Probleemoplossing voor DMVPN fase 2 spraak-naar-spraaktunnel

Inhoud

Inleiding

Dit document beschrijft hoe u een fase 2-spraakgerichte DMVPN-tunnel kunt oplossen wanneer deze niet tot stand komt.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over de volgende onderwerpen:

- Dynamisch Multipoint Virtual Private Network (DMVPN)
- IKE/IPSEC-protocollen
- Next Hop Resolution Protocol (NHRP)

Gebruikte componenten

Dit document is gebaseerd op deze softwareversie:

- Cisco CRS-1000V (VXE) - versie 17.03.08

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

Dit document beschrijft hoe u verschillende tools voor probleemoplossing kunt configureren en gebruiken bij een veel voorkomende DMVPN-kwestie. De kwestie is mislukte onderhandeling van een fase 2 DMVPN tunnel, waar de bron sprak, de staat DMVPN omhoog met de correcte niet-Uitzending Multi-Access (NBMA)/Tunnel-afbeelding aan de bestemming sprak toont. Echter, op de bestemming sprak een onjuiste afbeelding wordt weergegeven.

Theoretische achtergrond

Het is belangrijk om te begrijpen hoe spraaktunnels tot stand worden gebracht wanneer het hebben van een DMVPN fase 2 opstelling. Deze paragraaf geeft een korte theoretische samenvatting van het NHRP-proces tijdens deze fase.

In DMVPN fase 2 kun je op aanvraag dynamische spraaktunnels bouwen. Dit is mogelijk omdat op alle apparaten binnen de DMVPN-cloud (hub en spokes) de modus van de tunnelinterface verandert in Generic Routing Encapsulation (GRE) multipoint. Een van de belangrijkste kenmerken van deze fase is dat de hub niet wordt gezien als de volgende-hop door de andere apparaten. In plaats daarvan, hebben alle spokes de routing informatie van elkaar. Wanneer het opzetten van een spaak-to-spaak tunnel in fase 2, wordt een NHRP proces geactiveerd waar de spaken de informatie over andere spaken leren, en maakt een afbeelding tussen de NBMA en tunnel IP adressen.

De volgende stappen geven aan hoe het NHRP-afwikkelingsproces wordt geactiveerd:

1. Wanneer de bron sprak probeert om LAN van de bestemming te bereiken sprak, doet het een routeraadpleging die het bericht van het resolutieverzoek teweegbrengt om het adres van NBMA van de bestemming te krijgen gesproken. De bron sprak stuurt dit eerste bericht naar de hub.

2. De hub ontvangt het resolutieverzoek en stuurt het door naar de bestemming die gesproken wordt.

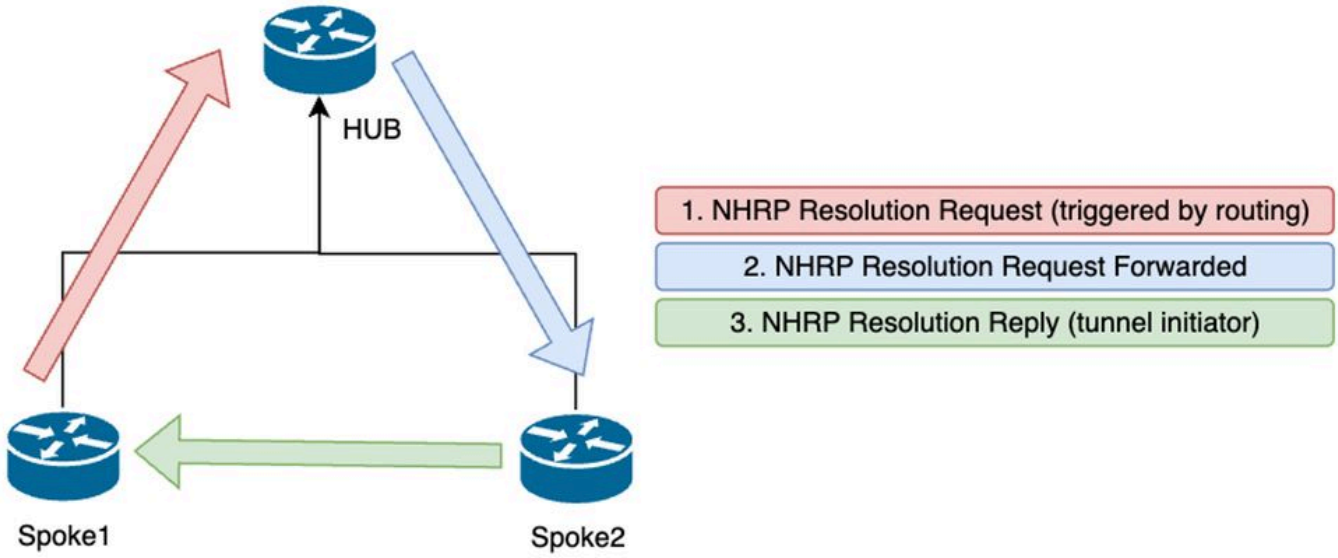
3. Het land dat het woord voert, stuurt de resolutie terug naar de bron die het woord voert. Als de tunnelconfiguratie een IPSEC-profiel heeft gekoppeld:

    - Het NHRP-resolutieproces wordt uitgesteld totdat IKE/IPSEC-protocollen kunnen worden vastgesteld.

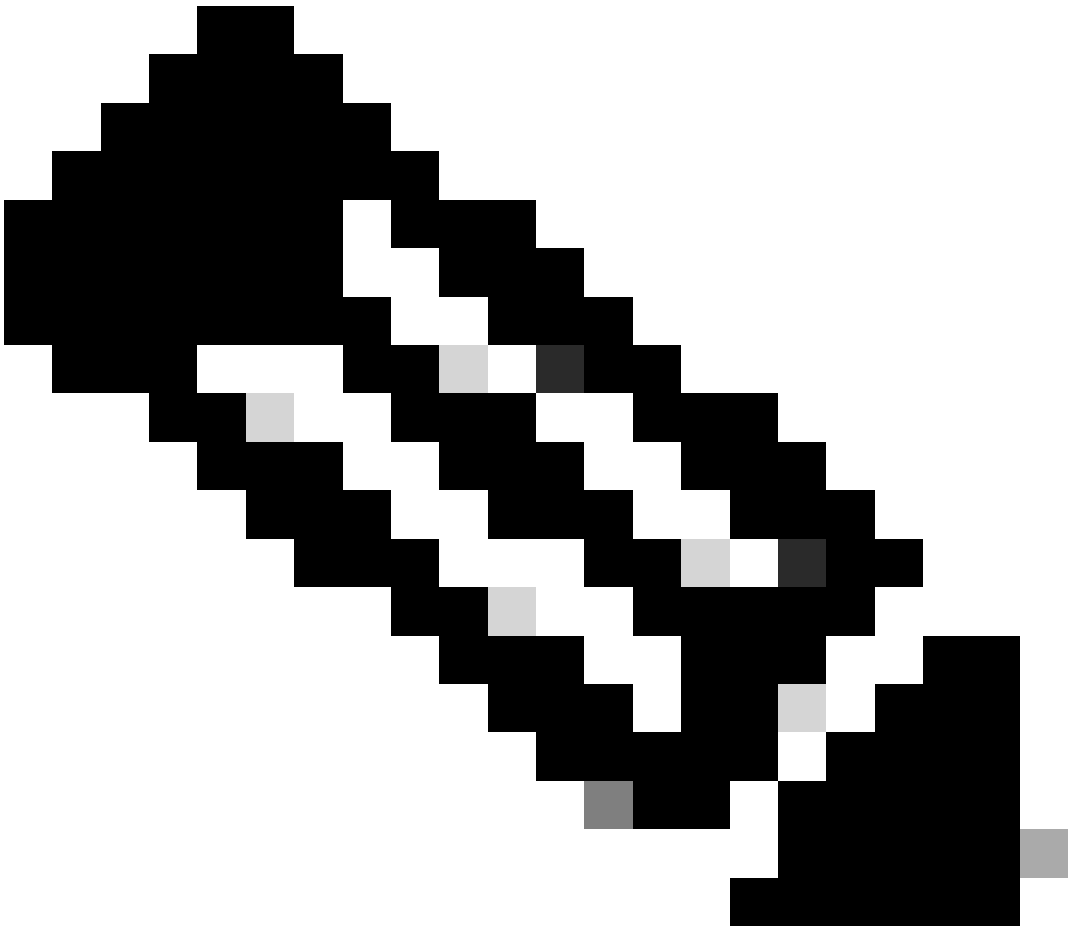
    - De bestemming sprak initieert en vestigt de tunnels IKE/IPSEC.

    - Vervolgens wordt het NHRP-proces hervat en de bestemmeling sprak stuurt de resolutie antwoord naar de bron gesproken met behulp van de IPSEC-tunnel als

transportmethode.



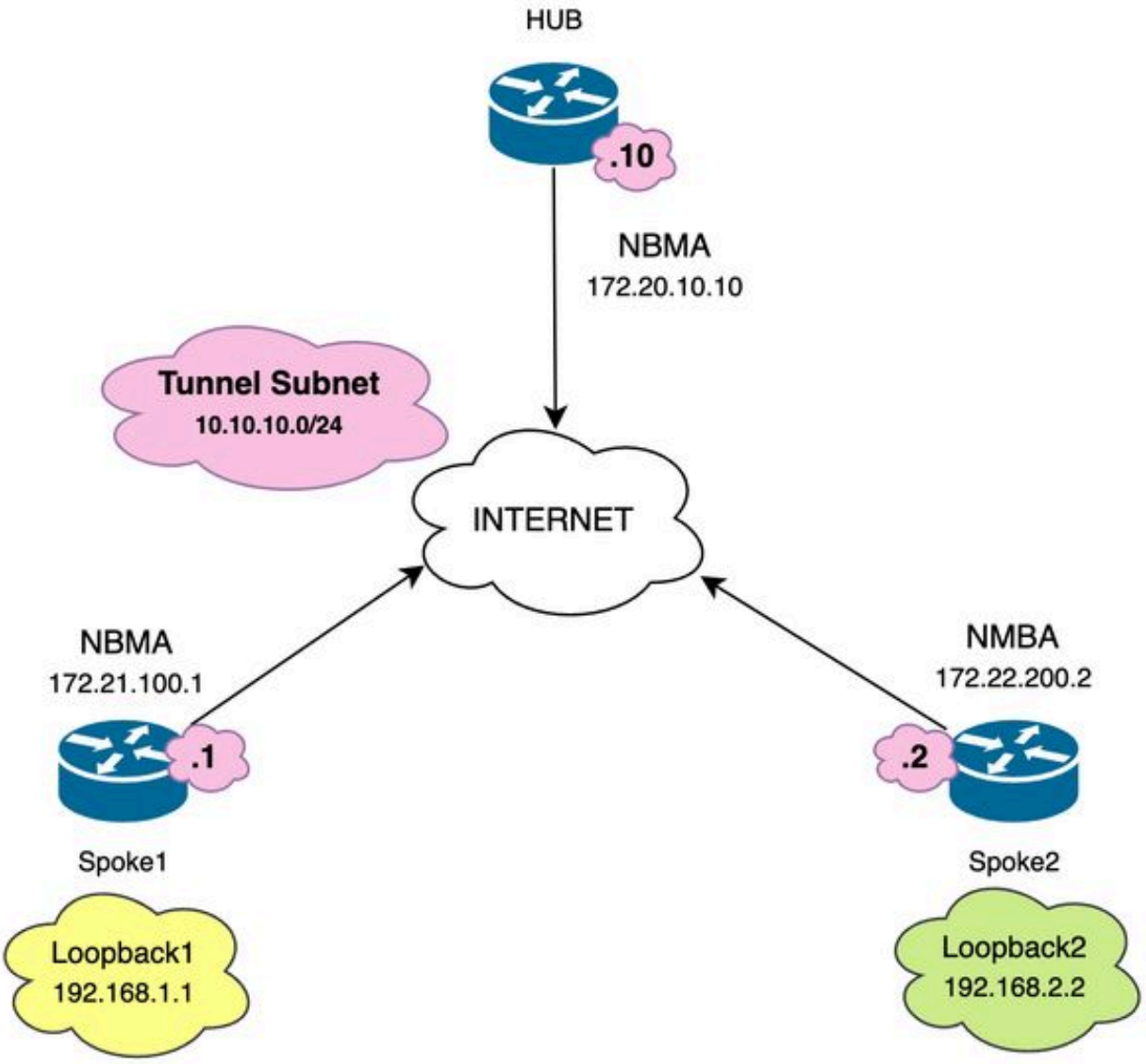
NHRP-berichtenstroom tussen de woordvoerders in fase 2



Opmerking: voordat het oplossingsproces kan starten, moeten alle spokes al geregistreerd zijn bij de HUB.

Topologie

Dit diagram toont de topologie die voor het scenario wordt gebruikt:



Gebruikte netwerkdiagrammen en IP-subnetten

Stappen voor probleemoplossing

In dit scenario is de spraakverbinding tussen Spoke1 en Spoke2 niet vastgesteld, waardoor de communicatie tussen hun lokale bronnen (weergegeven door loopback interfaces) wordt beïnvloed omdat ze elkaar niet kunnen bereiken.

```
SPOKE1#ping 192.168.2.2 source loopback1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Eerste validering

Wanneer het ontmoeten van zulk een scenario, is het belangrijk om te beginnen door de tunnelconfiguratie te bevestigen en ervoor te zorgen dat beide apparaten de correcte waarden binnen het hebben. Om de tunnelconfiguratie te bekijken, voer de opdracht tonen in werking stelt - in werking stellen interfacetunnel<ID>.

Spoke 1 tunnelconfiguratie:

<#root>

```
SPOKE1#show running-config interface tunnel10
Building configuration...

Current configuration : 341 bytes
!
interface Tunnel10
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN


ip nhrp map 10.10.10.10 172.20.10.10


ip nhrp map multicast 172.20.10.10


ip nhrp network-id 10
ip nhrp nhs 10.10.10.10


tunnel source GigabitEthernet1
tunnel mode gre multipoint


tunnel protection IPSEC profile IPSEC_Profile_1


end
```

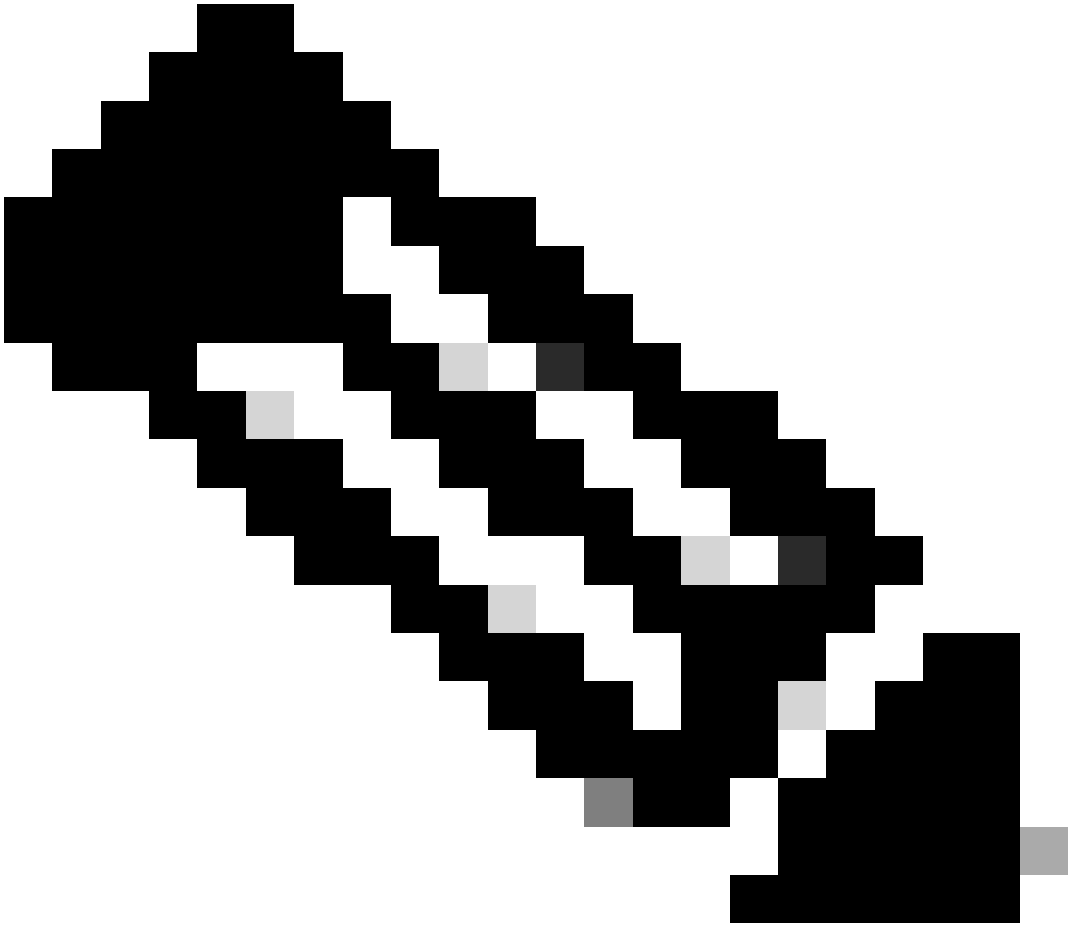
Spoke 2 tunnelconfiguratie:

<#root>

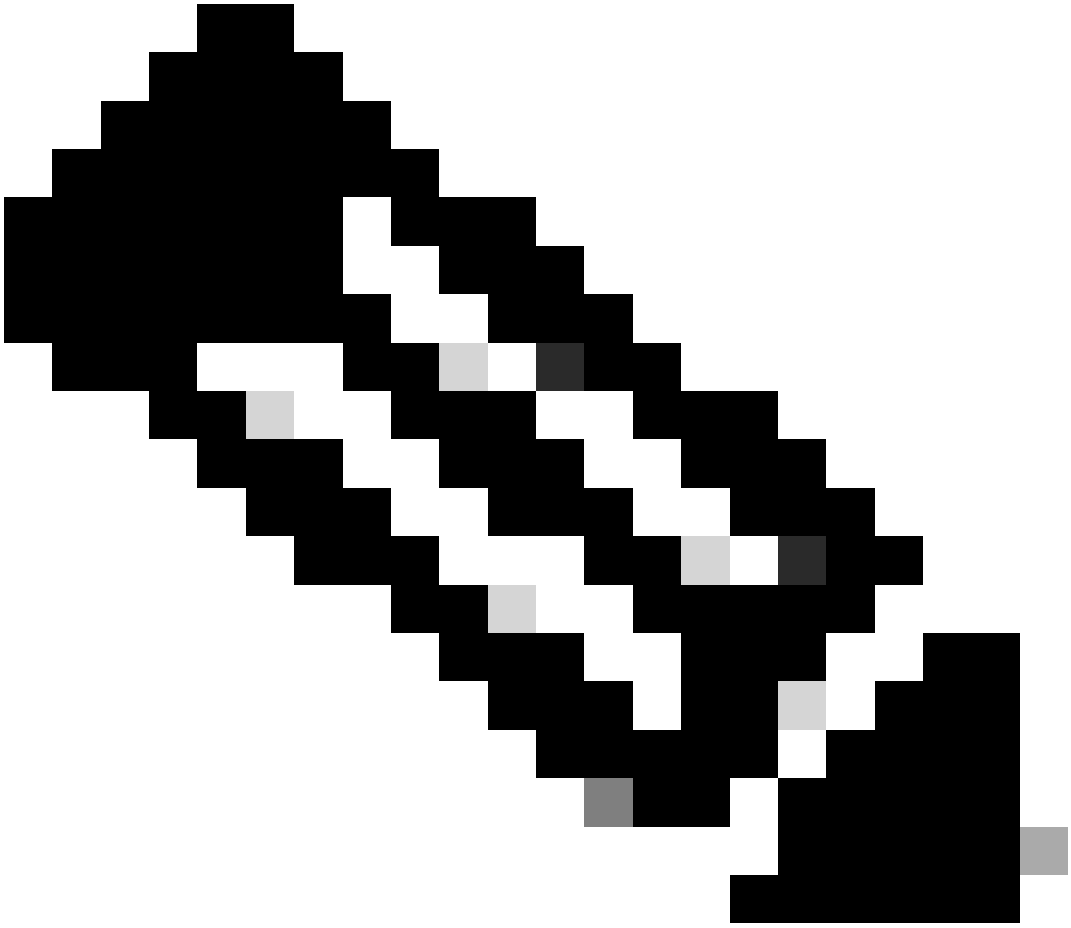
```
SPOKE2#show running-config interface tunnel10
Building configuration...

Current configuration : 341 bytes
!
interface Tunnel10
ip address 10.10.10.2 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN


ip nhrp map 10.10.10.10 172.20.10.10


ip nhrp map multicast 172.20.10.10


ip nhrp network-id 10
ip nhrp nhs 10.10.10.10


tunnel source GigabitEthernet1
tunnel mode gre multipoint


tunnel protection IPSEC profile IPSEC_Profile_1


end
```

Op de configuratie die u nodig hebt om te bevestigen dat de koppeling aan de HUB correct is, de NHRP-verificatietekenreeks komt overeen tussen de apparaten, beide spaken hebben dezelfde DMVPN-fase geconfigureerd, en, als IPSEC-bescherming wordt gebruikt, verifiëren dat de juiste crypto-configuratie wordt toegepast.

Als de configuratie correct is en IPSEC-beveiliging bevat, moet u controleren of de IKE- en IPSEC-protocollen correct werken. Dit komt doordat NHRP de IPSEC-tunnel gebruikt als transportmethode om volledig te onderhandelen. Om de staat van de protocollen IKE/IPSEC in werking te stellen het bevel toont crypto IPSEC als peer x.x.x.x (waar x.x.x.x het IP adres NBMA van de spaak is u probeert om de tunnel met te vestigen).



Opmerking: om te verifiëren of de IPSEC-tunnel is geopend, moet de ESP-sectie (inkomende en uitgaande insluitingsbeveiliging) de tunnelinformatie hebben (SPI, transformatie-set, enzovoort). Alle waarden die in dit gedeelte worden weergegeven, moeten aan beide uiteinden overeenkomen.



Opmerking: als er problemen met IKE/IPSEC worden geïdentificeerd, moet de probleemoplossing zich op die protocollen richten.

IKE/IPSEC tunnelstatus op Spoke1:

<#root>

SPOKE1#

show crypto IPSEC sa peer 172.22.200.2

```
interface: Tunnel10
Crypto map tag: Tunnel10-head-0, local addr 172.21.100.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.21.100.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.22.200.2/255.255.255.255/47/0)
current_peer 172.22.200.2 port 500
PERMIT, flags={origin_is_acl,}
```

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.21.100.1, remote crypto endpt.: 172.22.200.2
plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x6F6BF94A(1869347146)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x84502A19(2219846169)

transform: esp-256-aes esp-sha256-hmac

 ,
in use settings ={Transport, }
conn id: 2049, flow_id: CSR:49, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4608000/28716)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x6F6BF94A(1869347146)

transform: esp-256-aes esp-sha256-hmac

 ,
in use settings ={Transport, }
conn id: 2050, flow_id: CSR:50, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4608000/28716)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

IKE/IPSEC tunnelstatus op Spoke2:

<#root>

SPOKE2#

show crypto IPSEC sa peer 172.21.100.1

interface: Tunnel10
Crypto map tag: Tunnel10-head-0, local addr 172.22.200.2

protected vrf: (none)
local ident (addr/mask/prot/port): (172.22.200.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.21.100.1/255.255.255.255/47/0)
current_peer 172.21.100.1 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.200.2, remote crypto endpt.: 172.21.100.1
plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x84502A19(2219846169)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x6F6BF94A(1869347146)

transform: esp-256-aes esp-sha256-hmac ,

in use settings ={Transport, }
conn id: 2045, flow_id: CSR:45, sibling_flags FFFFFFFF80004008, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4608000/28523)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0x84502A19(2219846169)


transform: esp-256-aes esp-sha256-hmac

 ,
in use settings ={Transport, }
conn id: 2046, flow_id: CSR:46, sibling_flags FFFFFFFF80004008, crypto map: Tunnel10-head-0
sa timing: remaining key lifetime (k/sec): (4607998/28523)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

De uitgangen laten zien dat op beide spokes de IPSEC-tunnel omhoog is, maar Spoke2 toont versleutelde pakketten (encaps) maar geen gedecrypteerde pakketten (decaps). Ondertussen, toont Spoke1 geen pakketten die door de tunnel IPSEC stromen. Dit geeft aan dat het probleem zich kan voordoen bij het NHRP-protocol.

Troubleshooting-tools

Nadat u de eerste validatie hebt uitgevoerd en de configuratie en de IKE/IPSEC-protocollen (indien nodig) hebt bevestigd, veroorzaakt u het communicatieprobleem niet, kunt u de in deze sectie gepresenteerde tools gebruiken om door te gaan met het oplossen van problemen.

Nuttige opdrachten

De opdracht toont dmvpn-interfacetunnel<ID> die u DMVPN-specifieke sessieinformatie geeft (NBMA/Tunnel IP-adressen, status van de tunnel, up/down-tijd en attribuut). U kunt het detail sleutelwoord gebruiken om details van de crypto sessie/socket te tonen. Het is belangrijk te vermelden dat de toestand van de tunnel aan beide uiteinden moet overeenkomen.

Spoke 1 toont dmvpn-interfacetunnel<ID> uitvoer:

<#root>

```
SPOKE1#

show dmvpn interface tunnel10


Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override, B - BGP
C - CTS Capable, I2 - Temporary
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
```

```
Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add  State UpDn Tm  Attrb
----- --------------- --------------- ----- -------- -----
   2
```

172.20.10.10 10.10.10.2 UP 00:00:51 I2

10.10.10.10 UP 02:53:27 S

Spoke 2 toont dmvpn-interfacetunnel<ID> uitvoer:

<#root>

SPOKE2#

show dmvpn interface tunnel10

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
T1 - Route Installed, T2 - Nexthop-override, B - BGP
C - CTS Capable, I2 - Temporary
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
```

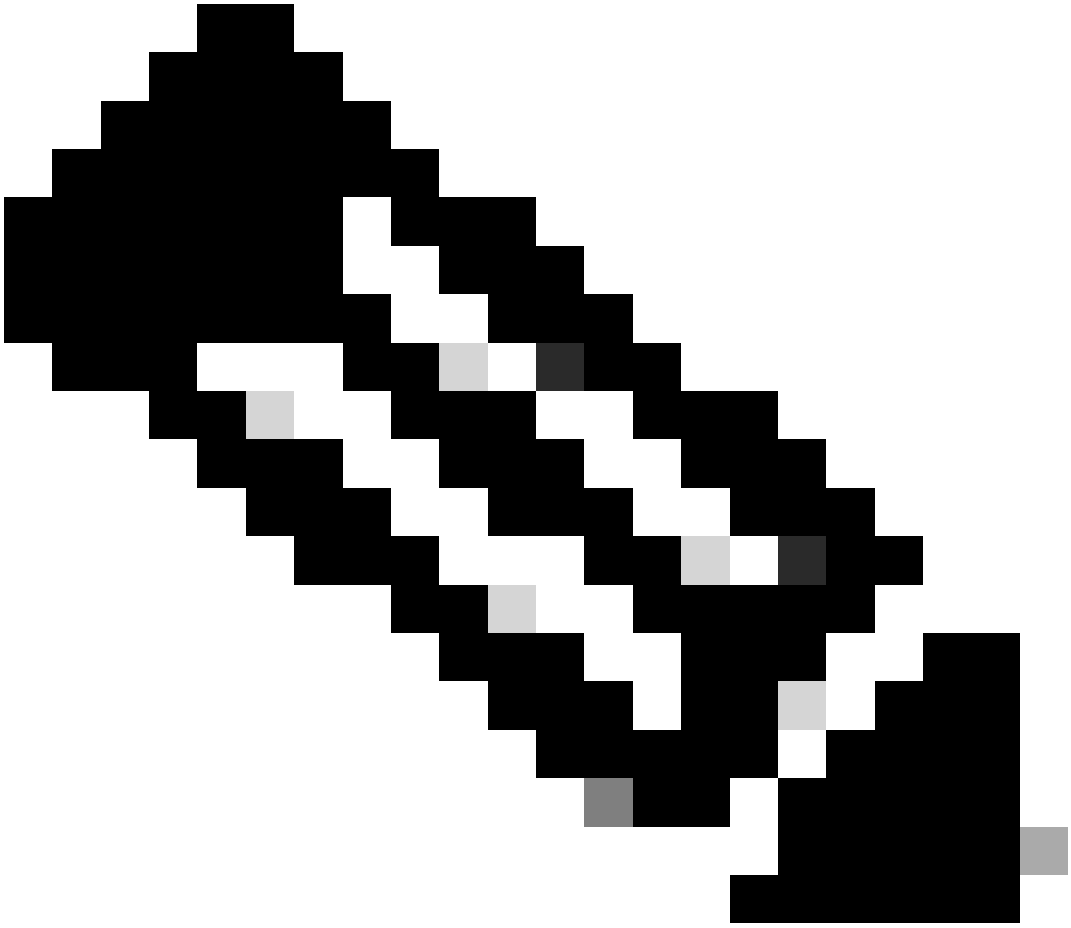
1 172.21.100.1 10.10.10.1 UP 00:03:53 D

1 172.20.10.10 10.10.10.10 UP 02:59:14 S

De output op elk apparaat toont verschillende informatie voor elke spaak. In de Spoke1 tabel kunt u zien dat de vermelding voor Spoke 2 niet het juiste NBMA IP-adres bevat en dat het kenmerk onvolledig lijkt (I2). Aan de andere kant laat de Spoke2-tabel de juiste mapping zien (NBMA/Tunnel IP-adressen) en de staat als omhoog die aangeeft dat er over de tunnel volledig onderhandeld wordt.

De volgende opdrachten kunnen nuttig zijn tijdens het proces voor probleemoplossing:

- toon ip nhrp: toon NHRP mapping informatie
- toon ip nhrp verkeersinterfacetunnel10: Toont NHRP verkeersstatistieken

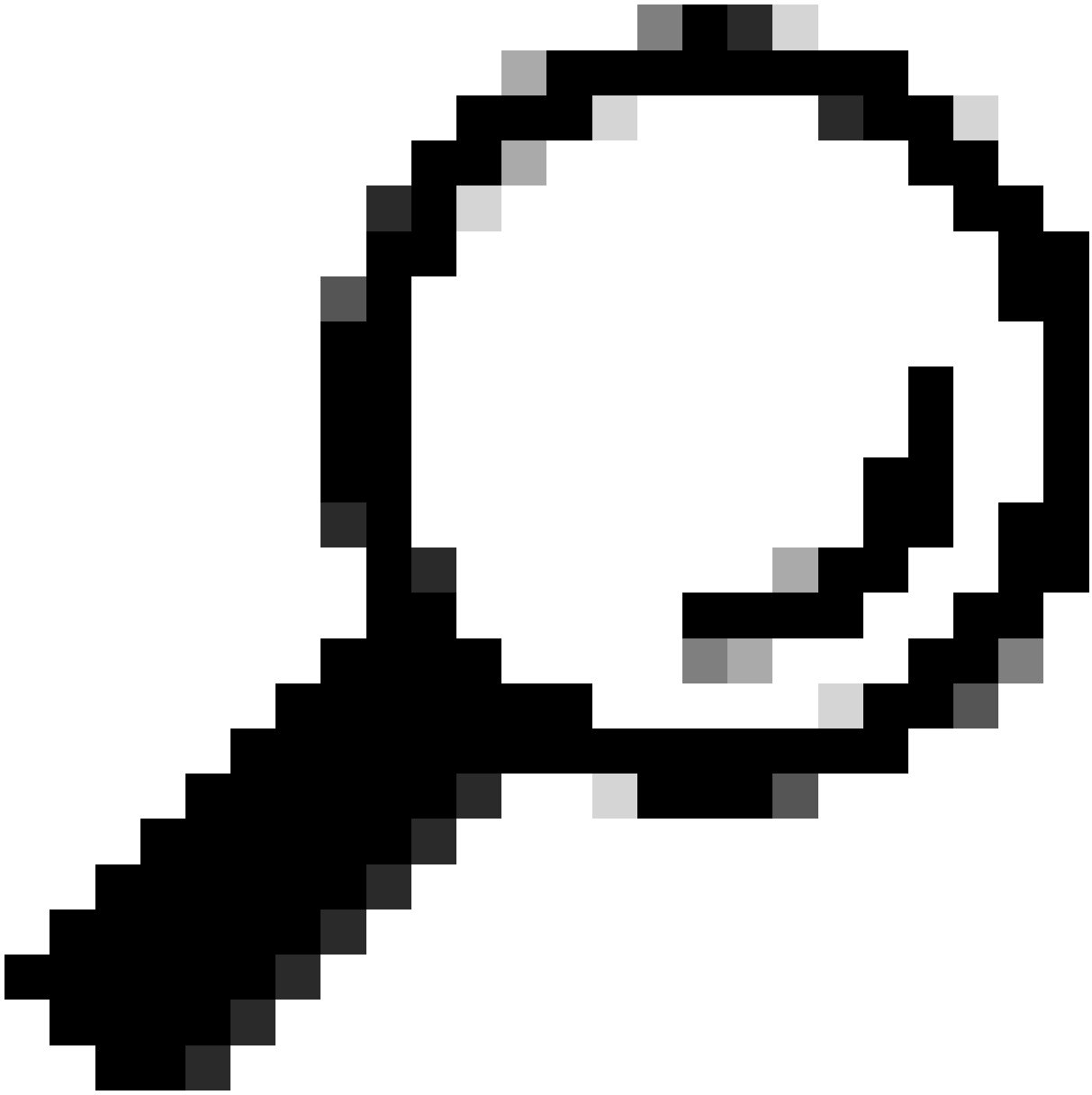


Opmerking: raadpleeg voor opdrachtspecificaties (syntaxis, beschrijving, trefwoorden, voorbeeld) de opdrachtreferentie: Cisco IOS security opdrachtreferentie: opdrachten S tot Z

Debugs

Na het verifiëren van de vorige informatie en bevestigde dat de tunnel onderhandelingskwesties ervaart, is het noodzakelijk om debugs toe te laten om waar te nemen hoe de NHRP-pakketten worden uitgewisseld. De volgende debugs moeten worden ingeschakeld op alle betrokken apparaten:

1. debug dmvpn voorwaarde peer NBMA x.x.x.x (waar x.x.x.x het verre apparaat IP adres is).
2. debug dmvpn all: deze opdracht maakt ISAKMP, IKEv2, IPSEC, DMVPN en NHRP debugging opdrachten mogelijk.



Tip: aanbevolen wordt om de peer-conditie commando te gebruiken elke keer dat u de debugs inschakelen zodat u de onderhandeling van die specifieke tunnel kunt zien.

Om de volledige NHRP-stroom te zien, werden de volgende debug-opdrachten gebruikt op elk apparaat:

Gesproken1

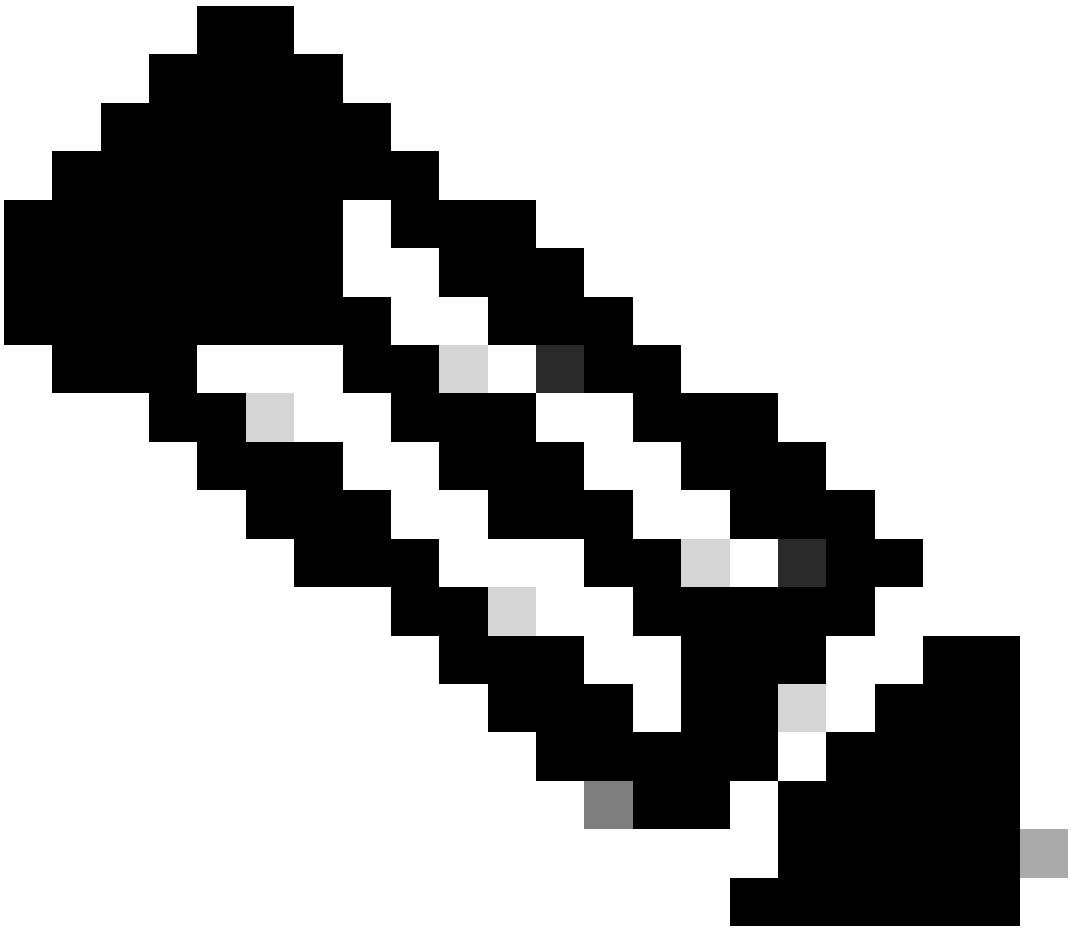
```
debug dmvpn condition peer NBMA 172.22.200.2
debug dmvpn condition peer NBMA 172.20.10.10
debug dmvpn all all
```

HUB

```
debug dmvpn condition peer NBMA 172.21.100.1
debug dmvpn condition peer NBMA 172.22.200.2
debug dmvpn all all
```

Gesproken2

```
debug dmvpn condition peer NBMA 172.21.100.1
debug dmvpn condition peer NBMA 172.20.10.10
debug dmvpn all all
```



Opmerking: de debugs moeten tegelijkertijd worden ingeschakeld en verzameld op alle

---

betrokken apparaten.

Debugs ingeschakeld op alle apparaten worden weergegeven met de opdracht show debug:

<#root>

```
ROUTER#
```

show debug

```
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop


IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address Port
------------------------------------------------------|----------

NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP detail debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
NHRP events debugging is on

Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
IKEV2:
IKEv2 error debugging is on
IKEv2 default debugging is on
IKEv2 packet debugging is on
IKEv2 packet hexdump debugging is on
IKEv2 internal debugging is on
Tunnel Protection Debugs:
Generic Tunnel Protection debugging is on

DMVPN:
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

Na het verzamelen van alle debugs, moet u beginnen te analyseren de debugs op de bron gesproken (Spoke1), dit staat u toe om de onderhandeling vanaf het begin te traceren.

Spoke1 debug uitvoer:

<#root>

```
---------------------- [IKE/IPSEC DEBUG OUTPUTS OMITTED]----------------------

*Feb 1 01:31:34.657: ISAKMP: (1016):

Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE


*Feb 1 01:31:34.657: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Feb 1 01:31:34.657: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
*Feb 1 01:31:34.657: CRYPTO_SS(TUNNEL SEC): Sending MTU Changed message
*Feb 1 01:31:34.661: IPSEC-IFC MGRE/Tu10(172.21.100.1/172.22.200.2): Got MTU message mtu 1458
*Feb 1 01:31:34.661: IPSEC-IFC MGRE/Tu10(172.21.100.1/172.22.200.2): connection lookup returned 80007F2
*Feb 1 01:31:34.662: CRYPTO_SS(TUNNEL SEC): Sending Socket Up message
*Feb 1 01:31:34.662: IPSEC-IFC MGRE/Tu10(172.21.100.1/172.22.200.2): connection lookup returned 80007F2
*Feb 1 01:31:34.662: IPSEC-IFC MGRE/Tu10(172.21.100.1/172.22.200.2):

tunnel_protection_socket_up


*Feb 1 01:31:34.662: IPSEC-IFC MGRE/Tu10(172.21.100.1/172.22.200.2): Signalling NHRP
*Feb 1 01:31:36.428: NHRP: Checking for delayed event NULL/10.10.10.2 on list (Tunnel10 vrf: global(0x0)
*Feb 1 01:31:36.429: NHRP: No delayed event node found.
*Feb 1 01:31:36.429: NHRP: There is no VPE Extension to construct for the request
*Feb 1 01:31:36.429: NHRP: Sending NHRP Resolution Request for dest: 10.10.10.2 to nexthop: 10.10.10.2
*Feb 1 01:31:36.429: NHRP: Attempting to send packet through interface Tunnel10 via DEST dst 10.10.10.2
*Feb 1 01:31:36.429: NHRP-DETAIL: First hop route lookup for 10.10.10.2 yielded 10.10.10.2, Tunnel10
*Feb 1 01:31:36.429: NHRP:

Send Resolution Request via Tunnel10 vrf: global(0x0), packet size: 85


*Feb 1 01:31:36.429: src: 10.10.10.1, dst: 10.10.10.2
*Feb 1 01:31:36.429: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 1 01:31:36.429: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 1 01:31:36.429: pktsz: 85 extoff: 52
*Feb 1 01:31:36.429: (M) flags: "router auth src-stable nat ",

reqid: 10


*Feb 1 01:31:36.429:

src NBMA: 172.21.100.1


*Feb 1 01:31:36.429:

src protocol: 10.10.10.1, dst protocol: 10.10.10.2


*Feb 1 01:31:36.429: (C-1) code: no error(0), flags: none
*Feb 1 01:31:36.429: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:36.429: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 1 01:31:36.429: Responder Address Extension(3):
*Feb 1 01:31:36.429: Forward Transit NHS Record Extension(4):
```

*Feb 1 01:31:36.429: Reverse Transit NHS Record Extension(5):
*Feb 1 01:31:36.429: Authentication Extension(7):
*Feb 1 01:31:36.429: type:Cleartext(1),

data:DMVPN

*Feb 1 01:31:36.429: NAT address Extension(9):
*Feb 1 01:31:36.430: NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address: 172.20.10
*Feb 1 01:31:36.430: NHRP: 109 bytes out Tunnel10
*Feb 1 01:31:36.430: NHRP-RATE:

Retransmitting Resolution Request for 10.10.10.2, reqid 10, (retrans ivl 4 sec)

*Feb 1 01:31:39.816: NHRP: Checking for delayed event NULL/10.10.10.2 on list (Tunnel10 vrf: global(0x0)
*Feb 1 01:31:39.816: NHRP: No delayed event node found.
*Feb 1 01:31:39.816: NHRP: There is no VPE Extension to construct for the request
*Feb 1 01:31:39.817: NHRP: Sending NHRP Resolution Request for dest: 10.10.10.2 to nexthop: 10.10.10.2
*Feb 1 01:31:39.817: NHRP: Attempting to send packet through interface Tunnel10 via DEST dst 10.10.10.2
*Feb 1 01:31:39.817: NHRP-DETAIL: First hop route lookup for 10.10.10.2 yielded 10.10.10.2, Tunnel10
*Feb 1 01:31:39.817: NHRP:

Send Resolution Request via Tunnel10 vrf: global(0x0), packet size: 85

*Feb 1 01:31:39.817: src: 10.10.10.1, dst: 10.10.10.2
*Feb 1 01:31:39.817: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 1 01:31:39.817: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 1 01:31:39.817: pktsz: 85 extoff: 52
*Feb 1 01:31:39.817: (M) flags: "router auth src-stable nat ",

reqid: 10

*Feb 1 01:31:39.817:

src NBMA: 172.21.100.1

*Feb 1 01:31:39.817:

src protocol: 10.10.10.1, dst protocol: 10.10.10.2

*Feb 1 01:31:39.817: (C-1) code: no error(0), flags: none
*Feb 1 01:31:39.817: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:39.817: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 1 01:31:39.817: Responder Address Extension(3):
*Feb 1 01:31:39.817: Forward Transit NHS Record Extension(4):
*Feb 1 01:31:39.817: Reverse Transit NHS Record Extension(5):
*Feb 1 01:31:39.817: Authentication Extension(7):
*Feb 1 01:31:39.817: type:Cleartext(1),

data:DMVPN

*Feb 1 01:31:39.817: NAT address Extension(9):
*Feb 1 01:31:39.817: NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address: 172.20.10
*Feb 1 01:31:39.818: NHRP: 109 bytes out Tunnel10
*Feb 1 01:31:39.818: NHRP-RATE:

Retransmitting Resolution Request for 10.10.10.2, reqid 10, (retrans ivl 8 sec)

*Feb 1 01:31:46.039: NHRP: Checking for delayed event NULL/10.10.10.2 on list (Tunnel10 vrf: global(0x0)

```
*Feb 1 01:31:46.040: NHRP: No delayed event node found.
*Feb 1 01:31:46.040: NHRP: There is no VPE Extension to construct for the request
```

Zodra het Spoke1 NHRP proces begint, tonen de logboeken aan dat het apparaat het NHRP resolutieverzoek verzendt. Het pakket bevat belangrijke informatie zoals het src NMBA en src protocol die het NBMA IP-adres en het tunnelIP-adres van de spaak zijn (Spoke1). U kunt ook de dst protocol waarde zien die het tunnel IP adres van de bestemming heeft gesproken (Spoke2). Dit duidt erop dat Spoke1 het NBMA-adres van Spoke2 aanvraagt om de mapping te voltooien. Ook op het pakket, kunt u de gevraagde waarde vinden die u kan helpen het pakket langs de weg volgen. Deze waarde blijft gedurende het hele proces gelijk en kan nuttig zijn om een specifieke stroom van de NHRP-onderhandeling te volgen. Het pakket heeft andere waarden die belangrijk zijn voor de onderhandeling, zoals de NHRP-verificatietekenreeks.

Nadat het apparaat het NHRP-resolutieverzoek verstuurt, tonen de logboeken aan dat een hertransmissie wordt verstuurd. Dit komt doordat het apparaat de NHRP resolutie respons niet ziet, waardoor het pakket opnieuw verstuurd wordt. Aangezien Spoke1 de reactie niet ziet, is het noodzakelijk om dat pakket op het volgende apparaat in de weg te volgen, die de HUB betekent.

HUB debug uitvoer:

<#root>

```
*Feb 1 01:31:34.262:
NHRP: Receive Resolution Request via Tunnel10 vrf: global(0x0), packet size: 85

*Feb 1 01:31:34.262: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 1 01:31:34.262: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 1 01:31:34.263: pktsz: 85 extoff: 52
*Feb 1 01:31:34.263: (M) flags: "router auth src-stable nat ",
reqid: 10

*Feb 1 01:31:34.263:
src NBMA: 172.21.100.1

*Feb 1 01:31:34.263:
src protocol: 10.10.10.1, dst protocol: 10.10.10.2

*Feb 1 01:31:34.263: (C-1) code: no error(0), flags: none
*Feb 1 01:31:34.263: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:34.263: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 1 01:31:34.263: Responder Address Extension(3):
*Feb 1 01:31:34.263: Forward Transit NHS Record Extension(4):
*Feb 1 01:31:34.263: Reverse Transit NHS Record Extension(5):
*Feb 1 01:31:34.263: Authentication Extension(7):
*Feb 1 01:31:34.263: type:Cleartext(1), data:DMVPN
*Feb 1 01:31:34.263: NAT address Extension(9):
*Feb 1 01:31:34.263: NHRP-DETAIL: netid_in = 10, to_us = 0
*Feb 1 01:31:34.263: NHRP-DETAIL:
```

Resolution request for afn 1 received on interface Tunnel10

 , for vrf: global(0x0) label: 0
*Feb 1 01:31:34.263: NHRP-DETAIL: Multipath IP route lookup for 10.10.10.2 in vrf: global(0x0) yielded
*Feb 1 01:31:34.263: NHRP:

Route lookup for destination 10.10.10.2

 in vrf: global(0x0) yielded interface Tunnel10, prefixlen 24
*Feb 1 01:31:34.263: NHRP-DETAIL: netid_out 10, netid_in 10
*Feb 1 01:31:34.263: NHRP: Forwarding request due to authoritative request.
*Feb 1 01:31:34.263: NHRP-ATTR:

NHRP Resolution Request packet is forwarded to 10.10.10.2 using vrf: global(0x0)

*Feb 1 01:31:34.263: NHRP: Attempting to forward to destination: 10.10.10.2 vrf: global(0x0)
*Feb 1 01:31:34.264: NHRP: Forwarding: NHRP SAS picked source: 10.10.10.10 for destination: 10.10.10.2
*Feb 1 01:31:34.264: NHRP: Attempting to send packet through interface Tunnel10 via DEST dst 10.10.10.2
*Feb 1 01:31:34.264: NHRP-DETAIL: First hop route lookup for 10.10.10.2 yielded 10.10.10.2, Tunnel10
*Feb 1 01:31:34.264: NHRP:

Forwarding Resolution Request via Tunnel10 vrf: global(0x0), packet size: 105

*Feb 1 01:31:34.264: src: 10.10.10.10, dst: 10.10.10.2
*Feb 1 01:31:34.264: (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Feb 1 01:31:34.264: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 1 01:31:34.264: pktsz: 105 extoff: 52
*Feb 1 01:31:34.264: (M) flags: "router auth src-stable nat ",

reqid: 10

*Feb 1 01:31:34.264:

src NBMA: 172.21.100.1

*Feb 1 01:31:34.264:

src protocol: 10.10.10.1, dst protocol: 10.10.10.2

*Feb 1 01:31:34.264: (C-1) code: no error(0), flags: none
*Feb 1 01:31:34.264: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:34.264: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 1 01:31:34.264: Responder Address Extension(3):
*Feb 1 01:31:34.264: Forward Transit NHS Record Extension(4):
*Feb 1 01:31:34.264: (C-1)

code: no error(0)

, flags: none
*Feb 1 01:31:34.264: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:34.264: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 1 01:31:34.264:

client NBMA: 172.20.10.10

*Feb 1 01:31:34.264:

client protocol: 10.10.10.10

*Feb 1 01:31:34.264: Reverse Transit NHS Record Extension(5):

```
*Feb 1 01:31:34.264: Authentication Extension(7):
*Feb 1 01:31:34.264: type:Cleartext(1),
```

data:DMVPN

```
*Feb 1 01:31:34.265: NAT address Extension(9):
*Feb 1 01:31:34.265: NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address: 172.22.20
*Feb 1 01:31:34.265: NHRP: 129 bytes out Tunnel10
```

Met behulp van de waarde van de vereiste, kunt u zien dat de HUB de resolutie aanvraag verzonden door Spoke1 ontvangt. In het pakket, zijn de waarden van src NBMA en src protocol de informatie van Spoke1, en de waarde van dst protocol is de tunnel IP van Spoke2, zoals het op de debugs van Spoke1 werd gezien. Wanneer de HUB het resolutieverzoek ontvangt, voert het een routerraadpleging uit en stuurt het pakket door naar Spoke2. In het doorgestuurde pakket, voegt de HUB een uitbreiding toe die zijn eigen informatie (NBMA IP adres en tunnel IP adres) bevat.

De vorige debugs tonen aan dat de HUB het resolutieverzoek om te spreken 2 correct doorstuurt. Daarom is de volgende stap te bevestigen Spoke2 ontvangt het, verwerkt het correct, en het verzenden van het resolutieantwoord naar Spoke1.

Spoke2 debug uitvoer:

<#root>

```
---------- [IKE/IPSEC DEBUG OUTPUTS OMITTED]----------

*Feb 1 01:31:34.647: ISAKMP: (1015):
```

Old State = IKE_QM_IPSEC_INSTALL_AWAIT New State = IKE_QM_PHASE2_COMPLETE

```
*Feb 1 01:31:34.647: NHRP: Process delayed resolution request src:10.10.10.1 dst:10.10.10.2 vrf: global
*Feb 1 01:31:34.648: NHRP-DETAIL: Resolution request for afn 1 received on interface Tunnel10 , for vrf
*Feb 1 01:31:34.648: NHRP-DETAIL: Multipath IP route lookup for 10.10.10.2 in vrf: global(0x0) yielded
*Feb 1 01:31:34.648: NHRP:
```

Route lookup for destination 10.10.10.2 in vrf: global(0x0) yielded interface Tunnel10, prefixlen 24

```
*Feb 1 01:31:34.648: NHRP-ATTR: smart spoke feature and attributes are not configured
*Feb 1 01:31:34.648:
```

NHRP:

Request was to us. Process the NHRP Resolution Request.

```
*Feb 1 01:31:34.648: NHRP-DETAIL: Multipath IP route lookup for 10.10.10.2 in vrf: global(0x0) yielded
*Feb 1 01:31:34.648: NHRP: nhrp_rtlookup for 10.10.10.2 in vrf: global(0x0) yielded interface Tunnel10,
*Feb 1 01:31:34.648: NHRP: Request was to us, responding with ouraddress
*Feb 1 01:31:34.648: NHRP: Checking for delayed event 10.10.10.1/10.10.10.2 on list (Tunnel10 vrf: glob
*Feb 1 01:31:34.648: NHRP: No delayed event node found.
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10: Checking to see if we need to delay for src 172.22.200.2 dst
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10: crypto_ss_listen_start already listening
```

```
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): Opening a socket with profile IPSE
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): connection lookup returned 80007F1
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): Socket is already open. Ignoring.
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): connection lookup returned 80007F1
*Feb 1 01:31:34.648: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): tunnel is already open!
*Feb 1 01:31:34.648: NHRP: No need to delay processing of resolution event NBMA src:172.22.200.2 NBMA d
*Feb 1 01:31:34.648: NHRP-MEF: No vendor private extension in NHRP packet
*Feb 1 01:31:34.649: NHRP-CACHE: Tunnel10: Cache update for target 10.10.10.1/32 vrf: global(0x0) label
*Feb 1 01:31:34.649: 172.21.100.1 (flags:0x2080)
*Feb 1 01:31:34.649: NHRP:
```

Adding Tunnel Endpoints (VPN: 10.10.10.1, NBMA: 172.21.100.1)

```
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10: crypto_ss_listen_start already listening
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): Opening a socket with profile IPSE
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): connection lookup returned 80007F1
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): Found an existing tunnel endpoint
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): tunnel_protection_stop_pending_tim
*Feb 1 01:31:34.649: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): Socket is already open. Ignoring.
*Feb 1 01:31:34.653:
```

NHRP: Successfully attached NHRP subblock for Tunnel Endpoints (VPN: 10.10.10.1, NBMA: 172.21.100.1)

```
*Feb 1 01:31:34.653: NHRP: Peer capability:0
*Feb 1 01:31:34.653: NHRP-CACHE: Inserted subblock node(1 now) for cache: Target 10.10.10.1/32 nhop 10.
*Feb 1 01:31:34.653: NHRP-CACHE: Converted internal dynamic cache entry for 10.10.10.1/32 interface Tun
*Feb 1 01:31:34.653: NHRP-EVE: NHP-UP: 10.10.10.1, NBMA: 172.21.100.1
*Feb 1 01:31:34.653: NHRP-MEF: No vendor private extension in NHRP packet
*Feb 1 01:31:34.653: NHRP-CACHE: Tunnel10: Internal Cache add for target 10.10.10.2/32 vrf: global(0x0)
*Feb 1 01:31:34.653: 172.22.200.2 (flags:0x20)
*Feb 1 01:31:34.653: NHRP: Attempting to send packet through interface Tunnel10 via DEST dst 10.10.10.1
*Feb 1 01:31:34.654: NHRP-DETAIL: First hop route lookup for 10.10.10.1 yielded 10.10.10.1, Tunnel10
*Feb 1 01:31:34.654:
```

NHRP: Send Resolution Reply via Tunnel10 vrf: global(0x0), packet size: 133

```
*Feb 1 01:31:34.654: src: 10.10.10.2, dst: 10.10.10.1
*Feb 1 01:31:34.654: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 1 01:31:34.654: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 1 01:31:34.654: pktsz: 133 extoff: 60
*Feb 1 01:31:34.654: (M) flags: "router auth dst-stable unique src-stable nat ",
```

reqid: 10

```
*Feb 1 01:31:34.654:
```

src NBMA: 172.21.100.1

```
*Feb 1 01:31:34.654:
```

src protocol: 10.10.10.1, dst protocol: 10.10.10.2

```
*Feb 1 01:31:34.654: (C-1) code: no error(0), flags: none
*Feb 1 01:31:34.654: prefix: 32, mtu: 9976, hd_time: 599
*Feb 1 01:31:34.654: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 1 01:31:34.654:
```

client NBMA: 172.22.200.2

```
*Feb 1 01:31:34.654:
client protocol: 10.10.10.2


*Feb 1 01:31:34.654: Responder Address Extension(3):
*Feb 1 01:31:34.654: (C) code: no error(0), flags: none
*Feb 1 01:31:34.654: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:34.654: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 1 01:31:34.654:
client NBMA: 172.22.200.2


*Feb 1 01:31:34.654:
client protocol: 10.10.10.2


*Feb 1 01:31:34.654: Forward Transit NHS Record Extension(4):
*Feb 1 01:31:34.654: (C-1) code: no error(0), flags: none
*Feb 1 01:31:34.654: prefix: 0, mtu: 9976, hd_time: 600
*Feb 1 01:31:34.654: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 1 01:31:34.654:
client NBMA: 172.20.10.10


*Feb 1 01:31:34.654:
client protocol: 10.10.10.10


*Feb 1 01:31:34.654: Reverse Transit NHS Record Extension(5):
*Feb 1 01:31:34.654: Authentication Extension(7):
*Feb 1 01:31:34.654: type:Cleartext(1),
data:DMVPN


*Feb 1 01:31:34.655: NAT address Extension(9):
*Feb 1 01:31:34.655: NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA Address: 172.21.10
*Feb 1 01:31:34.655: NHRP: 157 bytes out Tunnel10
*Feb 1 01:31:34.655: IPSEC-IFC MGRE/Tu10(172.22.200.2/172.21.100.1): connection lookup returned 80007F1
*Feb 1 01:31:34.655: NHRP-DETAIL: Deleted delayed event on interfaceTunnel10 dest: 172.21.100.1
```

De gevraagde waarde komt overeen met de waarde die in de vorige uitgangen wordt gezien, hiermee wordt bevestigd dat het NHRP-resolutieverzoekpakket verzonden door Spoke1 Spoke2 bereikt. Dit pakket leidt tot een routeraadpleging op Spoke2, en realiseert zich dat het resolutieverzoek voor zich is, daarom voegt Spoke2 de informatie van Spoke1 aan zijn NHRP-tabel toe. Alvorens het pakket van het resolutieantwoord terug naar Spoke1 te verzenden, voegt het apparaat zijn eigen informatie (NBMA IP adres en tunnel IP adres) toe zodat Spoke1 dat pakket kan gebruiken om die informatie aan zijn gegevensbestand toe te voegen.

Gebaseerd op alle debugs die gezien zijn, komt het NHRP Resolution Reply van Spoke2 niet aan bij Spoke1. De HUB kan worden verwijderd van het probleem terwijl het pakket met de NHRP-oplossingsaanvraag wordt ontvangen en doorgestuurd zoals verwacht. Daarom is de volgende stap om opnamen te maken tussen Spoke1 en Spoke2 om meer details te krijgen over de kwestie.

Ingesloten pakketvastlegging

Met de functie voor ingesloten pakketvastlegging kunt u het verkeer dat door het apparaat loopt, analyseren. De eerste stap om dit te configureren is het maken van een toegangslijst met het verkeer dat u op beide verkeersstromen wilt opnemen (inkomend en uitgaand).

Voor dit scenario worden de NBMA IP-adressen gebruikt:

```
ip access-list extended filter
10 permit ip host 172.21.100.1 host 172.22.200.2
20 permit ip host 172.22.200.2 host 172.21.100.1
```

Configureer vervolgens de opname met de opdrachtmonitor Capture <CAPTURE_NAME>, toegangslijst <ACL_NAME>, buffergrootte 10, interface <WAN_INTERFACE> en start de opname met de opdrachtmonitor Capture_NAME> start.

Capture configuratie op Spoke1 en Spoke2:

```
monitor capture CAP access-list filter buffer size 10 interface GigabitEthernet1 both
monitor capture CAP start
```

Om de output van de opname weer te geven gebruikt u de opdracht monitor Capture <CAPTURE_NAME> buffer memorandum.

Capture output Spoke1:

<#root>

```
SPOKE1#show monitor capture CAP buffer brief
------------------------------------------------------------------------------
#   size   timestamp     source             destination      dscp    protocol
------------------------------------------------------------------------------
   0  210    0.000000   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   1  150    0.014999   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   2  478    0.028990   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   3  498    0.049985   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   4  150    0.069988   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   5  134    0.072994   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   6  230    0.074993   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   7  230    0.089992   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   8  118    0.100993   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   9  218    0.108988   172.22.200.2    ->  172.21.100.1     48 CS6  ESP
  10   70    0.108988   172.21.100.1    ->  172.22.200.2     0  BE   ICMP
```

```
  11  218    1.907994   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

  12   70    1.907994   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

  13  218    5.818003   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

  14   70    5.818003   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

  15  218   12.559969   172.22.200.2    ->  172.21.100.1    48 CS6  ESP

  16   70   12.559969   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

  17  218   26.859001   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

  18   70   26.859001   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

  19  218   54.378978   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

  20   70   54.378978   172.21.100.1    ->  172.22.200.2     0  BE   ICMP
```

Capture output Spoke2:

<#root>

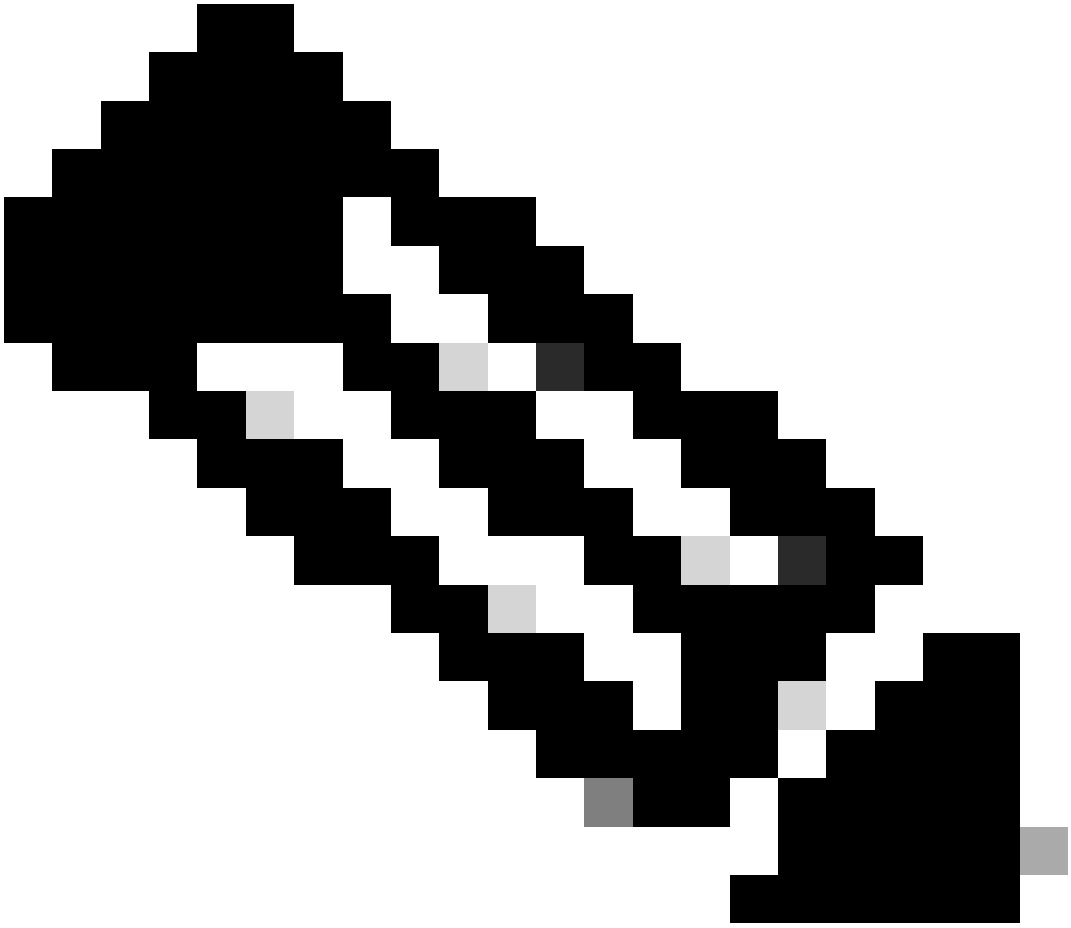
```
SPOKE2#show monitor capture CAP buffer brief
------------------------------------------------------------------------
#   size   timestamp     source             destination      dscp    protocol
------------------------------------------------------------------------
   0  210    0.000000   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   1  150    0.015990   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   2  478    0.027998   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   3  498    0.050992   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   4  150    0.069988   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   5  134    0.072994   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   6  230    0.074993   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
   7  230    0.089992   172.21.100.1    ->  172.22.200.2     48 CS6  UDP
   8  118    0.099986   172.22.200.2    ->  172.21.100.1     48 CS6  UDP
```

```
9  218    0.108988   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

  10   70    0.108988   172.21.100.1    ->  172.22.200.2     0  BE   ICMP
```

```
11  218    1.907994   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

12   70    1.909001   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

13  218    5.817011   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

14   70    5.818002   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

15  218   12.559968   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

16   70   12.560960   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

17  218   26.858009   172.22.200.2    ->  172.21.100.1     48 CS6  ESP

18   70   26.859001   172.21.100.1    ->  172.22.200.2     0  BE   ICMP

19  218   54.378978   172.22.200.2   ->  172.21.100.1     48 CS6  ESP

20   70   54.379970   172.21.100.1    ->  172.22.200.2     0  BE   ICMP
```

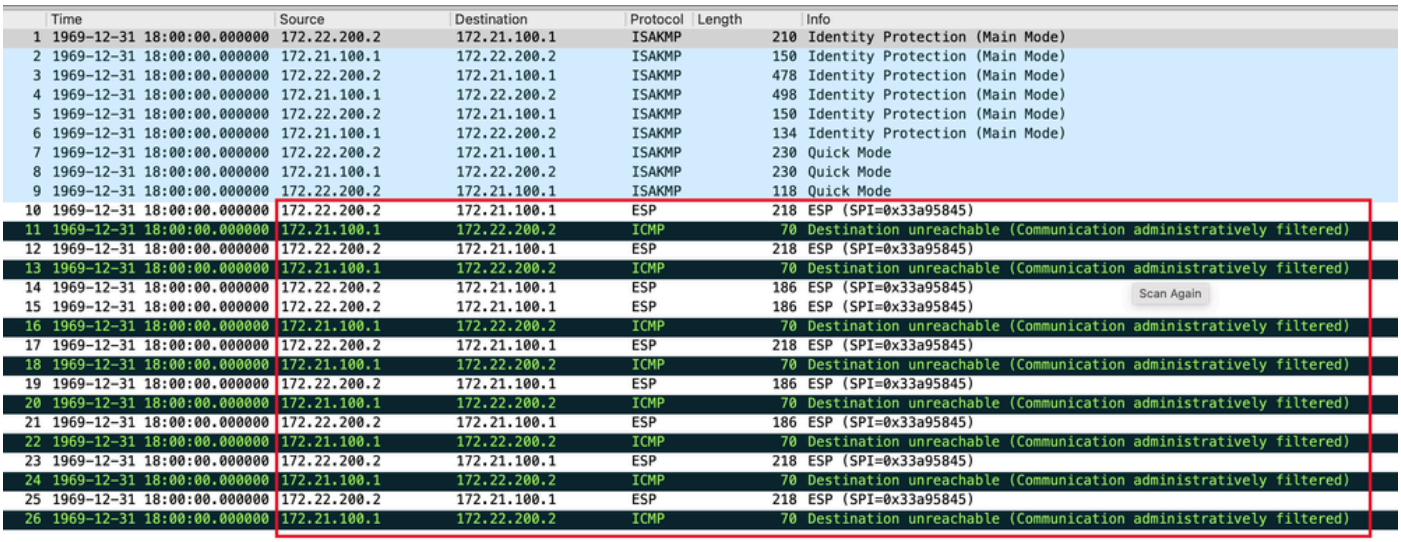
De output van de opnamen laat zien dat de eerste pakketten UDP-verkeer zijn, dat op de IKE/IPSEC-onderhandeling wijst. Daarna verstuurt Spoke2 de resolutie naar Spoke1, wat wordt gezien als ESP-verkeer (pakket 9). Hierna is de verwachte verkeersstroom in ESP, maar het volgende pakket dat wordt gezien is ICMP-verkeer dat van Spoke1 naar Spoke2 komt.

Om het pakket dieper te analyseren, kunt u het pcap-bestand van het apparaat exporteren door de opdracht monitor opname <CAPTURE_NAME> buffer dump uit te voeren. Gebruik vervolgens een decoder om de dump uitvoer naar een pcap bestand te converteren, zodat u het kunt openen met Wireshark.



Opmerking: Cisco heeft een pakketanalyzer waar u opnameconfiguratie, voorbeelden en een decoder kunt vinden: Cisco TAC Tool - Packet Capture Config Generator en Analyzer

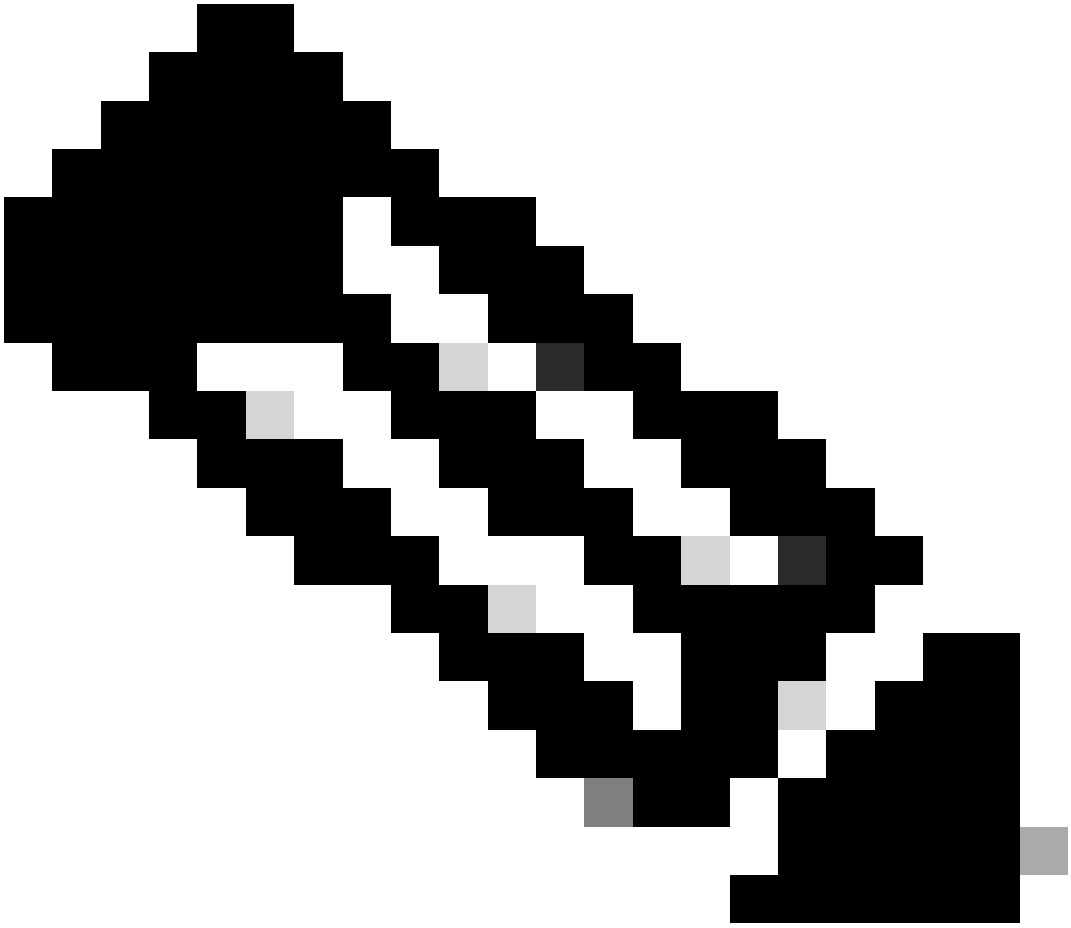
Wireshark-uitvoer:



	Time	Source	Destination	Protocol	Length	Info
1	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ISAKMP	210	Identity Protection (Main Mode)
2	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ISAKMP	150	Identity Protection (Main Mode)
3	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ISAKMP	478	Identity Protection (Main Mode)
4	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ISAKMP	498	Identity Protection (Main Mode)
5	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ISAKMP	150	Identity Protection (Main Mode)
6	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ISAKMP	134	Identity Protection (Main Mode)
7	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ISAKMP	230	Quick Mode
8	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ISAKMP	230	Quick Mode
9	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ISAKMP	118	Quick Mode
10	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	218	ESP (SPI=0x33a95845)
11	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
12	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	218	ESP (SPI=0x33a95845)
13	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
14	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	186	ESP (SPI=0x33a95845)
15	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	186	ESP (SPI=0x33a95845)
16	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
17	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	218	ESP (SPI=0x33a95845)
18	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
19	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	186	ESP (SPI=0x33a95845)
20	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
21	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	186	ESP (SPI=0x33a95845)
22	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
23	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	218	ESP (SPI=0x33a95845)
24	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)
25	1969-12-31 18:00:00.000000	172.22.200.2	172.21.100.1	ESP	218	ESP (SPI=0x33a95845)
26	1969-12-31 18:00:00.000000	172.21.100.1	172.22.200.2	ICMP	70	Destination unreachable (Communication administratively filtered)

Capture Output op WirelessShark

De inhoud van het ICMP-pakket heeft de foutmelding Bestemming onbereikbaar (administratief gefilterde communicatie). Dit geeft aan dat er een soort filter is, zoals een router ACL of firewall die het verkeer langs het pad beïnvloedt. Meestal wordt het filter ingesteld op het apparaat dat het pakket verstuurt (in dit geval Spoke1), maar middelmatige apparaten kunnen het ook versturen.



Opmerking: De Wireshark uitvoer is hetzelfde op beide spokes.

Cisco IOS® XE Datapath-pakkettractiefunctie

De eigenschap van het pakketspoor van Cisco IOS XE wordt gebruikt om te analyseren hoe het apparaat het verkeer verwerkt. Om het te configureren moet u een toegangslijst maken met het verkeer dat u op beide verkeersstromen wilt opnemen (inkomend en uitgaand).

Voor dit scenario worden de NBMA IP-adressen gebruikt.

```
ip access-list extended filter
10 permit ip host 172.21.100.1 host 172.22.200.2
20 permit ip host 172.22.200.2 host 172.21.100.1
```

Dan, vorm de fia-spooreigenschap en plaats de het zuiveren voorwaarde om de toegang-lijst te

gebruiken. Start de conditionering.

```
debug platform packet-trace packet 1024 fia-trace
debug platform condition ipv4 access-list filter both
debug platform condition start
```

- debug platform pakkettraceerpakket <count> fia-trace: maakt gedetailleerde fia-tracering mogelijk en stopt deze zodra de hoeveelheid geconfigureerde pakketten is opgenomen
- debug platform voorwaarde ipv4 access-list <ACL-NAME> beiden: stelt een voorwaarde op het apparaat in met behulp van de eerder geconfigureerde toegangslijst
- debug platform voorwaarde start: start de voorwaarde

Om de output van het fia-spoor te herzien gebruik de volgende bevelen.

```
show platform packet-trace statistics
show platform packet-trace summary
show platform packet-trace packet <number>
```

Spoke1 toont output van pakketsporenstatistieken:

<#root>

```
SPOKE1#show platform packet-trace statistics
Packets Summary
  Matched  18
  Traced   18
Packets Received
  Ingress  11
  Inject   7
    Count       Code  Cause
    4           2     QFP destination lookup
    3           9     QFP ICMP generated packet
Packets Processed
  Forward  7
  Punt     8
    Count       Code  Cause
    5           11    For-us data
    3           26    QFP ICMP generated packet
  Drop     3
    Count       Code  Cause
    3           8     Ipv4Acl
  Consume  0
```

```
          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              5
IP               0              0              5
IPV6             0              0              0
ARP              0              0              0

          PKT_DIR_OUT
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0
```

In de output van de pakketsporenstatistieken van het showplatform, kunt u de tellers voor de pakketten zien die door het apparaat worden verwerkt. Zo kunt u de inkomende en uitgaande pakketten zien en controleren of het apparaat pakketten laat vallen, samen met de reden van de val.

In de getoonde output laat Spoke1 een aantal pakketten met de beschrijving Ipv4Acl vallen. Om die pakketten verder te analyseren, kan de opdracht platform packet-trace samenvatting gebruiken.

Spoke1 toont platform pakkettracering samenvattende uitvoer:

<#root>

```
SPOKE1#show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
1     INJ.2                     Gi1                       FWD
2     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
3     INJ.2                     Gi1                       FWD
4     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     INJ.2                     Gi1                       FWD
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)

9     Gi1                       Gi1                       DROP   8   (Ipv4Acl)


10    Gi1                       internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
11    INJ.9                     Gi1                       FWD

12    Gi1                       Gi1                       DROP   8   (Ipv4Acl)


13    Gi1                       internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
14    INJ.9                     Gi1                       FWD

15    Gi1                       Gi1                       DROP   8   (Ipv4Acl)
```

```
16    Gi1                     internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
17    INJ.9                   Gi1                       FWD
18    Gi1                     Gi1                       DROP   8   (Ipv4Acl)
19    Gi1                     internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
20    INJ.9                   Gi1                       FWD
21    Gi1                     Gi1                       DROP   8   (Ipv4Acl)
22    Gi1                     internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
23    INJ.9                   Gi1                       FWD
24    Gi1                     Gi1                       DROP   8   (Ipv4Acl)
25    Gi1                     internal0/0/recycle:0     PUNT   26  (QFP ICMP generated packet)
26    INJ.9                   Gi1                       FWD
```

Met deze uitvoer kunt u elk pakket zien dat het apparaat aankomt en verlaat, evenals de in- en uitgangen. De status van het pakket wordt ook getoond, erop wijzend of het door:sturen, gelaten vallen, of intern verwerkt (punt).

In dit voorbeeld, deze output hielp om de pakketten te identificeren die door het apparaat worden gelaten vallen. Met de opdracht show platform packet-trace pakket <PACKET_NUMBER>, kunt u zien hoe het apparaat dat specifieke pakket verwerkt.

Spoke1 toont het pakket van het platform pakketspoor <PACKET_NUMBER> output:

<#root>

```
SPOKE1#show platform packet-trace packet 9
Packet: 9 CBUG ID: 9
Summary
Input : GigabitEthernet1

Output : GigabitEthernet1

State : DROP 8 (Ipv4Acl)

Timestamp
Start : 366032715676920 ns (02/01/2024 04:30:15.708990 UTC)
Stop : 366032715714128 ns (02/01/2024 04:30:15.709027 UTC)
Path Trace
  Feature: IPV4(Input)

Input : GigabitEthernet1

     Output : <unknown>
```

Source : 172.22.200.2

Destination : 172.21.100.1

Protocol : 50 (ESP)

Feature: DEBUG_COND_INPUT_PKT
Entry : Input - 0x812707d0

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 194 ns
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
Entry : Input - 0x8129bf74

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 769 ns
Feature: IPV4_INPUT_ARL_SANITY
Entry : Input - 0x812725cc

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 307 ns
Feature: EPC_INGRESS_FEATURE_ENABLE
Entry : Input - 0x812782d0

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 6613 ns
Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
Entry : Input - 0x8129bf70

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 272 ns
Feature: STILE_LEGACY_DROP
Entry : Input - 0x812a7650

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 278 ns
Feature: INGRESS_MMA_LOOKUP_DROP
Entry : Input - 0x812a1278

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 697 ns
Feature: INPUT_DROP_FNF_AOR
Entry : Input - 0x81297278

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 676 ns
Feature: INPUT_FNF_DROP
Entry : Input - 0x81280f24

Input : GigabitEthernet1

Output : <unknown>

Lapsed time : 1018 ns
Feature: INPUT_DROP_FNF_AOR_RELEASE
Entry : Input - 0x81297274

Input : GigabitEthernet1

Output : <unknown>

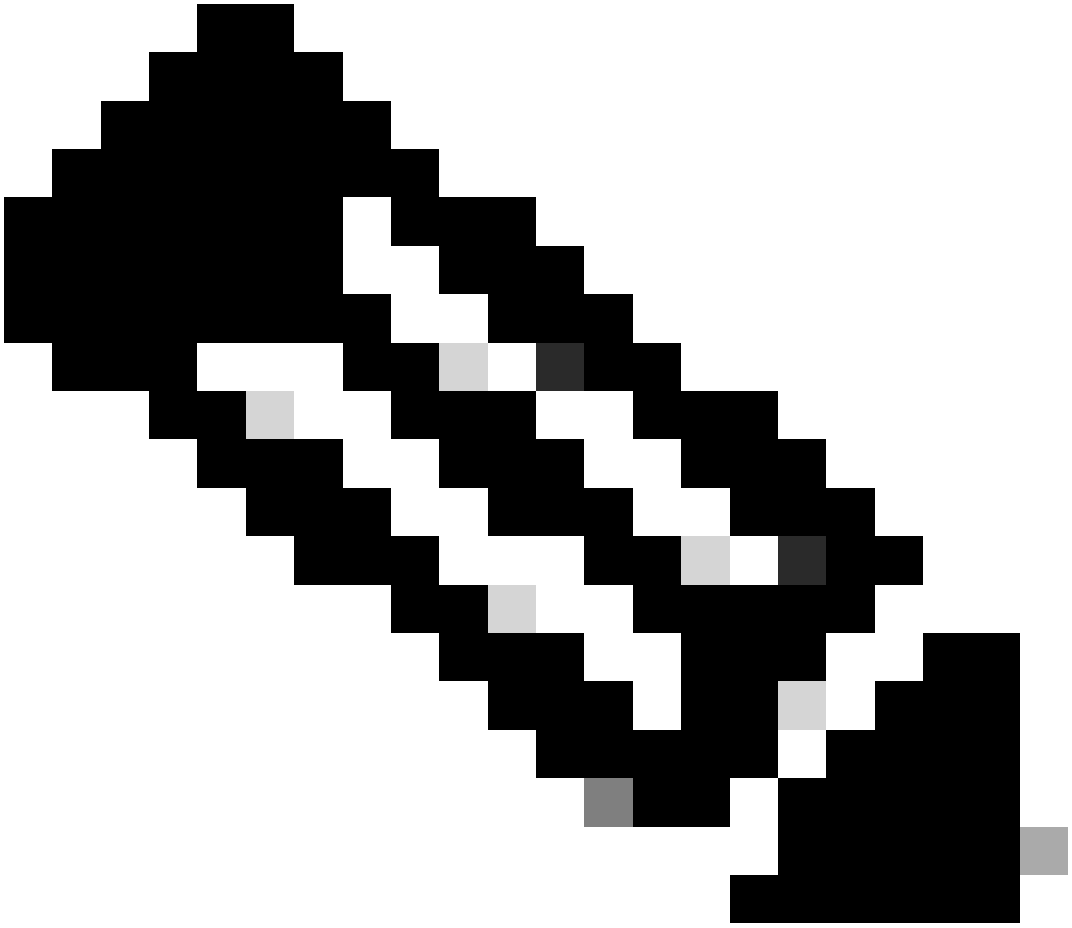
Lapsed time : 174 ns
Feature: INPUT_DROP

```
     Entry : Input - 0x8126e568

Input : GigabitEthernet1


     Output : <unknown>

     Lapsed time : 116 ns

Feature: IPV4_INPUT_ACL

     Entry : Input - 0x81271f70

Input : GigabitEthernet1


     Output : <unknown>

     Lapsed time : 12915 ns
```

In het eerste deel, kunt u de in- en uitgang interface, en de staat van het pakket zien. Dit wordt gevolgd door het tweede deel van de output waar u de bron en bestemmingsIP adressen en het protocol kunt vinden.

Elke volgende fase toont hoe het apparaat dit specifieke pakket verwerkt. Dit biedt inzichten in alle configuraties zoals Network Address Translation (NAT) of toegangslijsten of andere factoren die van invloed kunnen zijn op het netwerk.

In dit geval kan worden vastgesteld dat het pakketprotocol ESP is, de bron IP het NBMA IP-adres van Spoke2 is en de bestemming IP het NBMA IP-adres van Spoke1. Dit geeft aan dat dit het ontbrekende pakket is in de NHRP-onderhandeling. Ook wordt opgemerkt dat er in geen enkele fase een uitvalsinterface wordt gespecificeerd, wat suggereert dat iets het verkeer beïnvloedde voordat het kon worden doorgestuurd. Op de voorlaatste fase kunt u zien dat het apparaat het inkomende verkeer op de gespecificeerde interface laat vallen (Gigabit Ethernet1). De laatste fase toont een inkomende toegang-lijst, suggererend dat er één of andere configuratie op de interface kan zijn die de daling veroorzaakt.



Opmerking: als na het gebruik van alle tools voor probleemoplossing die in dit document worden vermeld, de spaken die betrokken zijn bij de onderhandeling geen tekenen tonen dat ze vallen of het verkeer beïnvloeden, dat de probleemoplossing op die apparaten beëindigt.

De volgende stap moet bestaan uit het controleren van middelste apparaten tussen deze apparaten, zoals firewalls, switches en ISP.

Oplossing

Als zo'n scenario wordt gezien, is de volgende stap om de interface te controleren die in de vorige uitgangen wordt getoond. Dit betekent dat de configuratie gecontroleerd moet worden om te controleren of er iets is dat het verkeer beïnvloedt.

WAN-interfaceconfiguratie:

<#root>

```
SPOKE1#show running-configuration interface gigabitEthernet1
Building configuration...

Current configuration : 150 bytes
!
interface GigabitEthernet1
ip address 172.21.100.1 255.255.255.0
ip access-group ESP_TRAFFIC in

negotiation auto
no mop enabled
no mop sysid
end
```

Als deel van zijn configuratie, heeft de interface een toegepaste toegang-groep. Het is belangrijk om te verifiëren dat de hosts die zijn geconfigureerd op de toegangslijst het verkeer dat wordt gebruikt voor de NHRP-onderhandeling niet storen.

<#root>

```
SPOKE1#show access-lists ESP_TRAFFIC
Extended IP access list ESP_TRAFFIC
10 deny esp host 172.21.100.1 host 172.22.200.2
20 deny esp host 172.22.200.2 host 172.21.100.1 (114 matches)

30 permit ip any any (22748 matches)
```

De tweede verklaring van de toegangslijst ontkent de communicatie tussen het NBMA IP-adres van Spoke2 en het NBMA IP-adres van Spoke1, waardoor de eerder waargenomen daling. Na het verwijderen van de toegangsgroep uit de interface, is de communicatie tussen de twee spokes succesvol:

```
SPOKE1#ping 192.168.2.2 source loopback1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/3 ms
```

De IPSEC-tunnel is omhoog en toont nu insluitingen en decaps op beide apparaten:

Gesproken1:

<#root>

```
SPOKE1#show crypto IPSEC sa peer 172.22.200.2

interface: Tunnel10
    Crypto map tag: Tunnel10-head-0, local addr 172.21.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.21.100.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.22.200.2/255.255.255.255/47/0)
   current_peer 172.22.200.2 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6



    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.21.100.1, remote crypto endpt.: 172.22.200.2
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0x9392DA81(2475874945)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xBF8F523D(3213840957)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2073, flow_id: CSR:73, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
         sa timing: remaining key lifetime (k/sec): (4607998/28783)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9392DA81(2475874945)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2074, flow_id: CSR:74, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
         sa timing: remaining key lifetime (k/sec): (4607999/28783)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Gesproken2:

<#root>

```
SPOKE2#show crypto IPSEC sa peer 172.21.100.1

interface: Tunnel10
    Crypto map tag: Tunnel10-head-0, local addr 172.22.200.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.22.200.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.21.100.1/255.255.255.255/47/0)
   current_peer 172.21.100.1 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7



    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.22.200.2, remote crypto endpt.: 172.21.100.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xBF8F523D(3213840957)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x9392DA81(2475874945)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2073, flow_id: CSR:73, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
         sa timing: remaining key lifetime (k/sec): (4607998/28783)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xBF8F523D(3213840957)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 2074, flow_id: CSR:74, sibling_flags FFFFFFFF80000008, crypto map: Tunnel10-head-0
         sa timing: remaining key lifetime (k/sec): (4607999/28783)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Nu toont de DMVPN-tabel van Spoke1 de juiste afbeelding op beide vermeldingen:

<#root>

```
SPOKE1#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override, B - BGP
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----


1 172.22.200.2     10.10.10.2    UP   00:01:31   D


     1 172.20.10.10     10.10.10.10    UP    1d05h     S
```

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.