DMVPN到FlexVPN软迁移配置示例

目录

简介

本文档介绍如何执行软迁移，*其中*动态多点VPN(DMVPN)和FlexVPN在设备上同时工作而无需解决方法，并提供了配置示例。

> **注意**：本文档对FlexVPN迁移中描述的概念进行了扩展：在相同设备上从DMVPN硬迁移到FlexVPN和FlexVPN迁移：从DMVPN硬性移动到FlexVPN在其他中心思科文章。这两份文档都描述了*硬*迁移，这会在迁移过程中对流量造成一些中断。这些文章的局限性是由于Cisco IOS®软件的缺陷，现已得到修正。

先决条件

要求

Cisco 建议您了解以下主题：

- DMVPN
- FlexVPN

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成多业务路由器(ISR)15.3(3)M或更高版本
- Cisco 1000系列聚合服务路由器(ASR1K)3.10或更高版本

> **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)。 有关信息，请参阅Cisco功能导航器。

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

较新的Cisco IOS平台和软件的一个优势是能够使用下一代加密技术。例如，如RFC 4106中所述，在Galois/Counter Mode(GCM)中使用高级加密标准(AES)在IPsec中进行加密。AES GCM可在某些硬件上实现更快的加密速度。

> **注意：**有关使用和迁移到下一代加密的详细信息，请参阅下一代加密思科文章。

配置

此配置示例重点介绍从DMVPN第3阶段配置到FlexVPN的迁移，因为这两种设计的工作方式类似。

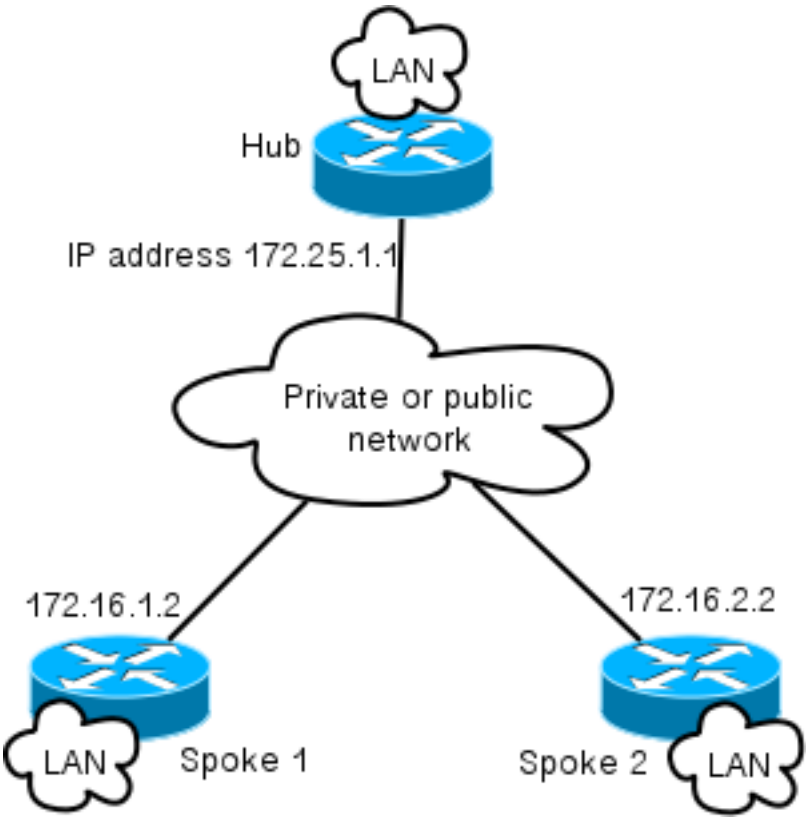
	DMVPN第2阶段	DMVPN第3阶段	FlexVPN
传输	基于 IPSec 的 GRE	基于 IPSec 的 GRE	基于IPsec的GRE、VTI
NHRP使用	注册和解决	注册和解决	分辨率
分支的下一跳	其他辐条或集线器	从集线器摘要	从集线器摘要
NHRP快捷方式交换	无	Yes	是（可选）
NHRP重定向	无	Yes	Yes
IKE和IPsec	IPsec可选，IKEv1典型	IPsec可选，IKEv1典型	IPsec、IKEv2

网络图

本节提供传输和重叠网络图。

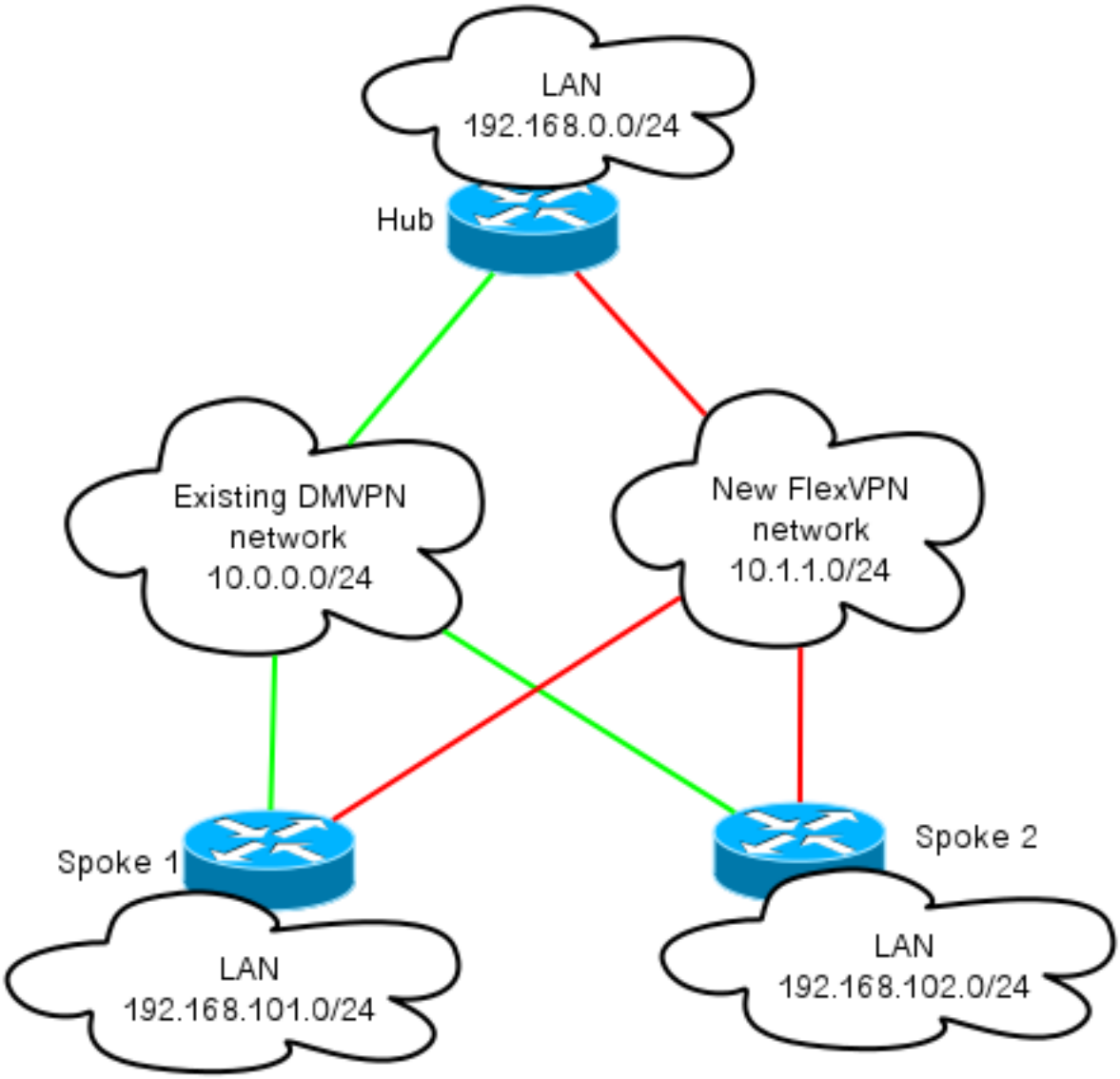
传输网络图

本示例中使用的传输网络包括一个连接了两个分支的集线器。所有设备都通过模拟Internet的网络连接。



重叠网络图

本示例中使用的重叠网络包括一个连接了两个分支的集线器。请记住，DMVPN和FlexVPN同时处于活动状态，但它们使用不同的IP地址空间。



配置

此配置通过增强型内部网关路由协议(EIGRP)将DMVPN第3阶段最常用的部署迁移到具有边界网关协议(BGP)的FlexVPN。思科建议将BGP与FlexVPN配合使用，因为它允许部署更好地扩展。

> **注意**：集线器在同一IP地址上终止IKEv1(DMVPN)和IKEv2(FlexVPN)会话。这只有在最新的Cisco IOS版本中才可能实现。

分支配置

这是非常基本的配置，有两个显着的例外允许IKEv1和IKEv2的互操作，以及两个使用IPsec通用路由封装(GRE)进行传输以共存的框架。

> **注意**：对互联网安全关联和密钥管理协议(ISAKMP)和IKEv2配置的相关更改以粗体突出显示。

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
```

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

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
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 key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub 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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS版本15.3允许您在隧道保护配置中将IKEv2和ISAKMP配置文件绑定在一起。这与对代码的一些内部更改一起，允许IKEv1和IKEv2在同一设备上同时运行。

由于Cisco IOS选择15.3之前版本中的配置文件（IKEv1或IKEv2）的方式，它导致了一些警告，例如IKEv1通过对等体发起到IKEv2的情况。IKE的分离现在基于配置文件级别，而不是通过新CLI实现的接口级别。

新Cisco IOS版本的另一个升级是添加隧*道密钥*。这是必需的，因为DMVPN和FlexVPN使用相同的源接口和相同的目标IP地址。在此情况下，GRE隧道无法知道使用哪个隧道接口来解封流量。通过隧道密钥，可以通过添加较小（4字节）开销来区分tunnel0和tunnel1。可以在两个接口上配置不同的密钥，但通常只需区分一个隧道。

注意：当DMVPN和FlexVPN共享同一接口时，不需要共享隧道保护选项。

因此，分支路由协议配置是基本的。EIGRP和BGP分开工作。EIGRP仅通过隧道接口通告以避免在分支到分支隧道上对等，这会限制可扩展性。BGP仅与中心路由器(10.1.1.1)保持关系，以便通告本地网络(192.168.101.0/24)。

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

中心配置

您必须在中心端配置上进行与“分支配置”部分中所述相似的更改。

注意：对ISAKMP和IKEV2配置的相关更改以粗体突出显示。

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface
```

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

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

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 key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

在中心端，IKE配置文件和IPsec配置文件之间的绑定在配置文件级别进行，这与分支配置不同，在分支配置中，通过**tunnel protection**命令完成此绑定。两种方法都是完成此绑定的可行方法。

请注意，对于云中的DMVPN和FlexVPN，下一跳解析协议(NHRP)网络ID不同。在大多数情况下，当NHRP在两个框架上创建单个域时，这是不可取的。

隧道密钥在GRE级别区分DMVPN和FlexVPN隧道，以实现“分支配置”部分中提到的**相同**目标。

集线器上的路由配置相当基本。中心设备与任何给定分支保持两种关系，一种使用EIGRP，另一种

使用BGP。BGP配置使用侦听范围以避免长时间的每分支配置。

总结地址引入两次。EIGRP配置使用隧道0配置(IP summary-address EIGRP 100)发送摘要，BGP使用聚合地址引入摘要。为确保NHRP重定向发生并简化路由更新，需要提供摘要。您可以发送NHRP重定向（与Internet非常相似）控制消息协议(ICMP)重定向)，指示给定目标是否存在更好的跳数，这允许建立分支到分支隧道。这些摘要还用于最小化中心和每个分支之间发送的路由更新量，从而允许设置更好地扩展。

```
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

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
```

验证

此配置示例的验证分为几个部分。

迁移前检查

由于DMVPN/EIGRP和FlexVPN/BGP同时运行，您必须验证分支与IKEv1和IKEv2在IPsec上保持关系，并且通过EIGRP和BGP获取适当的前缀。

在本例中，Spoke1显示与中心路由器的两个会话得到维护；一个使用IKEv1/Tunnel0,另一个使用IKEv2/Tunnel1。

> **注意**：为每个隧道维护两个IPsec安全关联(SA)（一个入站和一个出站）。

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
```

```
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

检查路由协议时，必须验证邻居关系已形成，且已获知正确的前缀。这首先与EIGRP一起检查。验证集线器是否可视为邻居，以及192.168.0.0/16地址（摘要）是否从集线器获知：

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

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 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

接下来，验证BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, 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
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

输出显示中心FlexVPN IP地址(10.1.1.1)是辐条接收一个前缀(192.168.0.0/16)的邻居。 此外，BGP通知管理员192.168.0.0/16前缀发生了路由信息库(RIB)故障。发生此故障是因为路由表中已存在用于该前缀的更好路由。此路由由EIGRP发起，如果您检查路由表，可以确认。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

迁移

上一节检验了IPsec和路由协议是否都已配置并按预期工作。在同一设备上从DMVPN迁移到FlexVPN的最简单方法之一是更改管理距离(AD)。在本例中，内部BGP(iBGP)的AD为**200**，而EIGRP的AD为**90**。

为了使流量正确通过FlexVPN，BGP必须具有更好的AD。在本例中，内部和外部路由的EIGRP AD分别更改为**230**和**240**。这使BGP AD(共**200**)更适合**192.168.0.0/16**前缀。

实现此目的的另一种方法是减少BGP AD。但是，迁移后运行的协议具有非默认值，这可能会影响部署的其他部分。

在本示例中，使用**debug ip routing**命令来验证分支上的操作。

> **注意：**如果此部分中的信息用于生产网络，请避免使用debug命令，并依赖下一节中列出的show命令。此外，分支EIGRP进程必须与中心重新建立邻接关系。

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

此输出中需要注意三个重要操作：

- 辐条发现AD已更改，并禁用邻接。
- 在路由表中，EIGRP前缀被保留，并引入BGP。
- 通过EIGRP与集线器的邻接关系恢复在线。

当您更改设备上的AD时，它只影响从设备到其他网络的路径；它不会影响其它路由器执行路由的方式。例如，在Spoke1上增加EIGRP距离（并在云上使用FlexVPN来路由流量）后，中心会维护已配置（默认）AD。这意味着它使用DMVPN将流量路由回**Spoke1**。

在某些情况下，这可能会导致问题，例如防火墙期望在同一接口上返回流量时。因此，在集线器上更改所有分支的AD之前，您应先更改它。只有在流量完成后，FlexVPN才会完全迁移流量。

EIGRP到EIGRP迁移

本文档不深入讨论从DMVPN到仅运行EIGRP的FlexVPN的迁移；但是，此处提及此内容是为了完整性。

可以将DMVPN和EIGRP同时添加到同一EIGRP自治系统(AS)路由实例中。在这种情况下，将在两种类型的云上建立路由邻接关系。这可能导致负载均衡发生，通常不建议这样做。

为确保选择FlexVPN或DMVPN，管理员可以按接口分配不同的**Delay**值。但是，必须记住，在虚拟模板接口上不可能更改，而存在相应的虚拟访问接口。

迁移后检查

与“迁移前检查”部**分中使用的**过程类似，必须验证IPsec和路由协议。

首先，检验IPsec:

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

与以前一样，会看到两个会话，两个会话都有两个活动IPsec SA。

在辐条上，汇聚路由(**192.168.0.0/16**)从中心点指向并通过BGP获知。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

同样，中心上前缀的分支LAN必须通过EIGRP知道。在本例中，检查**了Spoke2** LAN子网：

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
```

```
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

在输出中，转发路径已正确更新并指向虚拟访问接口。

其他注意事项

本节介绍与此配置示例相关的一些其他重要领域。

现有分支到分支隧道

从EIGRP迁移到BGP时，分支到分支隧道不会受到影响，因为快捷方式交换仍在运行。分支上的快捷方式交换会插入AD为250的更具体的NHRP路由。

以下是此类路由的示例：

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

迁移辐射点与未迁移辐射点之间的通信

如果已在FlexVPN/BGP上的分支希望与尚未开始迁移过程的设备通信，则流量始终会通过集线器传输。

此过程如下：

1. 辐条对目标执行路由查找，该目标通过集线器通告的总结路由。
2. 数据包将发送到集线器。
3. 集线器接收数据包并执行目的地的路由查找，目的地指向属于不同NHRP域的另一个接口。

注意：对于FlexVPN和DMVPN，上一个集线器配置中的NHRP网络ID不同。即使NHRP网络ID是统一的，迁移的分支在FlexVPN网络上路由对象时也可能出现问题。这包括用于配置快捷方式交换的指令。未迁移的分支尝试通过DMVPN网络运行对象，其特定目标是执行快捷方式交换。

故障排除

本节介绍为排除迁移故障通常使用的两个类别。

建立隧道尝试的问题

如果IKE协商失败，请完成以下步骤：

1. 使用以下命令检验当前状态：

   show crypto isakmp sa — 此命令显示IKEv1会话的数量、源和目标。**show crypto ipsec sa** — 此命令显示IPsec SA的活动。**注意：**与IKEv1不同，在此输出中，完全向前保密(PFS)Diffie-Hellman(DH)组值显示为**PFS(Y/N):N，DH组：第一**次隧道协商期间无；但是，在重新生成密钥后，会显示正确的值。虽然CSCug67056中描述了此行为，但这不是Bug。IKEv1和IKEv2之间的区别在于，在后者中，子SA是作为AUTH交换的一部分**创**建的。仅在重新生成密钥时使用在加密映射下配置的DH组。因此，您会看到**PFS(Y/N):N，DH组：直到第一次重新键。**使用IKEv1时，您会看到不同的行为，因为子SA创建发生在快速模式期间，而CREATE_CHILD_SA消息为转移密钥交换负载（指定DH参数以派生新的共享密钥）提供了相关规定。**show crypto ikev2 sa** — 此命令提供类似于ISAKMP的输出，但特定于IKEv2。**show crypto session** — 此命令提供此设备上加密会话的摘要输出。**show crypto socket** — 此命令显示加密套接字的状态。**show crypto map** — 此命令显示IKE和IPsec配置文件到接口的映射。**show ip nhrp** — 此命令提供来自设备的NHRP信息。这对FlexVPN设置中的分支到分支以及DMVPN设置中的分支到分支和分支到中心绑定都非常有用。
2. 使用以下命令调试隧道建立：

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

路由传播问题

以下是一些有用的命令，可用于排除EIGRP和拓扑故障：

- **show bgp summary** — 使用此命令验证连接的邻居及其状态。
- **show ip eigrp neighbor** — 使用此命令可显示通过EIGRP连接的邻居。
- **show bgp** — 使用此命令验证通过BGP获取的前缀。
- **show ip eigrp topology** — 使用此命令可显示通过EIGRP获取的前缀。

了解学习到的前缀与路由表中安装的前缀不同非常重要。有关此信息，请参阅Cisco路由器Cisco文章或Routing TCP/IP Cisco Press手册。

已知问题说明

ASR1K上存在与GRE隧道处理相类似的限制。这在Cisco Bug ID CSCue00443下进行跟踪。目前，此限制在Cisco IOS XE软件版本3.12中已安排修复。

如果在修复程序可用后需要通知，请监控此Bug。