FlexVPN迁移：从DMVPN的硬移动到在一台不同的集线器的FlexVPN

目录

简介

本文提供关于如何的信息从当前存在对在不同的集线器设备的FlexVPN的动态多点VPN (DMVPN)网络移植。两个框架的configuations在设备共存。在本文中，仅多数常见情况显示-与使用的DMVPN验证的预共享密匙和增强的内部网关路由选择协议(EIGRP)作为路由协议。在本文中，对边界网关协议(BGP)的迁移，是推荐的路由协议和少理想EIGRP被展示。

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**：不是所有的软件和硬件支持互联网密钥交换版本2 (IKEv2)。参考Cisco Feature Navigator欲知更多信息。

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)版本15.2(4)M1或以上
- Cisco聚合服务路由器1000系列(ASR1K) 3.6.2版本15.2(2)S2或更新

一个一更新的平台和软件的优点是能力使用下一代加密算法，例如高级加密标准(AES) Galois/计数器模式(GCM)加密在Internet协议安全性(IPsec)，如请求注释(RFC) 4106所述。AES GCM允许您到达在一些硬件的一更加快速的加密速度。为了看到在使用和迁移的Cisco推荐到下一代加密算法，参考下一代加密条款。

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，移植的推荐的方法从DMVPN到FlexVPN是为了同时运行两个的框架能。在ASR 3.10版本安排此限制就该删除的对新的迁移功能介绍，被跟踪在思科侧的multilple增强请求下，包括Cisco Bug ID CSCuc08066。那些功能应该取得到在2013年6月下旬。

两个框架在同样设备同时共存并且运行的迁移指**软的迁移**，指示最小影响和平稳的故障切换从一个框架到另一个。两个框架的配置共存的迁移，但是同时不运行指**硬迁移**。这表明从一个框架的一个切换到另一个含义缺乏在VPN的通信，即使最小。

两区别集线器之间的硬迁移

在本文中，从当前使用到一台新的FlexVPN集线器的DMVPN集线器的迁移讨论。此迁移允许在spoke之间的相互来往已经被移植到FlexVPN，并且在DMVPN在多个相位仍然运行，并且可以执行的那些，在每分开发言。

在路由信息适当地填充条件下，被移植的和nonmigrated spoke之间的通信应该依然是可能。然而，因为移植和nonmigrated spoke不构建在彼此之间的spoke-to-spoke通道另外的延迟可以被观察。同时，被移植的spoke应该能设立在他们自己之间的直接spoke-to-spoke通道。同样适用于nonmigrated spoke。

直到这新建的迁移功能是可用的，请完成这些步骤为了用一台不同的集线器进行迁移从DMVPN和FlexVPN ：

1. 验证在DMVPN的连接。
2. 添加FlexVPN配置，并且关闭属于新的配置的通道。
3. (在维护窗口期间)在每分支，逐个，请关闭DMVPN通道。
4. 在分支和一样在步骤3， unshut FlexVPN隧道接口。
5. 验证spoke-to-hub连接。
6. 验证在FlexVPN内的spoke-to-spoke连接。
7. 验证与DMVPN的spoke-to-spoke连接从FlexVPN。
8. 重复每步骤3至7分开发言。
9. 如果遇到与在步骤描述的验证的任何问题5， 6或者7，请关闭FlexVPN接口和unshut DMVPN接口为了恢复到DMVPN。
10. 验证在备份的DMVPN的spoke-to-hub通信。
11. 验证在备份的DMVPN的spoke-to-spoke通信。

自定义方法

如果上一个方法也许不是您的佳解决方案由于您的网络或路由复杂性，请开始与您的思科代表的一讨论，在您移植前。讨论自定义迁移进程是您的系统工程师或高级服务服务工程师的最好的人。

网络拓扑

传输网络网络拓扑结构

此图表显示主机典型的连接拓扑在互联网的。**loopback0** (**172.25.1.1**)的集线器的IP地址用于为了终止DMVPN IPSec会话。在新的集线器(**172.25.2.1**)的IP地址使用FlexVPN。

注意两集线器之间的链路。此链路是关键为了在迁移时允许FlexVPN和DMVPN网云之间的连接。它允许spoke已经被移植到FlexVPN通信与DMVPN网络反之亦然。

重叠网络拓扑

此拓扑图显示用于重叠的两独立的网云：DMVPN (绿色连接)和FlexVPN (红色连接)。LAN前缀为对应的站点显示。**10.1.1.0/24**子网不表示实际子网根据接口编址，然而代表IP空间大块投入FlexVPN网云。在此后的基本原理是讨论以后在**FlexVPN配置部分**。

配置

此部分描述DMVPN和FlexVPN配置。

DMVPN 配置

此部分描述DMVPN星型网的基本配置。

预先共享密钥(PSK)使用IKEv1验证。一旦IPsec设立，从spoke-to-hub的下一跳解析协议(NHRP)注册进行，以便集线器能了解spoke的非广播多路访问(NBMA)动态寻址。

当NHRP进行在分支和集线器时的注册，路由adjacancy能设立，并且路由可以被交换。在本例中，EIGRP使用作为一个基本路由协议覆盖网络。

分支DMVPN配置

您能找到DMVPN和EIGRP的基本示例配置与PSK验证的作为路由协议。

```
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

在集线器上配置，通道从loopback0来源用172.25.1.1的IP地址。其余是一台DMVPN集线器的一标准的部署有EIGRP的作为路由协议。

```
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根据这些同样基本的技术：

- **IPsec** ：不同于在DMVPN的默认， IKEv2用于而不是IKEv1为了协商IPSec安全关联(SAS)。IKEv2提供在IKEv1的改进，例如弹性和是需要的为了设立保护数据数据通道的通讯数量。
- **GRE** ：不同于DMVPN，使用静态和动态点对点接口和不仅一个静态multpoint GRE接口。此配置允许已添加灵活性，特别是每分支/每HUB行为。
- **NHRP** ：在FlexVPN， NHRP主要用于为了建立spoke-to-spoke通信。Spoke不注册到集线器。
- **路由**：由于spoke不进行NHRP注册到集线器，您在其他机制必须取决于为了确保星型网能通信双向。可以使用对DMVPN的Simliar，动态路由协议。然而， FlexVPN允许您使用IPsec为了引入路由信息。默认是介绍作为IP地址的/32路由在通道的另一侧，允许spoke-to-hub直接通信。

在从DMVPN的硬迁移到FlexVPN，两framemworks在同样设备同时不运作。然而，推荐保持他们分开。

分离他们在几个级别上：

- NHRP -请使用一不同的NHRP网络ID (建议使用)。
- 路由-请使用分开的路由进程(建议使用)。
- 虚拟路由和转发(VRF) - VRF分离允许已添加灵活性，但是没有讨论在这儿(可选)。

分支FlexVPN配置

其中一差异在辐条配置里在与DMVPN比较的FlexVPN是您潜在有两个接口。有spoke-to-hub通信的一个需要的通道和spoke-to-spoke通道的一个可选通道。如果选择没有动态spoke-to-spoke隧道，并且更喜欢一切通过集线器设备，您能消除虚拟模板接口，并且从隧道接口删除NHRP快捷方式交换。

注意静态隧道接口收到根据协商的IP地址。这允许集线器动态地提供隧道接口IP地址给分支，不用需要创建在FlexVPN网云的静态地址。

```
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，本地标识设置为了使用IP地址。因此在对等体的对应的匹配语句必须配比基于地址。如果需求是匹配基于在certifcate的特有名(DN)，则匹配必须完成与使用证书地图。

思科建议您以支持它的硬件使用AES GCM。

```
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
```

公共密钥基础设施(PKI)是执行大规模验证的推荐的方法在IKEv2。然而，只要您知道其限制，您能仍然使用PSK。

这是使用**cisco**作为PSK的配置示例。

```
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集线器上配置

一般，集线器只终止动态spoke-to-hub通道。这就是为什么您没找到FlexVPN的一个静态隧道接口在集线器上配置。反而，使用虚拟模板接口。

注意：在集线器端，您必须指示将分配的池地址到spoke。

从此池的地址是被添加的以后在路由表里作为**/32**路由每分支的。

```
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
```

思科建议您以支持它的硬件使用AES GCM。

```
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
```

注意：在此配置中， AES GCM操作注释。

```
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
```

使用在IKEv2的验证，同一个原理在集线器适用和在分支。对于可扩展性和灵活性，请使用证书。然而，您能重新使用PSK的相同的配置和在分支。

注意：IKEv2提供灵活性根据验证。一端能验证与PSK，当另一侧使用Rivest Shamir Adelman签名时(RSA-SIG)。

如果需求是使用预共享密匙验证，则配置更改类似于为分支路由器描述的那些此处。

相互HUB BGP连接

确保集线器知道特定前缀哪里查找。这变得愈加重要，因为一些spoke被移植了到FlexVPN，当一些其他spoke在DMVPN时。

这是根据DMVPN集线器上配置的相互HUB BGP连接：

```
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
```

流量迁移

对BGP的迁移作为重叠路由协议[Recommended]

BGP是根据单播交换的路由协议。由于其特性，它是在DMVPN网络的最好的扩展的协议。

在本例中，使用内部BGP (iBGP)。

分支BGP配置

分支迁移包括两部分。首先， enable (event) BGP作为动态路由：

```
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
```

在BGP邻居出现(看到下一部分)后，并且了解在BGP的新建的前缀，您能摇摆从当前DMVPN网云的流量到一新的FlexVPN网云。

集线器BGP配置

FlexVPN集线器-全双工BGP配置

在集线器上，为了避免保持每结邻配置分开发言，配置动态监听程序。在此设置， BGP不首次新连接，然而接受从IP地址的提供的池的连接。在这种情况下，前述池是10.1.1.0/24，是所有在新的FlexVPN网云的地址。

注释的两点：

- FlexVPN集线器通告特定前缀到DMVPN集线器;因而使用unsupress地图。
- 请通告FlexVPN子网10.1.1.0/24对路由表或者确保DMVPN集线器看到FlexVPN集线器作为下一跳。

本文显示后一个方案。

```
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集线器-全双工BGP和EIGRP配置

在DMVPN集线器的配置基本，因为只接收从从EIGRP了解的FlexVPN集线器的特定前缀并且通告前缀。

```
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
```

对BGP/FlexVPN的迁移流量

如上所述，您必须关闭DMVPN功能和提出FlexVPN为了进行迁移。

此步骤保证最小影响：

1. 在每分支，分开，请输入此：

   ```
   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
```

这时，请确保那里是没有IKEv1会话建立对此分支。如果检查输出**show crypto isakmp sa命令**并且监控**crypto记录日志**生成的系统消息**session命令，**这可以验证。一旦这被确认，您能继续启动FlexVPN。

2. 在同样分支，请输入此：

```
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
```

验证步骤

IPsec稳定性

评估IPsec稳定性的最佳方法是监控与**crypto记录日志会话配置**enabled命令的sylog。如果看到上升和下降的会话，这能指示在必须更正的IKEv2/FlexVPN级别上的一问题，在迁移能开始前。

填充的BGP信息

如果IPsec稳定的，请确保BGP表带有从spoke的从集线器的条目(在集线器)和摘要(在spoke)。一旦BGP，这可以用这些命令查看：

```
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
```

这是正确信息示例从FlexVPN集线器的：

```
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
```

输出显示集线器了解从其中每一个的一个前缀spoke，并且两个spoke是动态和明显的与星号(*)符号。它也显示从相互HUB连接的总共四个前缀接收。

这是相似的信息示例从分支的：

```
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
```

分支接收从集线器的两个前缀。一旦此设置，一个前缀应该是在FlexVPN集线器通告的摘要。其他是在DMVPN分支重新分配的DMVPN 10.0.0.0/24网络到BGP。

对新的通道的迁移有EIGRP的

EIGRP是在DMVPN网络的一普遍的选择由于其相对简单部署和快速收敛。然而，它比BGP扩展坏和不提供能由BGP直通使用箱外的许多先进的机制。下一部分描述其中一个方式移动向与一个新的EIGRP进程的FlexVPN。

更新辐条配置

新的自治系统(AS)添加与一个分开的EIGRP进程：

```
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
```

> **注意**：不设立在spoke-to-spoke通道的路由协议邻接是最佳的。所以，只请使接口tunnel1 (spoke-to-hub)不被动。

更新FlexVPN集线器上配置

同样地，对于FlexVPN集线器，请准备在appopriate AS的路由协议，匹配在spoke配置的一。

```
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
```

有使用为了提供往分支的摘要上一步的两个方法。

- 再分布静态路由对**null0** (首选)的该点。
  ```
  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
  ```

  此选项允许对摘要的控制和再分配，不用对集线器的虚拟化技术(VT)配置的修改。这是重要，因为不可能修改集线器的VT配置，如果有活动虚拟访问关联与它。

- 设置在虚拟模板的一DMVPN斯太尔summary-address。

  此配置没有*推荐*，由于前述摘要的内部处理和复制对每次虚拟访问的。它显示此处供参考。

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

  占的另一个方面是相互HUB路由交换。如果重新分配EIGRP实例对iBGP，这可以执行。

DMVPN集线器-更新BGP配置

配置依然是基本。您必须重新分配特定前缀从EIGRP到BGP:

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

FlexVPN集线器-更新BGP配置

类似于DMVPN集线器，在FlexVPN，您必须重新分配新的EIGRP进程的前缀到BGP:

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

对FlexVPN的迁移流量

您必须关闭DMVPN功能和带来FlexVPN在每分支，一次一个，为了进行迁移。此步骤保证最低的影响：

1. 在每分支，分开，请输入此：
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```
   这时，请确保那里是在此分支建立的没有IKEv1会话。如果检查输出**show crypto isakmp sa命令**并且监控**crypto记录日志**生成的系统消息**session命令，**这可以验证。一旦这被确认，您能继续启动FlexVPN。
2. 在同样分支，请输入此：
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```

验证步骤

IPsec稳定性

如果IPsec稳定的，和一旦BGP，您必须评估。如此要执行的最佳方法是监控与**crypto记录日志会话配置**enabled命令的sylog。如果看到会话上升和下降，这能指示在必须更正的IKEv2/FlexVPN级别上的一问题，在迁移能开始前。

EIGRP数据在拓扑表里

确保您的EIGRP拓扑表带有分支在集线器和摘要的LAN条目在spoke。如果输入此on命令集线器和分支，这可以验证：

show ip eigrp [AS_NUMBER] topology
这是从分支的一个输出示例：

```
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
```

输出显示分支知道关于其LAN子网(以*斜体字*)和那些的摘要(在**粗体**)。

这是从集线器的一个输出示例：

```
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)
```

输出通过协商显示集线器知道关于spoke的LAN子网(以通告的*斜体字*)，概略的前缀(在**粗体**)和每个spoke的指定的IP地址。

另外的考虑事项

已经存在的spoke-to-spoke通道

由于DMVPN隧道接口的关闭造成NHRP条目删除，已经存在的spoke-to-spoke通道将被切断。

清楚NHRP条目

FlexVPN集线器如何不依靠从分支的NHRP注册过程为了知道到路由流量上一步。然而，动态spoke-to-spoke通道依靠NHRP条目。

在DMVPN，如果清除在集线器的NHRP，它能导致短期的连接问题。在FlexVPN，在spoke的清除的NHRP将引起FlexVPN IPSec会话，涉及与spoke-to-spoke通道，被切断。清除在集线器的NHRP没有效果在FlexVPN会话。

这是因为，在FlexVPN默认情况下：

- Spoke不注册到集线器。
- 集线器仅工作作为NHRP转向器和不安装NHRP条目。
- NHRP快捷方式条目在spoke-to-spoke通道的spoke安装并且动态。

已知问题说明

spoke-to-spoke流量也许受Cisco Bug ID CSCub07382的影响。

相关信息

- **对FlexVPN软的迁移配置示例的DMVPN**
- **技术支持和文档 - Cisco Systems**