Configurez la Redondance ISP sur un DMVPN a parlé avec la configuration de Vrf-Lite

Contenu

Introduction

Ce document décrit comment configurer la Redondance de fournisseur de services Internet (ISP) sur un rai de VPN multipoint dynamique (DMVPN) par l'intermédiaire de la caractéristique virtuelle de routage et d'Expédition-Lite (Vrf-Lite).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de ces thèmes avant que vous tentiez la configuration qui est décrite dans ce document :

- Connaissance de base de VRF

- Connaissance de base de Protocole EIGPR (Enhanced Interior Gateway Routing Protocol)
- Connaissance de base de DMVPN

Composants utilisés

Les informations dans ce document sont basées sur la version 15.4(2)T de Cisco IOS®.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le VRF est une technologie incluse dans les Routeurs de réseau IP qui permet à des multiples instances d'une table de routage pour coexister dans un routeur et pour fonctionner simultanément. Ceci augmente la fonctionnalité parce qu'il permet les chemins réseau à segmenter sans utilisation de plusieurs périphériques.

L'utilisation de doubles ISP pour la Redondance est devenue une pratique commune. Les administrateurs utilisent deux liens ISP ; on agit en tant que connexion principale et l'autre agit en tant que connexion de sauvegarde.

Le même concept peut être mis en application pour la Redondance DMVPN sur un rai avec l'utilisation de doubles ISP. L'objectif de ce document est d'expliquer comment Vrf-*Lite* peut être utilisé afin d'isoler la table de routage quand un rai a de doubles ISP. Le routage dynamique est utilisé afin de fournir la redondance de chemin pour le trafic qui traverse le tunnel DMVPN. Les exemples de configuration qui sont décrits dans cette utilisation de document ce schéma de configuration :

Interface	Adresse IP	VRF	Description
Ethernet 0/0	172.16.1.1	VRF ISP 1	ISP primaire
Ethernet 0/1	172.16.2.1	VRF ISP 2	ISP secondaire

Avec la configuration de Vrf-Lite, le plusieurs routage/instances de transfert VPN peut être pris en charge sur le rai DMVPN. La caractéristique de Vrf-Lite force le trafic de plusieurs interfaces de tunnel multipoints de Generic Routing Encapsulation (mGRE) pour utiliser leurs tables de routage respectives de VRF. Par exemple, si l'ISP primaire se termine en VRF *ISP1* et l'ISP secondaire se termine en VRF *ISP2*, le trafic qui est généré dans le VRF *ISP2* utilise la table de routage du VRF *ISP2*, alors que le trafic qui est généré dans le VRF *ISP1* utilise la table de routage du VRF *ISP1*.

Un avantage qui est livré avec l'utilisation d'un VRF d'*entrée principale* (fVRF) est principalement de découper une table de routage distincte de la table de routage globale (où les interfaces de tunnel existent). L'avantage avec l'utilisation d'un VRF *intérieur* (iVRF) est de définir un espace privé afin de tenir le DMVPN et l'information réseau privée. Chacun des deux configurations

fournissent la Sécurité supplémentaire des attaques sur le routeur de l'Internet, où les informations de routage sont séparées.

Ces configurations de VRF peuvent être utilisées sur le les deux le hub and spoke DMVPN. Ceci donne le grand avantage par rapport à un scénario en lequel chacun des deux ISP se terminent dans la table globale de routage.

Si chacun des deux ISP se terminent en VRF global, elles partagent la même table de routage et chacun des deux interfaces de mGRE se fondent sur les informations de routage globales. Dans ce cas, si l'ISP primaire échoue, l'interface primaire ISP ne pourrait pas descendre si le point de panne est dans le réseau fédérateur des ISP et pas directement connecté. Ceci a comme conséquence un scénario où chacun des deux interfaces de tunnel de mGRE utilisent toujours le default route qui indique l'ISP primaire, qui fait échouer la Redondance DMVPN.

Bien qu'il y ait quelques contournements qui emploient des accords de niveau de service IP (IP SLA) ou des scripts inclus du gestionnaire d'événement (EEM) afin d'aborder cette question sans Vrf-Lite, ils ne pourraient pas toujours être le meilleur choix.

Méthodes de déploiement

Cette section fournit des brèves présentations des tunnels de Segmentation de tunnel et de spoke-to-spoke.

transmission tunnel partagée

Quand des sous-réseaux ou les récapitulatifs de routage spécifiques sont appris par l'intermédiaire d'une interface de mGRE, alors ce s'appelle la *Segmentation de tunnel*. Si le default route est appris par l'intermédiaire d'une interface de mGRE, alors il s'appelle tunnel-*tout*.

L'exemple de configuration qui est fourni dans ce document est basé sur la Segmentation de tunnel.

Tunnels de spoke-to-spoke

L'exemple de configuration qui est fourni dans ce document est une bonne conception pour la tunnel-toute méthode de déploiement (le default route est appris par l'intermédiaire de l'interface de mGRE).

L'utilisation de deux fVRFs isole les tables de routage et s'assure que les paquets encapsulés de POST-GRE sont expédiés au fVRF respectif, qui aide à s'assurer que le tunnel de spoke-to-spoke monte avec un ISP actif.

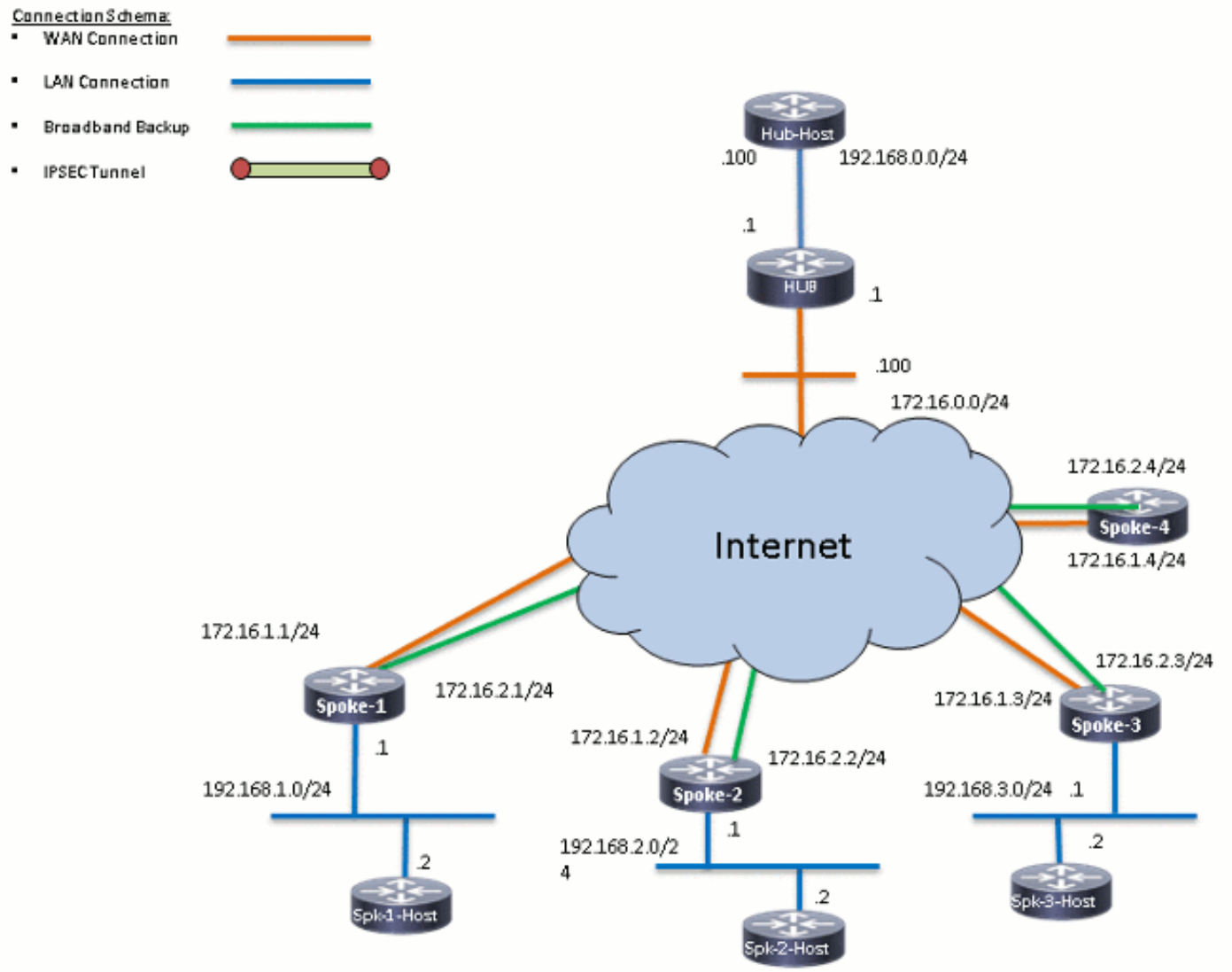
Configurez

Cette section décrit comment configurer la Redondance ISP sur un rai DMVPN par l'intermédiaire de la caractéristique de Vrf-Lite.

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

Diagramme du réseau

C'est la topologie qui est utilisée pour les exemples dans ce document :



Configuration du concentrateur

Voici quelques notes au sujet de la configuration appropriée sur le hub :

- Afin de placer *Tunnel0* comme interface principale dans cet exemple de configuration, le *paramètre de délai* a été changé, qui permet les artères qui sont apprises de *Tunnel0* pour devenir plus préférées.

- Le mot clé **partagé** est utilisé avec le tunnel protection et un seul *tunnel key* est ajouté sur toutes les interfaces de mGRE parce qu'ils utilisent le même *<interface> de source du tunnel*. Autrement, les paquets d'arrivée de tunnel d'Encapsulation de routage générique (GRE)

pourraient être donnés un coup de volée à l'interface de tunnel incorrecte après déchiffrement.

- Un résumé du routage est exécuté afin de s'assurer que tous les rais apprennent le default route par l'intermédiaire des tunnels de mGRE (tunnel-**tous**).

  Remarque: Seulement les sections afférentes 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 au sujet de la configuration appropriée sur le rai :

- Pour la Redondance de rai, *Tunnel0* et *Tunnel1* ont *Ethernet0/0* et *Ethernet0/1* comme interfaces de source du tunnel, respectivement. Ethernet0/0 est connecté à l'ISP et à l'Ethernet0/1 primaires est connecté à l'ISP secondaire.

- Afin d'isoler les ISP, la caractéristique de VRF est utilisée. L'ISP primaire utilise le VRF *ISP1*. Pour l'ISP secondaire, un VRF nommé *ISP2* est configuré.

- *Le tunnel vrf ISP1* et le *tunnel vrf ISP2* sont configurés sur les interfaces Tunnel0 et Tunnel1, respectivement, afin d'indiquer que la recherche de transfert pour le paquet encapsulé de POST-GRE est effectuée dans le VRF ISP1 ou l'ISP2.

- Afin de placer Tunnel0 comme interface principale dans cet exemple de configuration, le *paramètre de délai* a été changé, qui permet les artères qui sont apprises de Tunnel0 pour devenir plus préférées.

  Remarque: Seulement les sections afférentes 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
```

Vérifiez

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

ISP primaires et secondaires actifs

Dans ce scénario de vérification, les ISP primaires et secondaires sont en activité. Voici quelques notes supplémentaires au sujet de ce scénario :

- Le Phase 1 et la phase 2 pour chacun des deux interfaces de mGRE sont en hausse.
- Chacun des deux tunnels montent, mais les artères par l'intermédiaire de Tunnel0 (originaire par l'intermédiaire de l'ISP primaire) sont préférées.

Voici les **commandes show** appropriées que vous pouvez employer 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 primaire vers le bas/Active secondaire ISP

Dans ce scénario, les temporisateurs d'*attente* EIGRP expirent pour la proximité par Tunnel0 quand le lien ISP1 descend, et les artères au hub et aux autres rais indiquent maintenant Tunnel1 (originaire avec Ethernet0/1).

Voici les commandes show appropriées que vous pouvez employer 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 primaire de lien ISP

Quand la Connectivité par l'ISP primaire est restaurée, la crypto session Tunnel0 devient active, et les artères qui sont apprises par l'intermédiaire de 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
```

Dépannez

Afin de dépanner votre configuration, l'enable **mettent au point l'eigrp d'IP** et le **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 famille du Cisco MDS 9000, du Â d'âÂ de la release 2.x dépannant IPsec
- Support et documentation techniques - Cisco Systems