Dynamic Multipoint IPsec VPN's (met Multipoint GRE/NHRP voor Scale IPsec VPN's)

Inhoud

Inleiding

Dit document behandelt Dynamic Multipoint IPsec VPN's (DMVPN) en waarom een bedrijf hun netwerk wil ontwerpen of migreren om gebruik te maken van deze nieuwe IPsec VPN-oplossing in Cisco IOS® Software.

Achtergrondinformatie

Bedrijven moeten misschien veel sites onderling verbinden met een hoofdsite, en misschien ook met elkaar, via het internet, terwijl ze het verkeer versleutelen om het te beschermen. Het kan bijvoorbeeld zijn dat een stel detailhandelswinkels die voor inventaris en bestelling aan het hoofdkantoor van het bedrijf moeten worden gekoppeld, ook aan andere winkels in het bedrijf moeten sluiten om de beschikbaarheid van het product te controleren. In het verleden was de enige manier om de verbinding te maken een Layer 2 netwerk zoals ISDN of Frame Relay te gebruiken om alles onderling te verbinden. Het instellen en betalen van deze harde verbindingen voor intern IP-verkeer kan tijdrovend en duur zijn. Als alle sites (inclusief de hoofdsite) al relatief goedkope internettoegang hebben, kan deze internettoegang ook worden gebruikt voor interne IP-communicatie tussen de winkels en het hoofdkantoor door gebruik te maken van IPsec-tunnels om de privacy en de gegevensintegriteit te garanderen.

Om bedrijven grote IPsec-netwerken te kunnen bouwen die hun sites via het internet onderling verbinden, moet u het IPsec-netwerk kunnen opschalen. IPsec versleutelt verkeer tussen twee endpoints (peers) en de encryptie wordt uitgevoerd door de twee endpoints via een gedeeld "geheim". Omdat dit geheim slechts tussen deze twee eindpunten wordt gedeeld, zijn versleutelde netwerken inherent een verzameling point-to-point links. Daarom is IPsec een point-to-point tunnelnetwerk. De meest haalbare methode om een groot point-to-point netwerk te schalen is het te organiseren in een netwerk met een hub-and-sprak of volledig (gedeeltelijk) netwerk met mazen. In de meeste netwerken ligt het grootste deel van het IP-verkeer tussen de spaken en de hub, en heel weinig is tussen de spaken, dus het hub-and-sprak ontwerp is vaak de beste keuze. Dit ontwerp komt ook overeen met oudere Frame Relay-netwerken omdat het buitensporig duur was om voor links tussen alle sites in deze netwerken te betalen.

Wanneer de spokes het internet gebruiken als interconnectie tussen de hub en de spokes, hebben ze ook directe toegang tot elkaar zonder extra kosten, maar het was zeer moeilijk, zo niet onmogelijk, om een volledig (gedeeltelijk) maasnetwerk op te zetten en/of te beheren. Volledige of gedeeltelijke vermaasde netwerken zijn vaak wenselijk omdat er een kostenbesparing kan zijn als het op een lijn gebaseerde verkeer rechtstreeks door kan gaan in plaats van via de hub. Spoke-to-sprak verkeer dat de hub doorkruist gebruikt middelen van de hub en kan extra vertragingen veroorzaken, vooral wanneer u IPsec-encryptie gebruikt, aangezien de hub de inkomende pakketten van de verzendende spaken moet decrypteren en dan het verkeer opnieuw versleutel om het naar het ontvangende gesproken te verzenden. Een ander voorbeeld waar direct met iemand praat nuttig zou zijn is het geval waar twee woordvoerders in dezelfde stad zijn en de hub door het land.

Aangezien IPsec hub-and-sprak netwerken werden uitgevoerd en in grootte groeiden, werd het wenselijker om hen IP pakketten zo dynamisch mogelijk te laten leiden. In de oudere hub-en de gesproken netwerken van Frame Relay werd dit verwezenlijkt door een dynamisch routingprotocol zoals OSPF of DHCP via de verbindingen van Frame Relay uit te voeren. Dit was nuttig voor het dynamisch adverteren van de bereikbaarheid van gesproken netwerken en ook om redundantie in het IP-routingnetwerk te ondersteunen. Als het netwerk een hub router verloor, kon een router van de reservehub automatisch overnemen om netwerkconnectiviteit aan de gesproken netwerken te behouden.

Er is een fundamenteel probleem met IPsec-tunnels en dynamische routingprotocollen. Dynamische routingprotocollen zijn afhankelijk van het gebruik van IP multicast of broadcast-pakketten, maar IPsec ondersteunt niet het versleutelen van multicast of broadcast-pakketten. De huidige methode om dit probleem op te lossen is het gebruik van generieke Routing Encapsulation (GRE)-tunnels in combinatie met IPsec-encryptie.

GRE-tunnels ondersteunen het transport van IP multicast en uitgezonden pakketten naar het andere uiteinde van de GRE-tunnel. Het GRE-tunnelpakket is een IP-eenastpakket, zodat het

GRE-pakket kan worden versleuteld met IPsec. In dit scenario, doet GRE het tunneling werk en IPsec doet het encryptiegedeelte van het steunen van het VPN netwerk. Wanneer GRE-tunnels zijn geconfigureerd, moeten de IP-adressen voor de eindpunten van de tunnel (**tunnelbron ...**, **tunnelbestemming ...**) bekend zijn bij het andere eindpunt en routeerbaar zijn via het internet. Dit betekent dat het hub en alle gesproken routers in dit netwerk statische niet-privé IP adressen moeten hebben.

Voor kleine lokale verbindingen met het internet is het normaal voor het externe IP-adres van een gesproken om elke keer dat het verbinding maakt met het internet te wijzigen, omdat hun Internet Service Provider (ISP) dynamisch het externe interfaceadres (via Dynamic Host Configuration Protocol (DHCP)) aanbiedt telkens wanneer het woord online komt (asymmetrische digitale abonneelijn (ADSL) en kabelservices). Deze dynamische toewijzing van het "buiten adres" van de router staat toe ISP om het gebruik van hun adresruimte van het Internet te oversubscript, aangezien niet alle gebruikers tegelijkertijd online zullen zijn. Het kan aanzienlijk duurder zijn om de leverancier te betalen om een statisch adres voor de spaakrouter toe te wijzen. Het uitvoeren van een dynamisch routingprotocol via een IPsec VPN vereist het gebruik van GRE tunnels, maar u verliest de optie van het hebben van spaken met dynamisch toegewezen IP adressen op hun buitenkant fysieke interfaces.

De bovengenoemde beperkingen en enkele andere worden samengevat in de volgende vier punten:

- IPsec gebruikt een toegangscontrolelijst (ACL) om te definiëren welke gegevens moeten worden versleuteld. Dus elke keer dat een nieuw (sub)netwerk achter een spits of de hub wordt toegevoegd, moet de klant ACL op zowel de hub als de spaakrouters wijzigen. Als SP de router beheert, moet de klant SP op de hoogte stellen om IPsec ACL te veranderen zodat het nieuwe verkeer wordt versleuteld.
- Met grote hub-and-sprak netwerken kan de grootte van de configuratie op de Hub router zeer groot worden, tot die mate dat het onbruikbaar is. Bijvoorbeeld zou een hub router tot 3900 lijnen van configuratie nodig hebben om 300 SPRAAKrouters te ondersteunen. Dit is groot genoeg dat het moeilijk zou zijn om de configuratie te tonen en de sectie van de configuratie te vinden die relevant is voor een huidig probleem dat wordt gezuiverd. Ook deze grootteconfiguratie kan te groot zijn om in NVRAM te passen en zou op Flash geheugen moeten worden opgeslagen.
- GRE + IPsec moet het peer-adres van het eindpunt kennen. De IP-adressen van de spaken worden rechtstreeks via hun eigen ISP verbonden met het internet, en zij worden vaak ingesteld zodat hun externe interfaceadressen niet vast zijn. De IP-adressen kunnen telkens wanneer de site online komt (via DHCP) veranderen.
- Als de spaken elkaar direct met elkaar moeten praten over IPsec VPN, dan moet het netwerk van de hub en de spaak een volledig netwerk worden. Aangezien het nog niet bekend is welke woordvoerders rechtstreeks met elkaar moeten praten, is een volledige maaswijdte noodzakelijk, ook al hoeft elke spreker niet rechtstreeks met elkaar te spreken. Ook is het niet mogelijk IPsec op een kleine spuitrouter te configureren zodat deze directe connectiviteit heeft met alle andere spuitrouters in het netwerk; zo gesproken routers moeten misschien krachtiger routers zijn .

De DMVPN-oplossing

De DMVPN-oplossing maakt gebruik van Multipoint GRE (mGRE) en Next Hopprotocol (NHRP),

met IPsec en bepaalde nieuwe verbeteringen, om de bovenstaande problemen op een schaalbare manier op te lossen.

Automatische IPsec-encryptie

Wanneer u de DMVPN-oplossing niet gebruikt, wordt de IPsec-encryptie-tunnel niet gestart totdat er gegevensverkeer is waarvoor deze IPsec-tunnel nodig is. Het kan 1 tot 10 seconden duren om de opening van de IPsec-tunnel te voltooien en het gegevensverkeer wordt tijdens deze tijd gedaald. Wanneer u GRE met IPsec gebruikt, omvat de GRE-tunnelconfiguratie reeds het GRE-tunneladres (**tunnelbestemming ...**), dat ook het IPsec-peer-adres is. Beide adressen zijn vooraf ingesteld.

Als u Tunnel Endpoint Discovery (TED) en dynamische crypto kaarten op de hub router gebruikt, dan kunt u vermijden de IPsec peer adressen op de hub vooraf te configureren, maar er moet een TED-sonde en een TED-reactie worden verstuurd en ontvangen voordat de ISAKMP-onderhandeling kan starten. Dit zou niet nodig moeten zijn aangezien, wanneer GRE wordt gebruikt, de bron- en doeladressen al bekend zijn. Ze bevinden zich in de configuratie of opgelost met NHRP (voor GRE-tunnels met meerdere punten).

Met de DMVPN-oplossing wordt IPsec onmiddellijk geactiveerd voor zowel point-to-point als multi-point GRE-tunnels. Ook is het niet nodig om crypto ACL's te configureren, aangezien deze automatisch zullen worden afgeleid van de GRE-tunnelbron en de doeladressen. De volgende opdrachten worden gebruikt om de parameters voor de IPsec-encryptie te definiëren. Merk op dat er geen **ingestelde peer** is **...** of **overeenkomend adres ...**. opdrachten die vereist zijn omdat deze informatie rechtstreeks afkomstig is van de aangesloten GRE-tunnel of NHRP-mappingen.

```
crypto ipsec profile
```

```
 set transform-set
```

De volgende opdracht associeert een tunnelinterface met het IPsec-profiel.

```
interface tunnel
```

```
 ...
 tunnel protection ipsec profile
```

Dynamic Tunnel Creation voor "Spoke-to-Hub" links

Er wordt geen GRE- of IPsec-informatie over een onderwerp ingesteld op de hubrouter in het DMVPN-netwerk. De GRE-tunnel van de SPD-router is geconfigureerd (via NHRP-opdrachten) met informatie over de hubrouter. Wanneer de spaakrouter opstart, start hij automatisch de IPsec-tunnel met de hubrouter zoals hierboven beschreven. Het gebruikt dan NHRP om de hub router van zijn huidige fysieke interface IP-adres op de hoogte te stellen. Dit is om drie redenen nuttig:

- Als de hoofdrouter zijn fysieke interface-IP-adres dynamisch heeft toegewezen (zoals met ADSL of CableModem), dan kan de hub router niet met deze informatie worden geconfigureerd omdat elke keer dat de gemaakte router opnieuw wordt geladen, het een nieuw fysiek IP-adres krijgt.
- De configuratie van de hub router is verkort en vereenvoudigd omdat u geen GRE- of IPsec-informatie over de peer routers hoeft te hebben. Al deze informatie wordt dynamisch geleerd via NHRP.
- Wanneer u een nieuwe gemaakte router aan het netwerk DMVPN toevoegt, hoeft u de configuratie op de hub of op een van de huidige gesproken routers niet te wijzigen. De nieuwe spaakrouter is ingesteld met de informatie over de hub en wanneer hij start, registreert hij dynamisch met de router van de hub. Het dynamische routerprotocol verspreidt de routinginformatie voor dit gesproken in de hub. De hub verspreidt deze nieuwe routinginformatie naar de andere spokes. Het verspreidt ook de routinginformatie van de andere woordjes aan dit gesproken.

Dynamic Tunnel maken voor "Spoke-to-Spoke" verkeer

Zoals eerder vermeld, momenteel in een netwerk van netwerken, moeten alle point-to-point IPsec (of IPsec+GRE) tunnels op alle routers worden geconfigureerd, zelfs als een aantal/de meeste van deze tunnels niet of op elk moment nodig zijn. Met de DMVPN-oplossing is één router de hub, en alle andere routers (spokes) worden geconfigureerd met tunnels naar de hub. De snelheidstunnel zijn continu, en de woordvoerders hebben geen configuratie nodig voor directe tunnels naar een van de andere woordjes. In plaats daarvan, wanneer een toespraak een pakket naar een ander gesproken (zoals Subnet achter een andere gesproken) wil verzenden, gebruikt het NHRP om dynamisch het vereiste bestemmingsadres van het doel te bepalen dat gesproken wordt. De hub router werkt als de NHRP-server en behandelt dit verzoek voor de gebruikte bron. De twee spaken creëren dan dynamisch een IPsec-tunnel tussen hen (via de enkele mGRE-interface) en de gegevens kunnen rechtstreeks worden overgebracht. Deze dynamische, gesproken-tot-gesproken tunnel zal automatisch worden afgebroken na een (configureerbare) periode van inactiviteit.

Ondersteunende dynamische routingprotocollen

De DMVPN-oplossing is gebaseerd op GRE-tunnels die tunneling van multicast/broadcast IP-pakketten ondersteunen, zodat de DMVPN-oplossing ook dynamische routingprotocollen ondersteunt die via de IPsec+mGRE-tunnels worden uitgevoerd. Eerder, vereiste NHRP u om expliciet de uitzending/multicast afbeelding voor de IP-adressen van de tunnelbestemming te configureren om GRE-tunneling van multicast en Broadcast IP-pakketten te ondersteunen. Bijvoorbeeld, op het centrum zou u de **IP** kaart **van Nhrp multicast <sprak-n-addr>**configuratielijn voor elk sprak nodig hebben. Met de DMVPN oplossing zijn de gesproken adressen niet van

tevoren bekend, dus is deze configuratie niet mogelijk. In plaats daarvan kan NHRP worden geconfigureerd om elke sprak automatisch toe te voegen aan de multicast doellijst in het hub met de **IP Nhrp map multicast dynamische** opdracht. Met deze opdracht, wanneer de gesproken routers hun unicast NHRP-mapping met de NHRP-server (hub) registreren, zal NHRP ook een uitzending/multicast-mapping voor dit onderwerp maken. Dit heft de noodzaak op om de gesproken adressen van tevoren bekend te maken.

Cisco Express Forwarding Fast-switching voor mGRE

Op dit moment is het verkeer in een mGRE-interface procesgeschakeld, wat resulteert in slechte prestaties. De DMVPN-oplossing voegt Cisco Express Forwarding-switching toe voor het mGRE-verkeer, wat resulteert in veel betere prestaties. Er zijn geen configuratieopdrachten nodig om deze functie in te schakelen. Als Cisco Express Forwarding-switching is toegestaan op de GRE-tunnelinterface en de uitgaande/inkomende fysieke interfaces, dan zijn de GRE-tunnelpakketten met meerdere aansluitingen Cisco Express Forwarding-switched.

Dynamische routing via IPsec beschermde VPN's gebruiken

In dit gedeelte wordt de huidige (pre-DMVPN-oplossing) stand van zaken beschreven. IPsec wordt geïmplementeerd op Cisco-routers via een reeks opdrachten die de encryptie definiëren en vervolgens een opdracht voor **crypto-map <map-naam>** toepassen op de externe interface van de router. Vanwege dit ontwerp en het feit dat er momenteel geen standaard is voor het gebruik van IPsec om IP multicast/broadcast-pakketten te versleutelen, kunnen IP-routingpakketten niet worden "doorgestuurd" door de IPsec-tunnel en kunnen alle routingwijzigingen niet dynamisch worden doorgevoerd met de andere kant van de IPsec-tunnel.

Opmerking: Alle dynamische routingprotocollen behalve BGP-toepassingen en multicast IP-pakketten. GRE-tunnels worden gebruikt in combinatie met IPsec om dit probleem op te lossen.

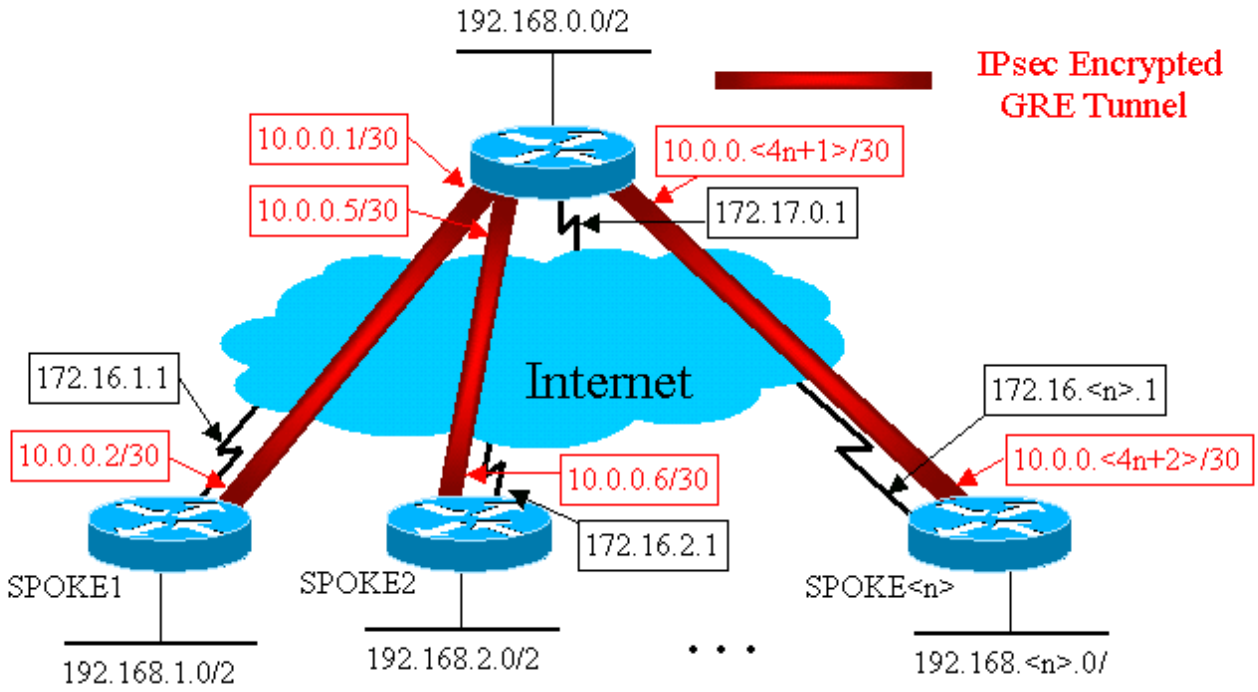
GRE-tunnels worden geïmplementeerd op Cisco-routers door gebruik te maken van een virtuele tunnelinterface (**interfacetunnel<#>**). Het GRE-tunneling-protocol is ontworpen om IP multicast/broadcast-pakketten aan te pakken, zodat een dynamisch routingprotocol "via" een GRE-tunnel kan worden uitgevoerd. GRE-tunnelpakketten zijn IP-pakketten die het oorspronkelijke IP multicast/unicast-pakket bevatten. U kunt IPsec dan gebruiken om het GRE-tunnelpakket te versleutelen. U kunt IPsec ook uitvoeren in transportmodus en 20 bytes opslaan omdat GRE het oorspronkelijke gegevenspakket al heeft ingekapseld, zodat u geen IPsec nodig hebt om het GRE IP-pakket in een andere IP-header in te sluiten.

Wanneer IPsec in transportmodus wordt uitgevoerd, is er een beperking dat de IP-bron en doeladressen van het te versleutelen pakket moeten overeenkomen met de IPsec peer-adressen (de router zelf). In dit geval betekent dit alleen dat het GRE-tunneleindpunt en de IPsec peer-adressen hetzelfde moeten zijn. Dit is geen probleem omdat de zelfde routers zowel IPsec als GRE tunnelendpoints zijn. Door GRE-tunnels te combineren met IPsec-encryptie, kunt u een dynamisch IP-routingprotocol gebruiken om de routingtabellen op beide eindpunten van de gecodeerde tunnel bij te werken. De IP-routingtabelitems voor de netwerken die door de versleutelde tunnel zijn geleerd, hebben het andere uiteinde van de tunnel (GRE-tunnelinterface-adres) als de IP-volgende hop. Als de netwerken dus aan weerszijden van de tunnel veranderen, dan zal de andere kant dynamisch van de verandering leren en de connectiviteit zonder configuratieveranderingen op de routers verder gaan.

basisconfiguratie

Het volgende is een standaard point-to-point IPsec+GRE-configuratie. Hierna is een reeks configuratievoorbeelden waar de specifieke eigenschappen van de DMVPN-oplossing in stappen worden toegevoegd om de verschillende mogelijkheden van DMVPN te tonen. Elk voorbeeld bouwt op de vorige voorbeelden om te tonen hoe te om de oplossing DMVPN in steeds complexere netwerkontwerpen te gebruiken. Deze reeks voorbeelden kan worden gebruikt als een sjabloon voor het migreren van een huidige IPsec+GRE VPN naar een DMVPN. U kunt "de migratie" op elk punt stoppen als dat bepaalde configuratievoorbeeld voldoet aan uw eisen voor het netwerkontwerp.

IPsec + GRE-hub en Rookgebied (n = 1,2,3,...)



Hub router

```
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.




 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




 !
 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
```

SPE1 router

```
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
```

Spoke2 router

```
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
```

Spoke<n> router

```
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.
```

In de bovenstaande configuratie worden ACL's gebruikt om te definiëren welk verkeer versleuteld wordt. Op zowel de hub en de gesproken routers, moet deze ACL slechts de GRE-tunnels IP-pakketten aanpassen. Ongeacht hoe de netwerken aan elk eind veranderen, zullen de GRE IP tunnelpakketten niet veranderen, zodat hoeft deze ACL niet te veranderen.

Opmerking: Wanneer u Cisco IOS-softwarereleases vóór 12.2(13)T gebruikt, moet u de configuratieopdracht **crypto map vpnmap1** op zowel de GRE-tunnelinterfaces (Tunnel<x>) als de fysieke interface (Ethernet0) toepassen. Met Cisco IOS versie 12.2(13)T en hoger past u alleen de configuratieopdracht van **crypto map vpnmap1** op de fysieke interface (Ethernet0) toe.

Voorbeelden van de routingtabellen op de hub en de neprouters

Routing-op-hubrouter

```
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>
```

Routing Tabel op Spoke1 router

```
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
```

Routing op tafel</n> router

```
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
```

Dit is een basiswerkconfiguratie, en wordt gebruikt als beginpunt voor vergelijking met de complexere configuraties mogelijk met behulp van de DMVPN-oplossing. De eerste verandering zal de grootte van de configuratie op de hub router verminderen. Dit is niet belangrijk met kleine aantallen gesproken routers, maar het wordt kritiek wanneer er meer dan 50 tot 100 SPA-routers zijn.

De grootte van de hubrouter beperken

In het volgende voorbeeld wordt de configuratie minimaal gewijzigd op de hubrouter van meerdere GRE point-to-point tunnelinterfaces naar één GRE multipoint tunnelinterface. Dit is een eerste stap in de DMVPN-oplossing.

Er is een uniek blok van configuratielijnen op de hub router om de crypto kaart eigenschappen voor elke spaakrouter te bepalen. Dit stuk van de configuratie definieert crypto ACL en de GRE-tunnelinterface voor die gesproken router. Deze kenmerken zijn meestal hetzelfde voor alle spaken, behalve IP-adressen (**ingesteld peer ...**, **tunnelbestemming ...**).

kijkend naar de bovenstaande configuratie op de hubrouter ziet u dat er ten minste 13 configuratielijnen per SPA-router zijn; vier voor de crypto kaart, één voor crypto ACL, en acht voor de GRE-tunnelinterface. Het totale aantal configuratielijnen, als er 300 SPRAAKrouters waren, is 3900 lijnen. U hebt ook 300 (2000/30) subnetten nodig voor het aanpakken van elke tunnelverbinding. Een configuratie van deze grootte is zeer moeilijk te beheren en nog moeilijker wanneer u een oplossing voor het VPN-netwerk zoekt. Om deze waarde te verminderen, zou je dynamische crypto kaarten kunnen gebruiken, die de bovenstaande waarde met 1200 lijnen zouden verminderen, waardoor 2700 lijnen achterbleven in een 300-netwerk.

Opmerking: Wanneer u dynamische crypto kaarten gebruikt, moet de IPsec encryptie tunnel geïnitieerd worden door de spaakrouter. U kunt ook **ip ongenummerd <interface>**gebruiken om het aantal subnetten nodig voor de GRE-tunnels te verminderen, maar dit kan het oplossen van problemen later bemoeilijken.

Met de DMVPN-oplossing kunt u één GRE-tunnelinterface met meerdere punten en één IPsec-profiel op de hubrouter configureren om alle gesproken routers af te handelen. Dit staat de grootte van de configuratie op de hub router toe om een constante te blijven, ongeacht hoeveel gesproken routers aan het VPN-netwerk worden toegevoegd.

De DMVPN-oplossing voert de volgende nieuwe opdrachten in:

```
crypto ipsec profile
```

De opdracht **crypto ipsec-profiel <name>** wordt gebruikt als een dynamische crypto map en is specifiek ontworpen voor tunnelinterfaces. Deze opdracht wordt gebruikt om de parameters voor de IPsec-encryptie te definiëren op de spits-to-hub en de spraak-to-spaanse VPN-tunnels. De enige parameter die onder het profiel vereist is, is de transformatieset. Het IPsec peer-adres en het **overeenkomende adres ...** clausule voor de IPsec-proxy worden automatisch afgeleid van de NHRP-mappings voor de GRE-tunnel.

De opdracht **voor tunnelbeveiliging** is ingesteld onder de GRE-tunnelinterface en wordt gebruikt om de GRE-tunnelinterface te koppelen aan het IPsec-profiel. Daarnaast kan de opdracht voor **tunnelbescherming** ook worden gebruikt met een point-to-point GRE-tunnel. In dit geval zal het de IPsec peer en volmacht informatie van de **tunnelbron** afleiden **...** en **tunnelbestemming ...** configuratie. Dit vereenvoudigt de configuratie aangezien de IPsec peer en de crypto's niet langer nodig zijn.

Opmerking: de **opdracht** voor **tunnelbescherming ...** specificeert dat de IPsec-encryptie zal worden uitgevoerd nadat de GRE-insluiting is toegevoegd aan het pakket.

Deze eerste twee nieuwe opdrachten zijn vergelijkbaar met het configureren van een crypto-kaart en het toewijzen van de crypto-kaart aan een interface met de opdracht **crypto-kaart <naam>**. Het grote verschil is dat u met de nieuwe opdrachten het IPsec-peer-adres of een ACL-naam niet hoeft te specificeren om zo de te versleutelen pakketten aan te passen. Deze parameters worden automatisch bepaald vanuit de NHRP-mappings voor de mGRE-tunnelinterface.

Opmerking: Bij gebruik van de **tunnelbescherming ...** opdracht op de tunnelinterface wordt een **crypto map ...** opdracht niet ingesteld op de fysieke uitgaande interface.

Met de laatste nieuwe opdracht, **ip Nhrp map multicast dynamic**, kan NHRP gesproken routers automatisch aan de multicast NHRP-mappings toevoegen wanneer deze gesproken routers de mGRE+IPsec-tunnel initiëren en hun unicast NHRP-mappings registreren. Dit is nodig om dynamische routingprotocollen mogelijk te maken om via de tunnels mGRE+IPsec tussen de hub en de spokes te werken. Als deze opdracht niet beschikbaar was, moest de hub router een afzonderlijke configuratielijn hebben voor een multicast mapping naar elk doel.

Opmerking: bij deze configuratie moeten de gesproken routers de tunnelverbinding mGRE+IPsec initiëren, omdat de hubrouter niet met informatie over de spaken is ingesteld. Maar, dit is geen probleem omdat met DMVPN de mGRE+IPsec-tunnel automatisch wordt geïnitieerd wanneer de gemaakte router opstart, en hij blijft altijd omhoog.

Opmerking: Het volgende voorbeeld toont point-to-point GRE tunnelinterfaces op de gesproken routers en lijnen van de NHRP-configuratie die op zowel de hub als de spuitrouters zijn toegevoegd om de mGRE-tunnel op de hubrouter te ondersteunen. De configuratie verandert als volgt.

Hub router (oud)

```
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.




!
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
```

Hub router (nieuw)

```
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
```

SPRAKE<n> router (oud)

```
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
 !
```

SPRAKE<n> router (nieuw)

```
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.




  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
 !
```

Op de gesproken routers, is het SUBNET masker gewijzigd, en de opdrachten NHRP zijn toegevoegd onder de tunnelinterface. De opdrachten NHRP zijn nodig omdat de router op het hub-kanaal nu NHRP gebruikt om het IP-adres van de gesproken tunnelinterface in kaart te brengen naar het gemaakte fysieke IP-adres van de interface.

ip address 10.0.0.

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
```

Subnet is nu /24 in plaats van /30, dus alle knopen zijn in zelfde vorm, in plaats van verschillende subnetten. De woordvoerders sturen nog steeds het gesproken-naar-gesproken verkeer via de hub omdat ze een punt-tot-punt GRE-tunnelinterface gebruiken. De **IP Nhrp authenticatie ...**, **ip Nhrp netwerk-id ...** en **tunneltoets ...** worden opdrachten gebruikt om de tunnelpakketten en de NHRP pakketten in kaart te brengen naar de juiste GRE-tunnelinterface en NHRP-netwerk wanneer ze op de hub worden ontvangen. De **ip** nhrp **map ...** en **ip nhrp nhs** ... opdrachten worden door NHRP op het onderwerp gebruikt om de spokes NHRP-mapping (10.0.0.<n+1> —> 172.16.<n>.1) naar het hub te adverteren. Het 10.0.0.<n+1>-adres wordt opgeroepen van het **ip-adres ...** opdracht in de tunnelinterface en het 172.16.<n>.1-adres wordt opgehaald uit de **tunnelbestemming ...** opdracht in de tunnelinterface.

In een geval waar er 300 SPRAAKrouters zijn, zou deze verandering het aantal configuratielijnen op de hub verminderen van 3900 lijnen naar 16 lijnen (een vermindering van 3884 lijnen). De configuratie op elke spuitrouter zou met 6 lijnen toenemen.

Ondersteuning van dynamische adressen op telefoons

Op een router van Cisco, moet elke IPsec peer met het IP adres van het andere IPsec peer worden gevormd voordat de IPsec tunnel kan worden verhoogd. Er is een probleem om dit te doen als een gemaakte router een dynamisch adres op zijn fysieke interface heeft, dat gemeenschappelijk is voor routers die via DSL of kabellinks worden aangesloten.

TED laat één IPsec peer toe om een andere IPsec peer te vinden door een speciaal pakket van de Vereniging van de Veiligheid en het Protocol van het Toetsbeheer (ISAKMP) te verzenden naar het IP bestemmingsadres van het originele gegevenspakket dat moest worden versleuteld. De veronderstelling is dat dit pakket het tussenliggende netwerk langs het zelfde pad zal overlopen zoals door het IPsec tunnelpakket wordt genomen. Dit pakket wordt opgepikt door de andere end IPsec peer, die op de eerste peer zal reageren. De twee routers zullen vervolgens onderhandelen over ISAKMP- en IPsec-beveiligingsassociaties (SA's) en de IPsec-tunnel herstellen. Dit werkt alleen als de te versleutelen gegevenspakketten routeerbare IP-adressen hebben.

TED kan worden gebruikt in combinatie met de GRE-tunnels zoals ingesteld in de vorige sectie. Dit is getest en werkt, alhoewel er een bug in eerdere versies van Cisco IOS software was waar TED al IP verkeer tussen de twee IPsec peers dwong te worden versleuteld, niet alleen de GRE-tunnelpakketten. De oplossing DMVPN verstrekt deze en extra mogelijkheden zonder de hosts gebruik te moeten maken van routeerbare IP-adressen en zonder de noodzaak om sonde- en antwoordpakketten te verzenden. Met een lichte verandering, kan de configuratie van de laatste sectie worden gebruikt om gesproken routers met dynamische IP adressen op hun buitenkant fysieke interfaces te ondersteunen.

Hub router (geen verandering)

```
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
```

SPRAKE<n> router (oud)

```
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.
```

SPRAKE<n> router (nieuw)

```
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
```

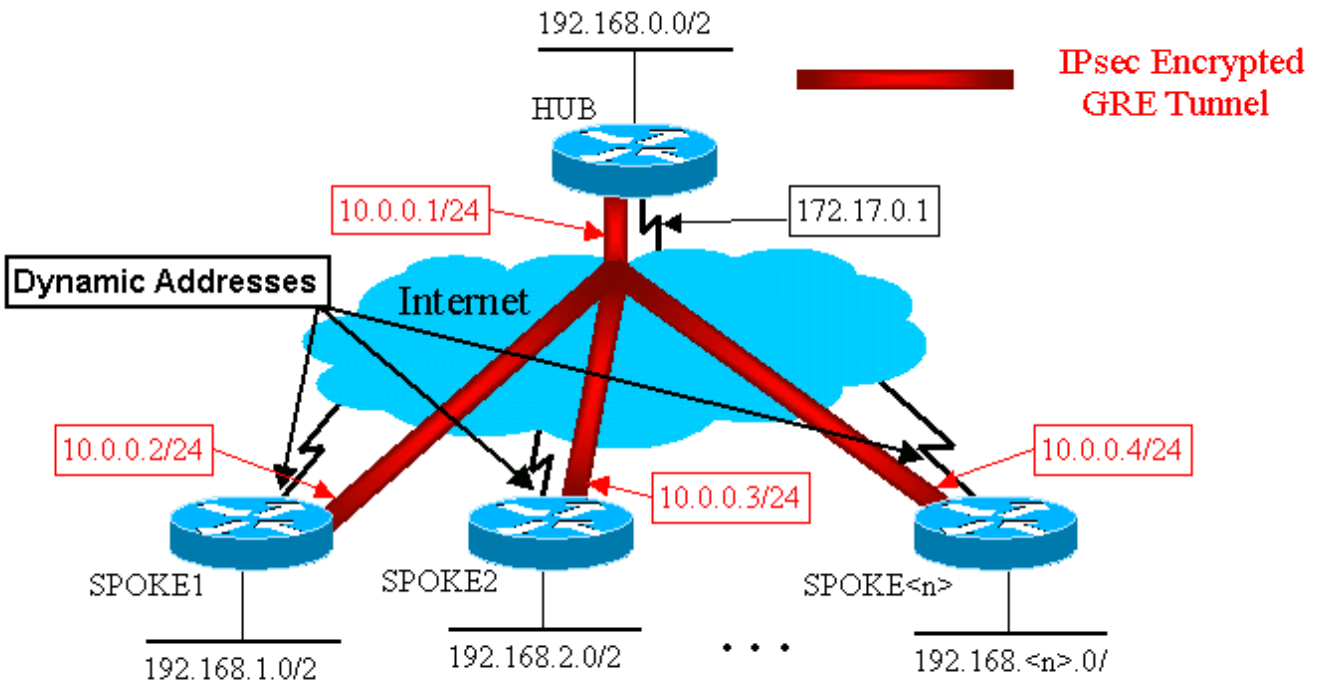
De functionaliteit die wordt gebruikt in de nieuwe configuratie is als volgt.

- Wanneer de GRE-tunnelinterface omhoog komt, zal zij NHRP-registratiepakketten naar de hubrouter gaan verzenden. Deze NHRP-registratiepakketten zullen IPsec activeren. Op de opgenomen router worden de ingestelde peer <peer-adres> en **match-ip access-lijst <ACL>**opdrachten ingesteld. ACL specificeert GRE als protocol, om het even welk voor de bron, en het hub IP adres voor de bestemming.**Opmerking:** Het is belangrijk om op te merken dat elke bron gebruikt wordt als bron in de ACL en dit moet het geval zijn aangezien het IP-adres van de spaakrouter dynamisch is en daarom niet bekend voordat de fysieke interface actief is. Een IP SUBNET kan voor de bron in ACL worden gebruikt als het dynamische gesproken interfaceadres beperkt zal zijn tot een adres binnen dat Subnet.
- De **ingestelde security-associatie niveau per-host** opdracht wordt gebruikt zodat de IP-bron in de spaken IPsec-proxy alleen het huidige fysieke interfaceadres (/32) van de spaken is, in

plaats van het 'enige' van de ACL. Als "om het even welk" van ACL als bron in de IPsec proxy werd gebruikt, zou dit verhinderen dat een andere beroemde router ook een IPsec+GRE-tunnel met deze hub installeert. Dit komt doordat de resulterende IPsec-proxy op de hub gelijk zou zijn aan **license gre host 172.17.0.1 of meer**. Dit zou betekenen dat alle GRE-tunnelpakketten die bestemd zijn voor om het even welke gesproken worden versleuteld en naar de eerste wordt verzonden die een tunnel met het centrum vormde, aangezien zijn IPsec-proxy-pakketten aansluit op GRE voor elke spreek.

- Zodra de IPsec-tunnel is ingesteld gaat een NHRP-registratiepakket van de gemaakte router naar de geconfigureerde Next Hop Server (NHS). De NHS is de hub router van dit knooppunt en het netwerk. Het NHRP-registratiepakket biedt de informatie voor de hubrouter om een NHRP-afbeelding voor deze gemaakte router te maken. Met deze afbeelding kan de router van de hub IP-gegevenspakketten naar deze gemaakte router doorsturen via de tunnel van mGRE+IPsec. Ook, voegt het hub de gesproken router toe aan zijn NHRP multicast mapping lijst. De hub zal dan beginnen om dynamische IP te verzenden die multicast pakketten naar de toespraak (als een dynamisch routingprotocol wordt gevormd) routeert. Spaan zal dan een routingprotocol buurman van de hub worden, en zij zullen routingupdates uitwisselen.

IPsec + mGRE-hub en hubknooppunt



Hub router

```
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
!
```

Merk in de bovenstaande hub-configuratie op dat de IP-adressen van de spraakrouters niet zijn geconfigureerd. De externe fysieke interface van de SPD en de omzetting in de IP-adressen van de tunnelinterface van de SPD worden door de hub via NHRP dynamisch geleerd. Dit staat toe het externe fysieke interface IP adres van de sprak dynamisch toe te wijzen.

SPE1 router

```
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
```

Spoke2 router

```
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
```

De belangrijkste dingen die te zien zijn over de uitgesproken configuraties zijn:

- Het externe fysieke interface (Ethernet0) IP-adres is dynamisch via DHCP.**IP-adreshostname Spoke2**
- Crypto ACL (101) specificeert een voorwerp als bron voor de IPsec proxy.**toegangslijst 101 vergunning gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- De volgende opdracht in de crypto kaart van IPsec specificeert dat de veiligheidsassociatie per host zal zijn.**veiligheidsniveau per host instellen**
- Alle tunnels maken deel uit van hetzelfde net, aangezien ze allemaal verbinden via dezelfde multi-point GRE interface op de hub router.**ip-adres 10.0.0.2 255.255.255.0**

De combinatie van deze drie opdrachten maakt het voor de externe fysieke interface-IP-adres van de gesproken niet nodig om te worden geconfigureerd. De proxy van IPsec die wordt gebruikt zal host-gebaseerd zijn in plaats van op subtype gebaseerd.

De configuratie op de gemaakte routers heeft het IP-adres van de hub router ingesteld, omdat deze de IPsec+GRE-tunnel moet openen. Merk op de overeenkomst tussen de Spoke1- en Spoke2-configuraties. Niet alleen zijn deze twee gelijkaardig, maar alle gesproken routerconfiguraties zullen gelijk zijn. In de meeste gevallen hebben alle spaken eenvoudig unieke IP-adressen op hun interfaces nodig, en de rest van hun configuraties zal hetzelfde zijn. Dit maakt het mogelijk om vele gesproken routers snel te configureren en in te voeren.

De NHRP-gegevens zien er op de hub als het volgende uit.

Hub router

```
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
```

SPE1 router

```
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
```

Dynamic Multipoint hub en Spoke

De configuratie op de genoemde routers is niet afhankelijk van functies van de DMVPN-oplossing, zodat de spraakrouters Cisco IOS-softwarereleases kunnen uitvoeren vóór 12.2(13)T. De configuratie op de hubrouter is gebaseerd op DMVPN-functies, dus moet u Cisco IOS versie 12.2(13)T of hoger uitvoeren. Dit geeft u enige flexibiliteit in het beslissen wanneer u uw gesproken routers moet verbeteren die reeds worden ingezet. Als uw gesproken routers ook Cisco IOS versie 12.2(13)T of hoger uitvoeren, kunt u de weergegeven configuratie als volgt vereenvoudigen.

Spoke<n> router (vóór 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
```

Spoke<n> router (na 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>
 !
```

Merk op dat we het volgende hebben gedaan:

1. Verwijderde de **crypto map vpnmap1 10 ipsec-isakmp** opdracht en verving deze met **crypto ipsec-profiel vpnprof**.
2. Verwijderde de opdracht **crypto map vpnmap1** van de Ethernet0 interfaces en plaats de opdracht **voor tunnelbescherming ipsec-profiel** op de Tunnel0 interface.
3. Verwijder crypto ACL, **toegangslijst 101 vergunning geeft elke host 172.17.0.1**.

In dit geval worden de IPsec peer adressen en proxy's automatisch afgeleid van de **tunnelbron ...** en **tunnelbestemming ...** configuratie. De peers en proxy's zijn als volgt (zoals gezien in de uitvoer van **show crypto ipsec als** opdracht):

```
...
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
...
```

Samengevat, omvatten de volgende volledige configuraties alle veranderingen die tot dit punt zijn gemaakt van de Base Configuration (IPsec+GRE hub en het gesproken).

Hub router

```
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
!
```

Er zijn geen wijzigingen in de hub configuratie.

SPE1 router

```
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
 !
```

Spoke2 router

```
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
 !
```

Dynamic Multipoint IPsec VPN

De concepten en configuratie in deze sectie tonen de volledige mogelijkheden van DMVPN. NHRP biedt de mogelijkheid voor de gesproken routers om het externe fysieke interfaceadres van de andere gesproken routers in het VPN-netwerk dynamisch te leren. Dit betekent dat een gemaakte router genoeg informatie zal hebben om dynamisch een IPsec+mGRE-tunnel rechtstreeks naar andere gesproken routers te bouwen. Dit is voordelig omdat, als dit sprak-aan-

sprak gegevensverkeer via de router van het hub werd verzonden, dan moet het worden versleuteld/decrypteerd, tweemaal om de vertraging en de lading op de router te verhogen. Om deze functie te kunnen gebruiken, moeten de gesproken routers worden overgeschakeld van point-to-point GRE (p-pGRE) naar multi-point GRE (mGRE) tunnelinterfaces. Ze moeten ook de (sub)netwerken leren die achter de andere woordjes met een IP volgende-hop van het tunnel IP adres van de andere gesproken router beschikbaar zijn. De gesproken routers leren deze (sub)netwerken via het dynamische IP-routeringsprotocol dat via de IPsec+mGRE-tunnel met het hub wordt uitgevoerd.

Het dynamische IP-routingprotocol dat op de router hub wordt uitgevoerd, kan worden geconfigureerd om de routes weer te geven die door één speld worden vanuit dezelfde interface naar alle andere spaken, maar de IP volgende-hop op deze routes zal gewoonlijk de hub router zijn, niet de spaakrouter waarvan de hub deze route heeft geleerd.

Opmerking: het dynamische routingprotocol werkt alleen op de hub en de gesproken links, het werkt niet op de dynamische sprak-aan-gesproken links.

De dynamische routeringsprotocollen (RIP, OSPF en EHW) moeten op de hubrouter worden geconfigureerd om de routes terug te geven in de mGRE-tunnelinterface en om de IP volgende-hop naar de oorspronkelijke gemaakte SPD-router in te stellen voor routes die van één spatie worden geleerd wanneer de route opnieuw naar de andere spaken wordt geadverteerd.

Het volgende is vereisten voor de routeringsprotocolconfiguraties.

RIP

U moet de gesplitste horizon op de mGRE-tunnelinterface op de hub uitschakelen, anders zal RIP geen routes die via de mGRE-interface zijn geleerd, buiten die zelfde interface adverteren.

```
no ip split-horizon
```

Er zijn geen andere wijzigingen nodig. RIP zal automatisch de originele IP volgende-hop op routes gebruiken die het uit de zelfde interface adverteert waar het deze routes leerde.

EINDTIJD

U moet de gesplitste horizon op de mGRE-tunnelinterface op de hub uitschakelen, anders zal u geen routes bekendmaken die via mGRE-interface zijn geleerd.

```
no ip split-horizon eigrp
```

Ecu zal standaard de IP next-hop instellen als de hubrouter voor routes die het adverteren is, zelfs wanneer zij die routes weer uit dezelfde interface adverteren waar zij ze geleerd hebben. In dit geval, heb u de volgende configuratieopdracht nodig om te Ecp te instrueren om de originele IP

volgende-hop te gebruiken wanneer het adverteren van deze routes.

```
no ip next-hop-self eigrp
```

Opmerking: de opdracht **no ip next-hop-self-eigrp** is beschikbaar vanaf Cisco IOS release 12.3(2). Voor Cisco IOS-releases tussen 12.2(13)T en 12.3(2) moet u het volgende doen:

- Indien dynamische tunnels met een spits niet gewild worden, dan is bovenstaand commando niet nodig.
- Als dynamische tunnels met een spaak worden gezocht, dan moet u processchakeling op de tunnelinterface op de gesproken routers gebruiken.
- Anders moet u een ander routingprotocol via DMVPN gebruiken.

OSPF

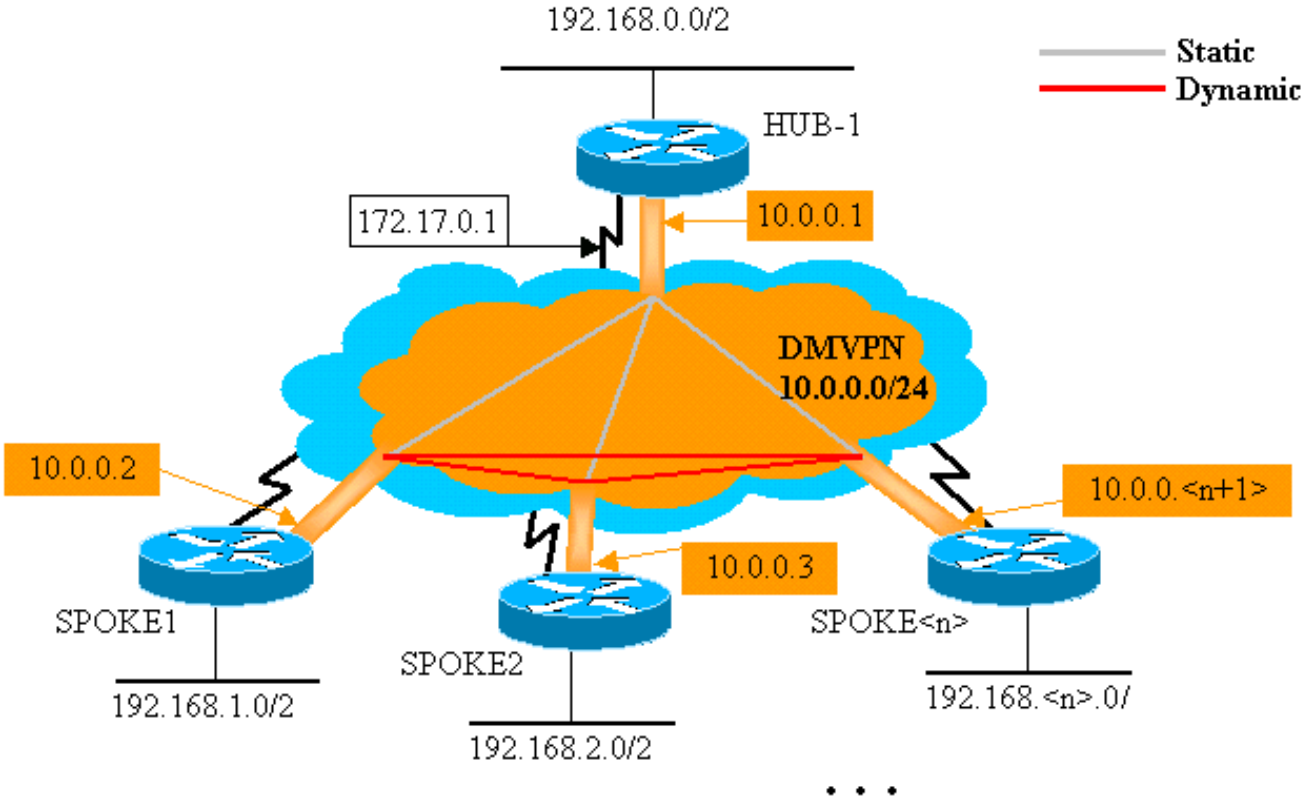
Aangezien OSPF een protocol is voor link-staat routing, zijn er geen problemen met gesplitste horizon. Normaal voor multipoint interfaces vormt u het OSPF-netwerktype om point-to-multipoint te zijn, maar dit zou OSPF ertoe aanzetten om host-routes aan de routingtabel op de gemaakte routers toe te voegen. Deze huurroutes zouden pakketten veroorzaken die aan netwerken achter andere gesproken routers zijn voorbestemd om via de hub te worden doorgestuurd, en dan direct aan andere gesproken. Om rond dit probleem te geraken, moet u het OSPF netwerktype configureren dat met de opdracht wordt uitgezonden.

```
ip ospf network broadcast
```

U moet er ook voor zorgen dat de hub router de Aangepaste router (DR) is voor het IPsec+mGRE-netwerk. Dit wordt gedaan door de OSPF prioriteit te plaatsen om groter dan 1 op de hub en 0 op de spaken te zijn.

- Hub: **ip - ospf - prioriteit 2**
- Gesproken: **ip - prioriteit 0**

DMVPN-single hub



Hub router

```
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
!
```

De enige verandering in de hub configuratie is dat OSPF het routeringsprotocol in plaats van DHCP is. Merk op dat het OSPF-netwerktype is ingesteld om uit te zenden en de prioriteit is ingesteld op 2. Wanneer u het OSPF-netwerktype instelt om uit te zenden, wordt OSPF-route voor netwerken achter de spaken-routers geïnstalleerd met een IP-adres voor de volgende hop als het GRE-tunneladres voor die gedeelde router.

SPE1 router

```
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
!
```

De configuratie op de uitgezonden routers lijkt nu sterk op de configuratie op de hub. De verschillen zijn als volgt:

- De OSPF-prioriteit is ingesteld op 0. De gemaakte routers kunnen niet worden toegestaan de DR voor het mGRE-netwerk (NBMA) voor niet-broadcast. Alleen de hub router heeft rechtstreekse statische verbindingen naar alle gesproken routers. De DR moet toegang hebben tot alle leden van het NBMA netwerk.
- Er zijn NHRP unicast en multicast mappings ingesteld voor de hub router.

  ```
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ```

  In de vorige configuratie, **was** de **IP** Nhrp **kaart multicast ...** opdracht niet nodig aangezien de GRE-tunnel punt tot punt was. In dat geval, zullen multicast pakketten automatisch door de tunnel aan de enige mogelijke bestemming worden ingekapseld. Deze opdracht is nu nodig omdat de spaken GRE-tunnel is veranderd in meerdere punten en er meer dan één mogelijke bestemming is.
- Wanneer de gesproken router omhoog komt, moet het de tunnelverbinding met de hub in werking stellen, aangezien de router van de hub niet met om het even welke informatie over de gesproken routers wordt gevormd, en de gesproken routers kunnen dynamisch toegewezen IP adressen hebben. De spaakrouters worden ook geconfigureerd met de hub als hun NHRP NHS.
  ```
  ip nhrp nhs 10.0.0.1
  ```
  Met de bovenstaande opdracht, zal de gemaakte router NHRP-registratiepakketten via de mGRE+IPsec-tunnel naar de hubrouter sturen met regelmatige tussenpozen. Deze registratiepakketten leveren de gemaakte NHRP-kaartinformatie die door de hubrouter nodig is om tunnelpakketten terug te plaatsen naar de gemaakte routers.

Spoke2 router

```
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
!
```

Spoke<n> router

```
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.
```

```
!
```

Merk op dat de configuraties van alle gemaakte routers zeer vergelijkbaar zijn. De enige verschillen zijn de IP-adressen op de lokale interfaces. Dit helpt bij het implementeren van een groot aantal spraakrouters. Alle gemaakte routers kunnen op identieke wijze worden geconfigureerd en alleen de lokale IP-interfaceadressen hoeven te worden toegevoegd.

Kijk op dit punt naar de routingtabellen en de NHRP-kaarttabellen op de routers voor de hub, Spoke1 en Spoke2 om de oorspronkelijke voorwaarden te zien (net nadat de routers Spoke1 en Spoke2 ter sprake zijn gekomen) en de voorwaarden nadat Spoke1 en Spoke2 een dynamische verbinding tussen hen hebben gecreëerd.

Aanvangsvoorwaarden

Routerinformatie voor hub

```
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
```

SPE1-routerinformatie

```
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
```

Spoke2-routerinformatie

```
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
```

Op dit punt pingelen we van 192.168.1.2 tot 192.168.2.3. Deze adressen zijn voor hosts achter de routers Spoke1 en Spoke2. De volgende opeenvolging van gebeurtenissen vindt plaats om de directe gesproken-aan-gesproken tunnel van mGRE+IPsec te bouwen.

1. De router Spoke1 ontvangt het ping-pakket met de bestemming 192.168.2.3. Het kijkt deze bestemming in de routingtabel op en vindt dat het dit pakket uit de interface van Tunnel0 naar de IP nexthop moet sturen, 10.0.0.3.
2. De router Spoke1 controleert de tabel van het NHRP-mapping voor de bestemming 10.0.3 en vindt dat er geen ingang is. De router Spoke1 maakt een NHRP-resolutie-verzoekpakket

en stuurt het naar de NHS-router (de Hub-router).

3. De hubrouter controleert zijn NHRP-mapping-tabel voor de bestemming 10.0.3 en vindt dat deze op de ADSL-router 172.16.2.75 wordt gericht. De Hub-router maakt een NHRP-antwoordpakket met resolutie en stuurt het naar de Spoke1-router.
4. De router Spoke1 ontvangt het NHRP-resolutie antwoord en gaat de 10.0.0.3 —>172.16.2.75 mapping in de NHRP-mapping tabel in. De toevoeging van de NHRP-afbeelding veroorzaakt IPsec om een IPsec-tunnel te openen met de peer 172.16.2.75.
5. De router Spoke1 initieert ISAKMP met 172.16.2.75 en onderhandelt over ISAKMP en IPsec SAs. De IPsec-proxy is afgeleid van de Tunnel0-**tunnelbron <adres>**opdracht en de NHRP-afbeelding.

```
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. Nadat de IPsec-tunnel is voltooid, worden alle verdere gegevenspakketten naar 192.168.2.0/24 subster direct naar Spoke2 verzonden.
7. Nadat een pakket dat is voorbestemd om 192.168.2.3 naar de host is doorgestuurd, zal deze host een retourpakket naar 192.168.1.2 verzenden. Wanneer de Spoke2-router dit pakket ontvangt dat is voorbestemd om 192.168.1.2 te ontvangen, zal hij deze bestemming in de routingtabel opzoeken en erachter komen dat deze pakje naar deze Packet nodig is om deze Packet door te sturen Keer0 interface naar de IP next-hop, 10.0.0.2.
8. De router Spoke2 controleert de NHRP mapping tabel voor de bestemming 10.0.2 en vindt dat er geen ingang is. De router Spoke2 maakt een NHRP-resolutie-verzoekpakket en stuurt het naar de NHS-router (de Hub-router).
9. De hubrouter controleert zijn NHRP-mapping-tabel voor de bestemming 10.0.2 en stelt vast dat deze op de ADSL-router 172.16.1.24 is gericht. De Hub-router maakt een NHRP-antwoordpakket met resolutie en stuurt het naar de Spoke2-router.
10. De router Spoke2 ontvangt het NHRP-resolutie antwoord en gaat de 10.0.0.2 —> 172.16.1.24 mapping in de NHRP-kaarttabel in. De toevoeging van de NHRP-mapping zorgt voor IPsec om een IPsec-tunnel te openen met de peer 172.16.1.24, maar er is al een IPsec-tunnel met peer 172.16.1.24, zodat er niets meer hoeft te worden gedaan.
11. Spoke1 en Spoke2 kunnen nu pakketten rechtstreeks aan elkaar doorsturen. Wanneer de NHRP-mapping niet is gebruikt voor het verzenden van pakketten voor de duur van het programma, wordt de NHRP-afbeelding verwijderd. Het wissen van de ingang van NHRP mapping zal IPsec starten om de IPsec SAs voor deze directe verbinding te verwijderen.

De voorwaarden nadat een dynamisch verband tussen Spoke1 en Spoke2 tot stand is gebracht

SPE1-routerinformatie

```
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
```

Spoke2-routerinformatie

```
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
```

Van de bovenstaande output kan je zien dat Spoke1 en Spoke2 NHRP-mappings voor elkaar hebben gekregen van de hubrouter, en ze hebben een mGRE+IPsec-tunnel gebouwd en gebruikt. De NHRP-mappings verlopen na vijf minuten (de huidige waarde van de NHRP holdtime = 300 seconden). Als de NHRP-mappings binnen de laatste minuut voor het verstrijken worden gebruikt, wordt een NHRP-resolutie-verzoek en een antwoord naar u gestuurd om de ingang te verfrissen voordat deze wordt verwijderd. Anders wordt de NHRP-mapping verwijderd en wordt IPsec geactiveerd om de IPsec SAs te wissen.

Dynamic Multipoint IPsec VPN met dubbele hub

Met een paar extra configuratielijnen naar de gesproken routers kunt u dubbele (of meerdere) hub routers instellen, voor redundantie. Er zijn twee manieren om dubbele hub DMVPN's te configureren.

- Een enkel DMVPN-netwerk met elk sprak door gebruik te maken van één GRE-

tunnelinterface met meerdere aansluitingen en door naar twee verschillende knooppunten te wijzen als de Next-Hopserver (NHS).De hubrouters zullen alleen één GRE-tunnelinterface met meerdere punten hebben.
- Dubbele DMVPN netwerken met elk die twee GRE-tunnelinterfaces (of punt tot punt of multipoint) hebben en elke GRE-tunnel die op een verschillende hub router wordt aangesloten.Opnieuw zullen de hubrouters slechts één GRE-tunnelinterface met meerdere punten hebben.

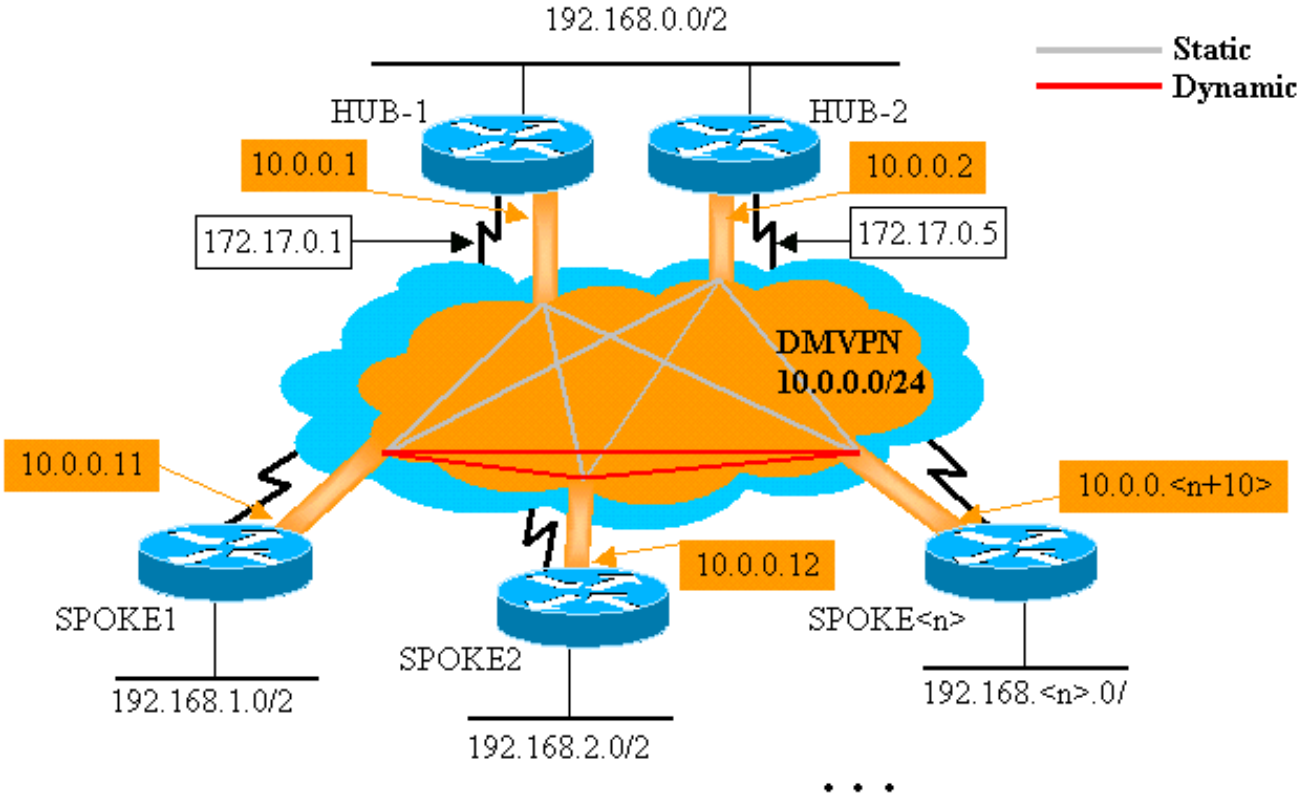
De volgende voorbeelden zullen kijken naar het configureren van deze twee verschillende scenario's voor dubbele hub DMVPN's. In beide gevallen zijn de gemarkeerde verschillen relatief tot de DMVPN enkele hubconfiguratie.

Dubbele hub - één DMVPN-lay-out

Het dubbele hub met één DMVPN-lay-out is vrij makkelijk in te stellen, maar het geeft u niet evenveel controle over het routeren over de DMVPN als het dubbele hub met dubbele DMVPN's lay-out. Het idee in dit geval is om één enkele "cloud" van DMVPN te hebben met alle hubs (twee in dit geval) en alle spokes verbonden met dit enige net ("cloud"). De statische NHRP-mappingen van de spaken naar de hubs definiëren de statische IPsec+mGRE-koppelingen waarover het dynamische routingprotocol wordt uitgevoerd. Het dynamische routerprotocol wordt niet via de dynamische IPsec+mGRE-koppelingen tussen spaken uitgevoerd. Aangezien de gesproken routers buren met de hub routers via dezelfde mGRE-tunnelinterface routeren, kunt u geen verbinding of interfaces verschillen (zoals metrische, kosten, vertraging of bandbreedte) gebruiken om de dynamische routingprotocolmetriek aan te passen om één hub boven de andere hub te prefereren wanneer ze allebei omhoog zijn. Als deze voorkeur nodig is, moeten de technieken intern aan de configuratie van het routeringsprotocol worden gebruikt. Om deze reden, kan het beter zijn om wanneer u een Ecp of RIP in plaats van OSPF voor het dynamische routeringsprotocol te gebruiken.

Opmerking: het bovenstaande probleem is meestal alleen een probleem als de hubrouters gezamenlijk zijn gevestigd. Wanneer zij niet samen gevestigd zijn, zal de normale dynamische routing waarschijnlijk hoger eindigen dan de voorkeur geven aan de juiste hubrouter, zelfs als het doelnetwerk via een van beide hubrouter kan worden bereikt.

Dubbele hub - één DMVPN-lay-out



Hub router

```
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
!
```

Hub2-router

```
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
!
```

De enige verandering in de Hub1 configuratie is OSPF te veranderen om twee gebieden te gebruiken. Gebied 0 wordt gebruikt voor het netwerk achter de twee knooppunten, en gebied 1 wordt gebruikt voor het netwerk DMVPN en de netwerken achter de gesproken routers. OSPF kon

één gebied gebruiken, maar twee gebieden werden hier gebruikt om de configuratie voor meerdere OSPF-gebieden aan te tonen.

De configuratie voor Hub2 is in wezen hetzelfde als de Hub1-configuratie met de juiste IP-adreswijzigingen. Het enige belangrijkste verschil is dat Hub2 ook een gezochte (of client) van Hub1 is, wat Hub1 het primaire hub en Hub2 het secundaire hub maakt. Dit wordt gedaan zodat Hub2 een OSPF buurman met Hub1 via de mGRE-tunnel is. Aangezien Hub1 de OSPF DR is, moet het een directe verbinding met alle andere OSPF routers over de mGRE-interface (NBMA-netwerk) hebben. Zonder het directe verband tussen Hub1 en Hub2 zou Hub2 niet in de OSPF-routing deelnemen wanneer Hub1 ook omhoog is. Wanneer Hub1 is gedaald, zal Hub2 de OSPF DR voor het netwerk DMVPN (NBMA) zijn. Wanneer Hub1 weer omhoog komt, zal het het zijn van de OSPF DR voor DMVPN overnemen.

De routers achter Hub1 en Hub2 zullen Hub1 gebruiken voor het verzenden van pakketten naar de SPD netwerken omdat de bandbreedte voor de GRE-tunnelinterface is ingesteld op 1000 Kb/sec versus 900 Kb/sec op Hub2. In contrast hiermee zullen de gesproken routers pakketten voor de netwerken achter de hub routers verzenden naar zowel Hub1 als Hub2, omdat er slechts één mGRE-tunnelinterface op elke Spredichte router is en er zal zijn twee gelijke kostenroutes . Als er een taakverdeling per pakket wordt gebruikt, kunnen er "out-of-order"-pakketten ontstaan.

SPE1 router

```
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
!
```

De verschillen in configuratie op de Spaanstalige routers zijn als volgt:

- In de nieuwe configuratie wordt het spraken gevormd met statische NHRP mappings voor Hub2 en Hub2 wordt toegevoegd als volgende hopserver.Origineel:

  ```
  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
  ```

  Nieuw:

  ```
  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
  ```

- De OSPF-gebieden op de gemaakte routers zijn gewijzigd in gebied 1.

Vergeet niet dat door de statische NHRP-mapping en NHS op een gemaakte router voor een hub te definiëren, u het dynamische routingprotocol via deze tunnel gaat uitvoeren. Dit definieert de hub en het gesproken routingnetwerk of het buurnetwerk. Merk op dat Hub2 een hub is voor alle spokes, en het is ook een spookplaat voor Hub1. Dit maakt het gemakkelijk om multilayer hub and sprak netwerken te ontwerpen, te vormen en aan te passen wanneer u de DMVPN-oplossing gebruikt.

Spoke2 router

```
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
!
```

Spoke<n> router

```
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.




!
```

Op dit punt kunt u de routingtabellen, de NHRP-kaarttabellen en de IPsec-verbindingen op de routers Hub1, Hub2, Spoke1 en Spoke2 bekijken om de initiële voorwaarden te zien (net nadat de routers Spoke1 en Spoke2 verschijnen).

Aanvangsvoorwaarden en wijzigingen

Hub1-routerinformatie

```
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
```

Hub2-routerinformatie

```
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
```

SPE1-routerinformatie

```
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
```

Spoke2-routerinformatie

```
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
```

Er zijn een paar interessante kwesties om aandacht te besteden aan de routingtabellen op Hub1, Hub2, Spoke1 en Spoke2:

- Beide hub routers hebben gelijke kostenroutes naar de netwerken achter de gemaakte routers.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
  ```

  Dit betekent dat Hub1 en Hub2 dezelfde kosten voor de netwerken achter de gesproken routers aan de routers in het netwerk achter de hubrouters zullen adverteren. Bijvoorbeeld, zou de routeringstabel op een router, R2, die direct op 192.168.0.0/24 LAN wordt aangesloten als het volgende lijken: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
  ```

- De gesproken routers hebben gelijke kostenroutes via beide hub routers naar het netwerk achter de hubrouters.Gesproken1:

  ```
  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
  ```

  Als de gesproken routers het in evenwicht brengen van de lading per pakket doen, dan zou u uit orde van orde pakketten kunnen krijgen.

Om asymmetrische routing of het in evenwicht brengen per pakketlading over de verbindingen naar de twee knooppunten te vermijden, moet u het routeringsprotocol configureren om één streep-naar-hub pad in beide richtingen te prefereren. Als u wilt dat Hub1 de primaire en Hub2 de backup is, dan kunt u de OSPF-kosten op de hub tunnelinterfaces instellen om anders te zijn.

Hub1:

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

Hub2:

```
interface tunnel0
```

```
...
ip ospf cost 20
...
```

De routes lijken nu op het volgende:

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
```

De twee hub routers hebben nu verschillende kosten op de routes voor de netwerken achter de gemaakte routers. Dit betekent dat Hub1 de voorkeur zal hebben voor het verzenden van verkeer naar de gesproken routers, zoals kan worden gezien op router R2. Dit zal zorgen voor het asymmetrische routingprobleem dat in de eerste kogel hierboven wordt beschreven.

De asymmetrische routing in de andere richting, zoals beschreven in de tweede kogel hierboven, is er nog steeds. Wanneer u OSPF als het dynamische routingprotocol gebruikt, kunt u dit met een tijdelijke oplossing repareren door de **afstand** te gebruiken **...** opdracht onder **router ospf 1** op de spaken om wegen te prefereren die via Hub1 via routes geleerd zijn via Hub2.

Gesproken1:

```
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
```

De routes lijken nu op het volgende:

Gesproken1:

```
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
```

De bovenstaande routingconfiguratie zal bescherming bieden tegen asymmetrische routing, terwijl tegelijkertijd failover naar Hub2 wordt toegestaan als Hub1 kleiner wordt. Het betekent dat wanneer beide hubs omhoog zijn, alleen Hub1 wordt gebruikt. Als u beide hubs wilt gebruiken

door de spaken over de knooppunten in balans te brengen, met overnambescherming en geen asymmetrische routing, dan kan de routingconfiguratie complex worden, vooral wanneer u OSPF gebruikt. Om deze reden kan het volgende dubbele hub met dubbele DMVPN-lay-out een betere keuze zijn.

Dubbele hub - dubbele DMVPN-lay-out

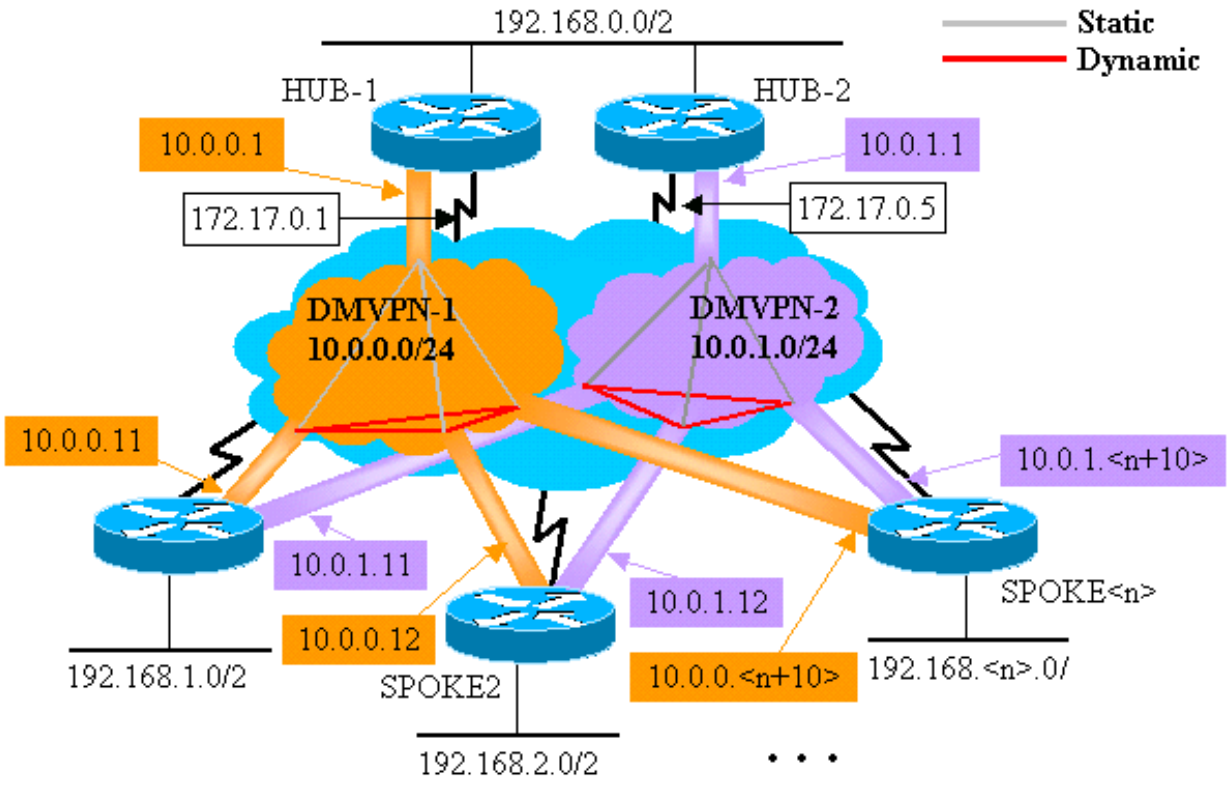
Het dubbele hub met dubbele DMVPN-lay-out is iets moeilijker in te stellen, maar het geeft u betere controle over het routing via DMVPN. Het idee is om een twee aparte DMVPN "wolken" te hebben. Elke hub (twee in dit geval) wordt aangesloten op één DMVPN-subnet ("cloud") en de spaken zijn verbonden met beide DMVPN-subnetten ("clouds"). Aangezien de gesproken routers buren met beide hub routers over de twee GRE-tunnelinterfaces routeren, kunt u interfacemoditeitsverschillen (zoals bandbreedte, kosten en vertraging) gebruiken om de dynamische routingprotocolmetriek aan te passen om één hub boven de andere hub te prefereren wanneer ze allebei omhoog zijn.

Opmerking: het bovenstaande probleem is meestal alleen relevant wanneer de hubrouters gezamenlijk zijn geïnstalleerd. Wanneer zij niet samen gevestigd zijn, zal de normale dynamische routing waarschijnlijk hoger eindigen dan de voorkeur geven aan de juiste hubrouter, zelfs als het doelnetwerk via een van beide hubrouter kan worden bereikt.

U kunt of p-pGRE of mGRE tunnelinterfaces op de gesproken routers gebruiken. De meerdere p-pGRE interfaces op een bepaalde router kunnen de zelfde **tunnelbron** gebruiken.. IP-adres, maar meerdere mGRE-interfaces op een bepaalde router moeten een unieke **tunnelbron** hebben... IP-adres. Dit komt doordat, wanneer IPsec start, het eerste pakket een ISAKMP-pakket is dat moet worden gekoppeld aan een van de mGRE-tunnels. Het ISAKMP-pakket heeft alleen het bestemming IP-adres (extern IPsec peer-adres) waarmee u deze associatie kunt maken. Dit adres is gelijk aan het **tunneladres...** maar aangezien beide tunnels dezelfde **tunnelbron** hebben... adres, is de eerste mGRE tunnelinterface altijd gelijk. Dit betekent dat inkomende multicast gegevenspakketten aan de verkeerde mGRE interface kunnen worden gekoppeld, waardoor een dynamisch routingprotocol wordt gebroken.

GRE-pakketten zelf hebben dit probleem niet omdat ze de **tunneltoets** hebben ... waarde om te differentiëren tussen de twee mGRE-interfaces. Vanaf het begin in Cisco IOS-softwarereleases 12.3(5) en 12.3(7)T is er een extra parameter geïntroduceerd om deze beperking te overwinnen: **tunnelbescherming...gedeeld**. Het **gedeelde** sleutelwoord wijst erop dat de meerdere mGRE interfaces de encryptie IPSec met het zelfde bron IP adres zullen gebruiken. Als u een eerdere release hebt, kunt u p-pGRE-tunnels in dit dubbele hub met dubbele DMVPN-lay-out gebruiken. In de p-pGRE tunnelzaak, zowel de **tunnelbron ...** als de **tunnelbestemming ...** IP-adressen kunnen worden gebruikt voor matching. Bij dit voorbeeld zullen p-pGRE tunnels in dit dubbele hub met dubbele DMVPN-lay-out worden gebruikt en niet de **gedeelde** kwalificatieversterker gebruiken.

Dubbele hub - dubbele DMVPN-lay-out



De volgende gemarkeerde veranderingen zijn relatief tot de dynamische multipoint hub en de Spaanstalige configuraties die eerder in dit document worden geïllustreerd.

Hub1 router

```
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
!
```

Hub2-router

```
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
!
```

In dit geval zijn de Hub1- en Hub2-configuraties vergelijkbaar. Het belangrijkste verschil is dat elk de hub van een andere DMVPN is. Elke DMVPN gebruikt een ander platform:

- IP-telefoon (10.0.0.0/24, 10.0.0.1/24)
- NHRP-netwerkid (100000, 100001)
- Tunneltoets (100000, 100001)

Het dynamische routerprotocol is overgeschakeld van OSPF naar DHCP, omdat het gemakkelijker is om een netwerk NBMA op te zetten en te beheren gebruikmakend van DHCP, zoals later in dit document beschreven.

SPE1 router

```
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
!
```

Elk van de gesproken routers is geconfigureerd met twee p-pGRE-tunnelinterface, één in elk van de twee DMVPN's. Het **IP-adres ...**, **ip Nhrp network-id ...**, **tunneltoets ...** en **tunnelbestemming ...** de waarden worden gebruikt om onderscheid te maken tussen de twee tunnels. Het dynamische routingprotocol, DHCP, wordt uitgevoerd over beide p-pGRE tunnelsubnetten en wordt gebruikt om één p-pGRE interface (DMVPN) over het andere te selecteren.

Spoke2 router

```
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
 !
```

Spoke<n> router

```
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.




  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.




  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
!
```

Op dit punt, laten we de routingtabellen, de NHRP-kaarttabellen en IPsec-verbindingen op de routers Hub1, Hub2, Spoke1 en Spoke2 bekijken om de initiële voorwaarden te zien (net nadat de routers Spoke1 en Spoke2 naar boven zijn gekomen).

Aanvangsvoorwaarden en wijzigingen

Hub1-routerinformatie

```
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
```

Hub2-routerinformatie

```
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
```

SPE1-routerinformatie

```
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
```

Spoke2-routerinformatie

```
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
```

Opnieuw zijn er een paar interessante dingen om op te merken over de routingtabellen op Hub1, Hub2, Spoke1 en Spoke2:

- Beide hub routers hebben gelijke kostenroutes naar de netwerken achter de gemaakte routers.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
  ```
  Dit betekent dat Hub1 en Hub2 dezelfde kosten voor de netwerken achter de gesproken routers aan de routers in het netwerk achter de hubrouters zullen adverteren. Bijvoorbeeld, zou de routeringstabel op een router, R2, die direct op 192.168.0.0/24 LAN wordt aangesloten als het volgende lijken: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
  ```
- De gesproken routers hebben gelijke kostenroutes via beide hub routers naar het netwerk achter de hubrouters.Gesproken1:
  ```
  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
  ```
  Als de gesproken routers bezig zijn met het in evenwicht brengen van de lading per pakket, dan zou u uit orde van orde pakketten kunnen krijgen.

Om asymmetrische routing of het in evenwicht brengen per pakketlading over de verbindingen naar de twee knooppunten te vermijden, moet u het routeringsprotocol configureren om één streep-naar-hub pad in beide richtingen te prefereren. Als je wilt dat Hub1 de primaire en Hub2 de back-up is, dan kan je de vertraging op de hub tunnelinterfaces anders instellen.

Hub1:

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

Hub2:

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

Opmerking: In dit voorbeeld werd 50 toegevoegd aan de vertraging op de tunnelinterface op Hub2 omdat het kleiner is dan de vertraging op Ethernet1-interface tussen de twee hubs (100). Door dit te doen, zal Hub2 pakketten rechtstreeks naar de gesproken routers doorsturen, maar het zal een minder wenselijke route dan Hub1 naar routers achter Hub1 en Hub2 adverteren. Als de vertraging met meer dan 100 was toegenomen, dan zou Hub2 pakketten voor de verspreide routers door Hub1 via de Ethernet1-interface doorsturen, alhoewel de routers achter Hub1 en Hub2 nog steeds liever Hub-1 hebben voor het verzenden van routers.

De routes lijken nu op het volgende:

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
```

De twee hub routers hebben verschillende kosten voor de netwerkroutes achter de verspreide routers, dus in dit geval zal Hub1 de voorkeur hebben voor het verzenden van verkeer naar de verspreide routers, zoals op R2 kan worden gezien. Dit houdt zich bezig met kwesties die in de eerste kogel hierboven zijn beschreven.

De kwestie die in de tweede kogel hierboven wordt beschreven is daar nog, maar aangezien u twee p-pGRE tunnelinterfaces hebt, kunt u de **vertraging...** op de tunnelinterfaces afzonderlijk instellen**... om** de metriek te veranderen van de Ecu voor de routes die van Hub1 versus Hub2 geleerd worden.

Gesproken1:

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

Spoke2:

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

De routes lijken nu op het volgende:

Gesproken1:

```
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
```

De bovenstaande routingconfiguratie zal bescherming bieden tegen asymmetrische routing, terwijl tegelijkertijd failover naar Hub2 wordt toegestaan als Hub1 kleiner wordt. Het betekent dat wanneer beide hubs omhoog zijn, alleen Hub1 wordt gebruikt.

Als u beide hubs wilt gebruiken door de spaken over de knooppunten in balans te brengen, met bescherming tegen overvallen en geen asymmetrische routing, dan is de routingconfiguratie complexer, maar u kunt het doen wanneer u gebruik maakt van DHCP. Om dit te bereiken, stel de **vertraging ...** op de tunnelinterfaces van de hub routers terug tot gelijk aan zijn en gebruik dan de **offset-lijst <acl> uit <offset>**-opdracht op de verspreide routers om de EHBO-metriek te verhogen voor routes die de GRE-tunnelinterfaces naar de reserveknop worden geadverteerd. De ongelijke **vertraging ...** tussen de interfaces Tunnel0 en Tunnel1 op het gesproken wordt nog gebruikt, zodat de SPA-router zijn primaire router liever zal hebben. De veranderingen op de gesproken routers zijn als volgt.

SPE1 router

```
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
 !
```

Spoke2 router

```
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
 !
```

Opmerking: de offset waarde van 12800 (50*256) werd toegevoegd aan de EHRM-waarde omdat deze kleiner is dan 25600 (100*256). Deze waarde (25600), is wat aan de metriek wordt toegevoegd Ecu voor routes die tussen de hub routers worden geleerd. Door 12800 in het bevel **offset-list** te gebruiken, zal de router van de backup hub pakketten rechtstreeks naar de spaakrouters doorsturen, in plaats van deze pakketten via Ethernet door te sturen om door de primaire router voor die spaken te gaan. De metriek op de routes die door de hub routers worden geadverteerd zal nog van dien aard zijn dat de juiste primaire router zal worden prefereerd. Onthoud dat de helft van de spaken Hub1 als hun primaire router hebben, en de andere helft heeft Hub2 als hun primaire router.

Opmerking: Als de offset waarde met meer dan 25600 (100*256) was verhoogd, zouden de hubs pakketten doorsturen voor de helft van de verspreide routers via de Ethernet1-interface, zelfs al zouden de routers achter de hubs nog steeds de juiste hub voor het verzenden van pakketten naar de gedeelde routers prefereren.

Opmerking: Het **distribueren-list 1 uit** commando werd ook toegevoegd aangezien het mogelijk is dat routes die van één hub router via één tunnelinterface op een gesproken werd geleerd, via de andere tunnel terug naar het andere hub zouden kunnen worden geadverteerd. De **verdeler-lijst...** opdracht waarborgt dat de uitgesproken router alleen zijn eigen routes kan adverteren.

N.B.: Als u liever de routingadvertenties op de hubrouters dan op de verspreide routers controleert, **kan** de **offset-lijst <acl1> in <waarde>**en **verdeellijst <acl2> in** opdrachten worden ingesteld op de hubrouters in plaats van op de spaken. De toegangslijst van <acl2> zou de routes van achter alle spokes opsommen en de toegangslijst van <acl1> zou alleen de routes van achter spokes opsommen waar een andere hubrouter het primaire hub moet zijn.

Met deze veranderingen zien de routes er als volgt uit:

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
```

Gesproken1:

```
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
```

Conclusie

De DMVPN-oplossing biedt de volgende functionaliteit om grote en kleine IPsec VPN-netwerken beter te kunnen schalen.

- DMVPN maakt het beter mogelijk om in volledige mesh of gedeeltelijke vermaasde IPsec VPN's te schalen.Het is vooral nuttig wanneer gesproken verkeer sporadisch is (bijvoorbeeld elke spreker stuurt niet voortdurend gegevens naar elkaar). Het staat elke gesproken persoon toe om gegevens direct naar elke andere gesproken te sturen, zolang er een directe IP verbinding tussen de woordvoerders is.
- DMVPN ondersteunt IPsec-knooppunten met dynamisch toegewezen adressen (zoals Cable,

ISDN en DSL).Dit is van toepassing op hub-and-sprak zowel als maasnetwerken. DMVPN kan de verbinding van de hub tot aan de sprak vereisen om constant omhoog te zijn.

- DMVPN vereenvoudigt de toevoeging van VPN-knooppunten.Wanneer u een nieuwe spuitrouter toevoegt, hoeft u alleen de gemaakte router te configureren en in het netwerk te stoppen (alhoewel, u kunt de ISAKMP autorisatie informatie voor het nieuwe die op het hub wordt gesproken toe moeten voegen). De hub zal dynamisch over het nieuwe gesproken worden leren en het dynamische routeringsprotocol zal het routing naar de hub en alle andere spaken propageren.
- DMVPN beperkt de grootte van de configuratie die nodig is voor alle routers in VPN.Dit is ook het geval voor GRE+IPsec hub-and-sprak-only VPN-netwerken.
- DMVPN gebruikt GRE en ondersteunt IP daarom multicast en dynamisch routingverkeer via VPN.Dit betekent dat een dynamisch routingprotocol kan worden gebruikt, en de overtollige "knooppunten" kunnen door het protocol worden ondersteund. Multicasttoepassingen worden ook ondersteund.
- DMVPN ondersteunt gesplitste tunneling op de spaken.

Gerelateerde informatie

- Dynamic Multipoint VPN (DMVPN)
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen