VPN IPSec multipoint dynamiques (utilisation de GRE multipoint/NHRP pour étendre les VPN IPsec)

Contenu

Introduction

Ce document discute des VPN IPsec multipoint dynamique (DMVPN) et pourquoi une société pourrait vouloir concevoir ou migrer leur réseau pour se servir de cette nouvelle solution VPN IPsec dans le logiciel Cisco IOS®.

Informations générales

Les sociétés peuvent avoir besoin d'interconnecter beaucoup de sites à un site principal, et peut-être également entre eux, à travers Internet tout en cryptant le trafic pour le protéger. Par exemple, des magasins qui doivent se connecter au siège social de la société pour la gestion des stocks et les commandes peuvent également avoir besoin de se connecter à d'autres magasins de la société pour vérifier la disponibilité des produits. Dans le passé, la seule façon d'établir la connexion était d'employer un réseau double couche tel que l'ISDN ou le Frame Relay pour interconnecter tout. L'installation et l'investissement pour ces liaisons câblées pour le trafic IP interne peuvent être longs et coûteux. Si tous les sites (site principal compris) ont déjà un accès Internet relativement bon marché, alors cet accès Internet peut également être utilisé pour la communication IP interne entre les magasins et le siège social à l'aide des tunnels IPsec pour assurer la confidentialité et l'intégrité des données.

Pour que les sociétés établissent de grands réseaux d'IPsec interconnectant leurs sites à travers Internet, vous devez être capable de faire évoluer le réseau d'IPsec. IPsec crypte le trafic entre deux points de terminaison (homologues), et le cryptage est fait par les deux points de terminaison à l'aide d'un « secret » partagé. Puisque ce secret est partagé seulement entre ces deux points de terminaison, les réseaux cryptés sont en soi une collection de liaisons point à point. Pour cette raison, IPsec est intrinsèquement un réseau tunnel point à point. La méthode la plus faisable pour faire évoluer un grand réseau point à point est de l'organiser en un réseau en étoile ou en un réseau maillé complet (partiel). Dans la plupart des réseaux, la majorité du trafic IP se fait entre les rayons et le concentrateur, et très peu entre les rayons, ainsi la conception de réseau étoile est souvent le meilleur choix. Cette conception s'accorde également avec des réseaux Frame relay plus anciens puisqu'il était beaucoup trop cher de payer des liaisons entre tous les sites dans ces réseaux.

En utilisant Internet comme l'interconnexion entre le concentrateur et les rayons, les rayons ont également l'accès direct entre eux sans frais supplémentaires, mais il a été très difficile, voire impossible, d'installer et/ou gérer un réseau maillé complet (partiel). Les réseaux maillés complets ou partiels sont souvent souhaitables parce qu'il peut y avoir des économies de coûts si le trafic de routage spoke-to-spoke peut se faire, au lieu de passer par le concentrateur. Le trafic spoke-to-spoke traversant le concentrateur utilise ses ressources et peut provoquer des délais, particulièrement en utilisant le cryptage IPsec, puisque le concentrateur devra décrypter les paquets des rayons envoyeurs, puis recrypter le trafic pour l'envoyer au rayon receveur. Un autre exemple où le trafic de routage direct spoke-to-spoke serait utile est le cas où deux rayons sont dans la même ville et le concentrateur se trouve à l'autre bout du pays.

Alors que les réseaux en étoile IPsec étaient déployés et se développaient en taille, il est devenu plus souhaitable de les faire router des paquets d'IP aussi dynamiquement que possible. Dans anciens réseaux en étoile Frame Relay, ceci a été accompli en exécutant un protocole de routage dynamique comme OSPF ou EIGRP sur des liaisons Frame Relay. C'était utile pour annoncer dynamiquement l'accessibilité des réseaux en étoile et prendre en charge également la redondance dans le réseau de routage IP. Si le réseau perdait un routeur concentrateur, un routeur de concentrateur de secours pouvait automatiquement lui succéder pour maintenir la connectivité réseau aux réseaux en étoile.

Il y a un problème fondamental avec les tunnels IPsec et les protocoles de routage dynamique. Les protocoles de routage dynamiques se basent sur l'utilisation de Multicast IP ou de paquets de diffusion, mais IPsec ne prend pas en charge le cryptage de multicast ou des paquets de diffusion. La méthode actuelle pour résoudre ce problème est d'utiliser les tunnels d'encapsulation de routage générique (GRE) en combination avec le chiffrement IPsec.

Les tunnels GRE prennent en charge le transport du Multicast IP et des paquets de diffusion à l'autre extrémité du tunnel GRE. Le paquet de tunnel GRE est un paquet de monodiffusion IP. Ainsi, le paquet GRE peut être crypté à l'aide d'IPsec. Dans ce scénario, GRE effectue le travail de tunnel et IPsec se charge de la partie cryptage pour supporter le réseau VPN. Lorsque des tunnels GRE sont configurés, les adresses IP pour les points de terminaison du tunnel (**source du tunnel…**, **destination du tunnel…**) doivent être connues de l'autre point de terminaison et doit être routable par Internet. Ceci signifie que le concentrateur et tous les routeurs en étoile dans ce réseau doivent avoir des adresses IP non-privées statiques.

Pour de petites connexions de site à Internet, il est courant que l'adresse IP externe d'un rayon change à chaque fois qu'il se connecte à Internet parce que leur fournisseur d'accès Internet (ISP) fournit dynamiquement l'adresse d'interface externe (par l'intermédiaire du protocole DHCP (Dynamic Host Configuration Protocol)) chaque fois que le rayon est en ligne (Ligne d'abonné numérique à débit asymétrique (ADSL) et services de câble). Cette allocation dynamique de « l'adresse externe » du routeur permet à l'ISP d'élargir l'utilisation de leur espace d'adresse Internet, puisque tous les utilisateurs ne seront pas en ligne en même temps. Il peut être considérablement plus cher de payer le fournisseur pour allouer une adresse statique au routeur en étoile. L'exécution d'un protocole de routage dynamique sur un VPN IPSec requiert l'utilisation de tunnels GRE, mais vous perdez la possibilité d'avoir des rayons avec des adresses IP dynamiquement alloués sur leurs interfaces physiques extérieures.

Les restrictions ci-dessus et quelques autres sont récapitulées aux quatre points suivants :

- IPsec emploie une liste de contrôle d'accès (ACL) pour définir quelles données doivent être chiffrées. Ainsi, chaque fois que un nouveau (sous-)réseau est ajouté derrière un rayon ou le concentrateur, le client doit modifier l'ACL sur le concentrateur et sur les routeurs en étoile. Si le fournisseur d'accès gère le routeur, alors le client doit informer le fournisseur d'accès afin que l'ACL IPsec soit modifié de sorte que le nouveau trafic de routage soit crypté.
- Avec de grands réseaux en étoile, la taille de la configuration sur le routeur concentrateur peut devenir très grande jusqu'à devenir inutilisable. Par exemple, un routeur concentrateur aurait besoin de jusqu'à 3 900 lignes de configuration pour prendre en charge 300 routeurs en étoile. C'est tellement grand qu'il serait difficile d'afficher la configuration et de rechercher la section de la configuration qui se rapporte à un problème actuel qui est en cours de débogage. Également, cette configuration de taille peut être trop grande pour la NVRAM et devrait être enregistrée en mémoire flash.
- GRE + IPsec doivent connaître l'adresse d'homologue du point de terminaison. Les adresses IP des rayons sont connectées directement à Internet par l'intermédiaire de leur propre FAI, et elles sont souvent installées de sorte que leurs adresse d'interface externe n'est pas fixe. Les adresses IP peuvent changer chaque fois que le site se met en ligne (par l'intermédiaire du DHCP).
- Si les rayons doivent parler directement entre eux via VPN IPSec, alors le réseau en étoile doit devenir un réseau maillé global. Comme il n'est pas possible de savoir quel rayon aura besoin de parler directement avec un autre, un réseau maillé global est nécessaire, même si chaque rayon n'aura peut-être pas besoin de parler directement avec tous les autres rayons. En outre, il n'est pas faisable de configurer IPsec sur un petit routeur en étoile de sorte qu'il ait une connexion directe avec tous les autres routeurs en étoile dans le réseau ; ainsi les routeurs en étoile peuvent avoir besoin d'être des routeurs plus puissants.

La solution DMVPN

La solution de routage DMVPN emploie le multipoint GRE (mGRE) et le protocole de résolution de sauts successifs (NHRP), avec IPsec et quelques nouvelles améliorations, pour résoudre les problèmes de routage ci-dessus d'une manière évolutive.

Démarrage automatique du cryptage IPsec

Quand la solution DMVPN n'est pas utilisée, le tunnel de cryptage IPsec n'est pas lancé jusqu'à ce qu'il y ait du trafic de données qui requiert l'utilisation de ce tunnel IPsec. Il peut falloir entre 1 et 10 secondes pour terminer le démarrage du tunnel IPsec et le trafic de données est stoppé pendant ce temps. En utilisant GRE avec IPsec, la configuration de tunnel GRE inclut déjà l'adresse de l'homologue de tunnel GRE (**destination du tunnel…**) , qui est également l'adresse d'homologue IPsec. Chacune des deux adresses est préconfigurée.

Si vous utilisez le Tunnel Endpoint Discovery (TED) et des cartes de chiffrement dynamique sur le routeur concentrateur, alors vous pouvez éviter de devoir préconfigurer les adresses d'homologue IPsec sur le concentrateur, mais un probe and response de TED doit être envoyé et reçu avant que la négociation ISAKMP puisse commencer. Ceci ne devrait pas être nécessaire puisque, en utilisant GRE, les adresses d'origine et de destination d'homologue sont déjà connues. Elles sont en configuration ou résolues avec le NHRP (pour les tunnels GRE multipoints).

Avec la solution de routage DMVPN, IPsec est déclenché immédiatement pour les tunnels GRE point par point et multipoints. En outre, il n'est pas nécessaire de configurer un ACL de cryptage, puisque ceux-ci seront automatiquement dérivés des adresses d'origine et de destination du tunnel GRE. Les commandes suivantes sont utilisées pour définir les paramètres de cryptage IPsec. Notez qu'il n'y a aucune commande **set peer ...** ou **match address ...** requise parce que ces informations sont dérivées directement des mappages du tunnel GRE ou du NHRP associés.

```
crypto ipsec profile <profile-name> set transform-set <transform-name>
```

La commande suivante associe une interface du tunnel au profil IPSec.

```
interface tunnel<number> ... tunnel protection ipsec profile <profile-name>
```

Création dynamique de tunnel pour les liaisons « Spoke-to-Hub »

Aucune information GRE ou IPsec sur un rayon n'est configurée sur le routeur concentrateur dans le réseau DMVPN. Le tunnel GRE du routeur en étoile est configuré (par l'intermédiaire des commandes de NHRP) avec des informations concernant le routeur concentrateur. Quand le routeur en étoile démarre, il lance automatiquement le tunnel IPsec avec le routeur concentrateur comme décrit ci-dessus. Il emploie alors le NHRP pour informer le routeur concentrateur de son adresse IP d'interface physique actuelle. Ceci est utile pour trois raisons :

- Si le routeur en étoile fait attribuer son adresse IP d'interface physique dynamiquement (comme avec l'ADSL ou le modem câble), alors le routeur concentrateur ne peut pas être configuré avec ces informations puisque chaque fois que le routeur en étoile se recharge il obtiendra une nouvelle adresse IP d'interface physique.
- La configuration du routeur concentrateur se raccourcit et est simplifiée puisqu'elle n'a pas besoin d'informations GRE ou IPsec concernant les routeurs partenaire. Toutes ces informations sont apprises dynamiquement via NHRP.
- Quand vous ajoutez un nouveau routeur en étoile au réseau DMVPN, vous n'avez pas besoin de modifier la configuration sur le concentrateur ou sur les routeurs en étoile actuels. Le

nouveau routeur en étoile est configuré avec les informations du concentrateur, et quand il démarre, il s'inscrit dynamiquement au routeur concentrateur. Le protocole de routage dynamique propage les informations de routage pour ce rayon au concentrateur. Le concentrateur propage ces nouvelles informations de routage aux autres rayons. Il propage également les informations de routage des autres rayons à ce rayon.

Création dynamique de tunnel pour les trafics « Spoke-to-Spoke »

Comme indiqué plus tôt, actuellement dans un réseau maillé, tous les tunnels point à point IPsec (ou IPsec+GRE) doivent être configurés sur tous les routeurs, même si certains/la plupart de ces tunnels ne sont pas nécessaires à tout moment. Avec la solution DMVPN, un routeur est le concentrateur, et tous les autres routeurs (rayons) sont configurés avec des tunnels vers le concentrateur. Les tunnels de rayon-à-concentrateur sont continuellement en ligne, et les rayons n'ont pas besoin de la configuration pour les tunnels directs aux autres rayons. Au lieu de cela, quand un rayon veut transmettre un paquet à un autre rayon (tel que le sous-réseau derrière un autre rayon), elle emploie NHRP pour déterminer dynamiquement l'adresse de destination requise du rayon cible. Le routeur concentrateur agit en tant que serveur NHRP et traite cette demande pour le rayon source. Les deux rayons créent alors dynamiquement un tunnel IPsec entre eux (par l'intermédiaire de l'interface simple mGRE) et des données peuvent être directement transférées. Ce tunnel dynamique de rayon à rayon sera automatiquement démoli après une période d'inactivité (configurable).

Prise en charge des protocoles de routage dynamiques

La solution DMVPN est basée sur les tunnels GRE qui prennent en charge des paquets de multicast/diffusion IP de transmission tunnel. Ainsi, la solution DMVPN prend en charge également les protocoles de routage dynamiques s'exécutant au-dessus des tunnels IPsec+mGRE. Précédemment, le NHRP vous obligeait à configurer explicitement le mappage diffusion/multicast pour que les adresses IP du tunnel de destination pour prendre en charge la transmission tunnel GRE des paquets IP multicast et de diffusion. Par exemple, au niveau du concentrateur vous auriez besoin de la ligne de configuration **ip nhrp map multicast <spoke-n-addr>** pour chaque rayon. Avec la solution DMVPN, les adresses des rayons ne sont pas connues à l'avance et cette configuration n'est donc pas possible. Au lieu de cela, NHRP peut être configuré pour ajouter automatiquement chaque rayon à la liste de destination multicast sur le concentrateur avec la commande **ip nhrp map multicast dynamic**. Avec cette commande, quand les routeurs en étoile enregistrent leur mappage de NHRP de monodiffusion avec le serveur NHRP (concentrateur), NHRP créera également un mappage diffusion/multicast pour ce rayon. Ceci élimine le besoin de connaître les adresses des rayons à l'avance.

Commutation rapide de Cisco Express Forwarding pour mGRE

Actuellement, le trafic dans une interface de mGRE est commuté par processus, ce qui entraîne des performances médiocres. La solution DMVPN ajoute la commutation de Cisco Express Forwarding pour le trafic mGRE, ce qui entraîne des performances bien meilleures. Il n'y a aucune commande de configuration nécessaire pour activer cette fonctionnalité. Si la commutation de Cisco Express Forwarding est autorisée sur l'interface de tunnel GRE et sur les interfaces physiques sortantes/entrantes, alors les paquets du tunnel GRE multipoints seront commutés par Cisco Express Forwarding.

Utilisation du routage dynamique sur les VPN protégés par IPsec

Cette section décrit la situation actuelle (antérieure à la solution DMVPN). IPsec est mis en application sur les routeurs Cisco par l'intermédiaire d'un ensemble de commandes qui définissent le cryptage, puis une commande **crypto map <map-name>** appliquée sur l'interface externe du routeur. En raison de cette conception et du fait qu'il n'y a actuellement aucune norme pour l'usage d'IPsec pour crypter des paquets IP multicast/diffusion, les paquets du protocole de routage IP ne peuvent pas « être transférés » par le tunnel IPsec et aucune modification du routage ne peut être dynamiquement propagée de l'autre côté du tunnel IPsec.

Remarque: Tous les protocoles de routage dynamiques excepté le BGP utilisent des paquets IP de diffusion ou de multicast. Les tunnels GRE sont utilisés en combinaison avec IPsec pour résoudre ce problème de routage.

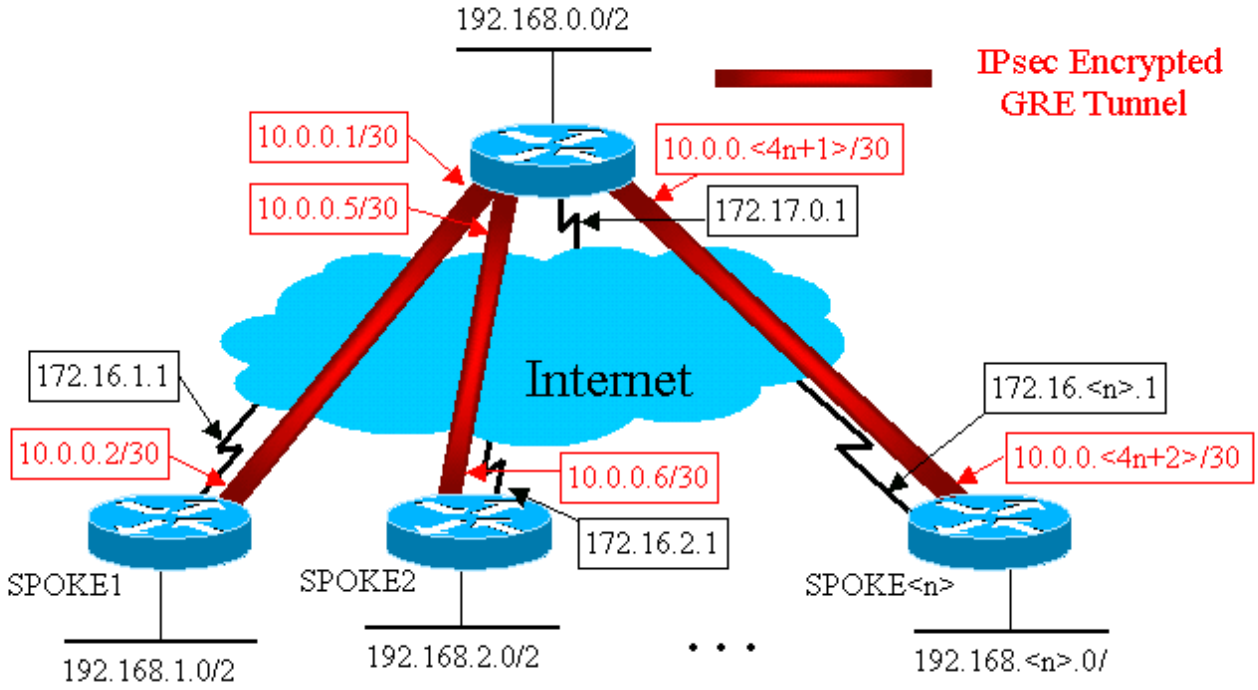
Les tunnels GRE sont mis en application sur les routeurs Cisco à l'aide d'une interface de tunnel virtuel (**interface tunnel<#>**). Le protocole de transmission tunnel GRE est conçu pour prendre en charge les paquets IP multicast/diffusion pour qu'un protocole de routage dynamique puisse être « exécuté » sur un tunnel GRE. Les paquets de tunnel GRE sont des paquets de monodiffusion IP qui encapsulent le paquet IP multicast/monodiffusion original. Vous pouvez alors utiliser IPsec pour crypter le paquet du tunnel GRE. Vous pouvez également exécuter IPsec en mode transport et économiser 20 octets puisque GRE a déjà encapsulé le paquet des données originales. Vous n'avez donc pas besoin qu'IPsec encapsule le paquet IP GRE dans un autre en-tête IP.

En exécutant IPsec en mode de transport, il y a une restriction qui fait que les adresses IP d'origine et de destination du paquet à chiffrer doivent correspondre aux adresses d'homologue IPsec (le routeur lui-même). Dans ce cas, ceci signifie juste que le point de destination du tunnel GRE et des adresses de l'homologue IPsec doivent être identiques. Ce n'est pas un problème puisque les mêmes routeurs sont à la fois les points de destination d'IPsec et du tunnel GRE. En combinant des tunnels GRE avec le cryptage IPsec, vous pouvez utiliser un protocole de routage dynamique IP pour mettre à jour les tables de routage aux deux extrémités du tunnel crypté. Les entrées de la table de routage IP pour les réseaux qui ont été appris via le tunnel crypté auront l'autre extrémité du tunnel (adresse IP de l'interface de tunnel GRE) comme prochain saut d'IP. Ainsi, si les réseaux changent d'un côté ou de l'autre du tunnel, alors l'autre côté apprendra dynamiquement la modification et la connectivité continuera sans aucune modification de configuration des routeurs.

Configuration de base

Ce qui suit est une configuration standard IPsec+GRE point à point. Après cela y a une série d'exemples de configuration où des caractéristiques spécifiques de la solution DMVPN sont ajoutées dans les étapes pour montrer les différentes fonctionnalités de DMVPN. Chaque exemple met à profit les exemples précédents pour montrer comment utiliser la solution DMVPN dans des conceptions de réseaux de plus en plus complexes. Cette succession d'exemples peut être utilisée comme modèle pour migrer un VPN IPsec+GRE actuel vers un DMVPN. Vous pouvez arrêter « le transfert » à n'importe quel point si cet exemple de configuration particulier correspond à vos exigences en termes de conception de réseaux.

Concentrateur et rayon IPsec + GRE (n = 1,2,3,…)



Routeur concentrateur

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.16.1.1 set
transform-set trans2 match address 101 crypto map
vpnmap1 20 ipsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10*n> ipsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-3> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! interface Ethernet1
ip address 192.168.0.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.0.0 0.0.0.255
no auto-summary ! access-list 101 permit gre host
172.17.0.1 host 172.16.1.1 access-list 102 permit gre
host 172.17.0.1 host 172.16.2.1 ... access-list <n+100>
permit gre host 172.17.0.1 host 172.16.<n>.1
```

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1 authentication pre-share crypto
isakmp key cisco47 address 0.0.0.0 ! crypto ipsec
transform-set trans2 esp-des esp-md5-hmac mode transport
! crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.1.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.6
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.2.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

Routeur Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport ! crypto map vpnmap1 local-address
Ethernet0 crypto map vpnmap1 10 ipsec-isakmp set peer
172.17.0.1 set transform-set trans2 match address 101 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.<4n-
```

```
2> 255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address
192.168.<n>.1 255.255.255.0 ! router eigrp 1 network
10.0.0.0 0.0.0.255 network 192.168.<n>.0 0.0.0.255 no
auto-summary ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1
```

Dans la configuration ci-dessus, les listes de contrôle d'accès sont utilisées pour définir quel trafic sera crypté. Sur le concentrateur et les routeurs en étoile, cette ACL doit seulement correspondre aux paquets IP du tunnel GRE. Peu importe comment les réseaux sont modifié à l'une ou l'autre extrémité, les paquets IP de tunnel GRE ne seront pas modifiés, donc cet ACL n'a pas besoin d'être modifié.

Remarque: En utilisant des versions du logiciel Cisco IOS antérieures à la 12.2(13)T, vous devez appliquer la commande de configuration **crypto map vpnmap1** aux interfaces de tunnel GRE (Tunnel<x>) et à l'interface physique (Ethernet0). Avec Cisco IOS version 12.2(13)T et ultérieures, vous appliquez seulement la commande de configuration **crypto map vpnmap1** à l'interface physique (Ethernet0).

Exemples des tableaux de routage sur les routeurs en étoile

Tableau de routage sur le routeur concentrateur

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Tableau de routage sur le routeur Spoke1

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Tableau de routage sur le routeur Spoke<n>

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 ...
 C        10.0.0.<4n-4> is directly connected, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 ...
 C    192.168.<n>.0/24 is directly connected, Ethernet0
```

Ceci est une configuration fonctionnelle de base qui est utilisée comme point de départ pour la comparaison avec des configurations plus complexes possibles en utilisant la solution DMVPN. La première modification réduira la taille de la configuration sur le routeur concentrateur. Ce n'est pas important avec un nombre restreint de routeurs en étoile, mais cela le devient quand il y a plus de 50 à 100 routeurs en étoile.

Réduction de la taille de la configuration du routeur concentrateur

Dans l'exemple suivant, la configuration est modifiée d'une façon minimale sur le routeur concentrateur et passe de plusieurs interfaces de tunnel GRE point à point, à une interface de tunnel GRE multipoint. C'est une première étape dans la solution DMVPN.

Il y a un seul bloc de lignes de configuration sur le routeur concentrateur pour définir les caractéristiques la carte de cryptage pour chaque routeur en étoile. Ce bloc de configuration définit l'ACL de cryptage et l'interface de tunnel GRE pour ce routeur en étoile. Ces caractéristiques sont en grande partie identiques pour tous les rayons, excepté pour les adresses IP (**homologue défini…**, **destination du tunnel…**).

En regardant la configuration du routeur concentrateur ci-dessus, vous voyez qu'il y a au moins 13 lignes de configuration par routeur en étoile ; quatre pour la carte de cryptage, un pour l'ACL de cryptage, et huit pour l'interface de tunnel GRE. Le nombre total de lignes de configuration, s'il y avait 300 routeurs en étoile, est 3 900 lignes. Vous avez besoin également de 300 (/30) sous-réseaux pour adresser chaque liaison de tunnel. Il est très difficile de gérer une configuration de cette taille et bien plus difficile lors du dépannage du réseau privé virtuel. Pour réduire cette valeur, vous pourriez utiliser des cartes de cryptage dynamique, qui réduiraient la valeur ci-dessus à 1 200, laissant 2 700 lignes dans un réseau de 300 rayons.

Remarque: En utilisant des cartes de cryptage dynamique, le tunnel de cryptage IPsec doit être lancé par le routeur en étoile. Vous pouvez également utiliser **ip unnumbered <interface>** pour réduire le nombre de sous-réseaux requis pour les tunnels GRE, mais ceci peut rendre le dépannage plus difficile plus tard.

Avec la solution DMVPN, vous pouvez configurer une seule interface de tunnel GRE multipoint et un seul profil IPSec sur le routeur concentrateur pour prendre en charge tous les routeurs en étoile. Ceci permet à la taille de la configuration sur le routeur concentrateur de rester identique,

quel que soit le nombre de routeurs en étoile ajoutés au réseau VPN.

La solution DMVPN introduit les nouvelles commandes suivantes :

crypto ipsec profile <name> <ipsec parameters> tunnel protection ipsec profile <name> ip nhrp map multicast dynamic

La commande **crypto ipsec profile <name>** est utilisée comme une carte de cryptage dynamique, et elle est conçue spécifiquement pour les interfaces de tunnel. Cette commande est utilisée pour définir les paramètres pour le cryptage IPsec sur les tunnels VPN de rayon à concentrateur et de rayon à rayon. Le seul paramètre qui est requis sous le profil est le jeu de transformations. L'adresse d'homologue IPsec et la clause **match address ...** pour le proxy IPsec sont automatiquement dérivées des mappages NHRP pour le tunnel GRE.

La commande **tunnel protection ipsec profile <name>** est configurée sous l'interface de tunnel GRE et est utilisée pour associer l'interface de tunnel GRE avec le profil IPSec. En outre, la commande **tunnel protection ipsec profile <name>** peut également être utilisée avec un tunnel GRE point à point. Dans ce cas elle dérivera les informations d'homologue et de proxy IPsec de la configuration **tunnel source…** et **tunnel destination…**. Ceci simplifie la configuration puisque l'homologue IPsec et l'ACL de cryptage ne sont plus nécessaires.

Remarque: La commande **tunnel protection…** spécifie que le cryptage IPsec sera fait après que l'encapsulation GRE ait été ajoutée au paquet.

Ces deux premières nouvelles commandes sont semblables à la configuration d'une carte de cryptage et à l'attribution de la carte de cryptage à une interface en utilisant la commande **crypto map <name>**. La grande différence est que, avec les nouvelles commandes, vous n'avez pas besoin de spécifier l'adresse d'homologue IPsec ou une ACL pour correspondre aux paquets à crypter. Ces paramètres sont automatiquement déterminés à partir des mappages NHRP pour l'interface de tunnel mGRE.

Remarque: En utilisant la commande **tunnel protection…** sur l'interface du tunnel, une commande **crypto map ...** n'est pas configurée sur l'interface sortante physique.

La dernière nouvelle commande, **ip nhrp map multicast dynamic**, permet au NHRP d'ajouter automatiquement des routeurs en étoile aux mappages NHRP multicast quand ces routeurs en étoile lancent le tunnel mGRE+IPsec et enregistrent leurs mappages de monodiffusion NHRP. Ceci est nécessaire pour permettre à des protocoles de routage dynamiques de fonctionner sur des tunnels mGRE+IPsec entre le concentrateur et les rayons. Si cette commande n'était pas disponible, alors le routeur concentrateur devrait avoir une ligne distincte de configuration pour un mappage multicast pour chaque rayon.

Remarque: Avec cette configuration, les routeurs en étoile doivent lancer la connexion en tunnel mGRE+IPsec, puisque le routeur concentrateur n'est configuré avec aucune information sur les rayons. Mais ce n'est pas un problème parce qu'avec DMVPN le tunnel mGRE+IPsec est automatiquement lancé quand le routeur en étoile démarre, et il reste toujours en ligne.

Remarque: Les exemples suivants montrent des interfaces de tunnel GRE point à point sur les routeurs en étoile et des lignes de configuration NHRP ajoutées sur le concentrateur et sur les routeurs en étoile pour prendre en charge le tunnel mGRE sur le routeur concentrateur. Les modifications de la configuration sont les suivantes.

Routeur concentrateur (vieux)

```
crypto map vpnmap1 10 IPsec-isakmp set peer 172.16.1.1
set transform-set trans2 match address 101 crypto map
vpnmap1 20 IPsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10n> IPsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-1> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! access-list 101
permit gre host 172.17.0.1 host 172.16.1.1 access-list
102 permit gre host 172.17.0.1 host 172.16.2.1 . . .
access-list <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

Routeur concentrateur (nouveau)

```
crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.1
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map multicast dynamic ip nhrp network-id 100000 ip
nhrp holdtime 600 no ip split-horizon eigrp 1 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0
```

Routeur Spoke<n> (vieux)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252 ip mtu 1400
delay 1000 tunnel source Ethernet0 tunnel destination
172.17.0.1 ! interface Ethernet0 ip address 172.16.<n>.1
255.255.255.252 crypto map vpnmap1 ! . . . ! access-list
101 permit gre host 172.16.<n>.1 host 172.17.0.1 !
```

Routeur Spoke<n> (nouveau)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip
```

```
nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp
nhs 10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 ! interface
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! . . . ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1 !
```

Sur les routeurs en étoile, le masque de sous-réseau a été modifié, et les commandes NHRP ont été ajoutées sous l'interface du tunnel. Les commandes NHRP sont nécessaires puisque le routeur concentrateur emploie maintenant NHRP pour mapper l'adresse IP d'interface du tunnel de rayon à l'adresse IP d'interface physique de rayon.

ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 ... tunnel key 100000

Le sous-réseau est maintenant /24 au lieu de /30. Ainsi tous les noeuds sont dans le même sous-réseau, au lieu d'être dans des sous-réseaux différents. Les rayons envoient toujours le trafic de rayon à rayon par l'intermédiaire du concentrateur puisqu'ils utilisent une interface de tunnel GRE point à point. Les commandes **ip nhrp authentication…**, **ip nhrp network-id ...** et **tunnel key…** sont utilisées pour mapper les paquets de tunnel et les paquets NHRP à l'interface de tunnel GRE multipoint et au réseau NHRP corrects quand ils sont reçus sur le concentrateur. Les commandes **ip nhrp map…** et **ip nhrp nhs**… sont utilisées par NHRP sur le rayon pour annoncer le mappage NHRP des rayons (10.0.0.<n+1> --> 172.16.<n>.1) au concentrateur. L'adresse 10.0.0.<n+1> est récupérée de la commande **ip address ...** sur l'interface de tunnel et l'adresse 172.16.<n>.1 est récupérée de la commande **tunnel destination ...** sur l'interface du tunnel.

Dans un cas où il y a 300 routeurs en étoile, cette modification ramènerait le nombre de lignes de configuration sur le concentrateur de 3 900 lignes à 16 lignes (une réduction de 3 884 lignes). La configuration sur chaque routeur en étoile augmenterait de 6 lignes.

Prise en charge des adresses dynamiques sur les rayons

Sur un routeur Cisco, chaque homologue IPsec doit être configuré avec l'adresse IP de l'autre homologue IPsec avant que le tunnel IPsec puisse être lancé. Faire ceci pose problème si un routeur en étoile a une adresse dynamique sur son interface physique, ce qui est répandu pour les routeurs qui sont connectés par DSL ou câble.

TED permet à un homologue IPsec de trouver un autre homologue IPsec en envoyant un paquet spécial d'Internet Security Association and Key Management Protocol (ISAKMP) à l'adresse IP de destination du paquet des données originales qui ont dû être chiffrées. L'hypothèse est que ce paquet traversera le réseau intervenant le long du même chemin que celui pris par le paquet de tunnel IPsec. Ce paquet sera pris par l'homologue IPsec à l'autre bout, qui répondra au premier homologue. Les deux routeurs négocieront alors ISAKMP et les Security Associations (SA) IPsec et amèneront le tunnel IPsec. Ceci fonctionnera seulement si les paquets de données à chiffrer ont des adresses IP routables.

TED peut être utilisé en combination avec les tunnels GRE comme configuré dans la section précédente. Ceci a été testé et fonctionne, bien qu'il ait y eu une bogue dans les versions antérieures du logiciel Cisco IOS où TED a forcé tout le trafic IP entre les deux homologues IPsec à chiffrer, pas seulement les paquets de tunnel GRE. La solution DMVPN fournit ceci et des fonctionnalités supplémentaires sans que les hôtes doivent utiliser des adresses IP routables par Internet et sans devoir envoyer des paquets probe and response. Avec une légère modification, la

configuration de la dernière section peut être utilisée pour prendre en charge des routeurs en étoile avec des adresses IP dynamiques sur leurs interfaces physiques extérieures.

Routeur concentrateur (aucune modification)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

Routeur Spoke<n> (vieux)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 ...
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

Routeur Spoke<n> (nouveau)

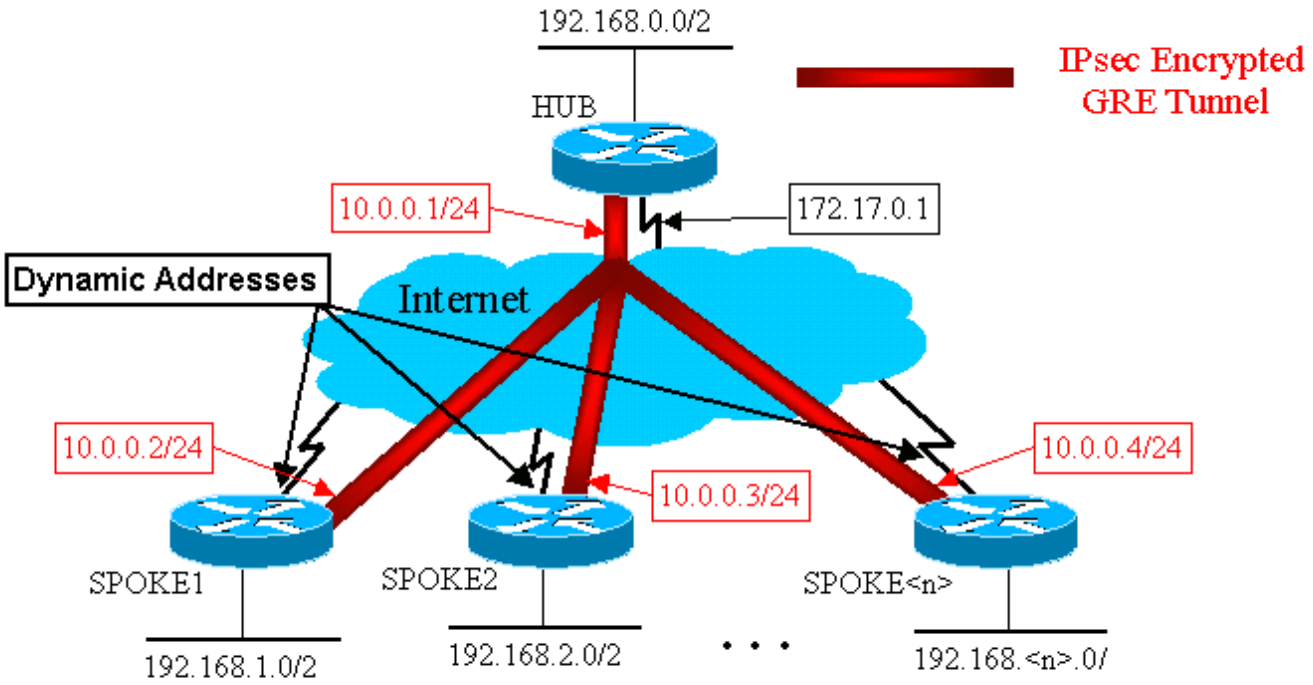
```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  set security-association level per-host match address
101 ! ... ! access-list 101 permit gre any host
172.17.0.1
```

La fonctionnalité qui est utilisée dans la nouvelle configuration en étoile est la suivante.

- Quand l'interface de tunnel GRE est lancée, elle commencera à envoyer des paquets d'enregistrement NHRP au routeur concentrateur. Ces paquets d'enregistrement NHRP déclencheront IPsec. Sur le routeur en étoile, les commandes set peer <peer-address> et **match ip access-list <ACL>** sont configurées. L'ACL spécifie GRE comme protocole, n'importe laquelle pour la source, et l'adresse IP du concentrateur pour la destination.**Remarque:** Il est important de noter que n'importe laquelle est utilisée comme source dans l'ACL, et ceci doit être le cas puisque l'adresse IP du routeur en étoile est dynamique et, en conséquence, non connue avant que l'interface physique soit en activité. Un sous-réseau IP peut être utilisé pour la source dans l'ACL si l'adresse dynamique d'interface du rayon sera restreinte à une adresse dans ce sous-réseau.

- La commande **set security-association level per-host** est utilisée de sorte que la source IP dans le proxy IPsec des rayons soit juste l'adresse actuelle d'interface physique des rayons (/32), plutôt que « n'importe laquelle » dans l'ACL. Si « n'importe laquelle » dans l'ACL était utilisée comme source dans le proxy IPsec, cela exclurait n'importe quel autre routeur en étoile d'installer également un tunnel IPsec+GRE avec ce concentrateur. C'est parce que le proxy IPsec résultant sur le concentrateur serait équivalent à **permit gre host 172.17.0.1 any**. Ceci signifierait que tous les paquets de tunnel GRE destinés à n'importe quel rayon seraient chiffrés et envoyés au premier rayon qui a établi un tunnel avec le concentrateur, puisque son proxy IPsec ajuste les paquets GRE pour chaque rayon.
- Une fois que le tunnel IPsec est installé, un paquet d'enregistrement NHRP va du routeur en étoile au serveur de prochain saut (NHS) configuré. NHS est le routeur concentrateur de ce réseau en étoile. Le paquet d'enregistrement NHRP fournit les informations pour que le routeur concentrateur crée un mappage NHRP pour ce routeur en étoile. Avec ce mappage, le routeur concentrateur peut alors transférer des paquets de données IP de monodiffusion à ce routeur en étoile sur un tunnel mGRE+IPsec. En outre, le concentrateur ajoute le routeur en étoile à sa liste de mappage multicast NHRP. Le concentrateur commencera alors à envoyer des paquets de routage IP multicast dynamiques (si un protocole de routage dynamique est configuré). Le rayon deviendra alors à un protocole de routage voisin du concentrateur, et ils s'échangeront des mises à jour de routage.

Concentrateur et rayon IPsec + mGRE



Routeur concentrateur

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
```

```
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map multicast dynamic ip
nhrp network-id 100000 ip nhrp holdtime 600 no ip split-
horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.1 255.255.255.0 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Notez que dans la configuration de concentrateur ci-dessus, les adresses IP des routeurs en étoile ne sont pas configurées. L'interface physique externe du rayon et le mappage aux adresses IP de l'interface du tunnel du rayon sont apprises dynamiquement par le concentrateur par l'intermédiaire de NHRP. Ceci permet à l'adresse IP de l'interface physique externe du rayon d'être attribuée dynamiquement.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke1 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.1.0
0.0.0.255 host 172.17.0.1
```

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
```

```
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.3 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke2 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.2.0
0.0.0.255 host 172.17.0.1
```

Les principales choses à noter au sujet des configurations en étoile sont :

- L'adresse IP de l'interface physique externe (ethernet0) est dynamique via DHCP.**ip address dhcp hostname Spoke2**
- Crypto ACL (101) spécifie un sous-réseau comme source pour le proxy IPsec.**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- La commande suivante dans la carte de cryptage IPsec spécifie que l'association de sécurité se fera par hôte.**set security-association level per-host**
- Tous les tunnels font partie du même sous-réseau, puisque tous se connectent par l'intermédiaire de la même interface multipoint GRE sur le routeur concentrateur.**ip address 10.0.0.2 255.255.255.0**

La combinaison de ces trois commandes rend inutile la configuration de l'adresse IP externe de l'interface physique du rayon. Le proxy IPsec qui est utilisé sera basé sur l'hôte plutôt que sur le sous-réseau.

La configuration sur les routeurs en étoile possède l'adresse IP configurée du routeur concentrateur, puisqu'elle doit lancer le tunnel IPsec+GRE. Notez la similarité entre les configurations Spoke1 et Spoke2. Non seulement ces deux-là sont semblables, mais toutes les configurations de routeur en étoile seront semblables. Dans la plupart des cas, tous les rayons ont besoin simplement d'adresses IP uniques sur leurs interfaces, et le reste de leurs configurations sera identique. Ceci permet de configurer et déployer beaucoup de routeurs en étoile rapidement.

Les données NHRP sur le concentrateur et le rayon ressemblent à cela.

Routeur concentrateur

```
Hub#show ip nhrp 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 01:25:18, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address: 172.16.1.4
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03 Type: dynamic, Flags: authoritative
```

```
unique registered NBMA address: 172.16.2.10 ...
10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created 00:06:00,
expire 00:04:25 Type: dynamic, Flags: authoritative
unique registered NBMA address: 172.16.<n>.41
```

Routeur Spoke1

```
Spoke1#sho ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 4d08h, never expire Type: static, Flags:
authoritative NBMA address: 172.17.0.1
```

Réseau en étoile multipoint dynamique

La configuration sur les routeurs en étoile ci-dessus ne se fonde pas sur des fonctionnalités de la solution DMVPN. Les routeurs en étoile peuvent donc exécuter des versions du logiciel Cisco IOS antérieures à la 12.2(13)T. La configuration sur le routeur concentrateur se fonde sur des fonctionnalités DMVPN. Elle doit donc exécuter Cisco IOS version 12.2(13)T ou ultérieure. Ceci vous permet de la souplesse pour décider quand vous devez mettre à jour vos routeurs en étoile qui sont déjà déployés. Si vos routeurs en étoile exécutent également Cisco IOS version 12.2(13)T ou ultérieures, alors vous pouvez simplifier la configuration en étoile comme suit.

Routeur Spoke<n> (avant Cisco IOS 12.2(13)T)

```
crypto map vpnmap1 10 IPsec-isakmp set peer 172.17.0.1
set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.<n+1> 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel
source Ethernet0 tunnel destination 172.17.0.1 tunnel
key 100000 ! interface Ethernet0 ip address dhcp
hostname Spoke<n> crypto map vpnmap1 ! . . . ! access-
list 101 permit gre any host 172.17.0.1
```

Routeur Spoke<n> (après Cisco IOS 12.2(13)T)

```
crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.<n+1>
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<n> !
```

Notez que nous avons fait ce qui suit :

1. Nous avons supprimé la commande **crypto map vpnmap1 10 ipsec-isakmp** et l'avons remplacée par **crypto ipsec profile vpnprof**.
2. Nous avons supprimé la commande **crypto map vpnmap1** des interfaces Ethernet0 et avons mis la commande **tunnel protection ipsec profile vpnprof** sur l'interface Tunnel0.
3. Nous avons supprimé l'ACL de cryptage, **access-list 101 permit gre any host 172.17.0.1**.

Dans ce cas les adresses et les proxys d'homologue IPsec sont automatiquement dérivés de la

configuration **tunnel source…** et **tunnel destination…**. Les homologues et les proxys sont comme suit (comme dans le résultat de la commande de **show crypto ipsec sa**) :

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

En résumé, les configurations complètes suivantes incluent toutes les modifications apportées à ce point de la Configuration de base (concentrateur et rayon IPsec+GRE).

Routeur concentrateur

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

Il n'y a aucun changement dans la configuration de concentrateur.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
!
```

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.3
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
!
```

VPN IPSec multipoint dynamique

Les concepts et la configuration dans cette section montrent les pleines fonctionnalités de DMVPN. NHRP fournit la fonctionnalité pour que les routeurs en étoile apprennent dynamiquement l'adresse extérieure d'interface physique des autres routeurs en étoile dans le réseau VPN. Ceci signifie qu'un routeur en étoile aura assez d'informations pour construire dynamiquement un tunnel IPsec+mGRE directement à d'autres routeurs en étoile. C'est avantageux puisque, si ce trafic de données de rayon-à-rayon était envoyé par l'intermédiaire du routeur concentrateur, alors il devrait être crypté/décrypté, multipliant par deux le délai et la charge sur le routeur concentrateur. Afin d'utiliser cette fonctionnalité, les routeurs en étoile doivent être

basculés de GRE point à point (p-pGRE) vers des interfaces du tunnel GRE multipoints (mGRE). Ils doivent également apprendre (les sous) réseaux qui sont disponibles derrière les autres rayons avec un prochain saut d'IP de l'adresse IP du tunnel de l'autre routeur en étoile. Les routeurs en étoile apprennent ces (sous) réseaux par l'intermédiaire du protocole de routage IP dynamique s'exécutant au-dessus du tunnel IPsec+mGRE avec le concentrateur.

Le protocole de routage IP dynamique exécuté sur le routeur concentrateur peut être configuré pour refléter les routes apprises d'un rayon vers la même interface de tous les autres rayons, mais le prochain saut d'IP sur ces routes sera habituellement le routeur concentrateur et non le routeur en étoile à partir duquel le concentrateur a appris la route.

Remarque: Le protocole de routage dynamique fonctionne seulement sur les liaisons du concentrateur et des rayons, il ne s'exécute pas sur les liaisons dynamiques de rayon à rayon.

Les protocoles de routage dynamique (RIP, OSPF et EIGRP) doivent être configurés sur le routeur concentrateur pour annoncer les routes vers l'interface de tunnel mGRE et pour définir le prochain saut d'IP au routeur en étoile d'origine pour des routes apprises d'un rayon lorsque la route est annoncée vers les autres rayons.

Ce qui suit sont des conditions requises pour les configurations du protocole de routage.

RIP

Vous devez désactiver le découpage de l'horizon sur l'interface de tunnel mGRE sur le concentrateur, autrement, RIP n'annoncera pas les routes apprises par l'intermédiaire de l'interface mGRE vers cette même interface.

`no ip split-horizon`
Aucune autre modification n'est nécessaire. Le routage RIP utilisera automatiquement le prochain saut d'IP initial sur les routes qu'il annonce vers la même interface où il a appris ces routes.

EIGRP

Vous devez désactiver le découpage de l'horizon sur l'interface de tunnel mGRE sur le concentrateur, autrement, EIGRP n'annoncera pas les routes apprises par l'intermédiaire de l'interface mGRE vers cette même interface.

`no ip split-horizon eigrp <as>`
Le routage EIGRP définira, par défaut, le prochain saut d'IP pour être le routeur concentrateur pour des routes qu'il annonce, même lorsqu'il annonce ces routes vers la même interface où il les a apprises. Donc, dans ce cas, vous avez besoin de la commande de configuration suivante pour demander à EIGRP d'utiliser le prochain saut initial d'IP en annonçant ces routes.

`no ip next-hop-self eigrp <as>`
Remarque: La commande **no ip next-hop-self eigrp <as>** sera disponible à partir de la version 12.3(2) de Cisco IOS. Pour des versions de Cisco IOS entre 12.2(13)T et 12.3(2) vous devez faire ce qui suit :

- Si des tunnels dynamiques de rayon à rayon ne sont pas voulus, alors la commande ci-

dessus n'est pas nécessaire.

- Si des tunnels dynamiques de rayon à rayon sont voulus, alors vous devez utiliser la commutation de processus sur l'interface de tunnel sur les routeurs en étoile.
- Autrement, vous devrez utiliser un protocole de routage différent au-dessus de DMVPN.

OSPF

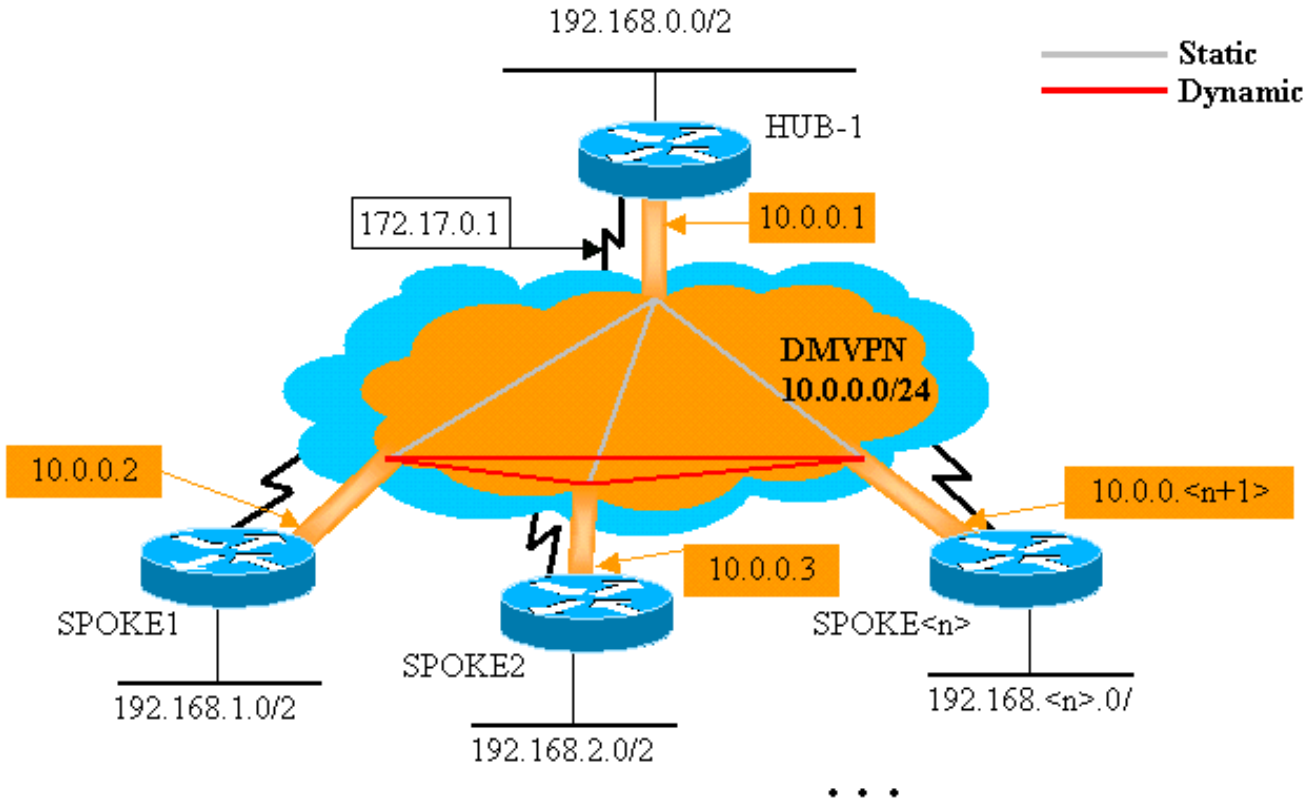
Puisque OSPF est un protocole de routage d'état de liaison, il n'y a aucun problème de découpage de l'horizon. Normalement, pour des interfaces multipoints, vous configurez le type de réseau OSPF pour être point à multipoint, mais ceci fait qu'OSPF ajoute des routes hôte à la table de routage sur les routeurs en étoile. Ces routes hôte font que les paquets destinés aux réseaux derrière d'autres routeurs en étoile sont transférés par l'intermédiaire du concentrateur, plutôt que transférés directement à l'autre rayon. Pour venir à bout de ce problème, configurez le type de réseau OSPF à diffuser en utilisant la commande.

```
ip ospf network broadcast
```

Vous devez également vous assurer que le routeur concentrateur sera le routeur désigné (DR) pour le réseau IPsec+mGRE. Ceci est fait en définissant la priorité OSPF à plus de 1 sur le concentrateur et à 0 sur les rayons.

- Hub : **ip ospf priority 2**
- Rai : **ip ospf priority 0**

Simple concentrateur DMVPN



Routeur concentrateur
`version 12.3`

```
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast ip ospf priority 2 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 ! interface Ethernet1 ip address
192.168.0.1 255.255.255.0 ! router ospf 1 network
10.0.0.0 0.0.0.255 area 0 network 192.168.0.0 0.0.0.255
area 0 !
```

La seule modification dans la configuration du concentrateur est que OSPF est le protocole de routage au lieu de EIGRP. Notez que le type de réseau OSPF est défini sur diffusion et la priorité est définie sur 2. Définir le type de réseau OSPF sur diffusion fera qu'OSPF installe des routes pour des réseaux derrière les routeurs en étoile avec une adresse du prochain saut d'IP correspondant à l'adresse de tunnel GRE pour ce routeur en étoile.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 ip ospf network broadcast ip
ospf priority 0 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
```

```
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 0 network 192.168.1.0
0.0.0.255 area 0 !
```

La configuration sur les routeurs en étoile est maintenant très semblable à la configuration sur le concentrateur. Les différences sont les suivantes :

- La priorité OSPF est fixée à 0. Les routeurs en étoile ne sont pas autorisés à devenir DR pour le réseau d'accès multiple sans diffusion (NBMA) de mGRE. Seul le routeur concentrateur a des connexions statiques directes vers tous les routeurs en étoile. Le DR doit avoir accès à tous les membres du réseau NBMA.
- Il y a des mappages de monodiffusion et de multicast NHRP configurés pour le routeur concentrateur.
  `ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1` Dans la configuration précédente, la commande **ip nhrp map multicast ...** n'était pas nécessaire puisque le tunnel GRE était point à point. Dans ce cas, des paquets multicast seront automatiquement encapsulés via le tunnel à la seule destination possible. Cette commande est nécessaire parce que le tunnel GRE des rayons est maintenant multipoint et il y a plus d'une destination possible.
- Quand le routeur en étoile est en ligne, il doit lancer la connexion en tunnel avec le concentrateur, puisque le routeur concentrateur est configuré avec aucune information sur les routeurs en étoile, et les routeurs en étoile peuvent avoir des adresses IP attribuées dynamiquement. Les routeurs en étoile sont également configurés avec le concentrateur en tant que leur NHRP NHS.`ip nhrp nhs 10.0.0.1`Avec la commande ci-dessus, le routeur en étoile enverra des paquets d'enregistrement NHRP via le tunnel mGRE+IPsec au routeur concentrateur à intervalles réguliers. Ces paquets d'enregistrement fournissent les informations de mappage NHRP de rayon qui sont nécessaires au routeur concentrateur pour acheminer à nouveau les paquets en tunnel vers les routeurs en étoile.

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
```

```
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.3.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Routeur Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<n> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

Notez que les configurations de tous les routeurs en étoile sont très semblables. Les seules différences sont les adresses IP sur les interfaces locales. Ceci est utile pour le déploiement d'un grand nombre de routeurs en étoile. Tous les routeurs en étoile peuvent être configurés de manière identique, et seules les adresses d'interface des IP locales doivent être ajoutées.

À ce moment, jetez un coup d'œil aux tables de routage et aux tables de mappage NHRP sur le concentrateur, les Routeurs Spoke1 et Spoke2 pour consulter les conditions initiales (juste après l'arrivée en ligne des routeurs Spoke1 et Spoke2) et les conditions après que Spoke1 et Spoke2 aient créé une liaison dynamique entre eux.

Conditions initiales

Informations du routeur concentrateur

```
Hub#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
```

```
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:19:53, Tunnel0 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:19:53, Tunnel0 Hub#show ip nhrp 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:57:27, expire 00:04:13
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24 10.0.0.3/32 via 10.0.0.3,
Tunnel0 created 07:11:25, expire 00:04:33 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 Hub#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 204
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 205
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 2628
Tunnel0 10.0.0.1 set HMAC_MD5 0 402 2629 Tunnel0
10.0.0.1 set HMAC_MD5 357 0 2630 Tunnel0 10.0.0.1 set
HMAC_MD5 0 427 2631 Tunnel0 10.0.0.1 set HMAC_MD5 308 0
```

Informations du routeur Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.24 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:31:46, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:31:46, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 Spoke1#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 2 Ethernet0 172.16.1.24 set
HMAC_SHA+DES_56_CB 0 0 2064 Tunnel0 10.0.0.2 set
HMAC_MD5 0 244 2065 Tunnel0 10.0.0.2 set HMAC_MD5 276 0
```

Informations du routeur Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:38:52, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:38:52, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 01:32:10, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 279 2071 Tunnel0
10.0.0.3 set HMAC_MD5 316 0
```

A ce moment nous effectuons un ping de 192.168.1.2 à 192.168.2.3. Ces adresses sont pour des hôtes derrière les routeurs Spoke1 et Spoke2, respectivement. La séquence d'opérations suivante a lieu pour construire le tunnel direct mGRE+IPsec de rayon à rayon.

1. Le routeur Spoke1 reçoit le paquet ping avec la destination 192.168.2.3. Il consulte cette destination dans la table de routage et découvre qu'il doit transférer ce paquet de l'interface Tunnel0 vers le prochain saut IP, 10.0.0.3.
2. Le routeur Spoke1 vérifie la table de mappage NHRP pour la destination 10.0.0.3 et découvre qu'il n'y a pas d'entrée. Le routeur Spoke1 crée un paquet de requête de résolution NHRP et l'envoie à NHS (le routeur concentrateur).

3. Le routeur concentrateur vérifie sa table de mappage NHRP pour la destination 10.0.0.3 et découvre qu'elle mappe à l'adresse 172.16.2.75. Le routeur concentrateur crée un paquet de réponse de résolution NHRP et l'envoie au routeur Spoke1.
4. Le routeur Spoke1 reçoit la réponse de résolution NHRP, et il entre le mappage 10.0.0.3 — >172.16.2.75 dans sa table de mappage NHRP. L'ajout du mappage NHRP déclenche IPsec qui démarre un tunnel IPsec avec l'homologue 172.16.2.75.
5. Le routeur Spoke1 lance ISAKMP avec 172.16.2.75 et négocie les SA ISAKMP et IPsec. Le proxy IPsec est dérivé de la commande **tunnel source <address>** et du mappage NHRP de Tunnel0.
   local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
6. Une fois que le tunnel IPsec est construit, tous les autres paquets de données vers le sous-réseau 192.168.2.0/24 sont envoyés directement à Spoke2.
7. Après qu'un paquet destiné à 192.168.2.3 ait été transféré à l'hôte, cet hôte enverra un paquet de retour à 192.168.1.2. Quand le routeur Spoke2 reçoit ce paquet destiné à 192.168.1.2, il recherche cette destination dans la table de routage et découvre qu'il doit transférer ce paquet de l'interface Tunnel0 au prochain saut d'IP, 10.0.0.2.
8. Le routeur Spoke2 vérifie la table de mappage NHRP pour la destination 10.0.0.2 et découvre qu'il n'y a pas d'entrée. Le routeur Spoke2 crée un paquet de requête de résolution NHRP et l'envoie à NHS (le routeur concentrateur).
9. Le routeur concentrateur vérifie sa table de mappage NHRP pour la destination 10.0.0.2 et découvre qu'elle mappe à l'adresse 172.16.1.24. Le routeur concentrateur crée un paquet de réponse de résolution NHRP et l'envoie au routeur Spoke2.
10. Le routeur Spoke2 reçoit la réponse de résolution NHRP, et il entre le mappage 10.0.0.2 — > 172.16.1.24 dans sa table de mappage NHRP. L'ajout du mappage NHRP déclenche IPsec qui démarre un tunnel IPsec avec l'homologue 172.16.1.24, mais il y a déjà un tunnel IPsec avec l'homologue 172.16.1.24 donc rien d'autre ne doit être fait.
11. Spoke1 et Spoke2 peuvent maintenant transférer des paquets directement entre eux. Quand le mappage NHRP n'a pas été utilisé pour transférer des paquets pendant la durée de conservation, le mappage NHRP sera supprimé. La suppression de l'entrée de mappage NHRP déclenchera IPsec qui supprimera les SA IPsec pour ce lien direct.

Conditions après la création d'une liaison dynamique entre Spoke1 et Spoke2

Informations du routeur Spoke1

```
Spoke1#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 02:34:16, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.3/32
via 10.0.0.3, Tunnel0 created 00:00:05, expire 00:03:35
Type: dynamic, Flags: router unique used NBMA address:
172.16.2.75 Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 3
Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2064
Tunnel0 10.0.0.2 set HMAC_MD5 0 375 2065 Tunnel0
10.0.0.2 set HMAC_MD5 426 0 2066 Tunnel0 10.0.0.2 set
HMAC_MD5 0 20 2067 Tunnel0 10.0.0.2 set HMAC_MD5 19 0
```

Informations du routeur Spoke2

```
Spoke2#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
```

```
created 02:18:25, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:00:24, expire 00:04:35
Type: dynamic, Flags: router unique used NBMA address:
172.16.1.24 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 18
Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 407 2071 Tunnel0
10.0.0.3 set HMAC_MD5 460 0 2072 Tunnel0 10.0.0.3 set
HMAC_MD5 0 19 2073 Tunnel0 10.0.0.3 set HMAC_MD5 20 0
```

A partir du résultat ci-dessus, vous pouvez voir que Spoke1 et Spoke2 ont des mappages NHRP l'un pour l'autre à partir du routeur concentrateur, et ils ont construit et ont utilisé un tunnel mGRE+IPsec. Les mappages NHRP expireront après cinq minutes (valeur actuelle de la durée de conservation NHRP = 300 secondes). Si les mappages NHRP sont utilisés dans la dernière minute avant l'expiration, alors une requête et une réponse de résolution NHRP seront envoyées pour réactualiser l'entrée avant qu'elle ne soit supprimée. Autrement, le mappage NHRP sera supprimé et cela déclenchera IPsec qui effacera les SA IPsec.

VPN IPSec multipoint dynamique avec doubles concentrateurs

Avec quelques lignes de configuration supplémentaires sur les routeurs en étoile, vous pouvez installer des routeurs concentrateurs doubles (ou multiples), pour la redondance. Il y a deux façons de configurer les DMVPN double concentrateur.

- Un réseau simple DMVPN avec chaque rayon utilisant une simple interface de tunnel GRE multipoint et pointant vers deux concentrateurs différents en tant que serveur de prochain saut (NHS).Les routeurs concentrateurs auront seulement une simple interface de tunnel GRE multipoints.
- Les réseaux DMVPN doubles avec chaque rayon ayant deux interfaces de tunnel GRE (point à point ou multipoint) et chaque tunnel GRE connecté à un routeur concentrateur différent.Encore une fois, les routeurs concentrateurs auront seulement une simple interface de tunnel GRE multipoints.

Les exemples suivants examineront la configuration de ces deux scénarios différents pour les DMVPN double concentrateurs. Dans les deux cas, les différences mises en valeur sont relatives à la configuration du concentrateur simple DMVPN.

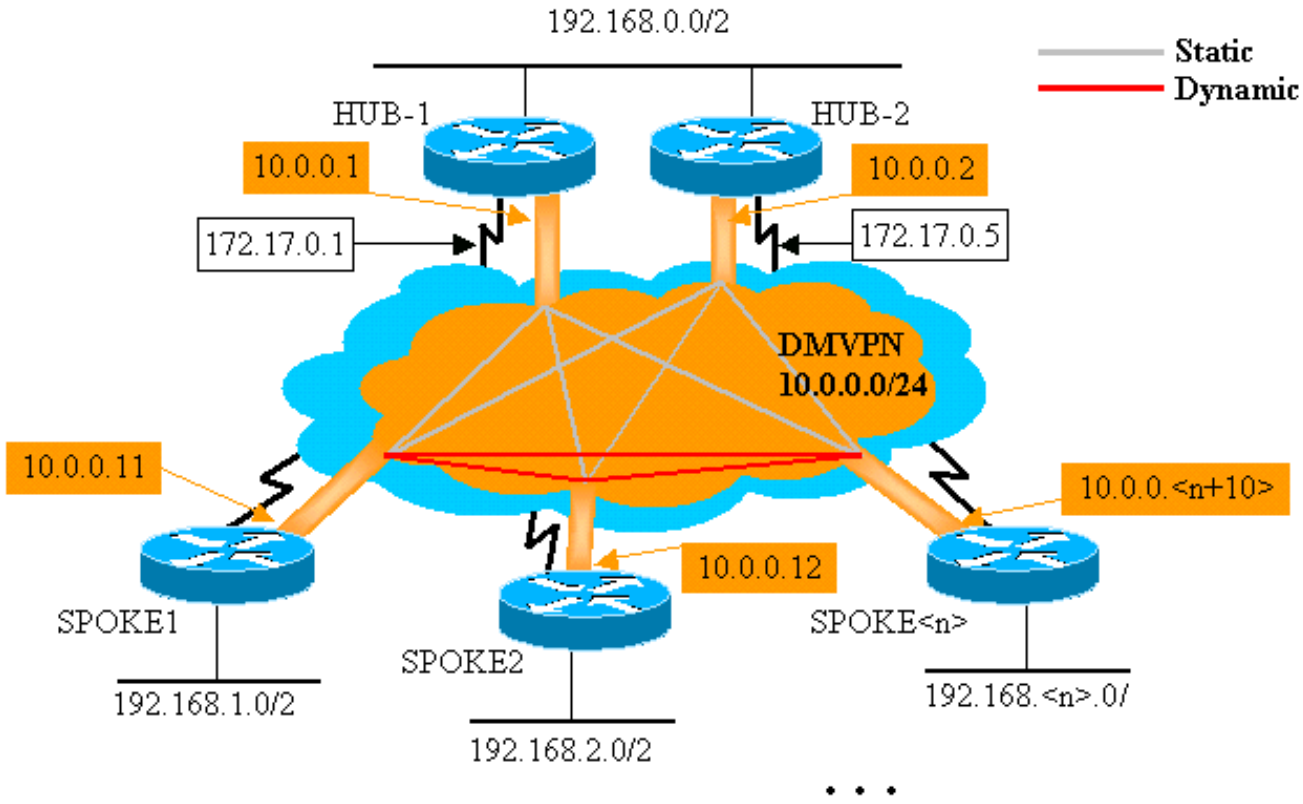
Double concentrateur - Affichage simple DMVPN

Il est assez facile d'installer le double concentrateur avec un affichage simple DMVPN, mais il ne vous permet pas de contrôler autant le routage à travers DMVPN que le double concentrateur avec double affichage DMVPN. L'idée est dans ce cas d'avoir un DMVPN simple fonctionnant avec tous les concentrateurs (deux dans ce cas) et tous les rayons connectés à ce sous-réseau unique (« entité »). Les mappages statiques NHRP des rayons aux concentrateurs définissent les liaisons IPsec+mGRE statiques sur desquelles le protocole de routage dynamique s'exécutera. Le protocole de routage dynamique ne s'exécutera pas sur des liaisons IPsec+mGRE dynamiques entre les rayons. Puisque les routeurs en étoile routent les voisins avec les routeurs concentrateurs sur la même interface de tunnel mGRE, vous ne pouvez pas utiliser des différences de liaisons ou d'interfaces (comme la métrique, le coût, le délai, ou la bande passante) pour modifier les métriques du protocole de routage dynamique pour privilégier un concentrateur par rapport à un autre lorsqu'ils sont tous les deux connectés. Si cette préférence est nécessaire,

alors des techniques internes à la configuration du protocole de routage doivent être utilisées. Pour cette raison, il peut être plus judicieux d'utiliser EIGRP ou RIP plutôt que OSPF en tant que protocole de routage dynamique.

Remarque: Habituellement, le problème ci-dessus constitue un problème seulement si les routeurs concentrateurs sont hébergés conjointement. Quand ils ne sont pas hébergés conjointement, le routage dynamique normal finira vraisemblablement par préférer le routeur concentrateur correct, même si le réseau de destination peut être atteint par l'intermédiaire de l'un ou l'autre routeur concentrateur.

[Double concentrateur - Affichage simple DMVPN]



Routeur concentrateur

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000 ip address 10.0.0.1 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
```

```
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip ospf network broadcast ip ospf priority
2 delay 1000 tunnel source Ethernet0 tunnel mode gre
multipoint tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Ethernet0 ip address
172.17.0.1 255.255.255.0 ! interface Ethernet1 ip
address 192.168.0.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 1 network 192.168.0.0
0.0.0.255 area 0 !
```

Routeur Hub2

```
version 12.3
 !
 hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 900 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.1 ip nhrp map
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip nhrp nhs 10.0.0.1 ip ospf network
broadcast ip ospf priority 1 delay 1000 tunnel source
Ethernet0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile vpnprof ! interface
Ethernet0 ip address 172.17.0.5 255.255.255.0 !
interface Ethernet1 ip address 192.168.0.2 255.255.255.0
! router ospf 1 network 10.0.0.0 0.0.0.255 area 1
network 192.168.0.0 0.0.0.255 area 0 !
```

La seule modification de la configuration Hub1 consiste à modifier OSPF pour utiliser deux zones. La zone 0 est utilisée pour le réseau derrière les deux concentrateurs, et la zone 1 est utilisée pour le réseau DMVPN et les réseaux derrière les routeurs en étoile. OSPF pourrait utiliser une seule zone, mais deux zones ont été utilisées ici pour expliquer la configuration pour plusieurs zones OSPF.

La configuration pour Hub2 est fondamentalement identique que la configuration Hub1 avec les modifications d'adresse IP appropriées. La principale différence est que Hub2 est également un rayon (ou client) de Hub1, faisant de Hub1 le concentrateur principal et de Hub2 le concentrateur secondaire. Ceci est fait de sorte que Hub2 soit un voisin OSPF de Hub1 sur le tunnel mGRE. Puisque Hub1 est le DR OSPF, il doit avoir une connexion directe avec tous les autres routeurs OSPF sur l'interface mGRE (réseau NBMA). Sans lien direct entre Hub1 et Hub2, Hub2 ne participerait pas au routage OSPF lorsque Hub1 est également en ligne. Quand Hub1 sera hors ligne, Hub2 sera le DR OSPF pour DMVPN (réseau NBMA). Quand Hub1 revient en ligne, il succédera à Hub2 pour redevenir le DR OSPF pour DMVPN.

Les routeurs derrière Hub1 et Hub2 utiliseront Hub1 pour envoyer des paquets aux réseaux en étoile car bande passante pour l'interface de tunnel GRE est définie à 1 000 Kb/sec contre 900 Kb/sec sur Hub2. En revanche, les routeurs en étoile enverront des paquets pour les réseaux

derrière les routeurs concentrateurs à Hub1 et à Hub2, puisqu'il y a seulement une interface simple de tunnel mGRE sur chaque routeur en étoile et il y aura deux itinéraires au coût égal. Si l'équilibrage de charge par paquet est utilisé, ceci peut entraîner des paquets en panne.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 1 network 192.168.1.0 0.0.0.255 area 1 !
```

Les différences de configuration sur les routeurs en étoile sont les suivantes :

- En nouvelle configuration, le rayon est configuré avec des mappages statiques NHRP pour Hub2 et Hub2 est ajouté en tant que serveur de prochain saut.Original :
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp nhs 10.0.0.1
  Nouveau :
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map 10.0.0.2 172.17.0.5 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
- Les zones OSPF sur les routeurs en étoile ont été modifiées en zone 1.

Souvenez-vous qu'en définissant le mappage statique NHRP et NHS sur un routeur en étoile pour un concentrateur, vous allez exécuter le protocole de routage dynamique sur ce tunnel. Ceci définit le routage du concentrateur et du rayon ou le réseau voisin. Notez que Hub2 est un concentrateur pour tous les rayons, et il est également un rayon pour Hub1. Ceci rend facile la conception, la configuration, et la modification des réseaux en étoile multicouche quand vous utilisez la solution DMVPN.

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
```

```
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Routeur Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+10> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<x> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

Àce moment, vous pouvez jeter un coup d'œil aux tables de routage, aux tables de mappage NHRP, et aux connexions IPsec sur les routeurs Hub1, Hub2, Spoke1 et Spoke2 pour consulter

les conditions initiales (juste après l'arrivée en ligne des routeurs Spoke1 et Spoke2).

Conditions initiales et modifications

Informations du routeur Hub1

```
Hub1#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:02:17, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:02:17, Tunnel0 Hub1#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15 Type: dynamic, Flags: authoritative unique
registered NBMA address: 172.17.0.5 10.0.0.11/32 via
10.0.0.11, Tunnel0 created 1w3d, expire 00:03:49 Type:
dynamic, Flags: authoritative unique registered NBMA
address: 172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0
created 1w3d, expire 00:04:06 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 3532
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 232 3533
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 212 0 3534
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 18 3535
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 17 0 3536
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 7 3537 Tunnel0
10.0.0.1 set HMAC_MD5+DES_56_CB 7 0
```

Informations du routeur Hub2

```
Hub2#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:29:15, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:29:15, Tunnel0 Hub2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.11/32 via 10.0.0.11, Tunnel0
created 1w3d, expire 00:03:15 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0 created
00:46:17, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 3520
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 351 3521
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 326 0 3522
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 311 3523
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 339 0 3524
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 25 3525
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 22 0
```

Informations du routeur Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:39:31, Tunnel0 [110/11] via 10.0.0.2,
00:39:31, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.12, 00:37:58, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2,
Tunnel0 created 00:56:40, never expire Type: static,
Flags: authoritative used NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active ID Interface
IP-Address State Algorithm Encrypt Decrypt 1 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2010 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 171 2011 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 185 0 2012 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 12 2013 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 13 0
```

Informations du routeur Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:57:56, Tunnel0 [110/11] via 10.0.0.2,
00:57:56, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:56:14, Tunnel0 C 192.168.2.0/24 is
directly connected, Ethernet1 Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 6w6d, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.5 Spoke2#show
crypto engine connection active ID Interface IP-Address
State Algorithm Encrypt Decrypt 2 Ethernet0 172.16.2.75
set HMAC_SHA+DES_56_CB 0 0 3 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 3712 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 302 3713 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 331 0 3716 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 216 3717 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 236 0
```

Il y a quelques problèmes intéressants à noter au sujet des tables de routage sur Hub1, Hub2, Spoke1 et Spoke2 :

- Les deux routeurs concentrateurs ont des itinéraires au coût égal vers les réseaux derrière les routeurs en étoile.Hub1 :`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0`
  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0`Hub2 :`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0`
  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0`Ceci signifie que Hub1 et Hub2 annonceront le même coût pour les réseaux derrière les routeurs en étoile aux routeurs dans le réseau derrière les routeurs concentrateur. Par exemple, la table de routage sur un routeur, R2, qui est connecté directement au LAN 192.168.0.0/24 ressemblerait à ce qui suit :R2 :`O IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3`

```
                        [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O
O     IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
                        [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
```

- Les routeurs en étoile ont des itinéraires au coût égal vers les deux routeurs concentrateurs du réseau derrière les routeurs concentrateurs.Spoke1 :`O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0`

  `[110/11] via 10.0.0.2, 00:39:31, Tunnel0`Spoke2 :`O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0`

  `[110/11] via 10.0.0.2, 00:57:56, Tunnel0`Si les routeurs en étoile font l'équilibrage de charge par paquet, alors vous pourriez obtenir des paquets en panne.

Pour éviter de faire du routage asymétrique ou de l'équilibrage de charge par-paquet à travers les liaisons vers les deux concentrateurs, vous devez configurer le protocole de routage pour privilégier un chemin de rayon à concentrateur dans les deux directions. Si vous voulez que Hub1 soit le routeur primaire et Hub2 le routeur de secours, alors vous pouvez définir des coût OSPF différents sur les interfaces du tunnel de concentrateur.

Hub1 :

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2 :

```
interface tunnel0
...
ip ospf cost 20
...
```

Maintenant les routes ressemblent à ce qui suit :

Hub1 :

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Hub2 :

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2 :

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Les deux routeurs concentrateurs ont maintenant différents coûts sur les routes pour les réseaux derrière les routeurs en étoile. Ceci signifie que Hub1 sera privilégié pour transférer le trafic aux routeurs en étoile, comme on peut le voir sur le routeur R2. Ceci résoudra le problème de routage asymétrique décrit dans la première puce ci-dessus.

Le routage asymétrique dans l'autre direction, comme décrit dans la deuxième puce ci-dessus, est toujours là. En utilisant le routage OSPF comme protocole de routage dynamique, vous pouvez régler ce problème avec une solution de contournement à l'aide de la commande **distance…** sous **router ospf 1** sur les rayons pour privilégier des routes apprises par l'intermédiaire de Hub1 par rapport à des routes apprises par l'intermédiaire de Hub2.

Spoke1 :

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Spoke2 :

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Maintenant les routes ressemblent à ce qui suit :

Spoke1 :

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Spoke2 :

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

La configuration de routage ci-dessus protégera contre le routage asymétrique, tout en permettant en même temps le basculement vers Hub2 si Hub1 est inactif. Cela signifie que quand les deux concentrateurs sont actifs, seul Hub1 est utilisé. Si vous voulez utiliser les deux concentrateurs en équilibrant les rayons à travers les concentrateurs, avec la protection de basculement et sans routage asymétrique, alors la configuration peut devenir complexe, particulièrement en utilisant OSPF. Pour cette raison, le double concentrateur suivant avec double affichage DMVPN peut être un meilleur choix.

Double concentrateur - Double affichage DMVPN

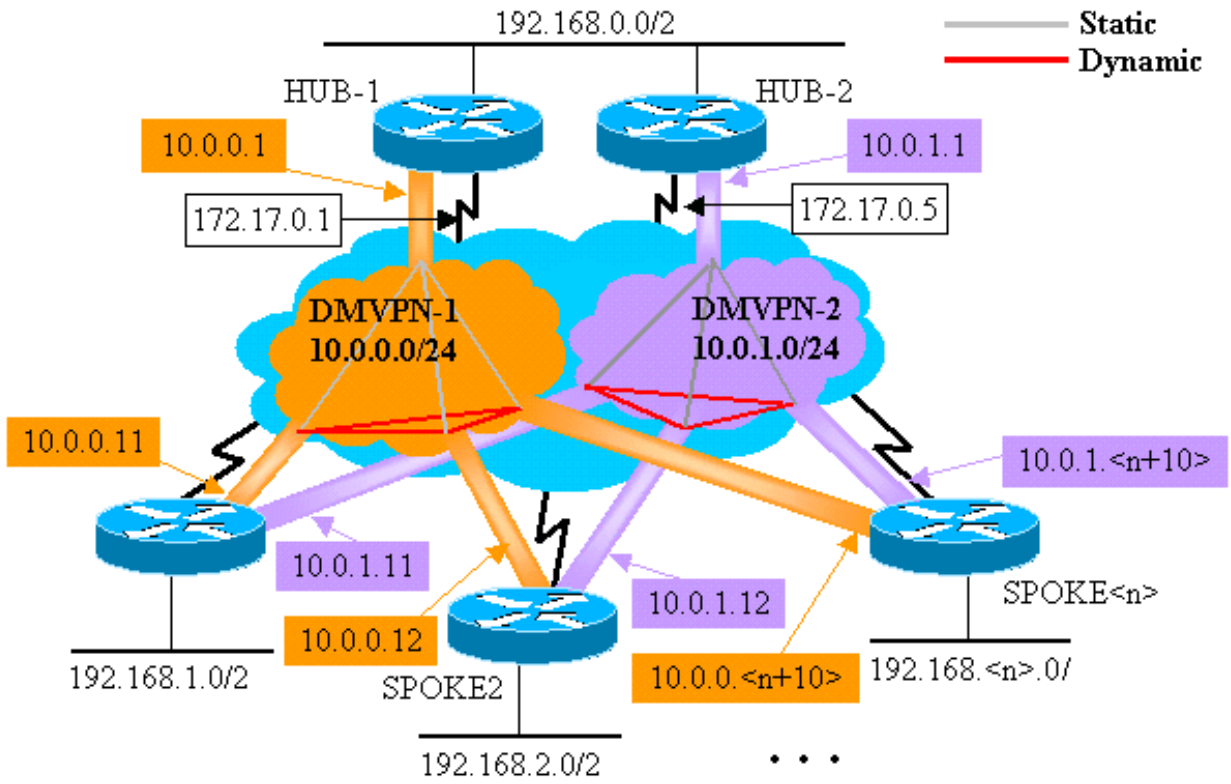
Il est légèrement plus difficile d'installer le double concentrateur avec double affichage DMVPN, mais il vous donne un meilleur contrôle du routage à travers DMVPN. L'idée est d'avoir des deux « nuages » DMVPN distincts. Chaque concentrateur (deux dans ce cas) est connecté à un sous-réseau DMVPN (« nuage ») et les rayons sont connectés aux deux sous-réseaux DMVPN (« nuages »). Puisque les routeurs en étoile routent les voisins avec les deux routeurs concentrateurs sur les mêmes interfaces de tunnel GRE, vous pouvez utiliser des différences de configuration d'interface (telles que la bande passante, le coût et le délai) pour modifier les métriques du protocole de routage dynamique pour privilégier un concentrateur par rapport à l'autre concentrateur quand ils sont tous les deux connectés.

Remarque: Habituellement, le problème ci-dessus est seulement approprié si les routeurs concentrateurs sont hébergés conjointement. Quand ils ne sont pas hébergés conjointement, le routage dynamique normal finira vraisemblablement par préférer le routeur concentrateur correct, même si le réseau de destination peut être atteint par l'intermédiaire de l'un ou l'autre routeur concentrateur.

Vous pouvez utiliser des interfaces de tunnel p-pGRE ou mGRE sur les routeurs en étoile. Différentes interfaces p-pGRE sur un routeur en étoile peuvent utiliser la même adresse IP **tunnel source…**, mais les différentes interfaces mGRE sur un routeur en étoile doivent avoir une adresse IP **tunnel source…** unique. C'est parce que quand IPsec se lance, le premier paquet est un paquet ISAKMP qui a besoin d'être associé à un des tunnels mGRE. Le paquet ISAKMP a seulement l'adresse IP de destination (adresse d'homologue IPsec distant) avec laquelle faire cette association. Cette adresse est mise en correspondance avec l'adresse **tunnel source…**, mais puisque les deux tunnels ont la même adresse **tunnel source…**, la première interface de tunnel mGRE correspond toujours. Ceci signifie que des paquets de données multicast entrants peuvent être associés à la mauvaise interface mGRE, interrompant tout protocole de routage dynamique.

Les paquets GRE eux-mêmes n'ont pas ce problème puisqu'ils ont la valeur **tunnel key…** pour se différencier entre les deux interfaces mGRE. À partir des versions 12.3(5) et 12.3(7)T du logiciel Cisco IOS, un paramètre supplémentaire a été introduit pour surmonter cette limitation : **tunnel protection….partagé**. Le mot clé **shared** indique que plusieurs interfaces mGRE utiliseront le cryptage IPSec avec la même adresse IP source. Si vous avez une version antérieure, vous pouvez utiliser des tunnels p-pGRE dans ce double concentrateur avec le double affichage DMVPN. Dans le cas de tunnel p-pGRE, les adresses IP **tunnel source…** et **tunnel destination…** peuvent être utilisés pour la mise en correspondance. Pour cet exemple, les tunnels p-pGRE seront utilisés dans ce double concentrateur avec le double affichage DMVPN et sans utiliser le qualificatif **shared**.

Double concentrateur - Double affichage DMVPN



Les modifications suivantes mises en valeur sont relatives aux configurations de réseau étoilé multipoints dynamique illustrées plus tôt dans ce document.

Routeur Hub1

```
version 12.3
 !
 hostname Hub1 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100000 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
```

```
ip address 172.17.0.1 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Routeur Hub2

```
version 12.3
 !
 hostname Hub2 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.1.1 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100001 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.5 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.2 255.255.255.0 ! router
eigrp 1 network 10.0.1.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Dans ce cas, les configurations Hub1 et Hub2 sont similaires. La principale différence est que chacun est le concentrateur d'un DMVPN différent. Chaque DMVPN utilise un différent :

- Sous-réseau IP (10.0.0.0/24, 10.0.0.1/24)
- ID réseau NHRP (100000, 100001)
- Clé tunnel (100000, 100001)

Le protocole de routage dynamique a été basculé de OSPF à EIGRP, puisqu'il est plus facile d'installer et de gérer un réseau NBMA en utilisant le EIGRP, comme décrit plus loin dans ce document.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.11
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
```

```
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255 no auto-summary !
```

Chacun des routeurs en étoile est configuré avec deux interfaces de tunnel p-pGRE, une dans chacun des deux DMVPN. Les valeurs **ip address ...**, **ip nhrp network-id ...**, **tunnel key ...** et **tunnel destination ...** sont utilisées pour faire la différence entre les deux tunnels. Le protocole de routage dynamique, EIGRP, est exécuté au-dessus des sous-réseaux de tunnel p-pGRE et est utilisé pour privilégier une interface p-pGRE (DMVPN) par rapport à l'autre.

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.12
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke2 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255 no auto-summary !
```

Routeur Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
```

```
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address
10.0.0.<n+10> 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip
nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs
10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Tunnel1
bandwidth 1000 ip address 10.0.1.<n+10> 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
10.0.1.1 172.17.0.5 ip nhrp network-id 100001 ip nhrp
holdtime 300 ip nhrp nhs 10.0.1.1 delay 1000 tunnel
source Ethernet0 tunnel destination 172.17.0.5 tunnel
key 100001 tunnel protection ipsec profile vpnprof !
interface Ethernet0 ip address dhcp hostname Spoke<x> !
interface Ethernet1 ip address 192.168.<n>.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.<n>.0 0.0.0.255 no auto-summary !
```

Àce moment, jetons un coup d'œil aux tables de routage, aux tables de mappage NHRP, et aux connexions IPsec sur les routeurs Hub1, Hub2, Spoke1 et Spoke2 pour consulter les conditions initiales (juste après l'arrivée en ligne des routeurs Spoke1 et Spoke2).

Conditions initiales et modifications

Informations du routeur Hub1

```
Hub1#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 D 10.0.1.0 [90/2611200] via
192.168.0.2, 00:00:46, Ethernet1 C 192.168.0.0/24 is
directly connected, Ethernet1 D 192.168.1.0/24
[90/2841600] via 10.0.0.11, 00:00:59, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34,
Tunnel0 Hub1#show ip nhrp 10.0.0.12/32 via 10.0.0.12,
Tunnel0 created 23:48:32, expire 00:03:50 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.0.11/32 via 10.0.0.11, Tunnel0 created
23:16:46, expire 00:04:45 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 15
Ethernet0 172.17.63.18 set HMAC_SHA+DES_56_CB 0 0 16
Ethernet0 10.0.0.1 set HMAC_SHA+DES_56_CB 0 0 2038
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 759 2039
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 726 0 2040
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 37 2041
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 36 0
```

Informations du routeur Hub2

```
Hub2#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.4 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets D 10.0.0.0
[90/2611200] via 192.168.0.1, 00:12:22, Ethernet1 C
10.0.1.0 is directly connected, Tunnel0 C 192.168.0.0/24
is directly connected, Ethernet1 D 192.168.1.0/24
```

```
[90/2841600] via 10.0.1.11, 00:13:24, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11,
Tunnel0 Hub2#show ip nhrp 10.0.1.12/32 via 10.0.1.12,
Tunnel3 created 06:03:24, expire 00:04:39 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.1.11/32 via 10.0.1.11, Tunnel3 created
23:06:47, expire 00:04:54 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 2098
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 722 2099
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 690 0 2100
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 268 2101
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 254 0
```

Informations du routeur Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:26:30, Tunnel1 [90/2841600] via 10.0.0.1,
00:26:30, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 D 192.168.2.0/24 [90/3097600] via
10.0.1.1, 00:26:29, Tunnel1 [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0 Spoke1#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 23:25:46, never expire Type:
static, Flags: authoritative NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire Type: static, Flags: authoritative NBMA
address: 172.17.0.5 Spoke1#show crypto engine connection
active ID Interface IP-Address State Algorithm Encrypt
Decrypt 16 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB
0 0 18 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
2118 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 181 2119
Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 186 0 2120
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 0 105 2121
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 110 0
```

Informations du routeur Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:38:04, Tunnel1 [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0 D 192.168.1.0/24 [90/3097600] via
10.0.1.1, 00:38:02, Tunnel1 [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 1d02h, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 10.0.1.1/32 via 10.0.1.1, Tunnel1 created
1d02h, never expire Type: static, Flags: authoritative
used NBMA address: 172.17.0.5 Spoke2#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 8 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 9 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 2036 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 585 2037 Tunnel0 10.0.0.12 set
```

```
HMAC_MD5+DES_56_CB 614 0 2038 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 0 408 2039 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 424 0
```

Encore une fois, il y a quelques éléments intéressants à noter au sujet des tables de routage sur Hub1, Hub2, Spoke1 et Spoke2 :

- Les deux routeurs concentrateurs ont des itinéraires au coût égal vers les réseaux derrière les routeurs en étoile.Hub1 :`D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0`
  `D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0`Hub2 :`D 192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0`
  `D 192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0`Ceci signifie que Hub1 et Hub2 annonceront le même coût pour les réseaux derrière les routeurs en étoile aux routeurs dans le réseau derrière les routeurs concentrateur. Par exemple, la table de routage sur un routeur, R2, qui est connecté directement au LAN 192.168.0.0/24 ressemblerait à ce qui suit :R2 :
  ```
  D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                              [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
  D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                      [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
  ```
- Les routeurs en étoile ont des itinéraires au coût égal vers les deux routeurs concentrateurs du réseau derrière les routeurs concentrateurs.Spoke1 :`D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1`
  `[90/3097600] via 10.0.0.1, 00:26:30, Tunnel0`Spoke2 :`D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1`
  `[90/3097600] via 10.0.0.1, 00:38:04, Tunnel0`Si les routeurs en étoile font l'équilibrage de charge par paquet, alors vous pourriez obtenir des paquets en panne.

Pour éviter de faire du routage asymétrique ou de l'équilibrage de charge par-paquet à travers les liaisons vers les deux concentrateurs, vous devez configurer le protocole de routage pour privilégier un chemin de rayon à concentrateur dans les deux directions. Si vous voulez que Hub1 soit le routeur primaire et Hub2 le routeur de secours, alors vous pouvez définir des délais différents sur les interfaces du tunnel de concentrateur.

Hub1 :

```
interface tunnel0
...
delay 1000
...
```

Hub2 :

```
interface tunnel0
...
delay 1050
...
```

Remarque: Dans cet exemple, 50 à été ajouté au délai sur l'interface du tunnel sur Hub2 parce qu'il est plus petit que le délai sur l'interface Ethernet1 entre les deux concentrateurs (100). En faisant cela, Hub2 transfèrera toujours des paquets directement aux routeurs en étoile, mais il annoncera un itinéraire moins souhaitable que Hub1 aux routeurs derrière Hub1 et Hub2. Si le délai était augmenté de plus de 100, alors Hub2 transfèrerait des paquets pour les routeurs en étoile par Hub1 par l'intermédiaire de l'interface Ethernet1, même si les routeurs derrière Hub1 et Hub2 privilégieraient néanmoins toujours Hub1 pour envoyer des paquets aux routeurs en étoile.

Maintenant les routes ressemblent à ce qui suit :

Hub1 :

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2 :

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2 :

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Les deux routeurs concentrateurs ont différents coûts pour les routes de réseau derrière les routeurs en étoile, ainsi, dans ce cas, Hub1 sera privilégié pour transférer du trafic aux routeurs en étoile, comme on peut le voir sur R2. Ceci règle le problème décrit dans la première puce ci-dessus.

Le problème décrit dans la deuxième puce ci-dessus est toujours là, mais puisque vous avez deux interfaces du tunnel p-pGRE, vous pouvez définir le **délai…** sur les interfaces du tunnel séparément pour modifier la métrique EIGRP pour les routes apprises par Hub1 plutôt que Hub2.

Spoke1 :

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2 :

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Maintenant les routes ressemblent à ce qui suit :

Spoke1 :

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2 :

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

La configuration de routage ci-dessus protégera contre le routage asymétrique, tout en permettant en même temps le basculement vers Hub2 si Hub1 est inactif. Cela signifie que quand les deux concentrateurs sont actifs, seul Hub1 est utilisé.

Si vous voulez utiliser les deux concentrateurs en équilibrant les rayons à travers les concentrateurs, avec la protection de basculement et sans routage asymétrique, alors la configuration est plus complexe, mais vous pouvez y arriver en utilisant EIGRP. Pour accomplir ceci, définissez le **delay…** sur les interfaces de tunnel des routeurs concentrateurs pour qu'ils soient de nouveau égaux, puis utilisez la commande **offset-list <acl> out <offset> <interface>** sur les routeurs en étoile pour augmenter la métrique EIGRP pour les routes annoncées sur les interfaces de tunnel GRE vers le concentrateur de secours. Le **delay ...** inégal entre les interfaces Tunnel0 et Tunnel1 sur le rayon est encore utilisé. Le routeur en étoile privilégiera donc son

routeur concentrateur principal. Les modifications sur les routeurs en étoile sont les suivantes.

Routeur Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1500 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.1.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.1.0 !
```

Routeur Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1500 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.2.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.2.0 !
```

Remarque: La valeur de compensation de 12 800 (50*256) a été ajoutée à la métrique EIGRP parce qu'elle est plus petite que 25 600 (100*256). Cette valeur (25 600), est ce qui est ajouté à la métrique EIGRP pour les routes apprise entre les routeurs concentrateurs. En utilisant 12 800 dans la commande **offset-list**, le routeur concentrateur de secours transfèrera des paquets directement aux routeurs en étoile, plutôt que par Ethernet par l'intermédiaire du routeur concentrateur principal pour ces rayons. La métrique sur les routes annoncées par les routeurs concentrateurs sera toujours telle que le routeur concentrateur principal correct sera privilégié. Souvenez-vous que la moitié des rayons ont Hub1 en tant que routeur primaire, et que l'autre moitié ont Hub2 en tant que routeur primaire.

Remarque: Si la valeur de compensation était augmentée de plus de 25 600 (100*256), alors les concentrateurs transfèreraient des paquets pour la moitié des routeurs en étoile par l'autre concentrateur par l'intermédiaire de l'interface Ethernet1, même si les routeurs derrière les concentrateurs privilégieraient toujours le concentrateur correct pour envoyer des paquets aux routeurs en étoile.

Remarque: La commande **distribute-list 1 out** a également été ajoutée puisqu'il est possible que les routes apprise par l'intermédiaire d'un routeur concentrateur via une interface du tunnel sur un rayon puissent être annoncées de nouveau à l'autre concentrateur par l'intermédiaire de l'autre tunnel. La commande **distribute-list…** s'assure que le routeur en étoile peut seulement annoncer ses propres routes.

Remarque: Si vous préférez contrôler les annonces de routage sur les routeurs concentrateur plutôt que sur les routeurs en étoile, alors les commandes **offset-list <acl1> in <value> <interface>** et **distribute-list <acl2> in** peuvent être configurées sur les routeurs concentrateurs au lieu de sur les rayons. La liste d'accès <acl2> listerait les routes par derrière tous les rayons et la liste d'accès <acl1> listerait seulement les routes par derrière les rayons où un autre routeur concentrateur doit être le concentrateur principal.

Avec ces modifications, les routes ressemblent à ce qui suit :

Hub1 :

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2 :

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2 :

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1 :

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2 :

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

Conclusion

La solution DMVPN fournit la fonctionnalité suivante pour mieux faire évoluer de grands et petits réseaux VPN IPSec.

- DMVPN permet une meilleure évolutivité dans les VPN IPsec à maillage global ou partiel.C'est particulièrement utile lorsque le trafic de rayon à rayon est sporadique (par exemple, chaque rayon n'envoie pas constamment des données à chaque autre rayon). Ceci permet à tout rayon d'envoyer des données directement à n'importe quel autre rayon, tant qu'il y a une connectivité IP directe entre les rayons.
- DMVPN prend en charge les noeuds IPsec avec des adresses attribuées dynamiquement (telles que câble, ISDN et DSL).Ceci s'applique aux réseaux en étoile aussi bien qu'aux réseaux maillés. DMVPN peut exiger que la liaison en étoile soit constamment active.
- DMVPN simplifie l'ajout de noeuds VPN.En ajoutant un nouveau routeur en étoile, vous devez seulement configurer le routeur en étoile et le brancher au réseau (cependant, vous pouvez devoir ajouter des informations d'autorisation ISAKMP pour le nouveau rayon du concentrateur). Le concentrateur se renseignera dynamiquement sur le nouveau rayon et le protocole de routage dynamique propagera le routage au concentrateur et à tous autres rayons.
- DMVPN réduit la taille de la configuration requise sur tous les Routeurs dans le VPN.C'est également le cas pour les réseaux VPN en étoile uniquement GRE+IPsec.
- DMVPN utilise GRE et prend en charge, en conséquence, le multicast IP et le trafic de routage dynamique à travers le VPN.Ceci signifie qu'un protocole de routage dynamique peut être utilisé, et des « concentrateurs » redondants peuvent être pris en charge par le protocole de routage. Les applications multidiffusion sont également prises en charge.
- DMVPN prend en charge la transmission tunnel partagée aux rayons.

Informations connexes

- VPN multipoint dynamique (DMVPN)
- Page d'assistance IPsec
- Support technique - Cisco Systems