采用FlexVPN客户端块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。

背景信息

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，在故障中更快恢复 • 在集线器之间分配流量的可能性更大，因为两个集线器的连接都处于活动状态	• 辐射型同时维资源
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	• 更慢的恢复时）对象跟踪 • 所有流量都必

本文档介绍第二种方法。

配置

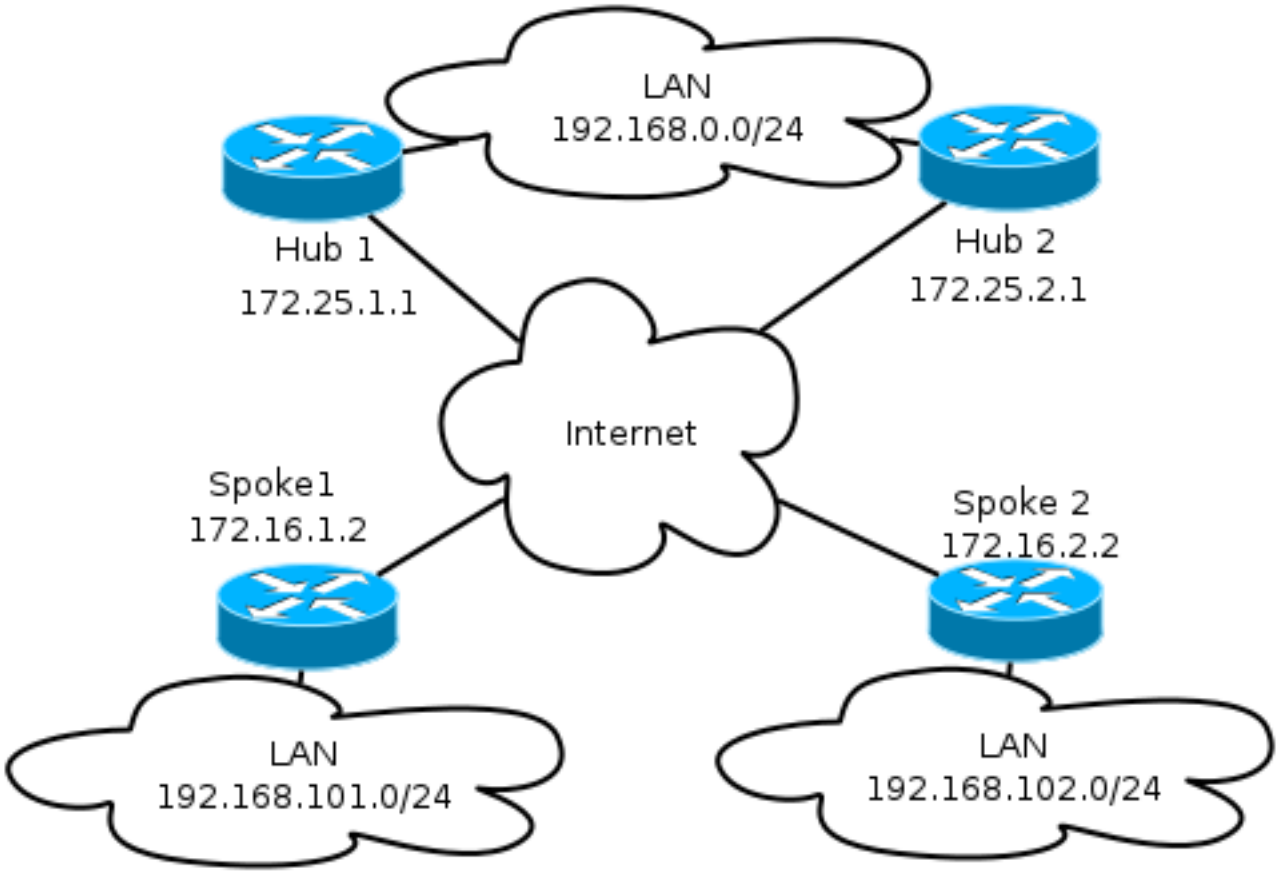
> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

这些图显示了传输和重叠拓扑图。

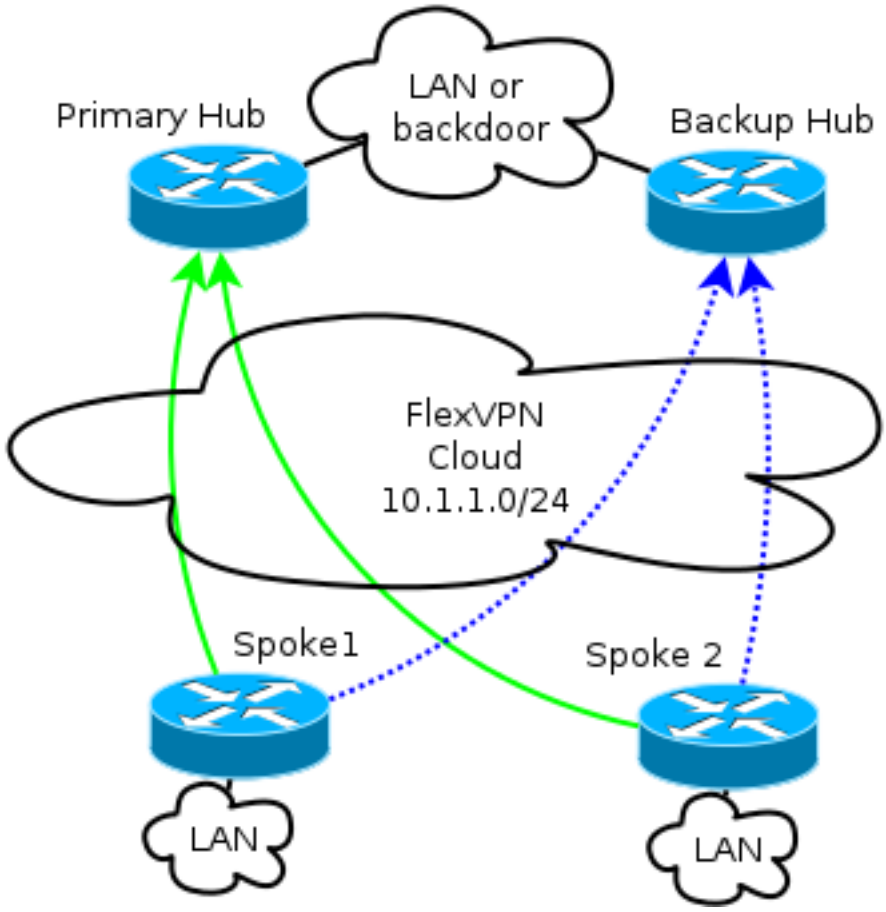
传输网络

此图说明了FlexVPN网络中通常使用的基本传输网络。



重叠网络

下图说明具有逻辑连接的重叠网络，该网络显示故障切换应如何工作。在正常操作期间，辐条1和辐条2仅与一个中心保持关系。



注意：在图中，绿色的实线显示主互联网密钥交换版本2(IKEv2)/Flex会话的连接和方向，蓝色的虚线表示在主集线器的互联网密钥交换(IKE)会话失败时备份连接。

/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。

分支和中心的基本配置

中心辐射点的基本配置基于从动态多点VPN(DMVPN)到FlexVPN的迁移文档。此配置在FlexVPN迁移中有所描述：“Hard Move from DMVPN to FlexVPN on Same Devices(在同一设备上从DMVPN硬移到FlexVPN)”文章。

分支配置调整

分支配置 — 客户端配置块

分支配置必须由客户端配置块扩展。

在基本配置中，指定了多个对等体。优先级最高（数量最小）的对等体优先于其他对等体。

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
```

```
client connect Tunnel1
```

必须更改隧道配置，才能根据FlexVPN客户端配置块动态选择隧道目标。

```
interface Tunnel1
 tunnel destination dynamic
```

必须记住，FlexVPN客户端配置块与接口关联，而不是与IKEv2或互联网协议安全(IPsec)配置文件关联。

客户端配置块提供多个选项以调整故障切换时间和操作，包括跟踪对象使用、拨号备份和备份组功能。

使用基本配置时，辐条依靠DPD来检测辐条是否无响应，一旦对等体被声明为失效，它就会触发更改。使用DPD的选项不是快速的，因为DPD的工作方式。管理员可能希望通过对象跟踪或类似的增强功能增强配置。

有关详细信息，请参阅**Cisco IOS配置指南**的**FlexVPN客户端配置**一章，该章节在本文档末尾的“**相关信息**”部分中进行链接。

完整分支配置 — 参考

```
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
```

中心配置

虽然大多数集线器配置保持不变，但必须解决以下几个方面的问题。其中大多数辐射点与一个或多个辐射点连接到一个集线器而其他辐射点与另一个集线器保持关系的情况有关。

分支地址

由于分支从集线器获取IP地址，因此通常需要集线器从不同子网或子网的不同部分分配地址。

例如：

集线器1

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

集线器2

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

这可防止重叠创建，即使地址未路由到FlexVPN云外，也可能影响故障排除。

中心重叠地址

两个集线器在虚拟模板接口上可以保留相同的IP地址；但是，在某些情况下，这会影响故障排除。此设计选择使部署和规划更加容易，因为辐条必须只有一个边界网关协议(BGP)的对等地址。

在某些情况下，可能并不需要它。

路由

集线器必须交换有关所连接的辐条的信息。

集线器必须能够交换其连接的设备的特定路由，并仍能向辐条提供总结。

由于思科建议您将iBGP与FlexVPN和DMVPN配合使用，因此仅显示该路由协议。

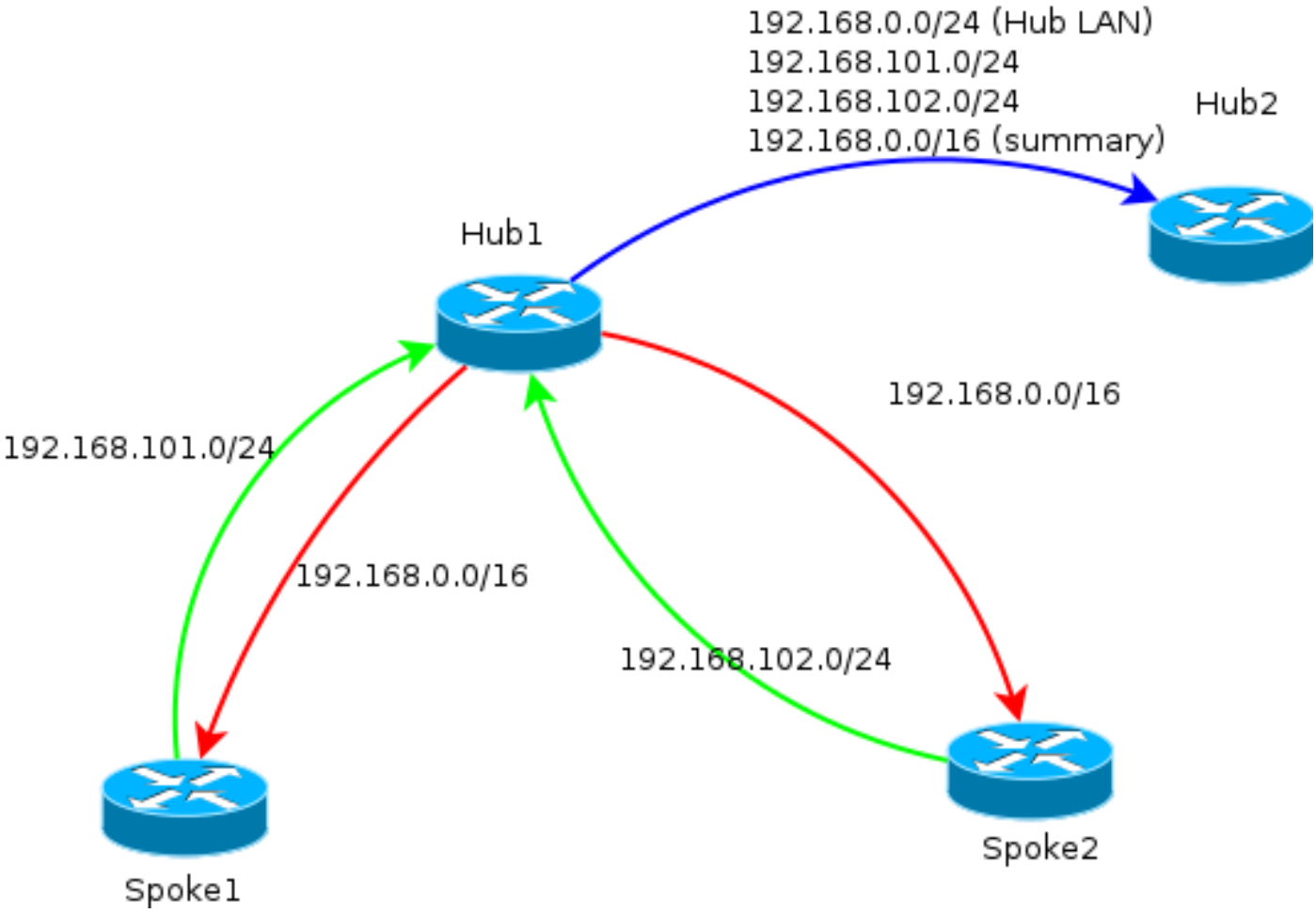
```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
```

```
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
```

此配置允许：

- 从分配给分支的地址中动态侦听程序
- 192.168.0.0/24**广告网络**
- 向所有分支通告**192.168.0.0/16**的总结路由。聚合地址配置通过null0接口为该前缀创建静态路由，该路由是用于防止路由环路的丢弃路由。
- 将特定前缀转发到另一个集线器
- 路由反射器客户端，确保集线器之间交换从辐条获知的信息

此图从其中一个集线器的角度表示此设置中BGP中的前缀交换。



注意：在此图中，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。

网络摘要使用

摘要在某些情况下可能不适用或不理想。在前缀中指定目标IP时请小心，因为iBGP在默认情况下不覆盖下一跳。

建议在频繁更改状态的网络中使用总结。例如，不稳定的Internet连接可能需要摘要，以便：避免删除和添加前缀，限制更新数量，并允许大多数设置正确扩展。

分支到分支隧道

在前面部分提到的场景和配置中，不同集线器上的辐条无法建立直接辐条到辐条隧道。连接到不同集线器的辐条之间的流量通过中心设备传输。

对此，有一个简单的解决方法。但是，它要求在集线器之间启用具有相同网络ID的下一跳解析协议(NHRP)。例如，如果在集线器之间创建点对点通用路由封装(GRE)隧道，就可以实现此目的。然后，不需要IPsec。

验证

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。

show crypto ikev2 **sa命令会**通知您分支当前连接的位置。

show crypto ikev2 client flexvpn命令允许管理员了解FlexVPN客户端操作的当前状态。

```
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 **configuration**成功进行故障切换后，会在分支设备上记录以下输出：

```
%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
```

在此输出中，分支断开与中心**172.25.1.1**的连接，Flex_Client客户端配置块检测故障并强制连接到**172.25.2.1**（其中出现隧道），并为分支分配IP **10.1.1.177**。

故障排除

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。

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

以下是相关的debug命令：

- debug crypto ikev2
- debug radius

相关信息

- FlexVPN和互联网密钥交换第2版配置指南，思科IOS版本15 M&T
- 技术支持和文档 - Cisco Systems