在不同集线器上从DMVPN到FlexVPN的硬迁移

目录

简介

本文档提供有关如何从当前存在的动态多点VPN(DMVPN)网络迁移到不同集线器设备上的FlexVPN的信息。两个框架的配置在设备上共存。在本文档中，仅显示最常见的场景 — 使用预共享密钥进行身份验证的DMVPN和增强型内部网关路由协议(EIGRP)作为路由协议。在本文档中，演示了向推荐的路由协议边界网关协议(BGP)和不太理想的EIGRP的迁移。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- DMVPN
- FlexVPN

使用的组件

> **注意**：并非所有软件和硬件都支持互联网密钥交换版本2(IKEv2)。 有关详细信息，请参阅Cisco功能导航器。

本文档中的信息基于以下软件和硬件版本：

- 思科集成多业务路由器(ISR)15.2(4)M1版或更高版本
- 思科聚合服务路由器1000系列(ASR1K)3.6.2版本15.2(2)S2或更高版本

较新的平台和软件的一个优势是能够使用下一代加密技术，如高级加密标准(AES)Galois/计数器模式(GCM)在互联网协议安全(IPsec)中进行加密，如请求注解(RFC)4106中所述。AES GCM允许您在某些硬件上实现更快的加密速度。要查看思科关于使用和迁移到下一代加密的建议，请参阅下一代加密文章。

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。

迁移步骤

目前，建议从DMVPN迁移到FlexVPN的方法是使两个框架不能同时运行。此限制计划因ASR 3.10版中将引入的新迁移功能而取消，该功能在思科端的多个增强请求(包括Cisco Bug ID CSCuc08066)下进行跟踪。这些功能应于2013年6月底提供。

在同一设备上同时共存和运行两个框架的迁移称为软迁移，它表示从一个框架到另一个框架的影响最小且故障切换平稳。两个框架的配置共存但不同时运行的迁移称为硬**迁移**。这表示从一个框架切换到另一个框架意味着VPN上缺乏通信，即使通信最少。

在两个不同的集线器之间进行硬迁移

在本文档中，将讨论从当前用于新FlexVPN集线器的DMVPN集线器迁移。此迁移允许已迁移到

FlexVPN的辐条与仍在DMVPN上运行的辐条之间的相互通信，并且可以在多个阶段中分别在每个辐条上执行。

如果路由信息已正确填充，则迁移辐射点和未迁移辐射点之间的通信应保持可能。但是，由于迁移的和未迁移的辐射点不会在彼此之间建立辐射到辐射点隧道，因此可以观察到额外的延迟。同时，迁移的分支应能够在它们之间建立直接的分支到分支隧道。这同样适用于未迁移的辐条。

在此新迁移功能可用之前，请完成以下步骤，以便使用与DMVPN和FlexVPN不同的集线器执行迁移：

1. 检验DMVPN上的连接。
2. 添加FlexVPN配置，并关闭属于新配置的隧道。
3. （在维护窗口期间）在每个辐条上逐个关闭DMVPN隧道。
4. 在与步骤3相同的分支上，取消关闭FlexVPN隧道接口。
5. 检验分支到中心的连接。
6. 验证FlexVPN中的分支到分支连接。
7. 从FlexVPN验证与DMVPN的分支到分支连接。
8. 分别对每个辐条重复步骤3到7。
9. 如果您在步骤5、6或7中描述的验证中遇到任何问题，请关闭FlexVPN接口，并取消关闭DMVPN接口以恢复为DMVPN。
10. 验证已备份DMVPN上的分支到中心通信。
11. 通过备份的DMVPN验证分支到分支通信。

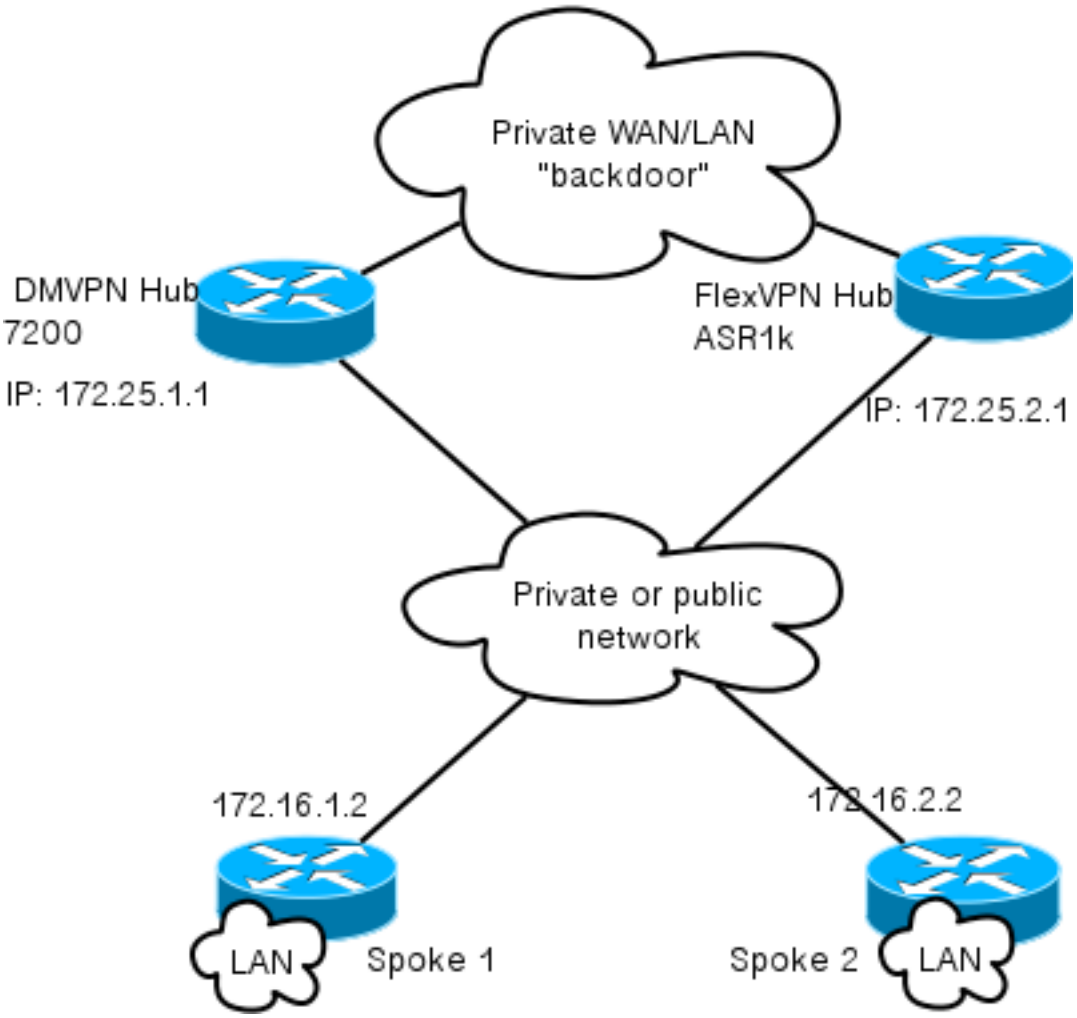
自定义方法

如果由于网络或路由复杂性，以前的方法可能不是最适合您的解决方案，请在迁移前与思科代表展开讨论。与您讨论自定义迁移流程的最佳人选是系统工程师或高级服务工程师。

网络拓扑

传输网络拓扑

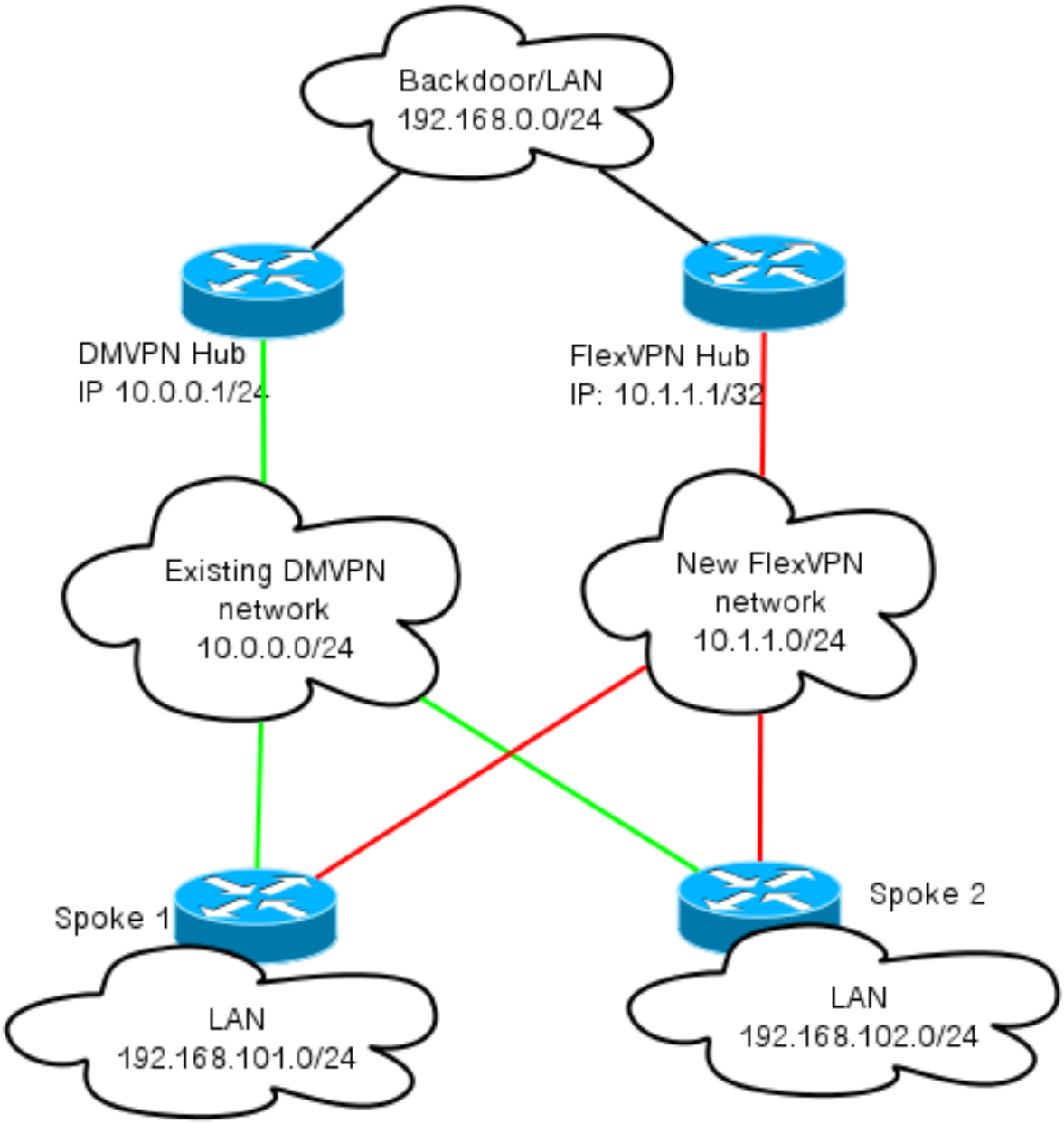
此图显示了Internet上主机的典型连接拓扑。使用集线器的IP地址loopback0(172.25.1.1)来终止DMVPN IPsec会话。新集线器(172.25.2.1)上的IP地址用于FlexVPN。



注意两个集线器之间的链路。此链路对于在迁移期间允许FlexVPN和DMVPN云之间的连接至关重要。它允许已迁移到FlexVPN的辐条与DMVPN网络通信，反之亦然。

重叠网络拓扑

此拓扑图显示了用于重叠的两个独立云：DMVPN（绿色连接）和FlexVPN（红色连接）。显示相应站点的LAN前缀。10.1.1.0/24 子网在接口编址方面并不代表实际的子网，而是代表专用于FlexVPN云的IP空间块。FlexVPN配置部分稍后将讨论其背后的原理。



配置

本节介绍DMVPN和FlexVPN配置。

DMVPN 配置

本节介绍DMVPN中心和分支的基本配置。

预共享密钥(PSK)用于IKEv1身份验证。建立IPsec后，从分支到中心执行下一跳解析协议(NHRP)注册，以便中心可以动态获取分支的非广播多路访问(NBMA)编址。

当NHRP在辐条和中心上执行注册时，可以建立路由邻接关系，并交换路由。在本例中，EIGRP用作重叠网络的基本路由协议。

分支DMVPN配置

在这里，您可以找到DMVPN的基本示例配置，其中PSK身份验证和EIGRP作为路由协议。

```
crypto isakmp policy 10
 encr aes
 authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
 keyring DMVPN_IKEv1
 match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport

crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1

interface Tunnel0

ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

集线器DMVPN配置

在集线器配置中，隧道源自IP地址为172.25.1.1的loopback0。其余是DMVPN集线器的标准部署，EIGRP作为路由协议。

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport
crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
```

```
interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0
```

FlexVPN配置

FlexVPN基于以下相同的基本技术：

- **IPSEC:**与DMVPN中的默认值不同，IKEv2用于协商IPsec安全关联(SA)，而不是IKEv1。IKEv2提供了IKEv1的改进，例如恢复能力和建立受保护数据通道所需的消息数。

- **GRE:**与DMVPN不同，使用静态和动态点对点接口，而且不仅使用一个静态多点GRE接口。此配置可增加灵活性，尤其是针对每分支/每中心行为。

- **NHRP**:在FlexVPN中，NHRP主要用于建立分支到分支通信。辐条不注册到集线器。

- **路由**:由于辐条不向集线器执行NHRP注册，因此必须依靠其他机制来确保集线器和辐条能够双向通信。与DMVPN类似，动态路由协议也可以使用。但是，FlexVPN允许您使用IPsec来引入路由信息。默认为隧道另**一端**的IP地址引入作为/32路由，允许分支到中心直接通信。

在从DMVPN硬迁移到FlexVPN时，两个框架不能在同一设备上同时工作。但是，建议将它们分开。

将它们分为多个级别：

- NHRP — 使用不同的NHRP网络ID（推荐）。
- 路由 — 使用单独的路由进程（推荐）。
- 虚拟路由和转发(VRF)- VRF分离可增加灵活性，但此处未讨论（可选）。

分支FlexVPN配置

与DMVPN相比，FlexVPN中分支配置的一个区别是您可能有两个接口。分支到中心通信需要一个隧道，分支到分支隧道有一个可选隧道。如果您选择不使用动态分支到分支隧道，并且希望所有内容都通过中心设备，则可以删除虚拟模板接口，并从隧道接口删除NHRP快捷方式交换。

请注意，静态隧道接口会根据协商接收IP地址。这样，集线器就可以动态地为分支提供隧道接口IP地址，而无需在FlexVPN云中创建静态编址。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

> **注意**：默认情况下，设置本地身份以使用IP地址。因此，对等体上的对应匹配语句也必须根据地址进行匹配。如果要求根据证书中的可分辨名称(DN)进行匹配，则必须使用证书映射完成匹配。

思科建议您将AES GCM与支持该AES GCM的硬件配合使用。

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport

crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

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
shutdown
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
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
```

公钥基础设施(PKI)是在IKEv2中执行大规模身份验证的推荐方法。但是，只要您知道PSK的局限性，您仍然可以使用PSK。

以下是使用**cisco**作为PSK的示例配置。

```
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
```

FlexVPN集线器配置

通常，中心仅终止动态分支到中心隧道。这就是为什么在集线器配置中找不到FlexVPN的静态隧道接口。而是使用虚拟模板接口。

注意：在中心端，必须指明要分配给分支的池地址。

来自此池的地址稍后会作为每个分支的/32路由添加到路由表中。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 authorization policy default
pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn hub.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

思科建议您将AES GCM与支持该AES GCM的硬件配合使用。

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport
```

注意：在此配置中，AES GCM操作已被注释掉。

```
crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
interface Loopback100
ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip nhrp network-id 2
ip nhrp redirect
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

在IKEv2中进行身份验证时，集线器上和辐条上应用相同的原则。为了实现可扩展性和灵活性，请使用证书。但是，您可以重用与分支上相同的PSK配置。

> **注意**：IKEv2在身份验证方面提供灵活性。一端可以使用PSK进行身份验证，而另一端使用Rivest-Shamir-Adleman签名(RSA-SIG)。

如果要求使用预共享密钥进行身份验证，则配置更改与此处对分支路由器描述的配置更改类似。

集线器间BGP连接

确保集线器知道特定前缀的位置。这变得越来越重要，因为有些分支已迁移到FlexVPN，而另一些分支仍在DMVPN上。

以下是基于DMVPN中心配置的集线器间BGP连接：

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

流量迁移

迁移到BGP作为重叠路由协议[推荐]

BGP是基于单播交换的路由协议。由于其特点，它是DMVPN网络中最佳的扩展协议。

在本示例中，使用内部BGP(iBGP)。

分支BGP配置

分支迁移包括两部分。首先，启用BGP作为动态路由：

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
```

在BGP邻居启动（请参阅下一节）并获知BGP上的新前缀后，您可以将流量从当前DMVPN云转移到新的FlexVPN云。

集线器BGP配置

FlexVPN中心 — 完整BGP配置

在集线器上，为避免单独保留每个分支的邻居关系配置，请配置动态侦听程序。在此设置中

，BGP不启动新连接，但接受来自提供的IP地址池的连接。在本例中，所述池为10.1.1.0/24，即新FlexVPN云中的所有地址。

需要注意两点：

- FlexVPN中心向DMVPN中心通告特定前缀；因此，正在使用未按下的映射。
- 将FlexVPN子网10.1.1.0/24通告到路由表，或确保DMVPN中心将FlexVPN中心视为下一跳。

本文档显示后一种方法。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

router bgp 65001
network 192.168.0.0
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

DMVPN中心 — 完整BGP和EIGRP配置

DMVPN中心上的配置是基本的，因为它仅从FlexVPN中心接收特定前缀并通告从EIGRP获取的前缀。

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

将流量迁移到BGP/FlexVPN

如前所述，您必须关闭DMVPN功能并启动FlexVPN才能执行迁移。

此程序可确保影响最小：

1. 在每个辐条上，分别输入以下内容：

   ```
   interface tunnel 0
    shut
   ```

   此时，请确保没有建立到此分支的IKEv1会话。如果您检查show crypto isakmp sa命令的输出并监控crypto logging session命令生成的系统日志消息，则可以验证此情况。确认后，您可以继续启动FlexVPN。

2. 在同一辐条上，输入以下内容：

```
interface tunnel 1
  no shut
```

验证步骤

IPsec稳定性

评估IPsec稳定性的最佳方法是在启用了crypto logging session配置**命令的情况下**监控系统日志。如果看到会话上下移动，这可能表示IKEv2/FlexVPN级别上的问题，在迁移开始之前必须纠正。

填充BGP信息

如果IPsec稳定，请确保BGP表中填充了来自辐条（在集线器上）的条目和来自集线器（在辐条上）的摘要。 对于BGP，可使用以下命令查看此信息：

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

以下是来自FlexVPN中心的正确信息示例：

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

输出显示，集线器已从每个辐条获取了一个前缀，并且两个辐条都是动态的，并标有星号(*)。它还显示，总共收到来自集线器间连接的四个前缀。

以下是来自辐条的类似信息的示例：

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

辐条已从中心收到两个前缀。在此设置中，一个前缀应是在FlexVPN集线器上通告的摘要。另一个是DMVPN 10.0.0.0/24网络，在DMVPN分支上重分发到BGP。

使用EIGRP迁移到新隧道

EIGRP部署相对简单且收敛快，因此在DMVPN网络中很受欢迎。但是，它的扩展性比BGP更差，并且没有提供许多可供BGP直接开箱使用的高级机制。下一节介绍使用新EIGRP进程迁移到FlexVPN的方法之一。

更新的分支配置

新的自治系统(AS)随单独的EIGRP进程添加：

```
router eigrp 200
network 10.1.1.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel1
```

> **注意**：最好不要在分支到分支隧道上建立路由协议邻接关系。因此，仅使tunnel1(spoke-to-hub)的接口不是被动的。

更新的FlexVPN中心配置

同样，对于FlexVPN集线器，请在适当的AS中准备路由协议，使其与分支上配置的路由协议匹配。

```
router eigrp 200
network 10.1.1.0 0.0.0.255
```

有两种方法可用于向辐条返回摘要。

- 重分布指向null0(首**选选**项)的静态路由。

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

此选项允许控制摘要和重分发，而无需修改集线器的虚拟化技术(VT)配置。这很重要，因为如果与集线器关联的活动虚拟访问，则无法修改集线器的VT配置。

- 在虚拟模板上设置DMVPN样式的摘要地址。

不建议使用*此配*置，因为内部处理和将该摘要复制到每个虚拟访问。此处显示供参考。

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

需要考虑的另一个方面是集线器间路由交换。如果将EIGRP实例重分发到iBGP，则可以执行此

操作。

DMVPN中心 — 更新的BGP配置

配置保持基本。您必须将特定前缀从EIGRP重分发到BGP:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

FlexVPN中心 — 更新的BGP配置

与DMVPN中心类似，在FlexVPN中，您必须将新EIGRP进程的前缀重新分发到BGP:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

将流量迁移到FlexVPN

要执行迁移，必须关闭DMVPN功能并在每个分支上启用FlexVPN（一次一个）。此程序可保证最低影响：

1. 在每个辐条上，分别输入以下内容：

   ```
   interface tunnel 0
    shut
   ```

   此时，请确保此分支上未建立IKEv1会话。如果您检查show crypto isakmp sa命令的输出并监控**crypto logging session命**令生成的系统日志消息，则可**以验证此**情况。确认后，您可以继续启动FlexVPN。
2. 在同一辐条上，输入以下内容：

   ```
   interface tunnel 1
     no shut
   ```

验证步骤

IPsec稳定性

与BGP一样，您必须评估IPsec是否稳定。执行此操作的最佳方法是启用加密日志记录会话**配置命令**来监控系统日志。如果看到会话上下移动，这可能表示IKEv2/FlexVPN级别上的问题，在迁移开始之前必须纠正。

拓扑表中的EIGRP信息

确保EIGRP拓扑表中填充了集线器上的分支LAN条目和分支上的摘要。如果在中心点和分支上输入以下命令，则可以验证此情况：

show ip eigrp [AS_NUMBER] topology

以下是辐条的输出示例：

```
Spoke1#show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
via Rstatic (26112000/0)
via 10.1.1.1 (26240000/128256), Tunnel1

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0

P 192.168.0.0/16, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

输出显示，辐条知道其LAN子网(*斜体*)和这些子网的摘要(**粗体**)。

以下是集线器输出的示例：

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

输出显示，集线器知道辐条的LAN子网（斜体）、它通告的汇总前缀(粗体)，以及每个辐条通过协商分配的IP地址。

其他注意事项

已存在的分支到分支隧道

由于DMVPN隧道接口关闭会导致NHRP条目被删除，因此已存在的分支到分支隧道将被关闭。

清除NHRP条目

FlexVPN中心不依赖来自分支的NHRP注册过程，以了解如何将流量路由回来。但是，动态分支到分支隧道依赖于NHRP条目。

在DMVPN中，如果清除集线器上的NHRP，则可能导致短期连接问题。在FlexVPN中，清除分支上的NHRP将导致与分支到分支隧道相关的FlexVPN IPsec会话断开。清除集线器上的NHRP对FlexVPN会话没有影响。

这是因为，在FlexVPN中，默认情况下：

- 辐条不注册到集线器。
- 集线器仅作为NHRP重定向器工作，不安装NHRP条目。
- NHRP快捷方式条目安装在分支到分支隧道的分支上，并且是动态的。

已知问题说明

分支到分支的流量可能受Cisco Bug ID CSCub07382（仅限注册用户）的影响。

相关信息

- DMVPN到FlexVPN软迁移配置示例
- 技术支持和文档 - Cisco Systems