Veelvoorkomende DMVPN-problemen oplossen

Inhoud

Inleiding

Dit document beschrijft de meest gebruikelijke oplossingen voor Dynamic Multipoint VPN (DMVPN) problemen.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de DMVPN-configuratie op Cisco IOS®routers.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS

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.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Dit document beschrijft de meest gebruikelijke oplossingen voor Dynamic Multipoint VPN (DMVPN) problemen. Veel van deze oplossingen kunnen voorafgaand aan elke diepgaande probleemoplossing van de DMVPN-verbinding worden geïmplementeerd. Dit document wordt gepresenteerd als een controlelijst van gebruikelijke procedures die u moet proberen voordat u een verbinding kunt oplossen en technische ondersteuning van Cisco kunt bellen.

Raadpleeg voor meer informatie de Dynamic Multipoint VPN Configuration Guide, Cisco IOS release 15M&T.

Raadpleeg Debug commando's begrijpen en gebruiken om IPsec problemen op te lossen om een uitleg te geven van de gebruikelijke debug commando's die worden gebruikt om IPsec-problemen op te lossen.

De DMVPN-configuratie werkt niet

Probleem

Een recent geconfigureerde of aangepaste DMVPN-oplossing werkt niet.

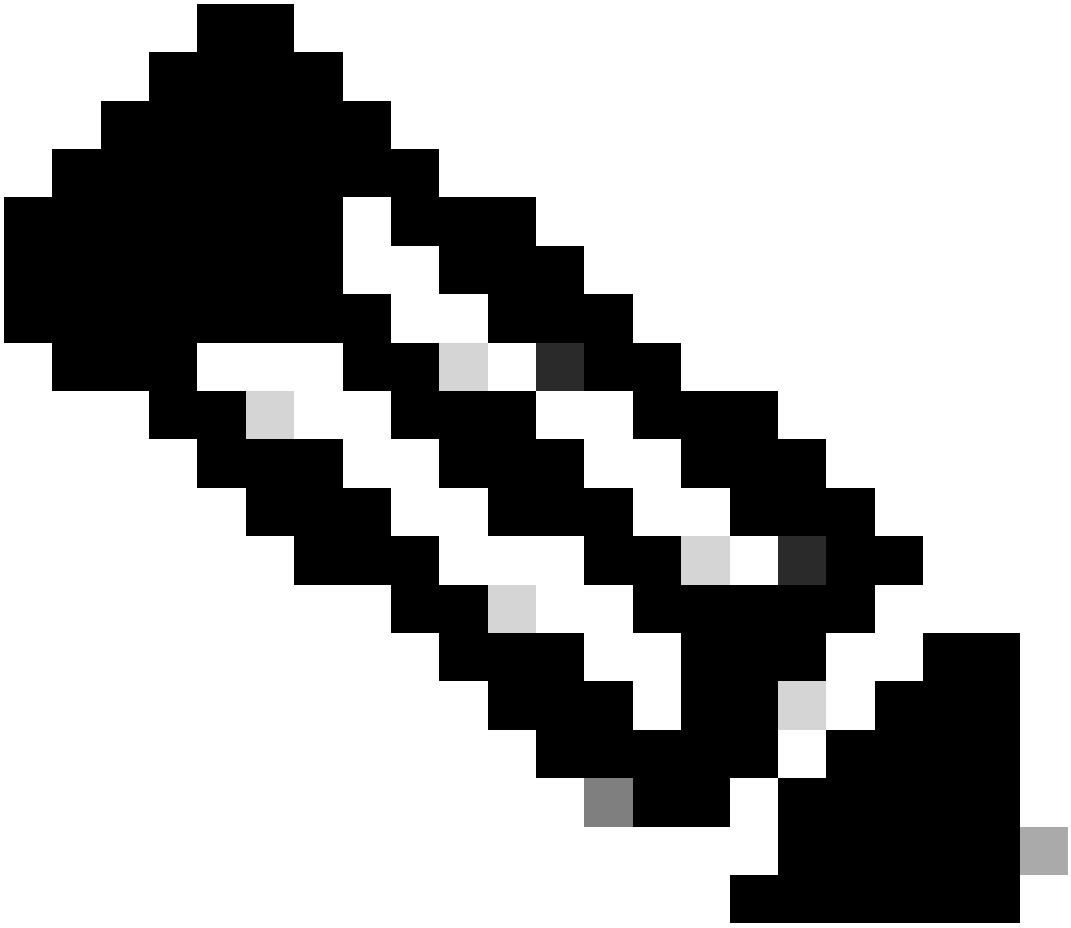
Een huidige DMVPN-configuratie werkt niet meer.

Oplossingen

Deze sectie bevat oplossingen voor de meest voorkomende DMVPN-problemen.

Deze oplossingen (in geen bepaalde orde) kunnen als controlelijst van punten worden gebruikt om te verifiëren of te proberen alvorens u problemen diepgaand oplost:

- Veelvoorkomende problemen
- Controleer of de pakketten Internet Security Association en Key Management Protocol (ISAKMP) zijn geblokkeerd bij de Internet Service Provider (ISP).
- Controleer of Generic Routing Encapsulation (GRE) werkt wanneer de tunnelbescherming is verwijderd.
- Registratie van Next-hop Resolution Protocol (NHRP) is mislukt.
- Controleer of de levensduur goed is ingesteld.
- Controleer of het verkeer in slechts één richting stroomt.
- Controleer dat de Routing Protocol Neighbour (Buurland van routingprotocol) is gevestigd.



Opmerking: controleer voordat u begint de volgende stappen:

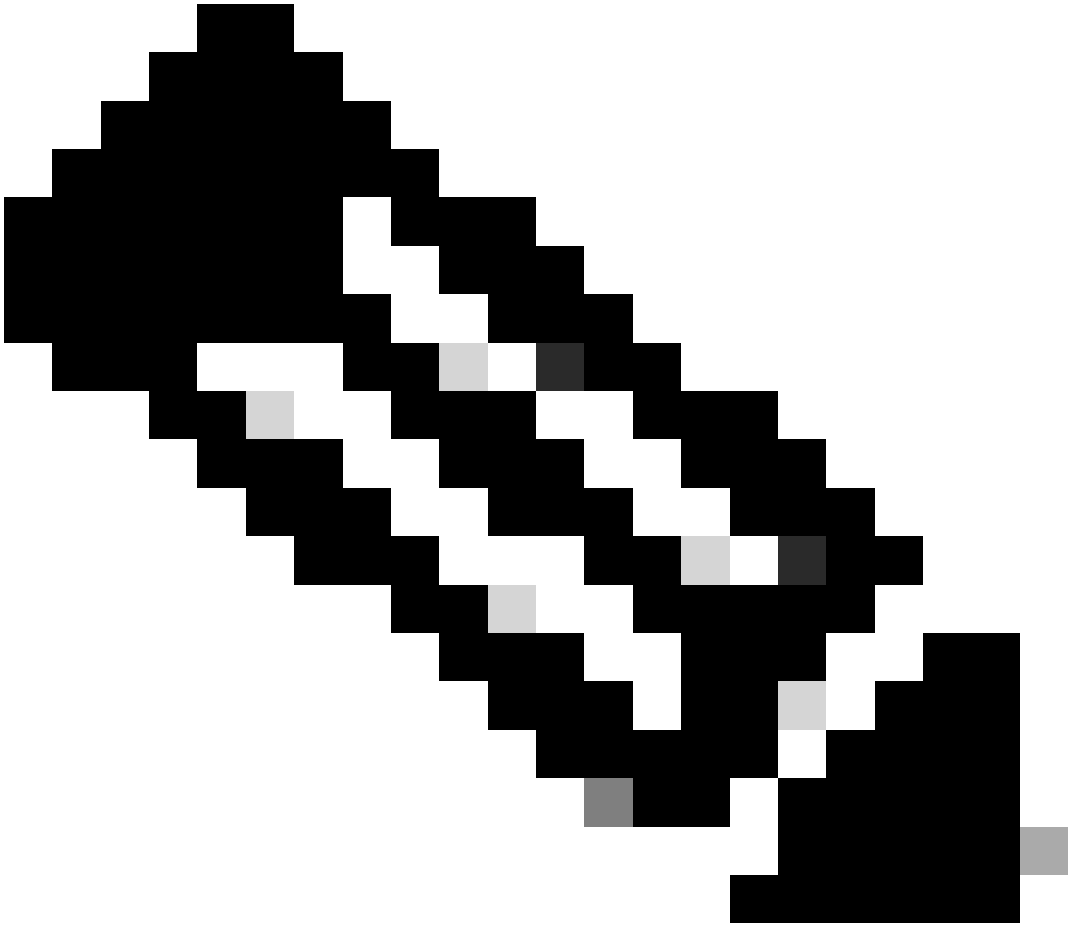
1. Synchroniseer de tijdstempels tussen de hub en de spaak
2. Msec debug en log timestamps inschakelen:

```
Router(config)#service timestamps debug datumtime msec

Router(config)#service timestamps log datetime msec
```

3. Schakel terminal exec prompt timestamp voor de debugging sessies in:

```
Router#terminal exec-prompt tijdstempel
```



Opmerking: op deze manier kunt u de debug-uitvoer eenvoudig correleren met de output van het showcommando.

Veelvoorkomende problemen

Controleer de basisconnectiviteit

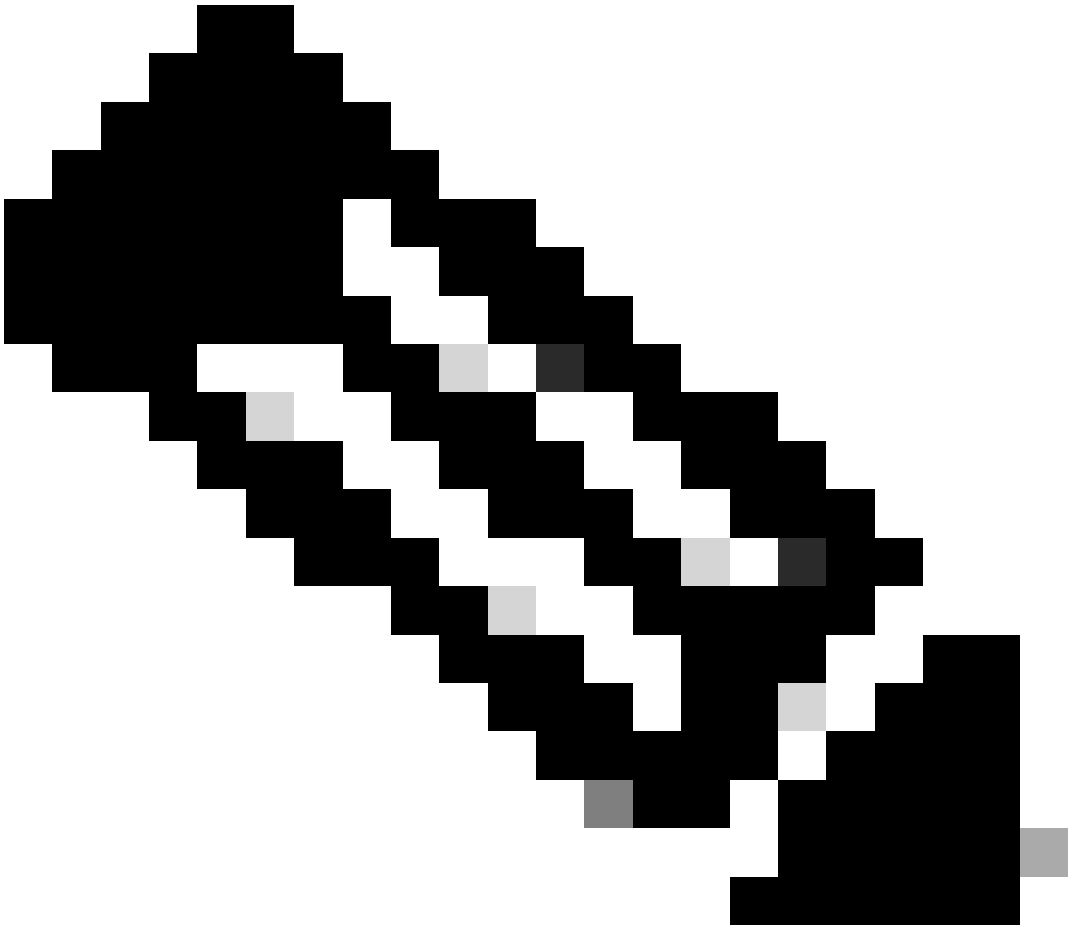
1. Ping van de hub naar de spaak met NBMA-adressen en omgekeerd.

   Deze pings moeten direct uit de fysieke interface, niet door de tunnel DMVPN gaan. Hopelijk is er geen firewall die pingpakketten blokkeert. Als dit niet werkt, controleer de routing en eventuele firewalls tussen de hub en spoke routers.

2. Gebruik ook traceroute om het pad te controleren dat door de versleutelde tunnelpakketten wordt genomen.

3. Gebruik de debug en toon opdrachten om te controleren of er geen verbinding is:

- debug ip icmp
- debug ip-pakket



Opmerking: de opdracht debug ip-pakket genereert een aanzienlijke hoeveelheid uitvoer en gebruikt een aanzienlijke hoeveelheid systeembronnen. Deze opdracht moet in productienetwerken met omzichtigheid worden gebruikt. Altijd gebruiken met de opdracht toegangslijst. Zie Probleemoplossing met IP-toegangslijsten voor meer informatie over het gebruik van de toegangslijst met debug-ip-pakket.

Verifiëren voor incompatibel ISAKMP-beleid

Als het ingestelde ISAKMP-beleid niet overeenkomt met het voorgestelde beleid door de externe peer, probeert de router het standaardbeleid van 65535. Als dat ook niet klopt, mislukt de ISAKMP-onderhandeling.

De opdracht show crypto isakmp sa toont dat de ISAKMP SA in MM_NO_STATE staat, wat

betekent dat de hoofdmodus is mislukt.

Controleer op onjuist vooraf gedeeld sleutelgeheim

Als de vooraf gedeelde geheimen aan beide kanten niet hetzelfde zijn, zal de onderhandeling mislukken.

De router retourneert het mislukte bericht van de redactionele controle.

Verifiëren voor incompatibele IPsec-transformatieset

Als de IPsec-transformatieset niet compatibel is of niet goed is afgestemd op de twee IPsec-apparaten, mislukt de IPsec-onderhandeling.

De router retourneert het laatste niet-acceptabele bericht voor het IPsec-voorstel.

Controleer of ISAKMP-pakketten worden geblokkeerd bij de ISP

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
Dst                src                  state       conn-id      slot       status
172.17.0.1      172.16.1.1        MM_NO_STATE         0              0       ACTIVE
172.17.0.1      172.16.1.1        MM_NO_STATE         0              0       ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE (deleted)
```

Het vorige voorbeeld toont de VPN-tunnelflapping.

Controleer ook debug crypto isakmp of de spaak-router een udp 500-pakket verstuurt:

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
```

04:14:44.450: ISAKMP:(0): beginning Main Mode exchange

```
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

De vorige debug output toont spaak router verzendt udp 500 pakket in elke 10 seconden.

Controleer bij ISP of de spraakrouter rechtstreeks is verbonden met de ISP router om er zeker van te zijn dat deze udp 500-verkeer toestaat.

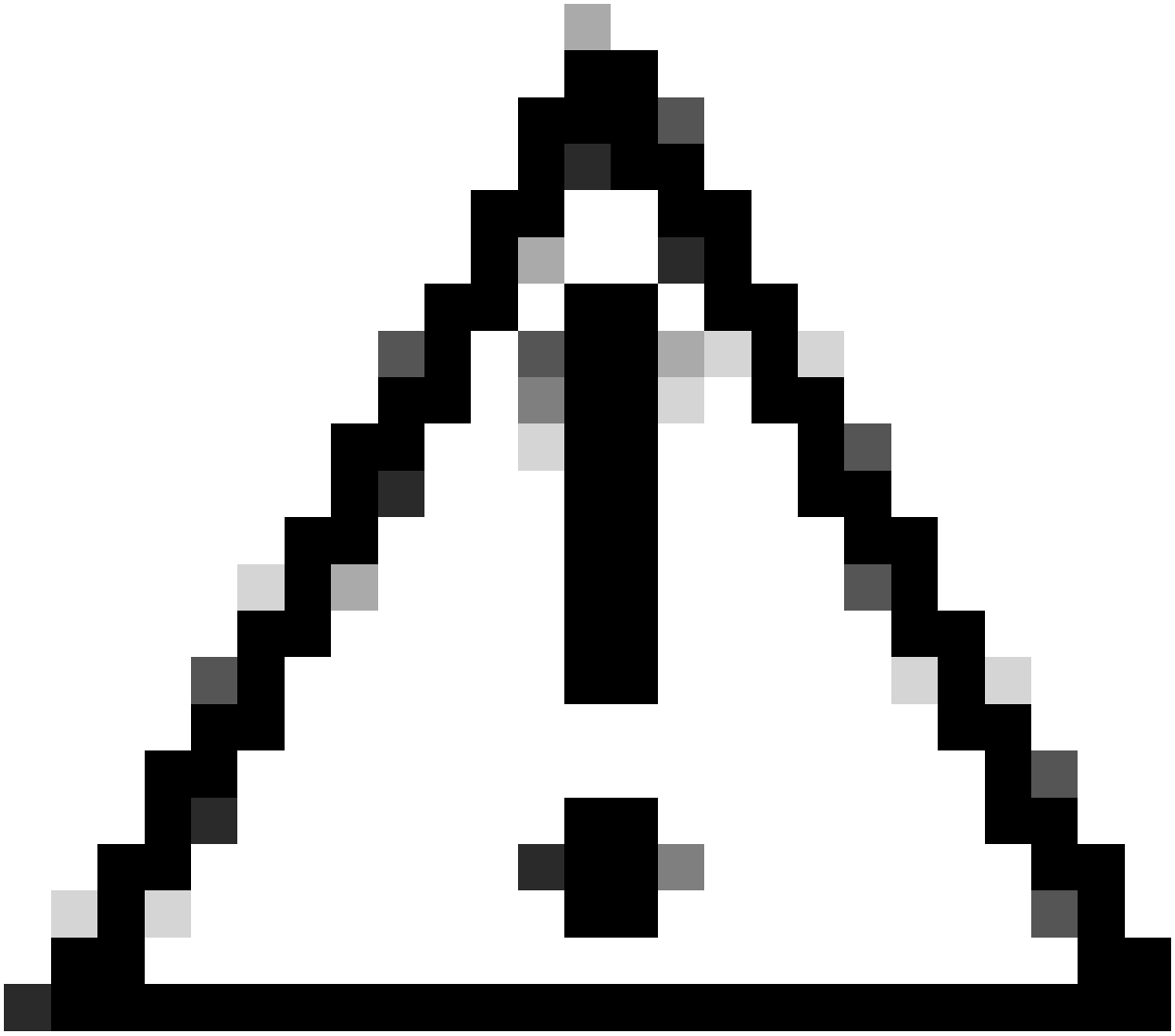
Nadat ISP udp 500 heeft toegestaan, voegt u inkomende ACL toe in uitgaande interface, wat een tunnelbron is om udp 500 toe te staan om er zeker van te zijn dat udp 500 verkeer in de router komt. Gebruik de show access-listopdracht om te verifiëren of hit increment aanpast.

```
    <#root>

Router#


show access-lists 101


Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```



Waarschuwing: Zorg ervoor dat u IP alle toegestane items in uw toegangslijst hebt. Anders kan al het andere verkeer worden geblokkeerd als een toegangslijst die inkomende op de uitgaande interface wordt toegepast.

Controleer of GRE werkt wanneer de tunnelbescherming is verwijderd

Wanneer DMVPN niet werkt, moet u, voordat u problemen met IPsec oplost, controleren of de GRE-tunnels werken zonder IPsec-encryptie.

Raadpleeg voor meer informatie Hoe u een GRE-tunnel configureert.

NHRP-registratie is mislukt

De VPN-tunnel tussen hub en spoke is omhoog, maar kan geen dataverkeer doorgeven:

<#root>

Router#

show crypto isakmp sa

dst	src	state	conn-id	slot	status
172.17.0.1	172.16.1.1	QM_IDLE	1082	0	ACTIVE

<#root>

Router#

show crypto IPSEC sa

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)

#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

inbound esp sas:
spi: 0xF830FC95(4163959957)

```
outbound esp sas:
spi: 0xD65A7865(3596253285)

!--- !--- Output is truncated !---
```

Het toont aan dat het terugkeerverkeer niet terugkomt van het andere uiteinde van de tunnel.

Controleer NHS invoer in de spaak router:

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0
```

req-failed 30

```
 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

Hieruit blijkt dat het NHS-verzoek is mislukt. Om dit probleem op te lossen, zorg ervoor dat de configuratie op de spaak router tunnelinterface correct is.

Configuratievoorbeeld:

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 172.17.0.1

!--- !--- Output is truncated !---

Configuratievoorbeeld met de juiste vermelding voor de NHS-server:

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 10.0.0.1

!--- !--- Output is truncated !---

Controleer nu of het NHS-nummer en de IPsec-encryptie/decryptie-tellers aanwezig zijn:

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0:        10.0.0.1 RE  req-sent 4
```

req-failed 0

```
repl-recv 3 (00:01:04 ago)

Router#
```

show crypto IPSec sa

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
```

#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)

!--- !--- Output is truncated !---
```

Controleer of de levensduur goed is geconfigureerd

Gebruik deze opdrachten om de huidige SA-levensduur en de tijd voor volgende heronderhandeling te verifiëren:

- **crypto isakmp als detail tonen**
- **crypto ipsec tonen als peer<NBMA-adres-peer>**

Zie de SA-levensduurwaarden. Als ze zich dicht bij de ingestelde levensduur bevinden (standaard is 24 uur voor ISAKMP en 1 uur voor IPsec), dan betekent dit dat er onlangs over deze SA's is onderhandeld. Als u even later kijkt en ze zijn opnieuw onderhandeld, dan kunnen de ISAKMP en/of IPsec op en neer springen.

<#root>

```
Router#
```

show crypto ipsec security-assoc lifetime

Security association lifetime: 4608000 kilobytes/3600 seconds

```
Router#
```

show crypto isakmp policy

```
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
```

Lifetime: 86400 seconds, no volume limit

```
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router#
```

show crypto ipsec sa

```
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
```

Controleer of het verkeer in slechts één richting stroomt

De VPN-tunnel tussen de spraakrouter is geactiveerd, maar kan geen dataverkeer doorgeven.

<#root>

```
Spoke1#
```

show crypto ipsec sa peer 172.16.2.11

```
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
```

```
#pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,



local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
      spi: 0x6AC801F4(1791492596)

!--- !--- Output is truncated !---


Spoke2#



sh crypto ipsec sa peer 172.16.1.1



   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)



 #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,



local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
     spi: 0x4C36F4AF(1278669999

!--- !--- Output is truncated !---
```

Er zijn geen decap-pakketten in spoke1, wat betekent dat esp-pakketten ergens in de path return worden gedropt van spoke2 naar spoke1.

De spoke2 router toont zowel encap als decap, wat betekent dat ESP verkeer wordt gefilterd voordat het spoke2 bereikt. Het kan gebeuren op het ISP eind bij spoke2 of bij om het even welke firewall in weg tussen spoke2 router en spoke1 router. Nadat zij ESP (IP Protocol 50) toestaan, spoke1 en spoke2 tonen zowel encaps als decaps tellerstoename.

<#root>

spoke1#

show crypto ipsec sa peer 172.16.2.11

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)

#pkts encaps: 300, #pkts encrypt: 300
#pkts decaps: 200, #pkts decrypt: 200

!--- !--- Output is truncated !---

spoke2#

sh crypto ipsec sa peer 172.16.1.1

local ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)

#pkts encaps: 316, #pkts encrypt: 316,
#pkts decaps: 300, #pkts decrypt: 310

!--- !--- Output is truncated !---

Controleer dat de Routing Protocol Neighbour (Routing Protocol) is opgericht

De sprekers kunnen geen routingprotocol naburige relatie instellen:

<#root>

Hub#

show ip eigrp neighbors

```
H   Address     Interface   Hold Uptime     SRTT    RTO       Q      Seq
                              (sec)             (ms)  Cnt     Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000       1      0
0   10.0.0.5     Tu0         11     00:00:47   1587   5000       0     1483
1   10.0.0.11    Tu0         13     00:00:56     1    5000       1      0
```

Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub#

show ip route eigrp

```
    172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     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, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Controleer of NHRP multicast mapping goed is geconfigureerd in de hub.

In de hub, is het vereist om dynamische nhrp multicast afbeelding te hebben die in de interface van de hubtunnel wordt gevormd.

Configuratievoorbeeld:

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Het voorbeeld van de configuratie met de correcte ingang voor dynamische multicast van nhrp afbeelding:

<#root>

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
```

ip nhrp map multicast dynamic

```
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Hierdoor kan NHRP automatisch spraakrouters toevoegen aan de multicast NHRP-toewijzingen.

Raadpleeg de ip nhrp map multicast dynamic opdracht in de referentie voor Cisco IOS IP-adresseringsservices voor meer informatie.

<#root>

Hub#

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 10
H   Address     Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                           (sec)    (ms)   Cnt    Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495

Hub#
```

show ip route

```
     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
```

D   192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0

```
     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, FastEthernet0/1

D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0

S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Routes naar de spokes worden geleerd via het EIGRP-protocol.

Probleem met externe VPN-toegang met DMVPN-integratie

Probleem

DMVPN werkt prima, maar kan de RAVPN niet opzetten.

Oplossing

Gebruik ISAKMP-profielen en IPsec-profielen om dit te bereiken. Maak afzonderlijke profielen voor de DMVPN en RAVPN.

Raadpleeg voor meer informatie DMVPN en Easy VPN Server with ISAKMP Profiles Configuration Voorbeeld.

Probleem met dual-hub-dual-dmvpn

Probleem

Probleem met dual-hub-dual-dmvpn. Met name tunnels dalen en kunnen niet opnieuw onderhandelen.

Oplossing

Gebruik het gedeelde sleutelwoord in de bescherming van de tunnel IPsec voor zowel de tunnelinterfaces op de hub als op de spaak.

Een configuratievoorbeeld:

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

Raadpleeg de **tunnel protection** opdracht in de referentie voor Cisco IOS-beveiligingsopdracht (A-C) voor meer informatie.

Probleem met inloggen op een server via DMVPN

Probleem

Probleemverkeer via de DMVPN-netwerkserver is niet toegankelijk.

Oplossing

Het probleem kan te maken hebben met de MTU en MSS grootte van het pakket dat GRE en IPsec gebruikt.

Nu, zou de pakketgrootte een kwestie met de fragmentatie kunnen zijn. U verwijdert dit probleem door de volgende opdrachten te gebruiken:

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

U kunt de **tunnel path-mtu-discovery**opdracht ook configureren om de MTU-grootte dynamisch te ontdekken.

Raadpleeg voor een gedetailleerdere uitleg het gedeelte IP-fragmentatie, MTU, MSS en PMTUD-problemen oplossen met GRE en IPSEC.

Kan geen toegang tot de servers op DMVPN krijgen via bepaalde poorten

Probleem

Kan geen toegang krijgen tot servers op DMVPN via specifieke poorten.

Oplossing

Controleer of de Cisco IOS-firewallfunctieset is uitgeschakeld en of het werkt.

Als het prima werkt, dan is het probleem gerelateerd aan de Cisco IOS firewallconfiguratie, niet aan DMVPN.

Gerelateerde informatie

- **Dynamisch Multipoint VPN (DMVPN)**
- **IPsec-onderhandeling/IKE-protocollen**
- **Cisco Technical Support en downloads**

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.