

FlexVPN在与双重Cloud方法配置示例的冗余集线器设计发言

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[传输网络](#)

[覆盖网络](#)

[辐条配置](#)

[分支隧道接口配置](#)

[分支边界网关协议\(BGP\)配置](#)

[集线器配置](#)

[本机地址池](#)

[集线器BGP配置](#)

[验证](#)

[故障排除](#)

简介

本文描述如何配置在FlexVPN网络的一分支与使用在多个集线器是可用的方案的FlexVPN客户端配置块。

[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：

- Cisco G2系列集成服务路由器(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

为冗余目的，分支也许需要连接到多个集线器。在辐射端的冗余允许连续作业，不用在集线器端的一个单点故障。

使用辐条配置的两最普通的FlexVPN冗余集线器设计是：

- **双重网云方法**，其中分支一直有两个单独的隧道活动对两集线器。
- **故障切换方法**，其中分支有一活动通道用一台集线器在所有给的此刻。

两个途径有特有的利弊。

方法	专业人员	缺点
双倍网云	<ul style="list-style-type: none"> • 在失败期间的更加快速的恢复，根据路由协议计时器 • 分发给在集线器中的流量的更多possibilities，因为对两集线器的连接是活跃的 	<ul style="list-style-type: none"> • 分支同时保养会
故障切换	<ul style="list-style-type: none"> • 容易配置-设置到FlexVPN • 在路由协议在失败里不取决于 	<ul style="list-style-type: none"> • 更加缓慢的恢复跟踪 • 所有流量被迫到

本文描述第一方法。对此配置的方法类似于动态多点VPN (DMVPN)双重网云配置。星型网基本配置根据从DMVPN的迁移文档到FlexVPN。参考[FlexVPN迁移：从DMVPN的硬移动到在同样设备条款的FlexVPN](#)此配置的说明的。

网络图

传输网络

此图表说明用于FlexVPN网络典型地的基本传输网络。

覆盖网络

图表说明与显示的逻辑连接的覆盖网络故障切换如何应该工作。在正常操作时，分支1和分支2维护一关系用两集线器。在失败，从一台集线器的路由协议交换机到另一个。

Note:在图表中，绿色线路显示互联网密钥交换版本2 (Hub1的IKEv2)/Flex会话和蓝线的连接和方向指示对集线器2的连接。

两集线器在重叠网云保留分开的IP寻址。/24寻址代表为此网云分配的地址池，不是实际接口编址。这是因为FlexVPN集线器典型地分配分支接口的一个动态IP地址，并且依靠通过路由in命令动态地插入的路由FlexVPN授权块。

辐条配置

分支隧道接口配置

用于此示例的典型配置是完全与两独立的目的地地址的两个隧道接口。

```
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spoke-to-spoke通道适当地形成，虚拟模板(VT)是需要的。

```
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
```

分支使用指示在虚拟路由和转发的未编号的接口(VRF)的LAN接口，在这种情况下全局。然而，参考回环接口也许是更加好的。这是因为回环接口依然是联机在几乎所有情况下。

分支边界网关协议(BGP)配置

因为思科推荐iBGP作为用于覆盖网络的路由协议，本文提及仅此配置。

Note:Spoke必须保留BGP可接通性到两集线器。

```
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
```

FlexVPN在此配置方面没有一个主要的或附属集线器概念。管理员决定路由协议是否更喜欢在别的一台集线器或，在某些情况下，执行负载平衡。

分支故障切换和收敛考虑事项

为了最小化它为花费的时间发言检测失败，使用这两个典型的方法。

- 缩短BGP计时器。默认hold-time原因故障切换。
- 配置BGP FALL在，在此条款discused，[快速对等会话去活的BGP技术支持](#)。
- 因为在多数FlexVPN部署，没有推荐请勿使用双向转发检测(BFD)。

spoke-to-spoke通道和故障切换

spoke-to-spoke通道使用下一跳解析协议(NHRP)快捷方式交换。Cisco IOS表明那些快捷方式是NHRP路由，例如：

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

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

当BGP连接超时，那些路由不超时;反而，他们为NHRP持有时间保持，默认情况下是两个小时。这意味着活动spoke-to-spoke通道在失败里依然是运转中。

集线器配置

本机地址池

如Network Diagram部分所述，两集线器保留分开的IP寻址。

Hub1

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

Hub2

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

集线器BGP配置

集线器BGP配置依然是类似于前面的示例。

此输出来自Hub1用192.168.0.1的LAN IP地址。

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

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

实质上，这是什么执行：

- 本地FlexVPN地址池是在Bgp listen范围。
- 本地网络是192.168.0.0/24。
- 摘要仅通告对spoke。Aggregate-address配置通过null0接口创建该前缀的静态路由，是丢弃路由使用为了防止路由环路。
- 所有特定前缀通告到另一台集线器。因为它也是iBGP连接，要求路由反射器配置。

此图表代表BGP前缀交换在spoke和集线器之间的在一FlexVPN网云。

Note:在图表中，绿色线路描述spoke提供的信息给集线器，红线描述每台集线器提供的信息给spoke (仅摘要)，并且蓝线代表前缀交换在集线器之间。

验证

因为每分支保留关联用两集线器，两IKEv2会话在显示crypto sa ikev2命令看到。

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

```
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
```

为了查看路由协议信息，输入这些命令：

```
show bgp ipv4 unicast
```

```
show bgp summary
```

在spoke，您应该看到概略的前缀从集线器接收，并且对两集线器的连接是活跃的。

```
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

有排除故障的两主要块：

- Internet 密钥交换 (IKE)
- Internet协议安全性(IPsec)

这是相关显示命令：

```
show crypto ipsec sa
```

```
show crypto ikev2 sa
```

这是相关调试指令：

```
debug crypto ikev2 [internal|packet]
```

```
debug crypto ipsec
```

```
debug vtemplate event
```

这是相关路由协议：

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

```
show bgp summary
```