Configuration de la redondance FAI sur une étoile DMVPN avec la fonction VRF-Lite

Contenu

Introduction

Ce document décrit comment configurer la redondance du fournisseur d'accès à Internet (FAI) sur un réseau VPN multipoint dynamique (DMVPN) en étoile via la fonctionnalité Virtual Routing and Forwarding-Lite (VRF-Lite).

Conditions préalables

Conditions requises

Cisco vous recommande de connaître ces rubriques avant de tenter la configuration décrite dans ce document :

- Connaissances de base de VRF

- Connaissances de base du protocole EIGRP (Enhanced Interior Gateway Routing Protocol)
- Connaissances de base du DMVPN

Components Used

Les informations de ce document sont basées sur Cisco IOS® Version 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.

Informations générales

Le VRF est une technologie incluse dans les routeurs de réseau IP qui permet à plusieurs instances d'une table de routage de coexister dans un routeur et de fonctionner simultanément. Cela augmente les fonctionnalités car cela permet de segmenter les chemins réseau sans utiliser plusieurs périphériques.

L'utilisation de deux FAI pour la redondance est devenue une pratique courante. Les administrateurs utilisent deux liaisons FAI ; l'une agit en tant que connexion principale et l'autre en tant que connexion de secours.

Le même concept peut être mis en oeuvre pour la redondance DMVPN sur un satellite avec l'utilisation de deux FAI. L'objectif de ce document est de démontrer comment *VRF-Lite* peut être utilisé afin de séparer la table de routage lorsqu'un rayon a deux FAI. Le routage dynamique est utilisé afin de fournir une redondance de chemin pour le trafic qui traverse le tunnel DMVPN. Les exemples de configuration décrits dans ce document utilisent ce schéma de configuration :

Interface	Adresse IP	VRF	Description
Ethernet0/0	172.16.1.1	VRF ISP1	FAI principal
Ethernet0/1	172.16.2.1	VRF ISP2	ISP secondaire

Avec la fonctionnalité VRF-Lite, plusieurs instances de routage/transfert VPN peuvent être prises en charge sur le satellite DMVPN. La fonctionnalité VRF-Lite force le trafic provenant de plusieurs interfaces de tunnel mGRE (Multipoint Generic Routing Encapsulation) à utiliser leurs tables de routage VRF respectives. Par exemple, si le FAI principal se termine dans le VRF du FAI1 et que le FAI secondaire se termine dans le VRF du FAI2, le trafic généré dans le VRF du FAI2 utilise la table de routage VRF du *FAI2*, tandis que le trafic généré dans le VRF du *FAI1* utilise la *table de routage VRF du*.

L'un des avantages de l'utilisation d'un VRF *de porte avant* (fVRF) consiste principalement à découper une table de routage séparée de la table de routage globale (où il existe des interfaces de tunnel). L'avantage de l'utilisation d'un VRF *interne* (iVRF) est de définir un espace privé afin de contenir le DMVPN et les informations de réseau privé. Ces deux configurations offrent une sécurité supplémentaire contre les attaques sur le routeur depuis Internet, où les informations de routage sont séparées.

Ces configurations VRF peuvent être utilisées à la fois sur le concentrateur DMVPN et le rayon. Cela offre un grand avantage par rapport à un scénario dans lequel les deux FAI se terminent dans la table de routage globale.

Si les deux FAI se terminent dans le VRF global, ils partagent la même table de routage et les deux interfaces mGRE dépendent des informations de routage globales. Dans ce cas, si le FAI principal échoue, l'interface principale du FAI peut ne pas tomber en panne si le point de défaillance se trouve dans le réseau fédérateur des FAI et n'est pas directement connecté. Cela entraîne un scénario dans lequel les deux interfaces de tunnel mGRE utilisent toujours la route par défaut qui pointe vers le FAI principal, ce qui entraîne l'échec de la redondance DMVPN.

Bien que certaines solutions de contournement utilisent des scripts IP SLA (IP Service Level Agreements) ou EEM (Embedded Event Manager) afin de résoudre ce problème sans VRF-Lite, elles peuvent ne pas toujours être le meilleur choix.

Méthodes de déploiement

Cette section fournit de brefs aperçus des tunnels de transmission tunnel partagée et des tunnels de rayon à rayon.

transmission tunnel partagée

Lorsque des sous-réseaux spécifiques ou des routes résumées sont appris via une interface mGRE, cela s'appelle *tunneling fractionné*. Si la route par défaut est apprise via une interface mGRE, elle est appelée *tunnel-all*.

L'exemple de configuration fourni dans ce document est basé sur la transmission tunnel partagée.

Tunnels satellite à satellite

L'exemple de configuration fourni dans ce document est une bonne conception pour la méthode de déploiement tunnel-all (la route par défaut est apprise via l'interface mGRE).

L'utilisation de deux fVRF sépare les tables de routage et garantit que les paquets encapsulés post-GRE sont transférés vers le fVRF respectif, ce qui permet de s'assurer que le tunnel de rayon à rayon est fourni avec un FAI actif.

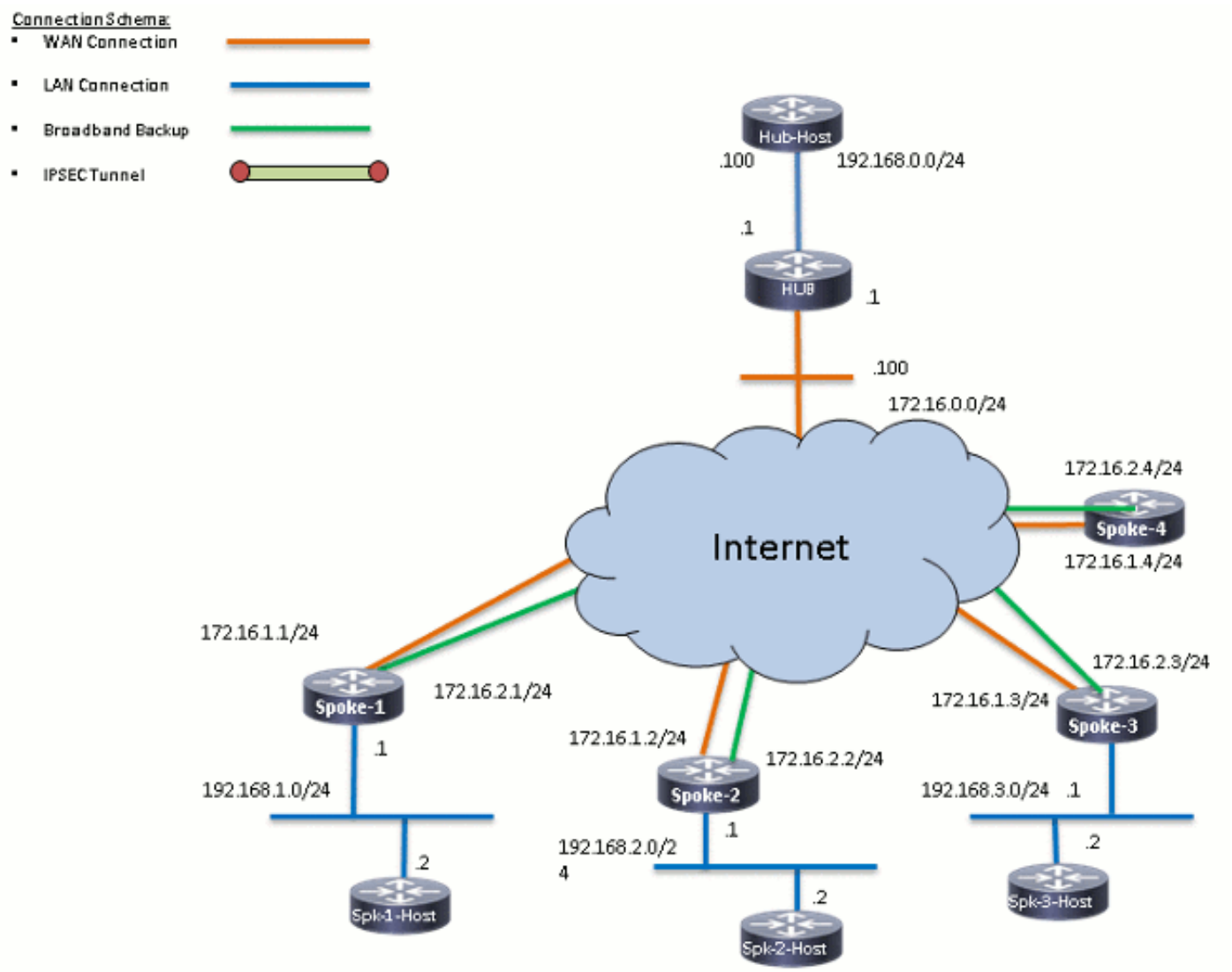
Configuration

Cette section décrit comment configurer la redondance ISP sur un satellite DMVPN via la fonctionnalité VRF-Lite.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Voici la topologie utilisée pour les exemples de ce document :



Configuration du concentrateur

Voici quelques notes sur la configuration appropriée sur le concentrateur :

- Afin de définir *Tunnel0* comme interface principale dans cet exemple de configuration, le paramètre *delay* a été modifié, ce qui permet aux routes apprises à partir de *Tunnel0* de devenir plus préférées.

- Le mot clé **partagé** est utilisé avec la protection du tunnel et une *clé de tunnel* unique est ajoutée sur toutes les interfaces mGRE parce qu'elles utilisent la même *source de tunnel <interface>*. Sinon, les paquets de tunnel GRE (Generic Routing Encapsulation) entrants peuvent être punis sur l'interface de tunnel incorrecte après le déchiffrement.

- Une récapitulation de route est effectuée afin de s'assurer que tous les rayons apprennent la route par défaut via les tunnels mGRE (**tunnel-all**).

Note: Seules les sections pertinentes de la configuration sont incluses dans cet exemple.

```
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
```

Configuration du rayon

Voici quelques notes sur la configuration pertinente sur le satellite :

- Pour la redondance en étoile, *Tunnel0* et *Tunnel1* ont *Ethernet0/0* et *Ethernet0/1* comme interfaces source du tunnel, respectivement. Ethernet0/0 est connecté au FAI principal et Ethernet0/1 au FAI secondaire.
- Afin de séparer les FAI, la fonctionnalité VRF est utilisée. Le FAI principal utilise le VRF *ISP1*. Pour le FAI secondaire, un VRF nommé *ISP2* est configuré.
- Les *tunnels vrf ISP1* et *tunnel vrf ISP2* sont configurés sur les interfaces Tunnel0 et Tunnel1, respectivement, afin d'indiquer que la recherche de transfert pour le paquet encapsulé post-GRE est effectuée dans VRF ISP1 ou ISP2.
- Afin de définir Tunnel0 comme interface principale dans cet exemple de configuration, le paramètre *delay* a été modifié, ce qui permet aux routes apprises à partir de Tunnel0 de devenir plus préférées.

Note: Seules les sections pertinentes de la configuration sont incluses dans cet exemple.

```
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
```

Vérification

Utilisez les informations décrites dans cette section afin de vérifier que votre configuration fonctionne correctement.

ISP principaux et secondaires actifs

Dans ce scénario de vérification, les FAI principal et secondaire sont actifs. Voici quelques notes supplémentaires sur ce scénario :

- Les phases 1 et 2 pour les deux interfaces mGRE sont actives.
- Les deux tunnels sont activés, mais les routes via Tunnel0 (source via le FAI principal) sont préférées.

Voici les commandes **show** appropriées que vous pouvez utiliser afin de vérifier votre configuration dans ce scénario :

```
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 désactivé/ISP secondaire actif

Dans ce scénario, les temporisateurs *d'attente* EIGRP expirent pour le voisinage via Tunnel0 lorsque la liaison ISP1 tombe en panne, et les routes vers le concentrateur et les autres rayons pointent maintenant vers Tunnel1 (source avec Ethernet0/1).

Voici les commandes **show** appropriées que vous pouvez utiliser afin de vérifier votre configuration dans ce scénario :

```
*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
```

Restauration de la liaison principale du FAI

Lorsque la connectivité via le FAI principal est restaurée, la session de chiffrement Tunnel0 devient active et les routes apprises via l'interface Tunnel0 sont préférées.

Voici un exemple :

```
*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
```

Dépannage

Afin de dépanner votre configuration, activez **debug ip eigrp** et **logging dmvpn**.

Voici un exemple :

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

Informations connexes

- Solutions de dépannage DMVPN les plus fréquentes
- Guide de dépannage de la gamme Cisco MDS 9000, version 2.x - âÂ Dépannage IPsec
- Support et documentation techniques - Cisco Systems