BGP via DMVPN fase 3 configureren

Inhoud

- Inleiding
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
- Achtergrondinformatie
  - Wat is DMVPN?
  - Hoe werkt DMVPN?
  - Wat zijn de verschillende typen DMVPN?
  - Traffic Flow voor DMVPN fase 3
- Netwerkdiagram
- Configuraties
  - Crypto-configuraties
  - DMVPN-configuratie
  - BGP-configuratie
    - eBGP met verschillende AS op de spaken
- Verifiëren
- Problemen oplossen

Inleiding

Dit document beschrijft de configuratie en werking van DMVPN fase 3 met behulp van BGP, inclusief gelaagde probleemoplossing voor IPsec via DMVPN-tunnels.

Voorwaarden

Voor de configuratie en debug van opdrachten in dit document hebt u twee Cisco-routers nodig die werken met Cisco IOS® release 15.3(3)M of hoger. Over het algemeen is voor een standaard Dynamic Multipoint VPN (DMVPN) fase 3 Cisco IOS release 12.4(6)T vereist, hoewel de functies en debugs die in dit document te zien zijn, niet volledig worden ondersteund.

Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- IKEV1/IKEV2 en IPsec
- DMVPN-componenten:

- Next Hop Resolution Protocol (NHRP): Maakt een gedistribueerde (NHRP) mapping database van alle spraaktunnels naar echte (publieke interface) adressen

- Multipoint Generic Routing Encapsulation (mGRE)-tunnelinterface: Single Generic Routing Encapsulation (GRE)-interface om meerdere GRE/IPsec-tunnels te ondersteunen, vereenvoudigt grootte en complexiteit van configuratie en ondersteunt dynamische tunnelcreatie
- IPsec-tunnelbescherming: Maakt dynamisch coderingsbeleid aan en past dit toe
- Routing: Dynamische netwerken; bijna alle routingprotocollen (Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), BGP en ODR) worden ondersteund

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco ASR 1000 Series Aggregation Services Routers, versie 17.6.5(MD).

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

Achtergrondinformatie

Wat is DMVPN?

DMVPN is een Cisco IOS-softwareoplossing voor de eenvoudige, dynamische en schaalbare bouw van IPsec+GRE VPN's. Het is een oplossing om een VPN-netwerk met meerdere sites te bouwen zonder alle apparaten statisch te moeten configureren. Het is een 'hub and spoke'-netwerk waar de spokes direct met elkaar kunnen communiceren zonder dat ze door de hub hoeven te gaan. Encryptie wordt ondersteund via IPsec waardoor DMVPN een populaire keuze is voor het verbinden van verschillende sites met behulp van reguliere internetverbindingen.

Hoe werkt DMVPN?

- Spokes bouwen een dynamische permanente GRE/IPsec tunnel naar de hub, maar niet naar andere spokes. Ze registreren als clients van de NHRP server (hub).
- Wanneer een spaak een pakket naar een bestemmings (privé) subnetje achter een andere spaak moet verzenden, vraagt het via NHRP naar het echte (buiten) adres van de bestemming spaak.
- Nu kan de oorspronkelijke spoke een dynamische GRE/IPsec-tunnel starten naar de target spoke (omdat het de peer address kent).
- De dynamische spraak-to-spraaktunnel is gebouwd over de mGRE-interface.
- Als het verkeer stopt, wordt de spraaktunnel verwijderd.

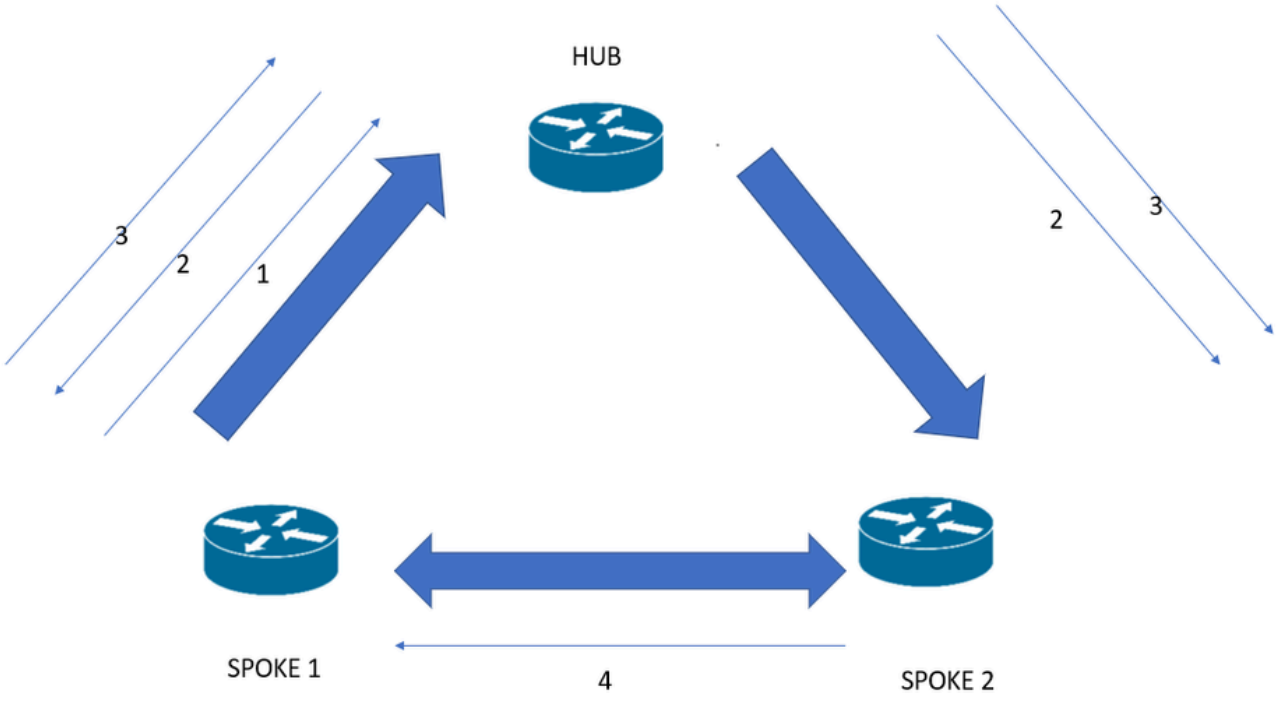
Wat zijn de verschillende typen DMVPN?

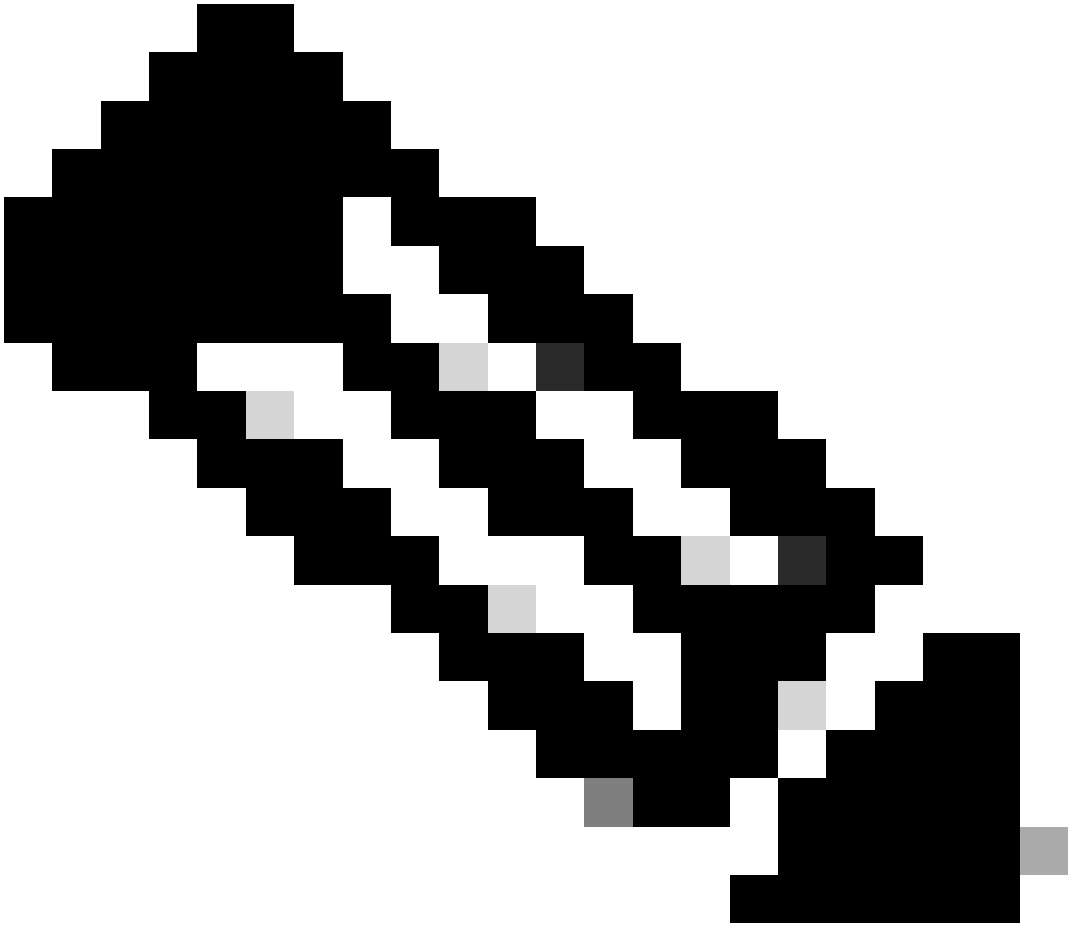
1. DMVPN fase I: Deze fase betreft een enkele mGRE interface op de hub, en alle spokes zijn nog statische tunnels, zodat u geen dynamische spraak-to-spoke connectiviteit krijgt.

2. DMVPN fase II: In deze fase wordt elke site met een mGRE-interface geconfigureerd, zodat u uw dynamische spraak-to-spoke connectiviteit krijgt.
3. DMVPN fase III: Deze fase breidt de schaalbaarheid van het DMVPN-netwerk uit. Dit impliceert het samenvatten in de wolk DMVPN. Samen met het configureren van NHRP-omleidingen en NHRP snelkoppeling. NHRP omleidt vertelt de bron om een betere weg naar de bestemming te vinden die het probeert te bereiken. Met NHRP-sneltoetsen kan DMVPN over andere netwerken achter andere DMVPN-routers leren.

Traffic Flow voor DMVPN fase 3

1. Het pakket wordt verzonden van Spoke's 1 netwerk naar Spoke's 2 netwerken via Hub (volgens de routeringstabel).
2. Hub routeert het pakket naar Spoke2 maar stuurt tegelijkertijd het NHRP Redirect bericht terug naar Spoke1 met informatie over het suboptimale pad naar Spoke2 en de tunnel IP van Spoke2.
3. Spoke1 geeft dan het NHRP Resolutie verzoek van 2 Nonbroadcast Multiaccess (NBMA) IP-adres van Spoke uit aan de Next Hop Server (NHS) met de bestemming IP van Spoke's 2-tunnel. Dit NHRP Resolutie verzoek wordt verzonden gericht naar Spoke2 via NHS (volgens de routeringstabel) - het is een normaal hop-door-hop NHRP doorsturen proces.
4. Spoke2 na het ontvangen van het resolutieverzoek inclusief de NBMA IP van Spoke1 stuurt het NHRP Resolutie antwoord direct naar Spoke1 - Antwoord niet dwars door de Hub!
5. Spoke1 na het ontvangen van de juiste NBMA IP van Spoke2 herschrijft de CEF-vermelding voor het doelprefix - deze procedure wordt NHRP Shortcut genoemd.
6. Spokes veroorzaken geen NHRP door het glimmen van nabijheid, maar de antwoorden van NHRP werken de CEF bij.



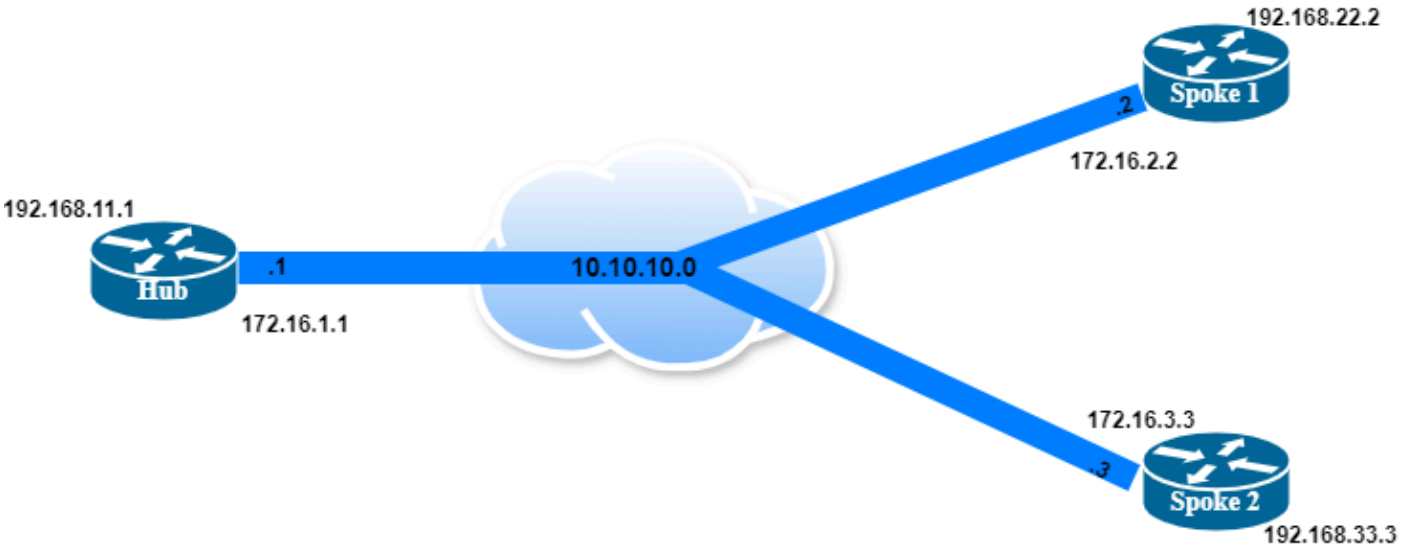


Opmerking:

DMVPN fase 2: In deze fase is het eerste spraakpakket inderdaad procesgeschakeld omdat de CEF-nabijheid zich in de 'glean'-staat bevindt. Dit betekent dat de router niet genoeg informatie heeft om het pakket door te sturen met CEF en een meer resource-intensieve processwitching moet gebruiken om de volgende hop op te lossen met NHRP (Next Hop Resolution Protocol).

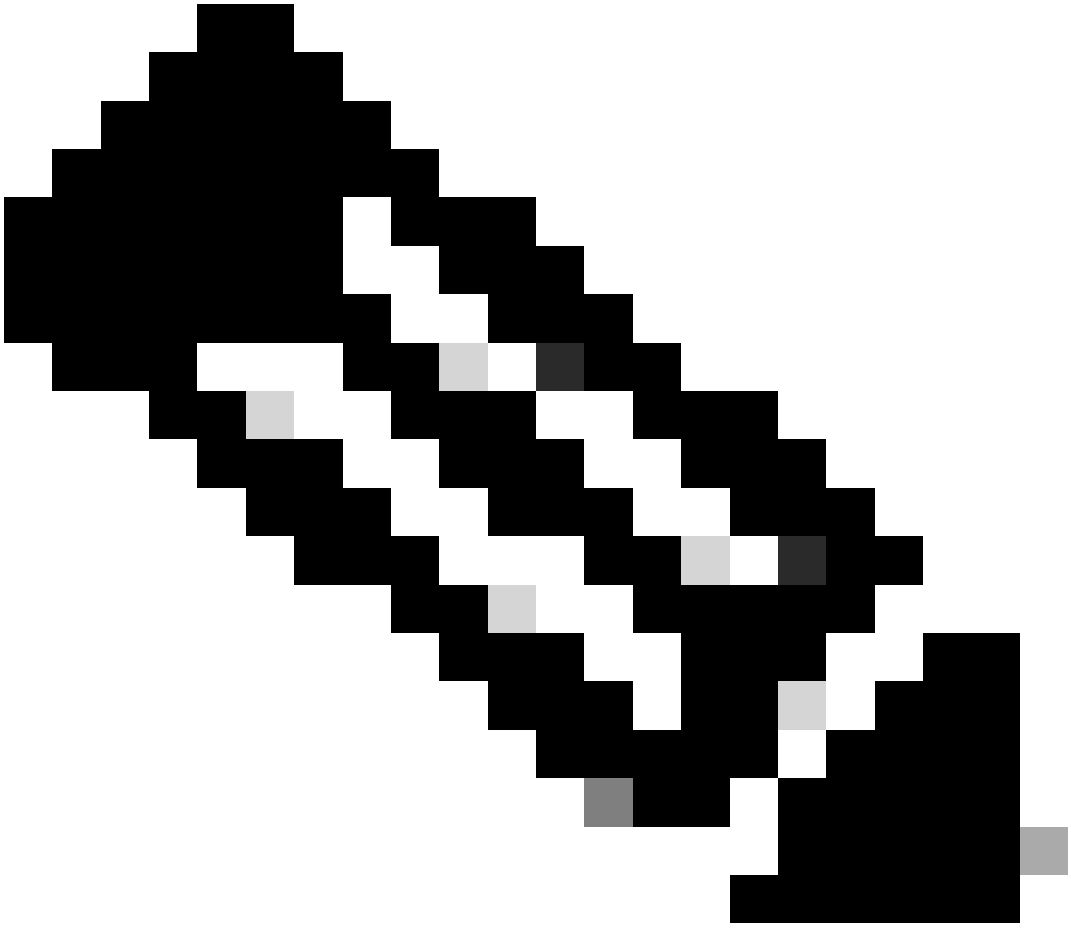
DMVPN fase 3: Deze fase verbetert zich ten opzichte van fase 2 door toe te staan dat het eerste spaak-to-spaak pakket van het begin af aan via CEF wordt geschakeld. Dit wordt bereikt door het gebruik van NHRP Redirect en NHRP Shortcut features, die snel helpen om direct spraaktelefonische tunnels te creëren. Hierdoor wordt CEF consistenter gebruikt, waardoor minder gebruik wordt gemaakt van processwitching.

Netwerkdiagram



Configuraties

Crypto-configuraties



Opmerking: Dit is hetzelfde op de hub en alle spaken.

1. Configureer een Ikev2 voorstel en keyring.

```
crypto ikev2 voorstel DMVPN
encryptie aes-cbc-256
integriteit sha256
groep 14
crypto ikev2 keyring IKEV2-KEYRING
peer-any
adres 0.0.0.0 0.0.0.0
vooraf gedeelde Cisco123-software
!
```

2. Configureer het Ikev2-profiel dat alle informatie over de verbinding bevat.

```
crypto ikev2 profiel IKEV2-PROF
```

match-adres lokale interface Gigabit Ethernet0/0/0
match identiteits-adres 0.0.0.0
lokale pre-share verificatie
verificatie vooraf delen op afstand
keyring local IKEV2-KEYRING

Hier vindt u de details van de opdrachten die in het ikev2-profiel worden gebruikt:

- match-adres lokale interface Gigabit Ethernet0/0/0: Lokale buiteninterface waar VPN wordt afgesloten, in dit geval Gigabit Ethernet0/0/0
- match identiteits-afstandsadres 0.0.0.0: Aangezien externe peer meerdere kan zijn, gebruik makend van 0.0.0.0 wat elke peer aangeeft
- authenticatie lokaal pre-share: De verificatiemodus op de lokale site wordt vooraf gedeeld
- verificatie vooraf delen op afstand: De verificatiemodus op de lokale site wordt vooraf gedeeld
- keyring local IKEV2-KEYRING: Gebruik dezelfde sleutelring die u eerder hebt gemaakt.

3. IPsec-profiel configureren.

crypto ipsec transformatie-set T-SET ESP-ase 256 esp-sha256-hmac
modustunnel

crypto ipsec-profiel IPSEC-IKEV2

set transformatie-set T-SET instellen
set ikev2-profile IKEV2-PROF

Maak een transformatieset voor de IPsec-tunnelonderhandeling en roep de transformatieset en het Ikev2-profiel aan onder het IPsec-profiel.

DMVPN-configuratie

1. Configureer de buiteninterface.

interface Gigabit Ethernet0/0/0

IP-adres 172.16.1.1 255.255.255.0
onderhandelingsauto
CDP inschakelen

2. De hubrouter voor mGRE- en IPsec-integratie configureren (d.w.z. de tunnel koppelen aan het IPsec-profiel dat in de vorige procedure is geconfigureerd)

interface-tunnel0
IP-adres 10.10.1 255.255.255.0
no ip redirects
IP NHRP-verificatie via DMVPN
ip Nhrp kaart multicast dynamisch

IP NHRP-netwerkid 1
IP NHRP omleiden <-------- Verplicht om DMVPN fase 3 op hubrouter in te schakelen
tunnelbron Gigabit Ethernet0/0/0
tunnelmodus gre multipoint
IPSEC-profiel voor tunnelbescherming IPSEC-IKEV2
!

Deze opdrachten worden gebruikt in tunnelinterfaceconfiguraties:

- IP NHRP-verificatie via DMVPN: In dit geval moet de 'DMVPN' verificatie string dezelfde waarde hebben op alle hubs en spokes die deel uitmaken van hetzelfde DMVPN netwerk.
- IP Nhrp kaart multicast dynamisch: Hiermee kan NHRP spaken dynamisch toevoegen aan NHRP multicast mapping.
- IP NHRP-netwerkid 1: 32-bits netwerkidentificatiecode die NHRP op een interface mogelijk maakt.
- IP nhrp omleiden: Maakt verkeersindicatie omleiden mogelijk als verkeer wordt doorgestuurd met het NHRP-netwerk.
- tunnelbron Gigabit Ethernet0/0/0: Hiermee stelt u het bronadres in voor een tunnelinterface. Hier gebruikt u het Gigabit Ethernet 0/0/0 IP-adres.
- tunnelmodus gre multipoint: Stelt de inkapselingsmodus in op mGRE voor deze tunnelinterface.
- tunnelbeveiliging ipsec-profiel IPSEC-IKEV2: Associeert een tunnelinterface met IPsec Profile dat reeds in crypto configuraties is gemaakt.

3. Configureer spraakrouters voor mGRE- en IPsec-integratie samen met een externe interface en terugkoppeling om BGP-connectiviteit (BGP) te testen.

GESPROKEN X: (Soortgelijke configuratie kan in alle spaken worden gebruikt)

interface Gigabit Ethernet0/0/0
IP-adres 172.16.3.3 255.255.255.0
snelheid 1000
geen onderhandelingsauto

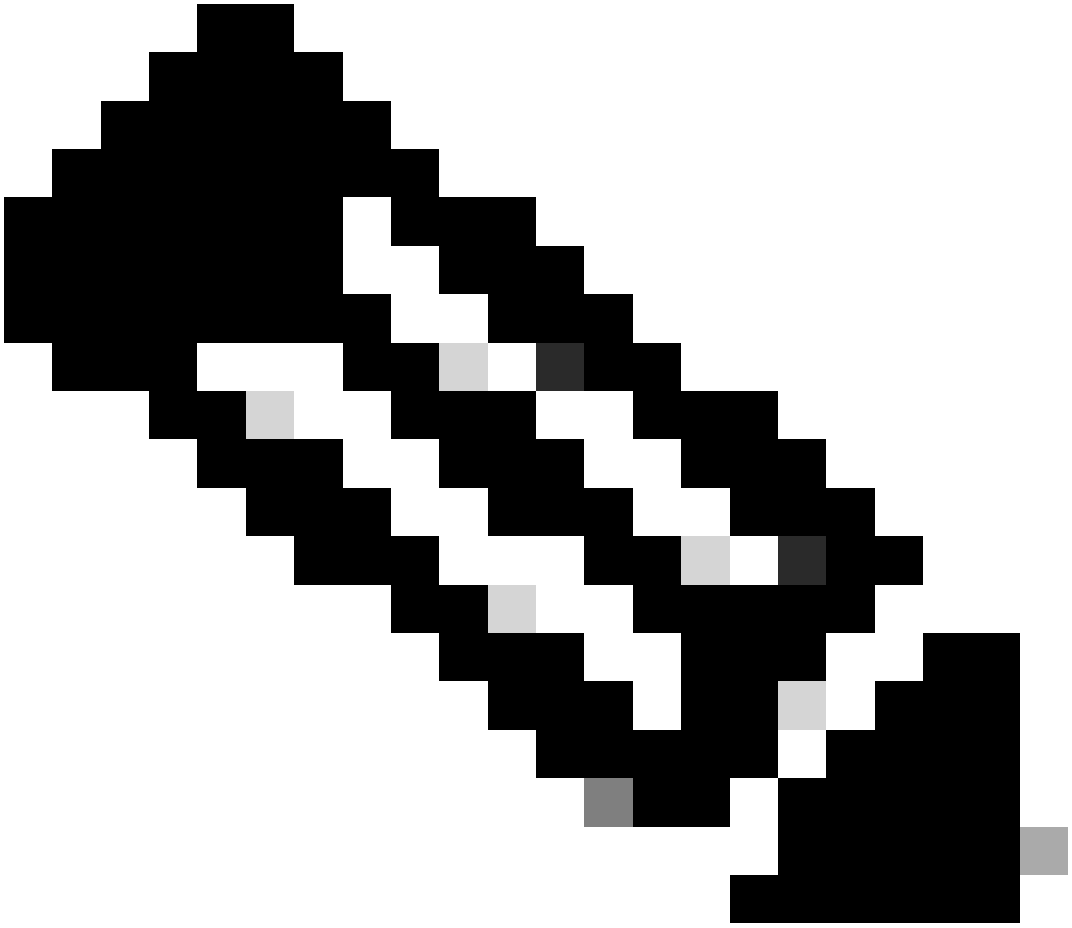
!

interface-Loopback10
IP-adres 192.168.33.3 255.255.255.0
!
interface-tunnel0
IP-adres 10.10.10.3 255.255.255.0
no ip redirects
IP NHRP-verificatie via DMVPN
ip nhrp-kaart 10.10.10.1 172.16.1.1
ip Nhrp map multicast 172.16.1.1
IP NHRP-netwerkid 1
ip NHRP 10.10.10.1
IP NHRP-sneltoets <-------- Verplicht om DMVPN fase 3 op spraakrouter in te schakelen

tunnelbron Gigabit Ethernet0/0/0
tunnelmodus gre multipoint
IPSEC-profiel voor tunnelbescherming IPSEC-IKEV2

Deze opdrachten worden gebruikt in tunnelinterfaceconfiguraties:

- IP NHRP-verificatie via DMVPN: In dit geval moet de 'DMVPN' verificatie string dezelfde waarde hebben op alle hubs en spokes die deel uitmaken van hetzelfde DMVPN netwerk.
- ip nhrp-kaart 10.10.10.1 172.16.1.1: Kaarten handmatig Hub NBMA IP-adres met tunnelinterface IP-adres.
- ip Nhrp map multicast 172.16.1.1: Richt al multicast verkeer naar de hub om.
- IP NHRP-netwerkid 1: 32-bits netwerkidentificatiecode die NHRP op een interface mogelijk maakt.
- ip nhrp nhs 10.10.10.1: De volgende hopserver die onze hub is, is met deze opdracht geconfigureerd.
- ip nhrp-sneltoets: Schakelt NHRP-sneltoets in op een interface.
- tunnelbron Gigabit Ethernet0/0/0: Hiermee stelt u het bronadres in voor een tunnelinterface. Hier gebruikt u het Gigabit Ethernet 0/0/0 IP-adres.
- tunnelmodus gre multipoint: Stelt de inkapselingsmodus in op mGRE voor deze tunnelinterface.
- tunnelbeveiliging ipsec-profiel IPSEC-IKEV2: Associeert een tunnelinterface met IPsec Profile dat reeds in crypto configuraties is gemaakt.



Opmerking: De opdracht ip nhrp redirect stuurt het bericht naar de Spokes dat zegt "Er is een betere route naar de bestemming Spoke dan via de Hub" en ip nhrp sneltoets legt installatie van deze route in de Forwarding Information Base (FIB) op de Spokes.

BGP-configuratie

Er zijn verschillende variaties waaruit u kunt kiezen:

- eBGP met een ander AS-nummer op elke spaak
- eBGP met hetzelfde AS-nummer op elke spaak
- iBGP

Het verklaren van alle drie scenario's valt buiten het bereik van dit document.

Er wordt een eBGP met een ander AS-nummer op alle spaken geconfigureerd, zodat dynamische buren niet kunnen worden gebruikt. Daarom moet u de buren handmatig configureren.

eBGP met verschillende AS op de spaken

1. BGP-configuratie op HUB:

Hub(config)#router bgp 65010

Hub (config-router)#bgp log-buurwijzigingen

Hub (configuratie-router)#network 192.168.11.1 masker 255.255.255.255

Hub (configuratie-router)#neighbor 10.10.10.2 op afstand 65011

Hub (configuratie-router)#neighbor 10.10.10.3 afstandsbediening als 65012

!

Deze opdrachten worden gebruikt in de BGP-configuratie op de hub:

- router bgp 65010: Configureert een BGP-routerproces. Gebruik het argument 'autonoom-systeem-nummer' dat het apparaat identificeert voor andere BGP-luidsprekers.
- netwerk 192.168.11.1 masker 255.255.255.255: Specificeert een netwerk als lokaal aan dit autonome systeem en voegt het toe aan de BGP-routeringstabel.
- buur 10.10.10.2 op afstand-als 65011: Voegt het IP-adres van de buurtaal Spoke 1 in het opgegeven autonome systeem toe aan de IPv4 multiprotocol BGP-buurtabel van het lokale apparaat.
- buurman 10.10.10.3 op afstand-als 65012: Voegt het IP-adres van de buurman Spoke 2 in het opgegeven autonome systeem toe aan de IPv4 multiprotocol BGP-buurtabel van het lokale apparaat.

2. BGP-configuratie op Spoke X:

Spoke2(config)#router bgp 65012

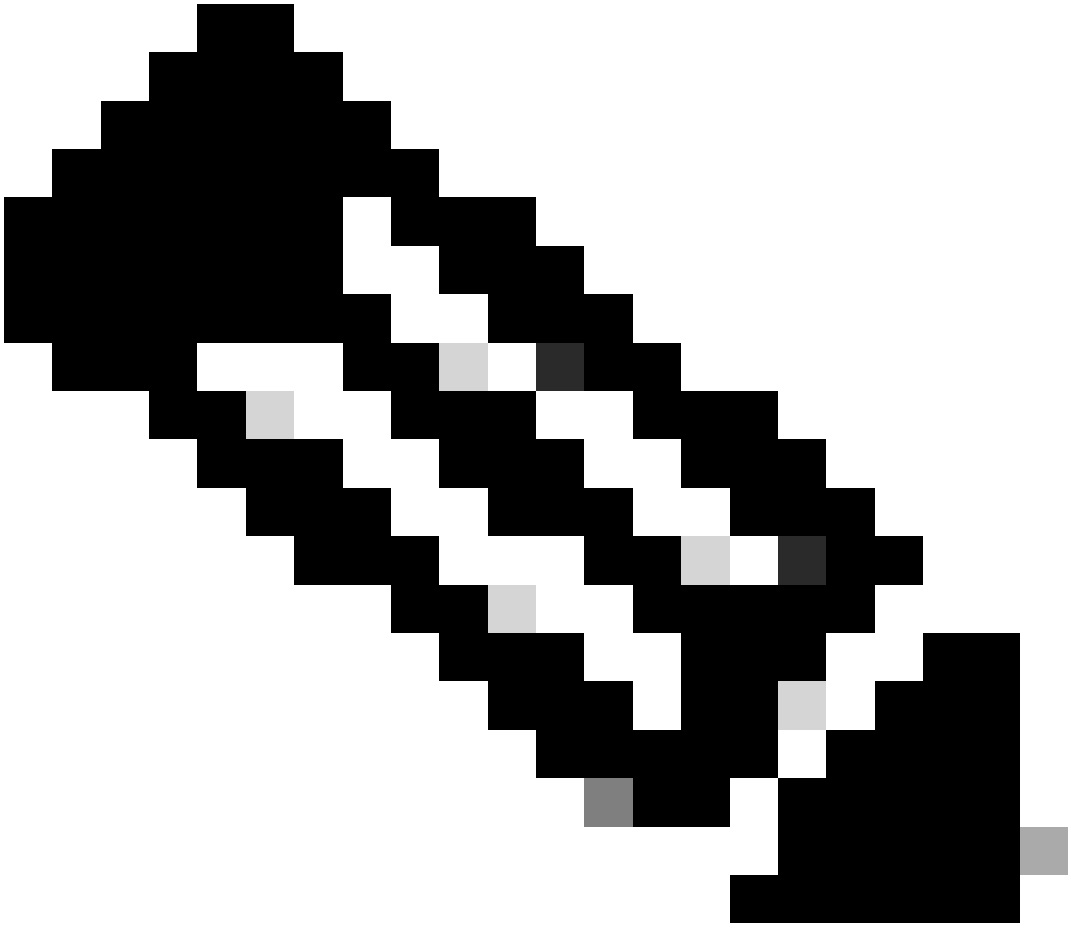
Spoke2 (config-router) #bgp log-buurwijzigingen

Spoke2 (configuratie-router)#-netwerk 192.168.33.3 masker 255.255.255.255

Spoke2 (config-router)#-buur 10.10.10.1 op afstand 65010

Deze opdrachten worden gebruikt in BGP-configuratie op Spoke X:

- router bgp 65012: Configureert een BGP-routerproces. Gebruik het argument 'autonoom-systeem-nummer' dat het apparaat identificeert voor andere BGP-luidsprekers.
- netwerk 192.168.33.3 masker 255.255.255.255: Specificeert een netwerk als lokaal aan dit autonome systeem en voegt het toe aan de BGP-routeringstabel.
- buur 10.10.10.1 op afstand-als 65010: Voegt het IP-adres van de hub in het gespecificeerde autonome systeem toe aan de IPv4 multiprotocol BGP-buurtabel van het lokale apparaat.



Opmerking: Een gelijkaardige configuratie moet op alle spaken in het netwerk van DMVPN worden gedaan.

Verifiëren

1. Verificatieopdrachten op hubapparaat:

HUB#sh dmpn

Hiermee wordt DMVPN-specifieke sessieinformatie weergegeven.

Verklaring: Eigenschappen —> S - Statisch, D - Dynamisch, I - Incompleet
N - NATed, L - Lokaal, X - Geen socket
T1 - Geïnstalleerde route, T2 - Nexthop-override
C - Geschikt voor CTS
Ent —> Aantal NHRP-vermeldingen met dezelfde NBMA-peer
NHS status: E —> Antwoorden verwachten, R —> Antwoord, W —> Wachten

Up Time —> Up of Down Time voor een tunnel
===

Interface: Tunnel 0, IPv4 NHRP-gegevens
Type:Hub, NHRP-peers:2, <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<: het apparaat fungeert als hub en er zijn 2 NHRP-peers aangesloten op deze HUB.

Ent Peer NBMA Addr peer-tunneladd status upDN ATM-kenmerk
----- --------------- -------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<: beide peers hebben zich dynamisch bij de hub geregistreerd en bevinden zich in de UP-staat.
1.172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip Nhrp

Toont de NBMA adrestoewijzing aan tunnelinterface IP van alle NHRP-peers die met Hub zijn verbonden. Hub beheert de database van alle spokes.

10.10.10.2/32 via 10.10.10.2
Tunnel0 gemaakt op 01:47:22, verlopen 01:32:27
Type: dynamische vlaggen: unieke geregistreerde gebruikte hop
NBMA-adres: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 gemaakt op 01:09:11, verlopen 01:29:58
Type: dynamische vlaggen: unieke geregistreerde gebruikte hop
NBMA-adres: 172.16.3.3

HUB#sh ip NHRP multicast

Hier wordt informatie over NHRP multicast-mapping weergegeven.

I/F NBMA-adres
Tunnel0 172.16.2.2 Vlaggen: dynamisch (ingeschakeld)
Tunnel0 172.16.3.3 Vlaggen: dynamisch (ingeschakeld)

HUB#sh crypto sockets

Aantal Crypto Socket verbindingen 2

Tu0-peers (lokaal/extern): 172.16.1.1/172.16.2.2
Lokaal incident (adres/masker/poort/poort): (172.16.1.1/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.2.2/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open (Openstaand)
Klant: "TUNNEL SEC" (clientstatus: Actief)
Tu0-peers (lokaal/extern): 172.16.1.1/172.16.3.3

Lokaal incident (adres/masker/poort/poort): (172.16.1.1/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.3.3/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open (Openstaand)
Klant: "TUNNEL SEC" (clientstatus: Actief)
Crypto Sockets in Listen staat:
Klant: Profiel "TUNNEL SEC": "IPSEC-IKEV2" Kaart-naam: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4-encryptie van IKEv2 SA

Tunnel-id lokale externe FVRF/ivrf-status
1 172.16.1.1/500 172.16.2.2/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/6524 sec

Tunnel-id lokale externe FVRF/ivrf-status
2 172.16.1.1/500 172.16.3.3/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:5,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/4234 sec

IPv6-encryptie van IKEv2 SA

HUB#sh ip bgp samenvatting

Toont de huidige staat van de BGP-sessie/het aantal prefixes dat de router heeft ontvangen van een buur of peer groep.

BGP-router-id 192.168.11.1 lokaal AS-nummer 65010
De BGP-tabelversie is 4, de hoofdversie van de routeringstabel is 4.
3 netwerkvermeldingen met 432 bytes geheugen
3 padvermeldingen met 252 bytes aan geheugen
3/3 BGP-vermeldingen van pad/bestpath met 480 bytes aan geheugen
2 BGP AS-PATH-vermeldingen met 48 bytes aan geheugen
0 BGP route-map cache-ingangen met 0 bytes geheugen
0 BGP-cacheingangen via filterlijst met 0 bytes geheugen
BGP met totaal 1212 bytes aan geheugen
BGP-activiteit 3/0 prefixes, 3/0 paden, scaninterval 60 seconden

MSSGrcvd MSSG Verzonden TBLv InQ OutQ Up/Down State/PFXRCD
10.10.10.2 4 65011 33 33 4 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 00:14:58 1

Hub#sh IP-route bgp

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP

D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2
E1 - OSPF extern type 1, E2 - OSPF extern type 2
i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2
ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker
o - ODR, P - Peridic Download statische route, H - NHRP, l - LISP
a-toepassingsroute
+ - gerepliceerde route, % - volgende hop opheffing, p - met voeten treedt van PfR

Gateway of last resort is 172.16.1.2 naar netwerk 0.0.0.0

192.168.0.0/16 is variabel subnetted, 4 subnetten, 2 maskers
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<<<Entry for Spoke 1 geadverteerde routes
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<Entry for Spoke 2 geadverteerde routes

2. Verificatieopdrachten op Spoke 1:

Spoke1#sh dmvpn

Verklaring: Eigenschappen —> S - Statisch, D - Dynamisch, I - Incompleet
N - NATed, L - Lokaal, X - Geen socket
T1 - Geïnstalleerde route, T2 - Nexthop-override
C - CTS Capable, I2 - Tijdelijk
Ent —> Aantal NHRP-vermeldingen met dezelfde NBMA-peer
NHS status: E —> Antwoorden verwachten, R —> Antwoord, W —> Wachten
Up Time —> Up of Down Time voor een tunnel
==========

Interface: Tunnel 0, IPv4 NHRP-gegevens
Type:gesproken, NHRP-peers:2,

Ent Peer NBMA Addr peer-tunneladd status upDN ATM-kenmerk
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<<<<<<<hub toont als S-statisch omdat we het als een statische ingang onder de tunnelinterface hebben geconfigureerd
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<<<<<<<<<<<<: Dynamische spraaktunnel naar spraaklijn die is gemaakt na het verzenden van verkeer naar Spoke 2

Spoke1#sh ip bgp samenvatting

BGP-router-id 192.168.22.2, lokaal AS-nummer 65011
De BGP-tabelversie is 4, de hoofdversie van de routeringstabel is 4.
3 netwerkvermeldingen met 744 bytes geheugen
3 padvermeldingen met 432 bytes aan geheugen
3/3 BGP-vermeldingen van pad/bestpath met 864 bytes aan geheugen

2 BGP AS-PATH-vermeldingen met 64 bytes aan geheugen
0 BGP route-map cache-ingangen met 0 bytes geheugen
0 BGP-cacheingangen via filterlijst met 0 bytes geheugen
BGP met 2104 totale bytes aan geheugen
BGP-activiteit 3/0 prefixes, 3/0 paden, scaninterval 60 seconden
3 netwerken piekten op 08:16:54 Jun 2 2022 UTC (01:11:51.732 geleden)

MSSGrcvd MSSG Verzonden TBLv InQ OutQ Up/Down State/PFXRCD
10.10.10.1 4 65010 85 85 4 0 01:12:21 2
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Wij hebben 2 voorvoegingen van Hub ontvangen, elk voor hub loopback en Spoke2 loopback2

Spoke1#sh ip route bgp

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2
E1 - OSPF extern type 1, E2 - OSPF extern type 2, m - OMP
n - NAT, Ni - NAT binnen, No - NAT buiten, NAT - NAT DIA
i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2
ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker
H - NHRP, G - NHRP geregistreerd, g - NHRP registratieoverzicht
o - ODR, P - Peridic Download statische route, l - LISP
a-toepassingsroute
+ - gerepliceerde route, % - volgende hop opheffing, p - met voeten treedt van PfR

De gateway van laatste redmiddel is 172.16.2.10 naar netwerk 0.0.0.0

B192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 >>>>>>>>>>>>>>>> Hub-netwerk rechtstreeks bereikbaar via hub

B192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>> Gesproken netwerk direct bereikbaar via spraaktunnel IP.

Spoke1#sh ip route

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2
E1 - OSPF extern type 1, E2 - OSPF extern type 2, m - OMP
n - NAT, Ni - NAT binnen, No - NAT buiten, NAT - NAT DIA
i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2
ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker
H - NHRP, G - NHRP geregistreerd, g - NHRP registratieoverzicht
o - ODR, P - Peridic Download statische route, l - LISP
a-toepassingsroute
+ - gerepliceerde route, % - volgende hop opheffing, p - met voeten treedt van PfR

De gateway van laatste redmiddel is 172.16.2.10 naar netwerk 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 is variabel subnetted, 2 subnetten, 2 maskers
C172.16.2.0/24 is rechtstreeks aangesloten, Gigabit Ethernet2
L 172.16.2.2/32 is rechtstreeks verbonden, Gigabit Ethernet2
10.0.0.0/8 is variabele subnetted, 2 subnetten, 2 maskers
C10.10.10.0/24 is direct verbonden via Tunnel0
L 10.10.10.2/32 is rechtstreeks verbonden via Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 is variabel subnetted, 2 subnetten, 2 maskers
C 192.168.22.0/24 is rechtstreeks aangesloten, Loopback10
L 192.168.22.2/32 is direct verbonden, Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip Nhrp nhs

Verklaring: E=Verwacht antwoorden, R=Reageren, W=Wachten, D=Dynamisch
Tunnel0:
10.10.10.1 RE-prioriteit = 0-cluster = 0 >>>>>>> Er is slechts één Next hop-server geconfigureerd

Spoke1#sh ip Nhrp verkeer

Tunnel0: Max. verzendlimiet:10000Pakketten/10 seconden, gebruik:0%
Verzonden: Totaal 52
1 Resolutie Verzoek 0 Resolutie Antwoord 51 Registratieaanvraag <<<<<<<<<<< Aantal keren dat registratieaanvragen naar Hub zijn verzonden
0 Registratie Antwoord 0 Ophalen Aanvraag 0 Ophalen Antwoord
0 foutmelding 0 verkeersindicatie 0 onderdrukking omleiden
RCPD: Totaal 25
0 Resolutie Verzoek 1 Resolutie Antwoord 0 Registratieverzoek <<<<<<<<<<<<<<<< Aantal keren dat we antwoorden op die registratieverzoeken hebben ontvangen
24 Registratieantwoord 0 aanvraag voor opschonen 0 antwoord op opschonen
0 foutmelding 0 verkeersindicatie 0 onderdrukking omleiden

Spoke1#sh ip NHRP multicast

I/F NBMA-adres
Tunnel0 172.16.1.1 Vlaggen: statisch (Ingeschakeld) <<<<<<<<<<<<<< Multicast verkeer is ingesteld om naar hub NBMA te worden doorgestuurd

Spoke1#sh crypto sockets

Aantal Crypto Socket verbindingen 2

Tu0-peers (lokaal/extern): 172.16.2.2/172.16.1.1
Lokaal incident (adres/masker/poort/poort): (172.16.2.2/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.1.1/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open <<<<<<<<<<<<<<<<<<<< Status of Socket voor deze specifieke peer
Klant: "TUNNEL SEC" (clientstatus: Actief)
Tu0-peers (lokaal/extern): 172.16.2.2/172.16.3.3
Lokaal incident (adres/masker/poort/poort): (172.16.2.2/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.3.3/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open (Openstaand)
Klant: "TUNNEL SEC" (clientstatus: Actief)
Crypto Sockets in Listen staat:
Klant: Profiel "TUNNEL SEC": "IPSEC-IKEV2" Kaart-naam: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4-encryptie van IKEv2 SA

Tunnel-id lokale externe FVRF/ivrf-status
2 172.16.2.2/500 172.16.3.3/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/287 sec

Tunnel-id lokale externe FVRF/ivrf-status
1 172.16.2.2/500 172.16.1.1/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/4643 sec

IPv6-encryptie van IKEv2 SA

Spoke1#traceroute 192.168.33.3 bron lo10

Typ vluchtvolgorde om af te breken.
De route overtrekken naar 192.168.33.3
VRF-informatie: (vrf in naam/id, vrf out name/id)
1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<<<<<<<<<<<<<<<: verkeer gaat rechtstreeks naar Spoke 2 router zonder door de hub te gaan.

Spoke2#sh dmvpn

Verklaring: Eigenschappen —> S - Statisch, D - Dynamisch, I - Incompleet
N - NATed, L - Lokaal, X - Geen socket
T1 - Geïnstalleerde route, T2 - Nexthop-override
C - CTS Capable, I2 - Tijdelijk

Ent —> Aantal NHRP-vermeldingen met dezelfde NBMA-peer
NHS status: E —> Antwoorden verwachten, R —> Antwoord, W —> Wachten
Up Time —> Up of Down Time voor een tunnel
==========

Interface: Tunnel 0, IPv4 NHRP-gegevens
Type:gesproken, NHRP-peers:2,

Ent Peer NBMA Addr peer-tunneladd status upDN ATM-kenmerk
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 T/M 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. Verificatieopdrachten op Spoke 2:

Spoke2#sh ip Nhrp

10.10.10.1/32 via 10.10.10.1
Tunnel0 gemaakt 01:36:06, nooit verlopen
Type: statisch, vlaggen:
NBMA-adres: 172.16.1.1
10.10.10.2/32 via 10.10.10.2
Tunnel0 gemaakt op 00:08:09, verlopen 00:01:50
Type: dynamische vlaggen: impliciet router
NBMA-adres: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 gemaakt op 00:08:09, verlopen 00:01:50
Type: dynamische vlaggen: router unieke lokale
NBMA-adres: 172.16.3.3
(zonder socket)
Spoke2#sh ip Nhrp mul
Spoke2#sh ip NHRP multicast
I/F NBMA-adres
Tunnel0 172.16.1.1 Vlaggen: statisch (ingeschakeld)
Spoke2#

Spoke2#sh crypto sockets

Aantal Crypto Socket verbindingen 2

Tu0-peers (lokaal/extern): 172.16.3.3/172.16.1.1
Lokaal incident (adres/masker/poort/poort): (172.16.3.3/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.1.1/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Status of Socket voor deze specifieke peer.
Klant: "TUNNEL SEC" (clientstatus: Actief)

Tu0-peers (lokaal/extern): 172.16.3.3/172.16.2.2
Lokaal incident (adres/masker/poort/poort): (172.16.3.3/255.255.255.255/0/47)
Afstandsinspuiting (adres/masker/poort/poort): (172.16.2.2/255.255.255.255/0/47)
IPsec-profiel: "IPSEC-IKEV2"
Toestand socket: Open (Openstaand)
Klant: "TUNNEL SEC" (clientstatus: Actief)
Crypto Sockets in Listen staat:
Klant: Profiel "TUNNEL SEC": "IPSEC-IKEV2" Kaart-naam: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4-encryptie van IKEv2 SA

Tunnel-id lokale externe FVRF/ivrf-status
2 172.16.3.3/500 172.16.2.2/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/509 sec

Tunnel-id lokale externe FVRF/ivrf-status
1 172.16.3.3/500 172.16.1.1/500 (geen/geen KLAAR)
Vermelding: AES-CBC, sleutelgrootte: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
autorisatieteken: PSK, controleer: PSK
Leven/actieve tijd: 86400/4866 sec

IPv6-encryptie van IKEv2 SA

Spoke2#sh ip bgp samenvatting

BGP-router-id 192.168.3.3, lokaal AS-nummer 65012
De BGP-tabelversie is 4, de hoofdversie van de routeringstabel is 4.
3 netwerkvermeldingen met 744 bytes geheugen
3 padvermeldingen met 432 bytes aan geheugen
3/3 BGP-vermeldingen van pad/bestpath met 864 bytes aan geheugen
2 BGP AS-PATH-vermeldingen met 64 bytes aan geheugen
0 BGP route-map cache-ingangen met 0 bytes geheugen
0 BGP-cacheingangen via filterlijst met 0 bytes geheugen
BGP met 2104 totale bytes aan geheugen
BGP-activiteit 3/0 prefixes, 3/0 paden, scaninterval 60 seconden
3 netwerken piekten op 08:16:54 Jun 2 2022 UTC (01:20:43.775 geleden)

MSSGrcvd MSSG Verzonden TBLv InQ OutQ Up/Down State/PFXRCD
10.10.10.1 465010 97 94 4 0 01:21:07 2 **>>>>>>>>>>>>>>>>>>>>>**. We hebben 2 prefixes van Hub ontvangen, elk voor hub loopback en Spoke2 loopback

Spoke2#sh ip route

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP

D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2
E1 - OSPF extern type 1, E2 - OSPF extern type 2, m - OMP
n - NAT, Ni - NAT binnen, No - NAT buiten, NAT - NAT DIA
i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2
ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker
H - NHRP, G - NHRP geregistreerd, g - NHRP registratieoverzicht
o - ODR, P - Peridic Download statische route, l - LISP
a-toepassingsroute
+ - gerepliceerde route, % - volgende hop opheffing, p - met voeten treedt van PfR

De gateway van laatste redmiddel is 172.16.3.10 naar netwerk 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 is variabel subnetted, 2 subnetten, 2 maskers
C172.16.3.0/24 is rechtstreeks aangesloten, Gigabit Ethernet3
L 172.16.3.3/32 is rechtstreeks aangesloten, Gigabit Ethernet3
10.0.0.0/8 is variabele subnetted, 2 subnetten, 2 maskers
C10.10.10.0/24 is direct verbonden via Tunnel0
L 10.10.10.3/32 is rechtstreeks verbonden via Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 is variabel subnetted, 2 subnetten, 2 maskers
C 192.168.33.0/24 is rechtstreeks aangesloten, Loopback10
L 192.168.33.3/32 is direct verbonden, Loopback10

Spoke2#sh ip route bgp

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP
D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2
E1 - OSPF extern type 1, E2 - OSPF extern type 2, m - OMP
n - NAT, Ni - NAT binnen, No - NAT buiten, NAT - NAT DIA
i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2
ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker
H - NHRP, G - NHRP geregistreerd, g - NHRP registratieoverzicht
o - ODR, P - Peridic Download statische route, l - LISP
a-toepassingsroute
+ - gerepliceerde route, % - volgende hop opheffing, p - met voeten treedt van PfR

De gateway van laatste redmiddel is 172.16.3.10 naar netwerk 0.0.0.0

B192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>Hubnetwerk rechtstreeks bereikbaar via hub
B192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>> Gesproken netwerk direct bereikbaar via spraaktunnel IP.

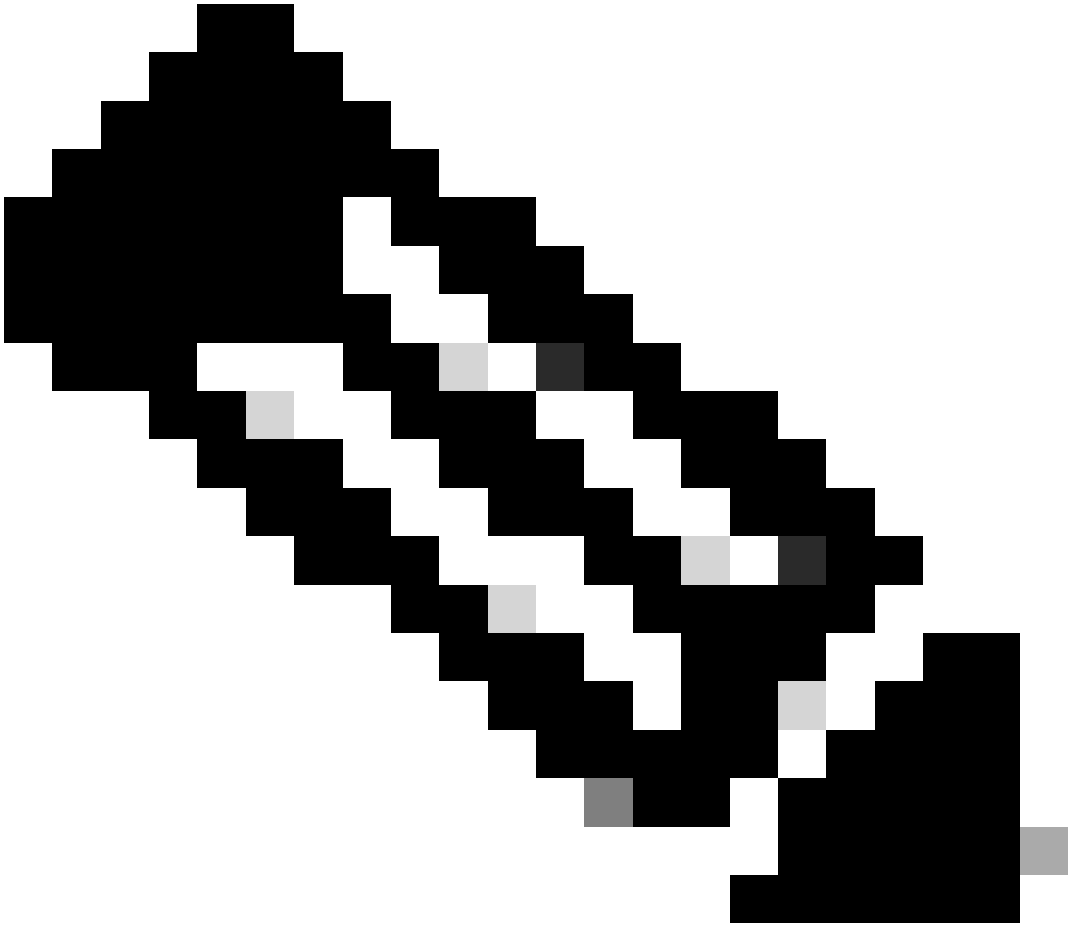
Spoke2#sh ip Nhrp nhs

Verklaring: E=Verwacht antwoorden, R=Reageren, W=Wachten, D=Dynamisch
Tunnel0:
10.10.10.1 RE-prioriteit = 0-cluster = 0 **>>>>>>>>>>** Er is slechts één Next hop-server geconfigureerd

Spoke2#traceroute 192.168.22.2 bron loopback 10

Typ vluchtvolgorde om af te breken.
De route naar 192.168.22.2 overtrekken
VRF-informatie: (vrf in naam/id, vrf out name/id)
1 10.10.10.2 4 msec 4 msec * **<<<<<<<<<<<<<<<<<<<<<<<<<<**: verkeer gaat rechtstreeks naar Spoke 1 router zonder via Hub door te gaan.

Problemen oplossen



Opmerking: Er wordt altijd gesuggereerd om voorwaardelijke debugs te gebruiken, omdat het uitvoeren van niet-voorwaardelijke debugs invloed kan hebben op de processor en dus op de productieomgeving. NBMA-adres komt overeen met het 'buitenste IP-adres' (IP-adres dat wordt gebruikt om de tunnelinterface te bronnen) en Tunnel IP komt overeen met het 'logische IP-adres, dat wil zeggen het IP-adres van de tunnelinterface'.

debug dmvpn voorwaarde peer <nmbma/tunnel> <NMBA IP- of Tunnel IP-adres van peer>
debug crypto voorwaarde peer-ipv4 <WAN IP of the peer>
debug van NHRM voorwaarde peer <nbma/tunnel> <NBMA of Tunnel IP-adres van peer>

Om problemen met DMVPN op te lossen, moet u een gelaagde aanpak kiezen:

debug dmvpn detail all

1. Encryptielaag: Na het bevestigen van de fysieke connectiviteit tussen twee peers, moet de encryptie worden geverifieerd. Deze Layer versleutelt GRE-pakketten.

Common Debug commando's die gebruikt worden om het encryptie onderdeel te verifiëren:

debug crypto voorwaarde peer-ipv4 <WAN IP-adres van peer>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 pakket

debug crypto ipsec

debug crypto ipsec fout

OF

debug dmvpn voorwaarde peer <nmbma/tunnel> <NMBA IP- of Tunnel IP-adres van peer>

debug crypto voorwaarde peer-ipv4 <WAN IP of the peer>

debug dmvpn detailcrypto

Raadpleeg de externe link voor een diepgaand begrip van probleemoplossing bij encryptielaag:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html.

2. GRE/NHRP: Enkele veelvoorkomende problemen zijn NHRP registratie mislukken en dynamische NBMA adreswijzigingen in spraakcommunicatie leiden tot inconsistente NHRP-mapping in de hub.

Gemeenschappelijke Debug-opdrachten gebruikt om NHRP-toewijzing te verifiëren:

debug van NHRM voorwaarde peer <nbma/tunnel> <NBMA of Tunnel IP-adres van peer>

debug nhrp cache

debug nhrp-pakket

debug nhrp-detail

debug nhrp-fout

Raadpleeg de externe link voor meer informatie over de meest gebruikelijke DMVPN-oplossingen voor probleemoplossing:

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html.

3. Routing: Het Routing Protocol controleert niet de status van on-demand spraaktunnels.

IP-routing, updates en IP-multicast gegevenspakketten passeren alleen de hub-and-spoke tunnels.

Unicast IP datapakketten passeren zowel de hub-and-spoke als on-demand spoke-spoke tunnels.

Debuggen: Diverse debug opdrachten afhankelijk van het routingprotocol.

Raadpleeg voor de BGP-routing deep dive de externe link:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.