Configure a redundância do ISP em um spoke DMVPN com o recurso VRF-Lite

Contents

Introduction

Este documento descreve como configurar a redundância do provedor de serviços de Internet (ISP) em um spoke Dynamic Multipoint VPN (DMVPN) via recurso Virtual Routing and Forwarding-Lite (VRF-Lite).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento desses tópicos antes de tentar a configuração descrita neste documento:

- Conhecimento básico de VRF

- Conhecimento básico do Enhanced Interior Gateway Routing Protocol (EIGRP)
- Conhecimento básico do DMVPN

Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS® versão 15.4(2)T.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O VRF é uma tecnologia incluída nos roteadores de rede IP que permite que várias instâncias de uma tabela de roteamento coexistam em um roteador e trabalhem simultaneamente. Isso aumenta a funcionalidade porque permite que os caminhos da rede sejam segmentados sem o uso de vários dispositivos.

O uso de ISPs duplos para redundância se tornou uma prática comum. Os administradores usam dois links ISP; uma atua como uma conexão principal e a outra como uma conexão de backup.

O mesmo conceito pode ser implementado para redundância de DMVPN em um spoke com o uso de ISPs duplos. O objetivo deste documento é demonstrar como *VRF-Lite* pode ser usado para segregar a tabela de roteamento quando um spoke tem ISPs duplos. O roteamento dinâmico é usado para fornecer redundância de caminho para o tráfego que atravessa o túnel DMVPN. Os exemplos de configuração descritos neste documento usam este esquema de configuração:

Interface	IP Address	VRF	Descrição
Ethernet0/0	172.16.1.1	VRF ISP1	ISP principal
Ethernet0/1	172.16.2.1	VRF ISP2	ISP secundário

Com o recurso VRF-Lite, várias instâncias de roteamento/encaminhamento de VPN podem ser suportadas no spoke DMVPN. O recurso VRF-Lite força o tráfego de várias interfaces de túnel de Encapsulamento de Roteamento Genérico Multiponto (mGRE - Multipoint Generic Routing Encapsulation) a usar suas respectivas tabelas de roteamento VRF. Por exemplo, se o ISP primário termina no VRF do ISP1 e o ISP secundário termina no VRF do ISP2, o tráfego gerado no VRF do ISP2 usa a tabela de roteamento VRF do *ISP2*, enquanto o tráfego gerado no VRF do *ISP1 usa oISP1* VRF tabela de roteamento.

Uma vantagem que vem com o uso de um VRF (fVRF) de *porta frontal* é primeiramente criar uma tabela de roteamento separada da tabela de roteamento global (onde existem interfaces de túnel). A vantagem com o uso de um VRF *interno* (iVRF) é definir um espaço privado para manter o DMVPN e as informações de rede privada. Ambas as configurações fornecem segurança extra contra ataques no roteador da Internet, onde as informações de roteamento são separadas.

Essas configurações de VRF podem ser usadas no hub DMVPN e no spoke. Isso oferece grande vantagem sobre um cenário no qual ambos os ISPs terminam na tabela de roteamento global.

Se ambos os ISPs terminam no VRF global, eles compartilham a mesma tabela de roteamento e ambas as interfaces mGRE dependem das informações de roteamento global. Nesse caso, se o ISP principal falhar, a interface primária do ISP pode não ficar inativa se o ponto de falha estiver na rede de backbone dos ISPs e não estiver diretamente conectado. Isso resulta em um cenário em que ambas as interfaces de túnel mGRE ainda usam a rota padrão que aponta para o ISP principal, o que faz com que a redundância de DMVPN falhe.

Embora haja algumas soluções alternativas que usam os scripts IP Service Level Agreements (IP SLA) ou Embedded Event Manager (EEM) para resolver esse problema sem VRF-Lite, elas nem sempre são a melhor opção.

Métodos de implantação

Esta seção fornece breves entrevistas de túneis divididos e túneis spoke-to-spoke.

Encapuslamento dividido

Quando sub-redes específicas ou rotas resumidas são aprendidas através de uma interface mGRE, é chamado de *tunelamento dividido*. Se a rota padrão for aprendida através de uma interface mGRE, então ela é chamada de *tunnel-all*.

O exemplo de configuração fornecido neste documento é baseado em tunelamento dividido.

Túneis spoke-to-spoke

O exemplo de configuração fornecido neste documento é um bom projeto para o método de implantação tunnel-all (a rota padrão é aprendida através da interface mGRE).

O uso de dois fVRFs segrega as tabelas de roteamento e garante que os pacotes encapsulados pós-GRE sejam encaminhados para o respectivo fVRF, o que ajuda a garantir que o túnel spoke-to-spoke venha com um ISP ativo.

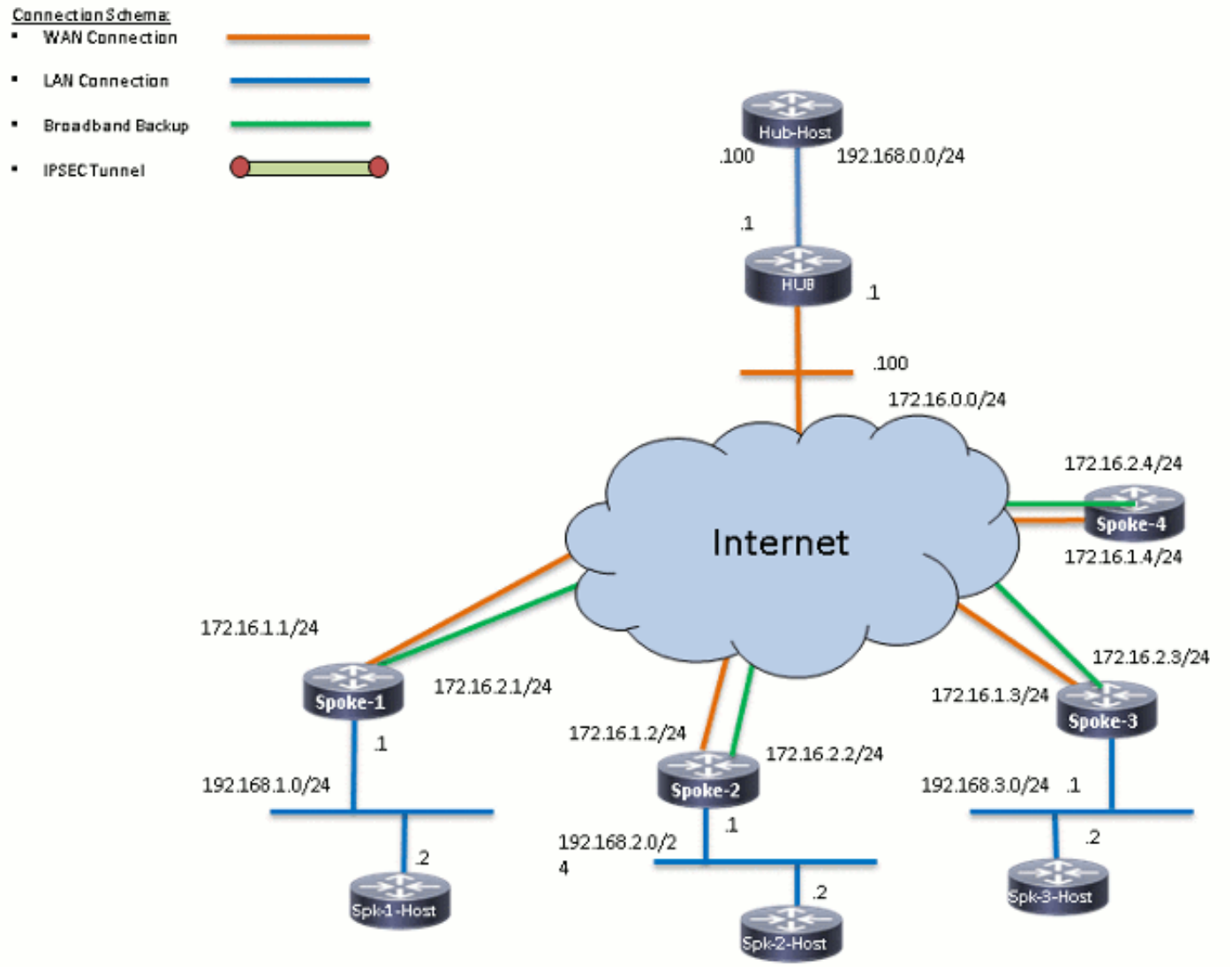
Configurar

Esta seção descreve como configurar a redundância do ISP em um spoke DMVPN através do recurso VRF-Lite.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Esta é a topologia usada para os exemplos neste documento:



Configuração do hub

Aqui estão algumas observações sobre a configuração relevante no hub:

- Para definir *Tunnel0* como a interface primária neste exemplo de configuração, o parâmetro *delay* foi alterado, o que permite que as rotas aprendidas do *Tunnel0* se tornem mais preferenciais.

- A palavra-chave **compartilhada** é usada com proteção de túnel e uma *chave de túnel* exclusiva é adicionada em todas as interfaces mGRE porque elas usam a mesma *origem de túnel <interface>*. Caso contrário, os pacotes de túnel GRE (Generic Routing Encapsulation) de entrada podem ser direcionados para a interface de túnel incorreta após a descriptografia.

- Uma sumarização de rota é executada para garantir que todos os spokes aprendam a rota padrão através dos túneis mGRE (**tunnel-all**).

Note: Apenas as seções relevantes da configuração estão incluídas neste exemplo.

```
version 15.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname HUB1
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback0
 description LAN
 ip address 192.168.0.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn shared
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile profile-dmvpn shared
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
```

```
!
end
```

Configuração de Spoke

Aqui estão algumas observações sobre a configuração relevante no spoke:

- Para redundância de spoke, *Tunnel0* e *Tunnel1* têm *Ethernet0/0* e *Ethernet0/1* como as interfaces origem do túnel, respectivamente. A Ethernet0/0 está conectada ao ISP principal e a Ethernet0/1 está conectada ao ISP secundário.
- Para segregar os ISPs, o recurso VRF é usado. O ISP principal usa o VRF *ISP1*. Para o ISP secundário, um VRF chamado *ISP2* é configurado.
- O *túnel vrf ISP1* e o *túnel vrf ISP2* estão configurados nas interfaces Tunnel0 e Tunnel1, respectivamente, para indicar que a pesquisa de encaminhamento para o pacote encapsulado pós-GRE é executada em VRF ISP1 ou ISP2.
- Para definir Tunnel0 como a interface primária neste exemplo de configuração, o parâmetro *delay* foi alterado, o que permite que as rotas aprendidas de Tunnel0 se tornem mais preferenciais.

Note: Apenas as seções relevantes da configuração estão incluídas neste exemplo.

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SPOKE1
!
vrf definition ISP1
 rd 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition ISP2
 rd 2:2
 !
 address-family ipv4
 exit-address-family
!
crypto keyring ISP2 vrf ISP2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring ISP1 vrf ISP1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp keepalive 10 periodic
!
```

```
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback10
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 description Primary mGRE interface source as Primary ISP
 bandwidth 1000
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel vrf ISP1
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 description Secondary mGRE interface source as Secondary ISP
 bandwidth 1000
 ip address 10.0.1.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100001
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.1.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel vrf ISP2
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 description Primary ISP
 vrf forwarding ISP1
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 description Seconday ISP
 vrf forwarding ISP2
 ip address 172.16.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 172.16.1.254
ip route vrf ISP2 0.0.0.0 0.0.0.0 172.16.2.254
!
```

```
logging dmvpn
!
end
```

Verificar

Use as informações descritas nesta seção para verificar se sua configuração funciona corretamente.

ISPs primários e secundários ativos

Neste cenário de verificação, os ISPs principal e secundário estão ativos. Aqui estão algumas notas adicionais sobre este cenário:

- A fase 1 e a fase 2 para ambas as interfaces mGRE estão ativadas.
- Ambos os túneis são ativados, mas as rotas via Tunnel0 (originadas através do ISP principal) são preferidas.

Estes são os comandos **show** relevantes que você pode usar para verificar sua configuração neste cenário:

```
SPOKE1#show ip route
<snip>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 1w0d, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>
```

```
Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

ISP principal inativo/ISP secundário ativo

Neste cenário, os temporizadores *de espera* do EIGRP expiram para a vizinhança através do Tunnel0 quando o link do ISP1 fica inativo, e as rotas para o hub e os outros spokes agora apontam para Tunnel1 (originado pela Ethernet0/1).

Estes são os comandos **show** relevantes que você pode usar para verificar sua configuração neste cenário:

```
*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/3072000] via 10.0.1.1, 00:00:20, Tunnel1

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
```

```
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: DOWN
Peer: 172.16.0.1 port 500
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

       Active SAs: 0, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive
```

Restauração de link do ISP principal

Quando a conectividade através do ISP principal é restaurada, a sessão de criptografia Tunnel0 se torna ativa e as rotas que são aprendidas através da interface Tunnel0 são preferidas.

Aqui está um exemplo:

```
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 00:00:45, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

Troubleshoot

Para solucionar problemas de configuração, habilite debug ip eigrp e logging dmvpn.

Aqui está um exemplo:

```
################## Tunnel0 Failed and Tunnel1 routes installed ####################
```

```
*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired
*Sep  2 14:07:33.374: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:07:33.391: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:33.399: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:36.686: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is DOWN
*Sep  2 14:07:36.686: %DMVPN-5-NHRP_NHS_DOWN: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason:
External(NHRP: no error)

################### Tunnel0 came up and routes via Tunnel0 installed ##################

*Sep  2 14:15:55.120: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is UP
*Sep  2 14:15:56.109: %DMVPN-5-NHRP_NHS_UP: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is  UP
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/2944000) origin(10.0.0.1)
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel0
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
```

Informações Relacionadas

- Soluções de problemas DMVPN mais comuns
- Guia de solução de problemas da família Cisco MDS 9000, versão 2.x âÂ Â solução de problemas de IPsec
- Suporte Técnico e Documentação - Cisco Systems