Configureer ISP-redundantie op een DMVPN-toets met de VRF-Lite-functie

Inhoud

Inleiding

Dit document beschrijft hoe u de redundantie van Internet Service Provider (ISP) kunt configureren op een Dynamic Multipoint VPN (DMVPN) dat via de virtuele routing en Forwarding-Lite (VRF-Lite) wordt gesproken.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van deze onderwerpen voordat u probeert de configuratie die in dit document wordt beschreven te configureren:

- Basiskennis van VRF

- Basiskennis van het Enhanced Interior Gateway Routing Protocol (DHCP)
- Basiskennis van DMVPN

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS® versie 15.4(2)T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Het VRF is een technologie die in de IP netwerkrouters is opgenomen die meerdere instanties van een routingtabel toestaat om in een router samen te leven en gelijktijdig te werken. Dit verhoogt functionaliteit omdat het netwerkpaden kan worden gesegmenteerd zonder het gebruik van meerdere apparaten.

Het gebruik van dubbele ISP's voor redundantie is een algemeen gebruik geworden. Beheerders gebruiken twee ISP-koppelingen. de ene functioneert als een primaire verbinding en de andere als een back - upverbinding .

Het zelfde concept kan voor DMVPN redundantie op een gesproken met het gebruik van dubbele ISPs worden geïmplementeerd. Het doel van dit document is om aan te tonen hoe *VRF-Lite* kan worden gebruikt om de routingtabel te scheiden wanneer een gesproken persoon dubbele ISP's heeft. Dynamische routing wordt gebruikt om padredundantie te bieden voor het verkeer dat de DMVPN-tunnel doorkruist. De configuratievoorbeelden die in dit document worden beschreven gebruiken dit configuratieschema:

Interface	IP-adres	VRF	Beschrijving
Ethernet0/0	172.16.1.1	ISP1 VRF	Primaire ISP
Ethernet0/1	172.16.2.1	ISP2 VRF	Secundaire ISP

Met de optie VRF-Lite kunnen de meerdere VPN-routing/Forwarding-instanties worden ondersteund op de door DMVPN vertegenwoordigde functie. De eigenschappen VRF-Lite dwingt het verkeer van de meervoudige Generic Routing Encapsulation (mGRE) tunnelinterfaces om hun respectieve VRF-routingtabellen te gebruiken. Als de primaire ISP bijvoorbeeld eindigt in de *ISP1* VRF en de secundaire ISP eindigt in de *ISP2* VRF, dan gebruikt het verkeer dat door *ISP2* VRF wordt gegenereerd de *ISP2* VRF-routingtabel, terwijl het verkeer dat door *ISP VRF* wordt gegenereerd*,* de *VRF-routing gebruikt.*

Een voordeel dat met het gebruik van een *front door* VRF (fVRF) komt is primair om een afzonderlijke routingtabel uit de mondiale routingtabel te halen (waar tunnelinterfaces bestaan). Het voordeel met het gebruik van een *binnen* VRF (iVRF) is om een privé ruimte te definiëren om de DMVPN en privé netwerkinformatie te houden. Beide configuraties bieden extra beveiliging van aanvallen op de router van het internet, waar de routinginformatie wordt gescheiden.

Deze VRF-configuraties kunnen worden gebruikt op zowel het DMVPN-knooppunt als het gesprek. Dit geeft groot voordeel over een scenario waarin beide ISPs in de globale routingtabel eindigen.

Als beide ISP's in het globale VRF eindigen, delen zij de zelfde routingtabel en beiden van de mGRE interfaces vertrouwen op de globale routinginformatie. In dit geval, als de primaire ISP faalt, zal de primaire ISP-interface niet vallen, als het mislukkingspunt in het backbone netwerk van ISP's is gelegen en niet rechtstreeks is aangesloten. Dit resulteert in een scenario waar beide van de mGRE tunnelinterfaces nog de standaardroute gebruiken die naar de primaire ISP wijst, wat de redundantie van DMVPN om te falen veroorzaakt.

Hoewel er een paar tijdelijke oplossingen zijn die IP Service Level Agreements (IP SLA's) of Embedded Event Manager (EEM) scripts gebruiken om deze kwestie zonder VRF-Lite aan te pakken, zijn ze misschien niet altijd de beste keuze.

implementatiemethoden

Dit deel bevat korte overzichten van gesplitste tunneling en met de hand uitgedrukte tunnels.

Split-tunneling

Wanneer specifieke subnetten of samengevatte routes via een mGRE interface worden geleerd, dan wordt het *gesplitste tunneling* genoemd. Als de standaardroute via een mGRE-interface wordt geleerd, dan wordt hij *tunnel-all* genoemd.

Het configuratievoorbeeld dat in dit document beschikbaar is, is gebaseerd op een gesplitste tunneling.

Spoke-to-Spoke tunnels

Het configuratievoorbeeld dat in dit document wordt gegeven is een goed ontwerp voor de tunnel-all stationeringsmethode (de standaardroute wordt geleerd via de mGRE-interface).

Het gebruik van twee fVRF's scheidt de routing tabellen en zorgt ervoor dat de post-GRE ingekapselde pakketten naar de respectievelijke fVRF worden doorgestuurd, wat helpt om te verzekeren dat de toespraak-to-Speeltunnel met een actieve ISP komt.

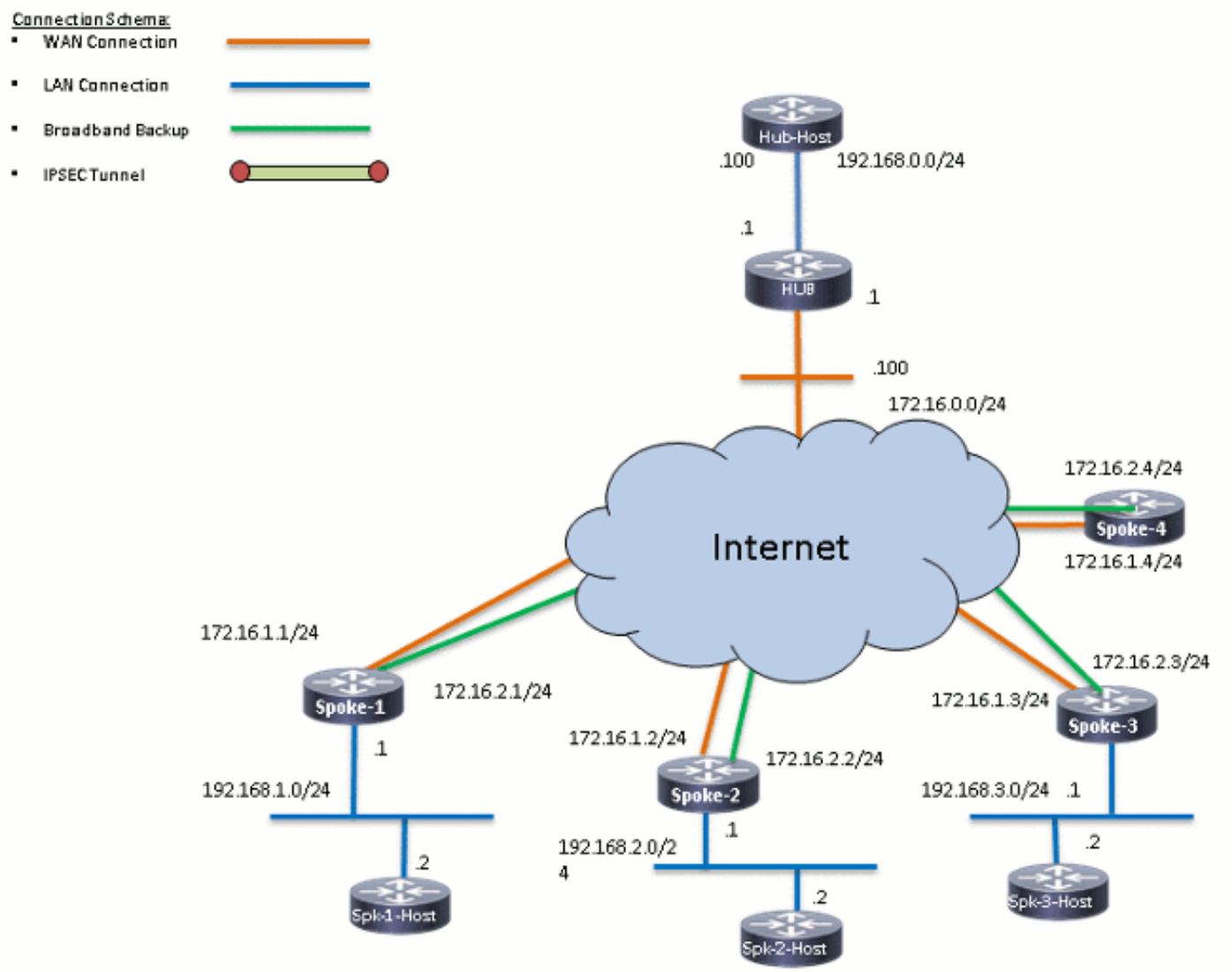
Configureren

In deze sectie wordt beschreven hoe u ISP-redundantie op een DMVPN kunt configureren dat via de VRF-Lite-functie wordt gesproken.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit is de topologie die voor de voorbeelden in dit document wordt gebruikt:



Hub-configuratie

Hier volgen wat opmerkingen over de relevante configuratie op het hub:

- Om *Tunnel0* in te stellen als de primaire interface in dit configuratievoorbeeld, *is* de vertragingsparameter gewijzigd, wat de routes die van *Tunnel0* worden geleerd om meer voorkeursbehandeling toestaat.

- Het **gedeelde** sleutelwoord wordt gebruikt met tunnelbescherming en een unieke *tunnelsleutel* wordt toegevoegd op alle mGRE interfaces omdat zij dezelfde *tunnelbron <interface>* gebruiken. Anders kunnen de inkomende Generic Routing Encapsulation (GRE) tunnelpakketten worden gestraft naar de onjuiste tunnelinterface na decryptie.

- Er wordt een routesamenvatting uitgevoerd om ervoor te zorgen dat alle woordjes de standaardroute via de mGRE-tunnels (**tunnels-all**) leren.

Opmerking: In dit voorbeeld zijn alleen de relevante delen van de configuratie opgenomen.

```
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
```

Spoelconfiguratie

Hier volgen wat opmerkingen over de configuratie in kwestie op de toespraak:

- Voor gesproken redundantie hebben *Tunnel0* en *Tunnel1 Ethernet0/0* en *Ethernet0/1* als de tunnelbroninterfaces. Ethernet0/0 wordt aangesloten op de primaire ISP en Ethernet0/1 wordt aangesloten op de secundaire ISP.

- Om de ISP's te scheiden, wordt de VRF-functie gebruikt. De primaire ISP gebruikt de *ISP* VRF. Voor de secundaire ISP wordt een VRF met de naam *ISP2* geconfigureerd.

- De *tunnel vrf ISP1* en de *tunnel vrf ISP2* zijn geconfigureerd op interfaces Tunnel0 en Tunnel1, respectievelijk om aan te geven dat de verzendraadpleging voor het ingekapselde pakket van na-GRE wordt uitgevoerd in VRF ISP1 of ISP2.

- Om Tunnel0 in te stellen als de primaire interface in dit configuratievoorbeeld, is de *vertragingsparameter* veranderd, die de routes die van Tunnel0 worden geleerd om meer voorkeur te geven aan.

  Opmerking: In dit voorbeeld zijn alleen de relevante delen van de configuratie opgenomen.

```
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
```

Verifiëren

Gebruik de informatie die in dit gedeelte wordt beschreven om te controleren of uw configuratie correct werkt.

Primaire en secundaire ISP's actief

In dit verificatiescenario zijn zowel de primaire als de secundaire ISP's actief. Hier volgen wat extra opmerkingen over dit scenario:

- Fase 1 en fase 2 voor beide mGRE-interfaces zijn omhoog.
- Beide tunnels komen naar boven, maar de routes via Tunnel0 (bron via de primaire ISP) hebben de voorkeur.

Hier zijn de relevante opdrachten **voor** de **show** die u kunt gebruiken om de configuratie van het apparaat in dit scenario te controleren:

```
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
```

Primaire ISP Down/Secundaire ISP actief

In dit scenario, verlopen de *tijden* van het*Houd* Ecu voor het buren door Tunnel0 wanneer de verbinding ISP1 omlaag gaat, en de routes naar de hub en de andere spaken richten nu naar Tunnel1 (bron met Ethernet0/1).

Hier zijn de relevante opdrachten voor de show die u kunt gebruiken om de configuratie van het apparaat in dit scenario te controleren:

```
*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
```

Herstel van primaire ISP-link

Wanneer de connectiviteit door de primaire ISP wordt hersteld, wordt de crypto sessie van Tunnel0 actief, en de routes die via de interface van Tunnel0 worden geleerd worden verkiest.

Hierna volgt een voorbeeld:

```
*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
```

Problemen oplossen

U kunt als volgt uw configuratie oplossen door ip eigrp en houtkap dmvpn te debug.

Hierna volgt een voorbeeld:

```
################### 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
```

Gerelateerde informatie

- Meest gebruikelijke DMVPN-probleemoplossing
- Cisco MDS 9000 Series handleiding voor probleemoplossing, release 2.x -oplossing voor IPsec probleemoplossing
- Technische ondersteuning en documentatie – Cisco Systems