Configurar a Redundância ISP em um DMVPN falou com a característica de VRF-Lite

Índice

Introdução

Este documento descreve como configurar a Redundância do provedor de serviço do Internet (ISP) em um spoke do Dynamic Multipoint VPN (DMVPN) através da característica do roteamento virtual e do Transmissão-Lite (VRF-Lite).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente a configuração que está descrita neste documento:

- Conhecimento básico do VRF

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

Componentes Utilizados

A informação neste documento é baseada na versão 15.4(2)T do ® do Cisco IOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O VRF é uma tecnologia incluída no Roteadores da rede IP que permita que as múltiplas instâncias de uma tabela de roteamento coexistam em um roteador e trabalhem simultaneamente. Isto aumenta a funcionalidade porque permite que os caminhos de rede sejam segmentados sem o uso dos dispositivos múltiplos.

O uso de ISP duplos para a Redundância transformou-se uma prática comum. Os administradores usam dois links ISP; se atua como uma conexão principal e o outro atua como uma conexão de backup.

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

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

Com a característica de VRF-Lite, as instâncias de roteamento/encaminhamento de VPN múltiplas podem ser apoiadas no spoke DMVPN. A característica de VRF-Lite força o tráfego das interfaces de túnel multipontos múltiplas do encapsulamento de roteamento genérico (mGRE) para usar suas tabelas de roteamento respectivas VRF. Por exemplo, se o ISP principal termina no *ISP1* VRF e o ISP secundário termina no *ISP2* VRF, o tráfego que é gerado no *ISP2* VRF usa a tabela de roteamento *ISP2* VRF, quando o tráfego que está gerado no *ISP1* VRF usar a tabela de roteamento *ISP1* VRF.

Uma vantagem que venha com o uso de uma *porta frontal* VRF (fVRF) é primeiramente cinzelar para fora uma tabela de roteamento separada da tabela de roteamento global (onde as interfaces de túnel existem). A vantagem com o uso de um VRF *interno* (iVRF) é definir um espaço privado a fim guardar a informação DMVPN e de rede privada. Both of these configurações fornecem a Segurança extra dos ataques no roteador do Internet, onde a informação de roteamento é

separada.

Estas configurações de VRF podem ser usadas em ambos o hub and spoke DMVPN. Isto dá a grande vantagem sobre uma encenação em que ambos os ISP terminam na tabela de roteamento global.

Se ambos os ISP terminam no VRF global, compartilham da mesma tabela de roteamento e ambas as relações mGRE confiam na informação de roteamento global. Neste caso, se o ISP principal falha, a relação do ISP principal não pôde ir para baixo se o ponto da falha está na rede de backbone dos ISP e conectada não diretamente. Isto conduz a uma encenação onde ambas as interfaces de túnel mgre ainda usem a rota padrão que aponta ao ISP principal, que faz com que a Redundância DMVPN falhe.

Embora há algumas ações alternativas que usam os acordos do nível de serviço IP (IP SLA) ou scripts encaixados do gerente do evento (EEM) a fim endereçar esta edição sem VRF-Lite, não puderam sempre ser a melhor escolha.

Métodos do desenvolvimento

Esta seção fornece breves visões gerais do Split Tunneling e de túneis spoke-to-spoke.

Divisão de túnel

Quando as sub-redes ou as rotas resumida específicas são instruídas através de uma relação mGRE, a seguir está chamado *Split Tunneling*. Se a rota padrão é instruída através de uma relação mGRE, a seguir está chamada túnel-*toda*.

O exemplo de configuração que é fornecido neste documento é baseado no Split Tunneling.

Túneis spoke-to-spoke

O exemplo de configuração que é fornecido neste documento é um bom projeto para túnel-todo método do desenvolvimento (a rota padrão é instruída através da relação mGRE).

O uso de dois fVRFs segrega as tabelas de roteamento e assegura-se de que os pacotes encapsulado cargo-GRE estejam enviados ao fVRF respectivo, que ajuda a se assegurar de que o túnel spoke-to-spoke venha acima com um ISP ativo.

Configurar

Esta seção descreve como configurar a Redundância ISP em um spoke DMVPN através da característica de 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 que é usada para os exemplos dentro deste documento:

Configuração do hub

Estão aqui algumas notas sobre a configuração relevante no hub:

- A fim ajustar o *tunnel0* como a interface principal neste exemplo de configuração, o *parâmetro de retardo* foi mudado, que permite as rotas que são instruídas do *tunnel0* se tornar mais preferidas.
- A palavra-chave **compartilhada** é usada com proteção do túnel e uma *chave do* túnel exclusivo é adicionada em todas as relações mGRE porque usam o mesmo *<interface> do origem de túnel*. Se não, os pacotes de entrada do túnel de encapsulamento de roteamento genérico (GRE) puderam ser punted à interface de túnel incorreta após a descriptografia.
- Uma sumarização de rota?à fim assegurado-se de que todo o spokes aprenda a rota padrão através dos túneis mGRE (túnel-**todos**).

Note: Somente as seções relevantes da configuração são 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 raio

Estão aqui algumas notas sobre a configuração relevante no spoke:

- Para a Redundância do spoke, o *tunnel0* e *Tunnel1* têm o *Ethernet0/0* e o *Ethernet0/1* como as relações do origem de túnel, respectivamente. O Ethernet0/0 é conectado ao ISP principal e Ethernet0/1 é conectado ao ISP secundário.

- A fim segregar os ISP, a característica VRF é usada. O ISP principal usa o *ISP1* VRF. Para o ISP secundário, um VRF *ISP2* nomeado é configurado.

- *O vrf ISP1 do túnel* e o *vrf ISP2 do túnel* são configurados no tunnel0 das relações e no Tunnel1, respectivamente, a fim indicar que a consulta de encaminhamento para o pacote encapsulado cargo-GRE está executada em VRF ISP1 ou em ISP2.

- A fim ajustar o tunnel0 como a interface principal neste exemplo de configuração, o *parâmetro de retardo* foi mudado, que permite as rotas que são instruídas do tunnel0 se tornar mais preferidas.

Note: Somente as seções relevantes da configuração são 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 a informação que é descrita nesta seção a fim verificar que sua configuração trabalha corretamente.

ISP preliminares e secundários ativos

Nesta encenação da verificação, os ISP preliminares e secundários são ativos. Estão aqui algumas notas adicionais sobre esta encenação:

- A fase 1 e a fase 2 para ambas as relações mGRE estão acima.
- Ambos os túneis vêm acima, mas as rotas através do tunnel0 (originado através do ISP principal) são preferidas.

Estão aqui os **comandos show** relevantes que você pode usar a fim verificar sua configuração nesta encenação:

```
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 para baixo/Active secundário ISP

Nesta encenação, os temporizadores da *posse* EIGRP expiram para o neighborship com o tunnel0 quando o link ISP1 vai para baixo, e as rotas ao hub e o outro spokes apontam agora a Tunnel1 (originado com Ethernet0/1).

Estão aqui os **comandos show** relevantes que você pode usar a fim verificar sua configuração nesta encenação:

```
*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 do link do ISP principal

Quando a Conectividade através do ISP principal é restaurada, a sessão de criptografia do tunnel0 torna-se ativa, e as rotas que são instruídas através da relação do 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
```

Troubleshooting

A fim pesquisar defeitos sua configuração, permita debugam o eigrp IP e o dmvpn de registro.

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

- A maioria de soluções comuns do Troubleshooting DMVPN
- Guia de Troubleshooting da família do Cisco MDS 9000, IPsec do Troubleshooting do do Â do âÂ da liberação 2.x
- Suporte Técnico e Documentação - Cisco Systems