命令：

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

以下是相关路由协议：

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

show bgp summary
```