DMVPN fase 1 Problemen oplossen

Inhoud

Inleiding

Dit document beschrijft de debug-berichten die u op het hub zou tegenkomen en sprak over een Dynamic Multipoint Virtual Private Network (DMVPN) fase 1.

Voorwaarden

Voor de configuratie en het debug van opdrachten in dit document hebt u twee Cisco-routers nodig die Cisco IOS release 12.4(9)T of hoger uitvoeren. In het algemeen is voor een basisDMVPN-fase 1 Cisco IOS release 12.2(13)T of hoger of release 12.2(33)XNC voor de aggregation services router (ASR) nodig, hoewel de functies en tekortkomingen die in dit document zijn gezien, mogelijk niet worden ondersteund.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Generic Routing Encapsulation (GRE)
- Next Hop Solutions Protocol (NHRP)
- Internet Security Association en Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Internet Protocol Security (IPSec)
- Ten minste één van deze routingprotocollen: Enhanced Interior Gateway Routing Protocol (DHCP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP) en Border Gateway Protocol (BGP)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 2911 geïntegreerde services routers (ISR's) die Cisco IOS release 15.1(4)M4 uitvoeren.

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 de potentiële impact van elke opdracht begrijpen.

Belangrijke verbeteringen

Deze Cisco IOS-versies hebben belangrijke functies of oplossingen voor DMVPN fase 1:

- release 12.2(18)SXF5 - betere ondersteuning voor ISAKMP bij gebruik van openbare sleutelinfrastructuur (PKI)
- release 12.2(33)XNE - ASR, IPSec-profielen, tunnelbescherming, IPSec Network-adresomzetting (NAT)
- release 12.3(7)T - ondersteuning voor interne routing en Forwarding (iVRF)
- release 12.3(11)T - ondersteuning voor voorwaartse virtuele routing en Forwarding (fVRF)
- release 12.4(9)T - ondersteuning voor verschillende DMVPN-gerelateerde debugs en opdrachten
- release 12.4(15)T - gedeelde tunnelbescherming
- release 12.4(20)T - IPv6 via DMVPN
- release 15.0(1)M - NHRP-tunnelbewaking

Conventies

Raadpleeg Cisco Technical Tips Convention voor informatie over documentconventies.

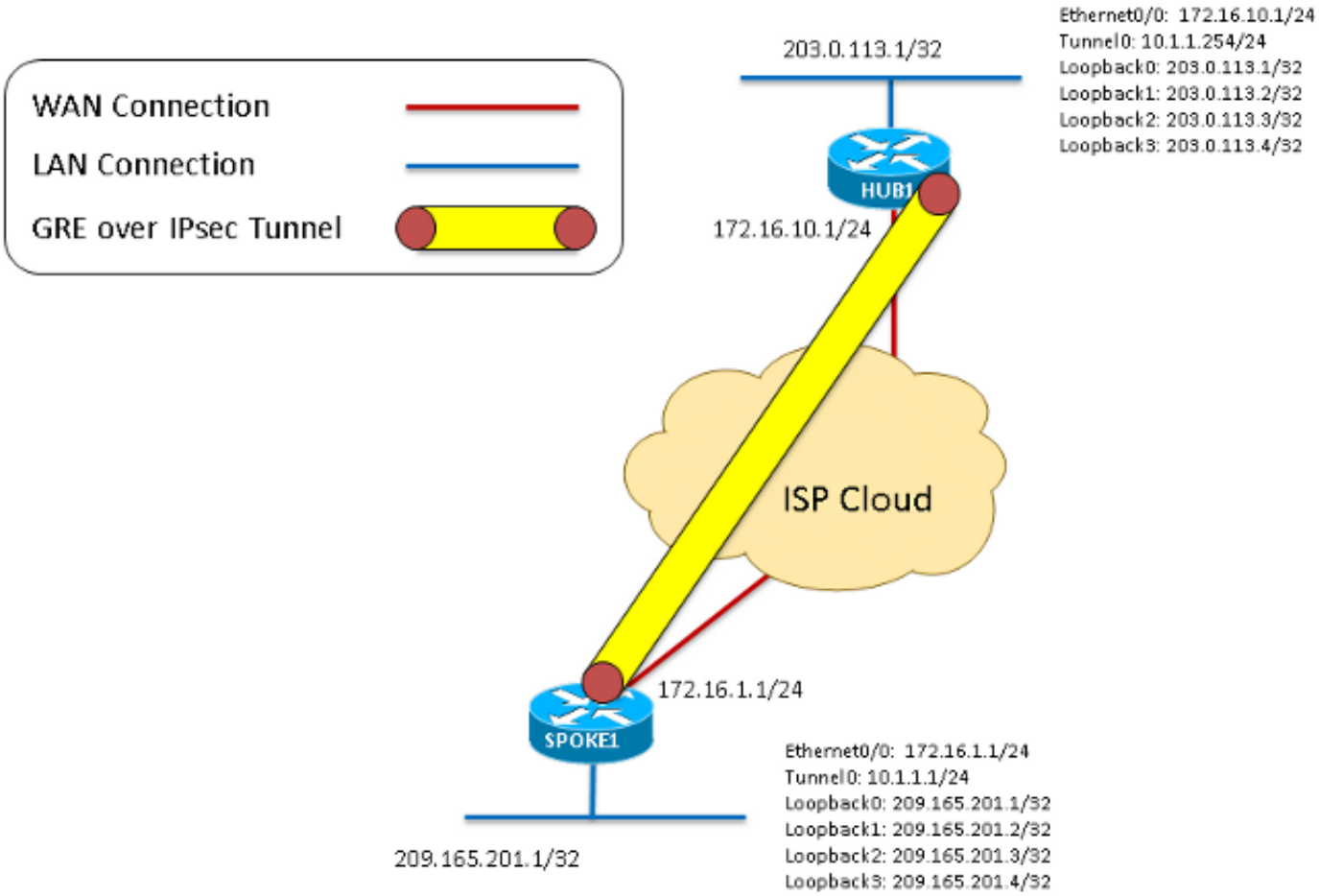
Relevante configuratie

Overzicht van topologie

Voor deze topologie werden twee 2911 ISR's die release 15.1(4)M4 uitvoeren, geconfigureerd voor DMVPN fase 1: een als een hub en een als een sprak. Ethernet0/0 werd gebruikt als de "internet"-interface op elke router. De vier loopback interfaces worden geconfigureerd om lokale gebiednetwerken te simuleren die op de hub of op een gesproken locatie wonen. Aangezien dit een DMVPN Phase 1 topologie is met slechts één gesproken, wordt de gesproken met een punt-

tot-punt GRE tunnel in plaats van een multipoint GRE-tunnel. Dezelfde crypto configuratie (ISAKMP en IPSec) werd gebruikt op elke router om er zeker van te zijn dat ze exact overeenkomen.

Afbeelding 1



Crypto

Dit is hetzelfde op de hub en de spits.

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

hub

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map multicast dynamic
```

```
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

Spoken

```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end

interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
```

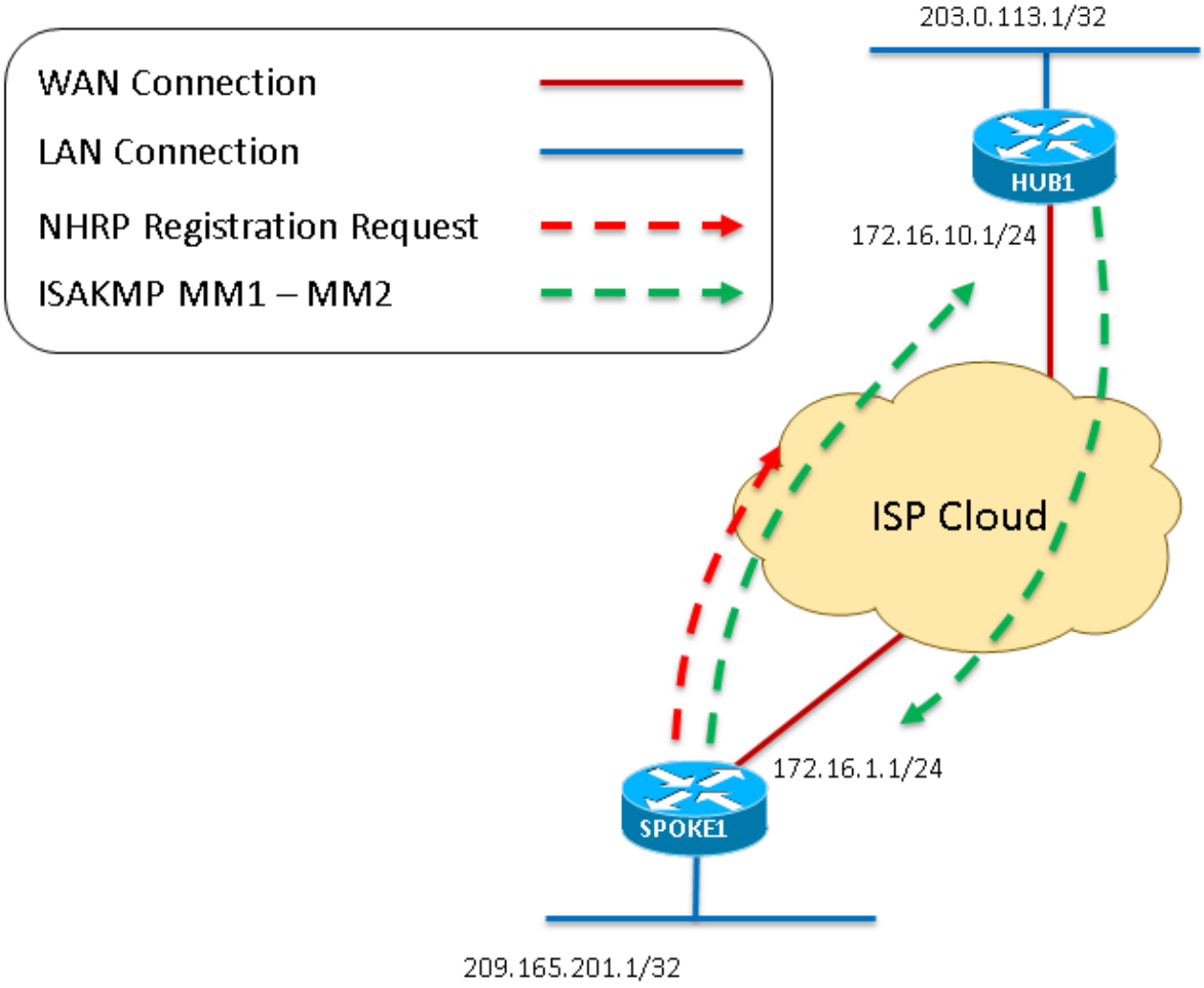
```
network 10.1.1.0 0.0.0.255
```

Debugs

Packet Flow-visualisatie

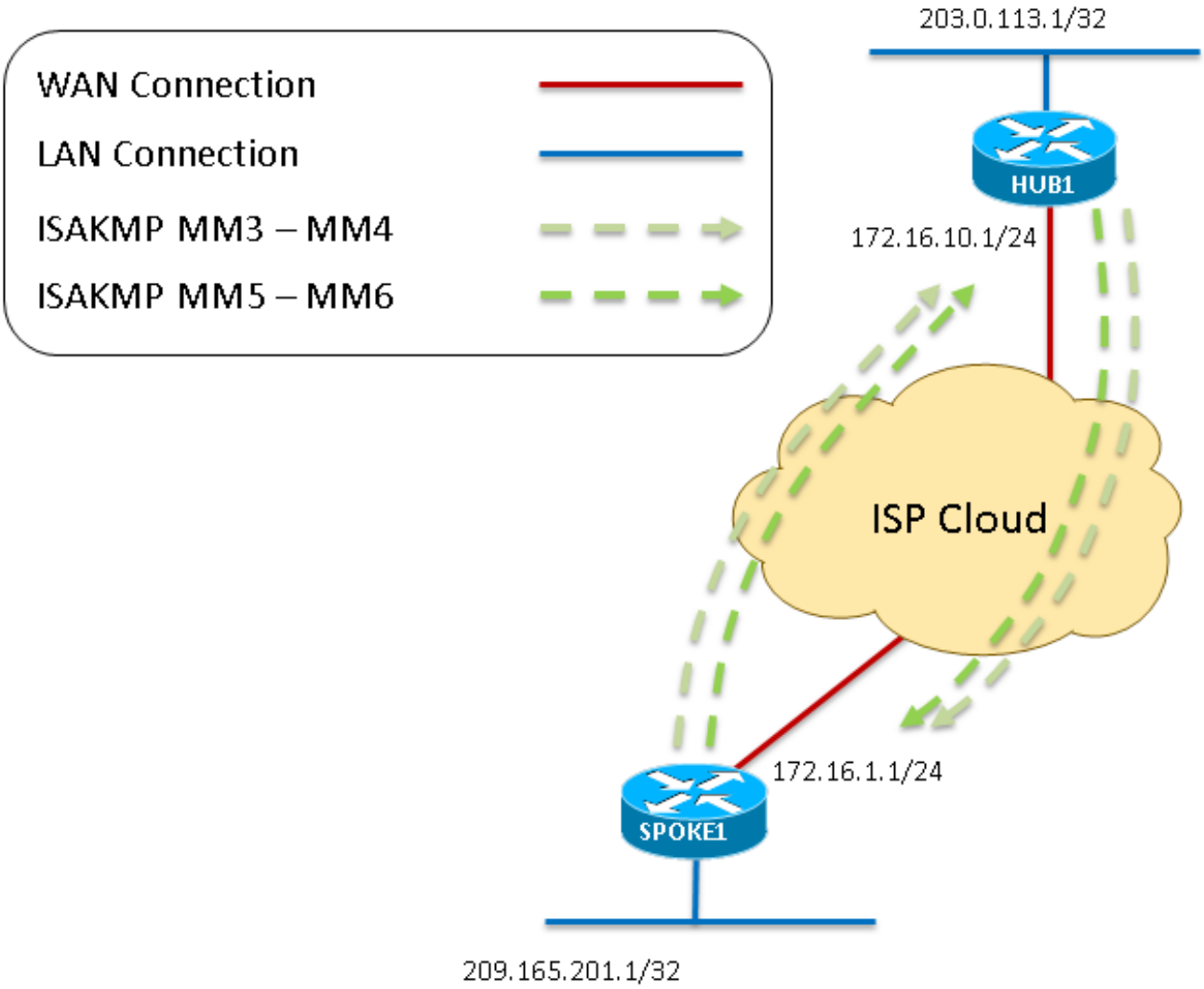
Dit is een visualisatie van de gehele DMVPN-pakketstroom zoals in dit document wordt weergegeven. Er zijn ook gedetailleerdere ideeën opgenomen die elk van de stappen verklaren.

1. Wanneer de Tunnel op Spoke "geen shutdown" is genereert het een NHRP Registratieaanvraag, die het DMVPN-proces start. Aangezien de configuratie van de hub volledig dynamisch is, moet de Spoke het eindpunt zijn dat de verbinding initieert.
2. Het NHRP-registratieverzoek wordt vervolgens ingekapseld in GRE, waardoor het cryptoproces wordt gestart.
3. Op dit moment wordt het eerste bericht met de ISAKMP-hoofdmodus (ISAKMP MM1) van de Spoke naar de hub van poort op UDP500 verzonden.
4. De hub ontvangt en verwerkt MM1 en reageert met ISAKMP MM2, omdat het een corresponderend ISAKMP-beleid heeft.
   Figuur 2 - verwijst naar stappen 1 t/m 4

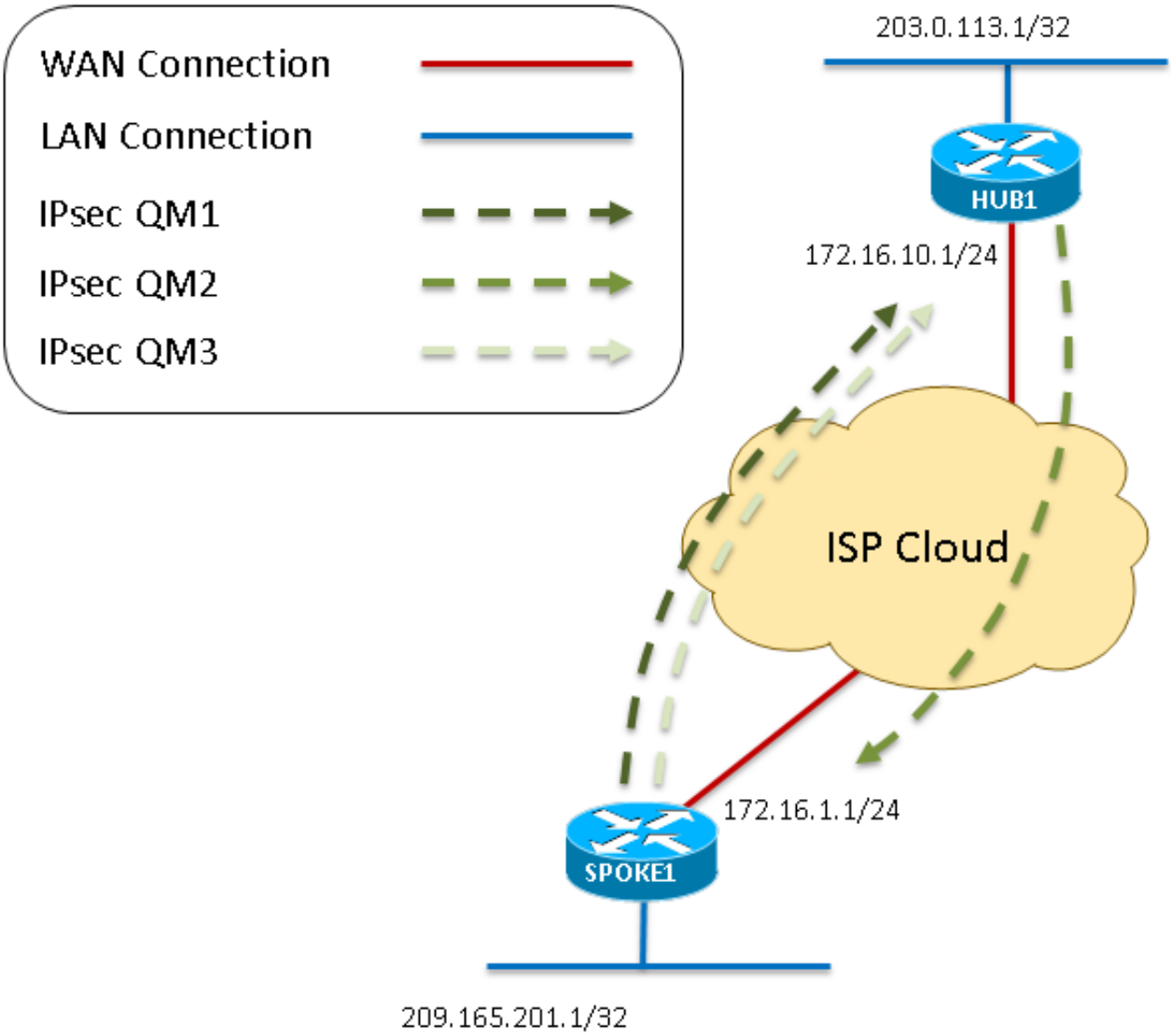


5. Zodra de Spoke de MM2 heeft ontvangen, reageert hij met MM3. Net als bij MM1 bevestigt de Spoke dat het ontvangen ISAKMP-beleid geldig is.
6. De hub ontvangt MM3 en reageert met MM4.

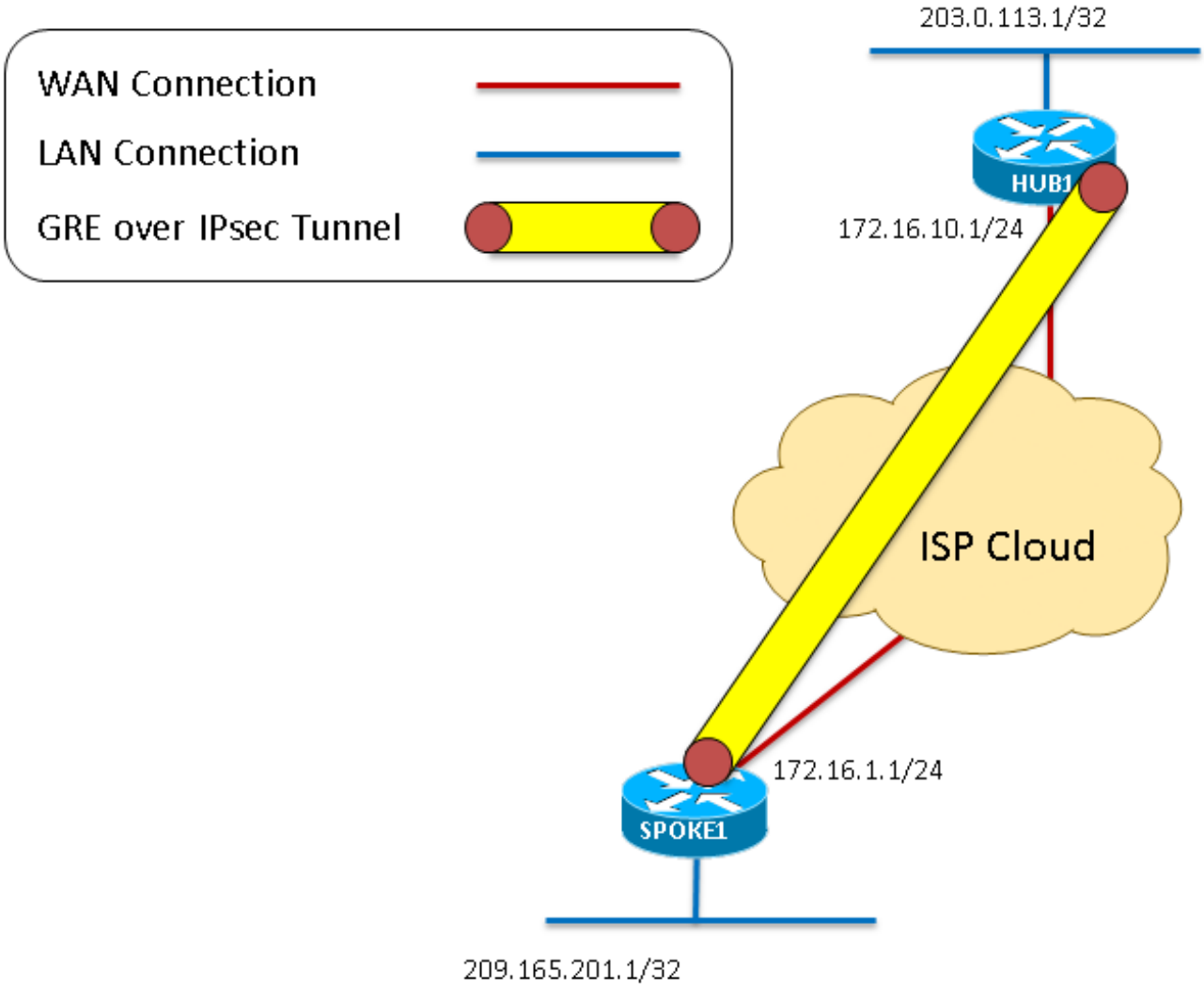
7. Op dit moment in de onderhandelingen met ISAKMP, zou de Spoke op port UDP4500 kunnen reageren als NAT wordt gedetecteerd in het doorvoerpad. Als echter geen NAT wordt gedetecteerd, gaat de Spoke door en verstuurt MM5 op UDP500. Ten slotte reageert de hub met MM6 om de hoofdmodus-uitwisseling te voltooien.
   Figuur 3 - verwijst naar stappen 5 t/m 7



8. Zodra de Spoke MM6 van de Hub ontvangt, stuurt het QM1 naar de Hub op UDP500 om de Snelle Modus te beginnen.
9. De hub ontvangt QM1 en reageert met QM2, omdat alle ontvangen eigenschappen worden geaccepteerd. Op dit punt creëert de hub de fase 2 SA's voor deze sessie.
10. Als laatste stap van de onderhandeling over de Quick Mode wordt QM2 door de Spoke ontvangen. The Spoke creëert vervolgens zijn fase 2 SA's en stuurt QM3 als antwoord. Dit is het afronden van de onderhandelingen tussen ISAKMP en IPSec. Er is nu een IPSec-sessie die GRE-verkeer tussen deze twee peers versleutelt.
    Figuur 4 - verwijst naar stappen 8 t/m 10

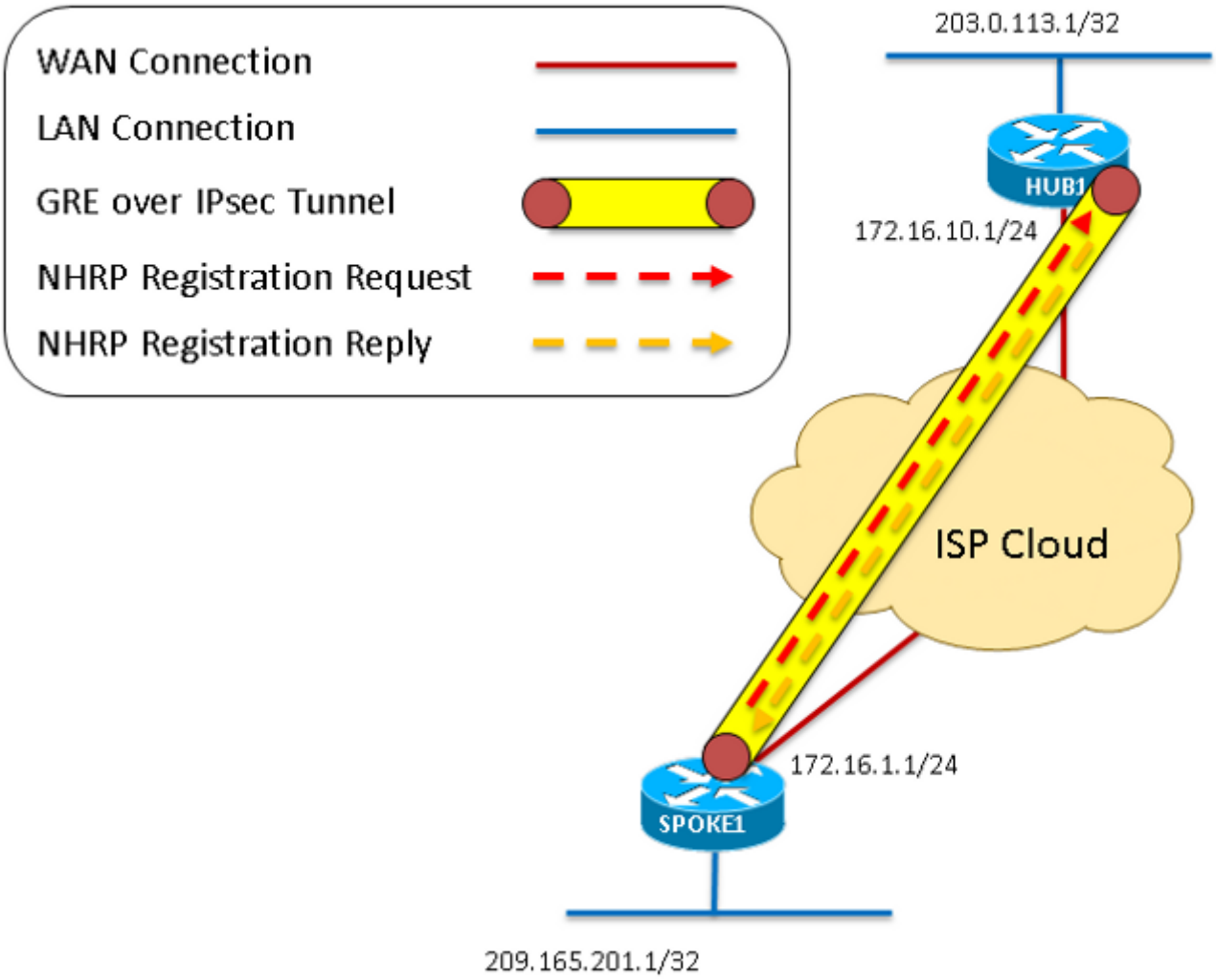


11. Nu de crypto sessie omhoog en door verkeer kan gaan, worden deze pakketten ingekapseld binnen de GRE over IPSec tunnel.
    Figuur 5 - verwijst naar stap
    11



12. Zoals in de eerste stappen werd gezien, genereert de Spoke een NHRP Registratieaanvraag die via de GRE via de IPSec-tunnel wordt verzonden.
13. De hub ontvangt de NHRP-registratieaanvragen en stuurt een NHRP-registratierapport nadat deze bevestigt dat de Spoke een geldig Tunnel- en niet-uitgezonden multiaccess-adres (NBMA) heeft. De Spoke ontvangt dit NHRP-registratieantwoord dat het registratieproces voltooit.

Figuur 6 - verwijst naar stappen 12 t/m 13



Deze termen zijn het resultaat wanneer het **debug dmvpn alle** opdracht op de hub en gesproken routers wordt ingevoerd. Deze specifieke opdracht maakt deze debugs mogelijk:

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug


NHRP:
NHRP protocol debugging is on
NHRP activity 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
IKEV2:
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail 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
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
```

Debugs met uitleg

Aangezien dit een configuratie is waar IPSec wordt geïmplementeerd, tonen de beelden alle ISAKMP en IPSec-uitvindingen. Als geen crypto is ingesteld, negeer dan alle uiteinden die met "IPsec" of "ISAKMP" beginnen.

HUB DEBUG-UITLEG	ACHTERVOLGENDE DEBUGS	UITLEG VAN SPO DEBUG
Deze eerste paar debug-berichten worden gegenereerd door een opdracht om **niet** uit te schakelen in de tunnelinterface. Berichten worden gegenereerd door crypto-, GRE- en NHRP-diensten die worden gestart. Een NHRP-registratiefout wordt op een hub gezien omdat deze geen geconfigureerde Next Hop Server (NHS) heeft (de hub is de NHS voor onze DMVPN-cloud). Dit wordt verwacht.	IPSEC-IFC MGRE/TU0: De tunnelstatus controleren. **NHRP: if_up: Tunnel 0-poorten 0** IPSEC-IFC MGRE/TU0: tunnel IPSEC-IFC MGRE/TU0: reeds luisteren naar crypto_ss_call_start **%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP IS INGESCHAKELD** **NHRP: Kan registratie niet verzenden - er zijn geen NHS's ingesteld** %LINK-3-UPDOWN: Interface Tunnel0, veranderde status in omhoog NHRP: if_up: Tunnel 0-poorten 0 NHRP: Kan registratie niet verzenden - er zijn geen NHS's ingesteld IPSEC-IFC MGRE/TU0: tunnel IPSEC-IFC MGRE/TU0: reeds luisteren naar crypto_ss_call_start **%LINEPROTO-5-UPDOWN: Het protocol van de lijn op Interface Tunnel0, veranderde staat in omhoog** IPSEC-IFC GRE/TU0: De tunnelstatus controleren. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): terugblik op verbinding 0 **IPSEC-IFC GRE/TU0: reeds luisteren naar crypto_ss_call_start** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Een socket met profiel, DMVPN-IPSEC openen** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): terugblik op verbinding 0 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Tandtunnel meteen. IPSEC-IFC GRE/TU0: Tunnel0-tunnelinterface toevoegen aan gedeelde lijst **NHRP: if_up: Tunnel 0-poorten 0** **NHRP: Tunnel0: Cache Add voor target 10.1.1.254/32 next-hop 10.1.254** **172.16.10.1**	Deze eerste paar deb berichten worden gegenereerd door ee opdracht om **niet** uit t schakelen in de tunnelinterface. Beric worden gegenereerd crypto, GRE en NHR diensten die worden gestart. Daarnaast voegt de s een ingang aan zijn e NHRP cache toe voo eigen NBMA en tunneladres.

IPSEC-IFC GRE/TU0: tunnel
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220
IPSEC-IFC GRE/TU0: reeds luisteren naar crypto_ss_call_start
IPSEC-IFC GRE/TU0: reeds luisteren naar crypto_ss_call_start
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Een socket met profiel, DMVPN-IPSEC openen
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket is al geopend. Negeren.
CRYPTO_SS (TUNNEL SEC): Toepassingen beginnen te luisteren
kaart in kaart brengen AVL mislukt, kaart + ace-paar bestaat al op de kaart
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP IS INGESCHAKELD
CRYPTO_SS (TUNNEL SEC): Active Open, socket informatie: lokaal 172.16.1.1 172.16.1.1/255.255.255.255/0, op afstand 172.16.10.1 172.16.10.1/255.255.255.255/0, poort 47, ifc Tu0

START VAN DE ONDERHANDELING OVER ISAKMP (FASE I)

IPSEC(recalculate_mtu): reset sadb_root 94EFDC0 mtu naar 1500
IPSEC(sa_request): ,
(key eng. msg) OUTBOUND Local= 172.16.1.1:500, Remote= 172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),
Remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transformatie= ESP-3des esp-sha-hmac (transport),
lifedur= 3600s en 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
ISAKMP:(0): SA-aanvraagprofiel is (NULL)
ISAKMP: Gemaakt een peer constructie voor 172.16.10.1, PoE poort 500
ISAKMP: Nieuwe peer gecreëerd peer = 0x95F6858 peer_handle = 0x8000004
ISAKMP: Schuif peer struct 0x95F6858, reftel 1 voor isakmp_initiator
ISAKMP: lokale poort 500, externe poort 500
ISAKMP: nieuw knooppunt 0 instellen op QM_IDLE
ISAKMP:(0):invoegen als geslaagd = 8A26FB0
ISAKMP:(0):Kan Aggressief niet starten in de hoofdmodus.
ISAKMP:(0):gevonden peer-pre-Shared key matching 172.16.10.1
ISAKMP:(0): Geconstrueerde NAT-T-verkoper-RFC3947-ID

De eerste stap zodra tunnel 'geen shutdow is het starten van de onderhandeling. Hier creëert de sprak een verzoek, probeert om Aggressive Mode te beginnen en faalt teru naar Hoofdmodus.
Aangezien de agress modus niet op een va beide routers is inges wordt dit verwacht.
De toespraak begint hoofdmodus en verst het eerste bericht var ISAKMP, MM_NO_S
De status van ISAKM verandert van IKE_R in IKE_I_MM1.
De NAT-T verkoper-I berichten worden geb bij het detecteren en verplaatsen van NAT boodschappen worde verwacht tijdens de onderhandelingen ov ISAKMP, ongeacht o al dan niet wordt

	ISAKMP:(0): geconstrueerde NAT-T-verkoper-07-ID ISAKMP:(0): Geconstrueerde NAT-T-verkoper-03-ID ISAKMP:(0): gebouwd NAT-T-verkoper-02-ID **ISAKMP:(0):Input = IKE_MESG_VAN_IPSEC, IKE_SA_REQ_MM** **ISAKMP:(0):Oude staat = IKE_READY New State = IKE_I_MM1** **ISAKMP:(0): Startmodus** **ISAKMP:(0): pakje naar 172.16.10.1 mijn_poort 500 per poort 500 (I) MM_NO_STATE** ISAKMP:(0):verzenden van een IKE IPv4-pakket. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): boodschap van kant	geïmplementeerd. Ne zoals de Aggressive berichten, worden de verwacht.
Nadat de tunnel van het praatje "geen shutdown" is, ontvangt het knooppunt het IKE NEW SA (Main Mode 1) bericht op poort 500. Als Responder maakt het knooppunt een ISAKMP Security Association (SA). De status van ISAKMP verandert van IKE_READY in IKE_R_MM1.	**ISAKMP (0): ontvangen pakket van 172.16.1.1. poorten 500 sport 500 Global (N) NEW SA** **ISAKMP: Gemaakt een peer constructie voor 172.16.1.1, PoE poort 500** ISAKMP: Nieuwe peer gecreëerd peer = 0x8CACD00 peer_handle = 0x8000003 ISAKMP: Vergrendeling van peer struct 0x8CACD00, refcount 1 voor crypto_isakmp_process_block ISAKMP: lokale poort 500, externe poort 500 **ISAKMP:(0)invoegen als geslaagd = 6A5BDE8** ISAKMP:(0):Input = IKE_MESG_VAN_PEER, IKE_MM_EXCH **ISAKMP:(0):Oude staat = IKE_READY Nieuwe staat = IKE_R_MM1**	
Het ontvangen IKE hoofdmodus 1-bericht wordt verwerkt. Het knooppunt bepaalt dat de peer de ISAKMP-eigenschappen met elkaar in overeenstemming brengt en ze zijn ingevuld in de pas opgerichte ISAKMP SA. De berichten laten zien dat de peer 3DES-CBC gebruikt voor encryptie, het hashing van SHA, Diffie Hellman (DH) groep 1, preShared Key voor authenticatie en de standaard SA-levensduur van 86400 seconden (0x00x51 0x80 = 0x15180 = 8640 seconden) . De ISAKMP-staat is nog steeds IKE_R_MM1 omdat het woord niet is	ISAKMP:(0): verwerking van SA-lading. bericht-ID = 0 ISAKMP:(0): verbruikersid **ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 69 fouten** **ISAKMP (0): verkoper-id is NAT-T RFC 3947** ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 245 foutieve antwoorden ISAKMP (0): verkoper-id is NAT-T v7 ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 157 foutieve antwoorden ISAKMP:(0): verkoper-id is NAT-T3 ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 123 foutieve antwoorden ISAKMP:(0): verkoper-id is NAT-T v2 **ISAKMP:(0):gevonden peer-pre-gedeeld key matching 172.16.1.1** **ISAKMP:(0): lokale , vooraf gedeelde sleutel gevonden** ISAKMP : Snijprofielen voor breedte... **ISAKMP:(0):Controle op ISAKMP-transformatie 1 op basis van prioritair beleid 1**	

ontvangen. De NAT-T verkoper-ID-berichten worden gebruikt bij het detecteren en verplaatsen van NAT. Deze boodschappen worden verwacht tijdens de onderhandelingen over ISAKMP, ongeacht of NAT al dan niet wordt geïmplementeerd. Gelijkaardige berichten worden gezien voor Dead Peer Detection (DPD).	**ISAKMP: encryptie 3DES-CBC** **ISAKMP: Hash SHA** **ISAKMP: standaardgroep 1** **ISAKMP: auth pre-Share** **ISAKMP: levensduur in seconden** **ISAKMP: levensduur (VPI) van 0x00x10x51 0x80** **ISAKMP:(0):Atten zijn acceptabel. Volgende lading is 0** **ISAKMP:(0):Aanvaardbare atten:feitelijke levensduur: 0** **ISAKMP:(0):Aanvaardbare atten:leven: 0** **ISAKMP:(0):Vullen van atts als vpi_length:4** **ISAKMP:(0):Vullen als life_in_seconden:86400** **ISAKMP:(0):Feitelijke levensduur teruggeven: 86400** **ISAKMP:(0):Starttimer: 86400.**
	ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 69 fouten ISAKMP (0): verkoper-id is NAT-T RFC 3947 ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 245 foutieve antwoorden ISAKMP (0): verkoper-id is NAT-T v7 ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 157 foutieve antwoorden ISAKMP:(0): verkoper-id is NAT-T3 ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 123 foutieve antwoorden ISAKMP:(0): verkoper-id is NAT-T v2 ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0)Oude staat = IKE_R_MM1 Nieuwe staat = IKE_R_MM1
MM_SA_SETUP (hoofdmodus 2) wordt naar het woordvoerder verzonden, dat bevestigt dat MM1 werd ontvangen en geaccepteerd als een geldig ISAKMP-pakket. De status van ISAKMP verandert van IKE_R_MM1 in IKE_R_MM2.	ISAKMP:(0): Geconstrueerde NAT-T-verkoper-RFC3947-ID **ISAKMP:(0): pakketten verzenden naar 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP** ISAKMP:(0):verzenden van een IKE IPv4-pakket. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0)Oude staat = IKE_R_MM1 Nieuwe staat = IKE_R_MM2**
	ISAKMP (0): ontvangen pakket van 172.16.10.1 depoort 500 sport 500 Global (I) MM_NO_STATE **ISAKMP:(0):Input = IKE_MESG_VAN_PEER, IKE_MM_EXCH** **ISAKMP:(0)Oude staat = IKE_I_MM1 Nieuwe staat = IKE_I_MM2**

In antwoord op het be
van MM1 dat naar de
is verstuurd, komt MM
aan die bevestigt dat
is ontvangen. Het
ontvangen IKE
hoofdmodus 2-berich

	ISAKMP:(0): verwerking van SA-lading. bericht-ID = 0 ISAKMP:(0): verbruikersid **ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 69 fouten** ISAKMP (0): verkoper-id is NAT-T RFC 3947 ISAKMP:(0):gevonden peer-pre-Shared key matching 172.16.10.1 ISAKMP:(0): lokale , vooraf gedeelde sleutel gevonden ISAKMP : Snijprofielen voor breedte... **ISAKMP:(0):Controle op ISAKMP-transformatie 1 op basis van prioritair beleid 1** **ISAKMP: encryptie 3DES-CBC** **ISAKMP: Hash SHA** **ISAKMP: standaardgroep 1** **ISAKMP: auth pre-Share** **ISAKMP: levensduur in seconden** **ISAKMP: levensduur (VPI) van 0x00x10x51 0x80** **ISAKMP:(0):Atten zijn acceptabel. Volgende lading is 0** **ISAKMP:(0):Aanvaardbare atten:feitelijke levensduur: 0** **ISAKMP:(0):Aanvaardbare atten:leven: 0** **ISAKMP:(0):Vullen van atts als vpi_length:4** **ISAKMP:(0):Vullen als life_in_seconden:86400** **ISAKMP:(0):Feitelijke levensduur teruggeven: 86400** **ISAKMP:(0):Starttimer: 86400.**	wordt verwerkt. Het a realiseert zich dat het hub eigenschappen v ISAKMP heeft en dez eigenschappen zijn ingevuld in de ISAKM dat is gecreëerd. Dit toont dat de peer 3DE CBC voor encryptie, hashing van SHA, Di Hellman (DH) groep preShared Key voor authenticatie gebruik de standaard SA- levensduur van 8640 seconden (0x00x51 0 0x15180 = 8640 seco . Naast de NAT-T beric is er een uitwisseling bepalen of de sessie zal gebruiken. De status van ISAKM verandert van IKE_I_ in IKE_I_MM2.
	ISAKMP:(0): verbruikersid ISAKMP:(0): verkoper-id lijkt Unity/DPD maar grote 69 fouten ISAKMP (0): verkoper-id is NAT-T RFC 3947 ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(0)Oude staat = IKE_I_MM2 Nieuwe staat = IKE_I_MM2 **ISAKMP:(0): pakketten verzenden naar 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP** ISAKMP:(0):verzenden van een IKE IPv4-pakket. ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(0)Oude staat = IKE_I_MM2 Nieuwe staat = IKE_I_MM3**	MM_SA_SETUP (Hoofdmodus 3) word de hub gestuurd, die bevestigt dat de gesp heeft MM2 ontvange zou willen doorgaan. De status van ISAKM verandert van IKE_I_ in IKE_I_MM3.
MM_SA_SETUP (hoofdmodus 3) wordt ontvangen door een hub. De hub concludeert dat de peer een ander Cisco IOS apparaat is en geen NAT voor ons of onze peer wordt gedetecteerd. De status van ISAKMP	**ISAKMP (0): Ontvangen pakket van 172.16.1.1 depoorts 500 sport 500 Global (R) MM_SA_SETUP** ISAKMP:(0):Input = IKE_MESG_VAN_PEER, IKE_MM_EXCH **ISAKMP:(0)Oude staat = IKE_R_MM2 Nieuwe staat = IKE_R_MM3** ISAKMP:(0): verwerking van KE-lading. bericht-ID = 0 ISAKMP:(0): verwerking NONCE-lading. bericht-ID = 0	

verandert van IKE_R_MM2 in IKE_R_MM3.	**ISAKMP:(0):gevonden peer-pre-gedeeld key matching 172.16.1.1** ISAKMP:(1002) verbruikersid ISAKMP:(1002) verkoper-id: DPD ISAKMP:(1002) verbruikersid **ISAKMP:(1002) spreken met een andere IOS doos!** ISAKMP:(1002) verbruikersid ISAKMP:(1002) verkoper-id lijkt Unity/DPD maar grote 225 foutieve antwoorden ISAKMP:(1002) verkoper-id is XAUTH ISAKMP:ontvangen lading type 20 **ISAKMP (1002): Zijn hash geen match - dit knooppunt buiten NAT** ISAKMP:ontvangen lading type 20 **ISAKMP (1002): Geen NAT gevonden voor zelf of peer** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Oude staat = IKE_R_MM3 Nieuwe staat = IKE_R_MM3	
MM_KEY_EXCH (hoofdmodus 4) wordt verstuurd door de hub. De status van ISAKMP verandert van IKE_R_MM3 in IKE_R_MM4.	**ISAKMP:(1002) pakketten verzenden naar 172.16.1.1 mijn_poort 500 peer_port 500 (R) MM_KEY_EXCH** ISAKMP:(1002):verzenden van een IKE IPv4-pakket. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Oude staat = IKE_R_MM3 Nieuwe staat = IKE_R_MM4**	
	ISAKMP (0): ontvangen pakket van 172.16.10.1 depoorts 500 sport 500 Global (I) MM_SA_SETUP ISAKMP:(0):Input = IKE_MESG_VAN_PEER, IKE_MM_EXCH **ISAKMP:(0)Oude staat = IKE_I_MM3 Nieuwe staat = IKE_I_MM4** ISAKMP:(0): verwerking van KE-lading. bericht-ID = 0 ISAKMP:(0): verwerking NONCE-lading. bericht-ID = 0 **ISAKMP:(0):gevonden peer-pre-Shared key matching 172.16.10.1** ISAKMP:(1002) verbruikersid ISAKMP:(1002) verkoper-id is eenheid ISAKMP:(1002) verbruikersid ISAKMP:(1002) verkoper-id: DPD ISAKMP:(1002) verbruikersid **ISAKMP:(1002) spreken met een andere IOS doos!** ISAKMP:ontvangen lading type 20 **ISAKMP (1002): Zijn hash geen match - dit knooppunt buiten NAT** ISAKMP:ontvangen lading type 20 **ISAKMP (1002): Geen NAT gevonden voor zelf of peer** ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Oude staat = IKE_I_MM4 Nieuwe	MM_SA_SETUP (hoofdmodus 4) word ontvangen door iema anders. De toespraak concludeert dat de pe een ander Cisco IOS apparaat is en geen I voor ons of onze pee wordt gedetecteerd. De status van ISAKM verandert van IKE_I_ in IKE_I_MM4.

	staat = IKE_I_MM4 ISAKMP:(1002):eerste contact verzenden **ISAKMP:(1002):SA doet pre-gedeelde belangrijke authenticatie met id type ID_IPV4_ADDR.** ISAKMP (1002): ID-lading volgende lading : 8 type: 1 adres : 172.16.1.1 protocol : 17 haven : 500 lengte: 12 ISAKMP:(1002):Totale lengte van de lading: 12 **ISAKMP:(1002) pakje verzenden naar 172.16.10.1 mijn_poort 500 per poort 500 (I) MM_KEY_EXCH** ISAKMP:(1002):verzenden van een IKE IPv4-pakket. ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Oude staat = IKE_I_MM4 Nieuwe staat = IKE_I_MM5**	MM_KEY_EXCH (hoofdmodus 5) word het woord verzonden De status van ISAKM verandert van IKE_I_ in IKE_I_MM5.
MM_KEY_EXCH (hoofdmodus 5) wordt ontvangen door het hub. De status van ISAKMP verandert van IKE_R_MM4 in IKE_R_MM5. Bovendien wordt "peer matches * geen* van de profielen" gezien door het gebrek aan een ISAKMP-profiel. Omdat dit het geval is, gebruikt ISAKMP geen profiel.	**ISAKMP (1002): Ontvangen pakket van 172.16.1.1. poorten 500 sport 500 Global (R) MM_KEY_EXCH** ISAKMP:(1002):Invoer = IKE_MESG_VAN_PEER, IKE_MM_EXCH **ISAKMP:(1002):Oude staat = IKE_R_MM4 Nieuwe staat = IKE_R_MM5** ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 0 ISAKMP (1002): ID-lading volgende lading : 8 type: 1 adres : 172.16.1.1 protocol : 17 haven : 500 lengte: 12 **ISAKMP:(0): peer overeenkomsten *geen* van profielen** ISAKMP:(1002) HASH-lading verwerken. bericht-ID = 0 ISAKMP:(1002) EERSTE_CONTACT protocol 1 VERWERKEN spi 0, bericht ID = 0, sa = 0x6A5BDE8 ISAKMP:(1002):SA-authenticatiestatus: geauthentiseerd ISAKMP:(1002):SA is echt bevonden met 172.16.1.1 ISAKMP:(1002):SA-authenticatiestatus: geauthentiseerd ISAKMP:(1002) eerste contact verwerken de bestaande fase 1 en 2 SA's met lokale 172.16.10.1 verafgelegen 172.16.1.1 afgelegen poort 500 **ISAKMP: Proberen een peer 172.16.10.1/172.16.1.1/500/, in te voegen en met succes 8CACD00 in te voegen.** ISAKMP:(1002):Input = IKE_MESG_INTERNAL,	

IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Oude staat = IKE_R_MM5 Nieuwe staat = IKE_R_MM5

IPSEC(key_engine): heeft een rijgebeurtenis met 1 KMI-bericht(en)
ISAKMP:(1002):SA doet pre-gedeelde belangrijke authenticatie met id type ID_IPV4_ADDR.
ISAKMP (1002): ID-lading
volgende lading : 8
type: 1
adres : 172.16.10.1
protocol : 17
haven : 500
lengte: 12
ISAKMP:(1002):Totale lengte van de lading: 12

Het laatste pakket MM_KEY_EXCH (hoofdmodus 6) wordt verzonden door het hub. Dit voltooit de onderhandeling van Fase 1 die dit apparaat voor Fase 2 (IPSec Quick Mode) klaar maakt. De status van ISAKMP verandert van IKE_R_MM5 in IKE_P1_COMPLETE.

ISAKMP:(1002) pakketten verzenden naar 172.16.1.1 mijn_poort 500 peer_port 500 (R) MM_KEY_EXCH
ISAKMP:(1002):verzenden van een IKE IPv4-pakket.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Oude staat = IKE_R_MM5 Nieuwe staat = IKE_P1_COMPLETE

ISAKMP:(1002):Invoer = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Oude staat = IKE_P1_COMPLETE Nieuwe staat = IKE_P1_COMPLETE

Het laatste pakket MM_KEY_EXCH (hoofdmodus 6) word ontvangen door het w Dit voltooit de onderhandeling van F die dit apparaat voor 2 (IPSec Quick Mode maakt. De status van ISAKM verandert van IKE_I_ in IKE_I_MM6, en da onmiddellijk in IKE_P1_COMPLETE Bovendien wordt "pe matches * geen* van profielen" gezien doo gebrek aan een ISAK profiel. Omdat dit het is, gebruikt ISAKMP profiel.

ISAKMP (1002): ontvangen pakket van 172.16.10.1 depoort 500 sport 500 Global (I) MM_KEY_EXCH
ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 0
ISAKMP (1002): ID-lading
volgende lading : 8
type: 1
adres : 172.16.10.1
protocol : 17
haven : 500
lengte: 12
ISAKMP:(0): peer overeenkomsten *geen* van profielen
ISAKMP:(1002) HASH-lading verwerken. bericht-ID = 0
ISAKMP:(1002):SA-authenticatiestatus:
geauthentiseerd
ISAKMP:(1002):SA is echt bevonden met 172.16.10.1
ISAKMP: Proberen een peer 172.16.1.1/172.16.10.1/500/, in te voegen en met succes 95F6858 in te voegen.
ISAKMP:(1002):Invoer = IKE_MESG_VAN_PEER, IKE_MM_EXCH
ISAKMP:(1002):Oude staat = IKE_I_MM5 Nieuwe staat = IKE_I_MM6

	ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE ISAKMP:(1002):Oude staat = IKE_I_MM6 Nieuwe staat = IKE_I_MM6 ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE **ISAKMP:(1002):Oude staat = IKE_I_MM6 Nieuwe staat = IKE_P1_COMPLETE**
EINDTIJD VAN DE ONDERHANDELING OVER ISAKMP (FASE I), BEGIN VAN DE ONDERHANDEL OVER IPSEC (FASE II)	
	ISAKMP:(1002):begin snelle-mode-uitwisseling, M-ID van 3464373979 ISAKMP:(1002):QM-initiator krijgt spi **ISAKMP:(1002) pakje verzenden naar 172.16.10.1 mijn_poorts 500 per poort 500 (I) QM_IDLE** ISAKMP:(1002):verzenden van een IKE IPv4-pakket. ISAKMP:(1002):Node 3464373979, Invoer = IKE_MESG_INTERNAL, IKE_INIT_QM **ISAKMP:(1002):Oude staat = IKE_QM_READY New State = IKE_QM_I_QM1** ISAKMP:(1002):Invoer = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE ISAKMP:(1002):Oude staat = IKE_P1_COMPLETE Nieuwe staat = IKE_P1_COMPLETE
Het knooppunt ontvangt het eerste QM-pakket (Quick Mode) met het IPSec-voorstel. De ontvangen eigenschappen specificeren dat: Encaps flag ingesteld op 2 (transportmodus, vlag van 1 zou tunnelmodus zijn), default SA-levensduur van 3600 seconden en 4608000 kilobytes (0x465000 in hex), HMAC-SHA voor verificatie en 3DES voor encryptie. Omdat dit dezelfde eigenschappen zijn die in de lokale configuratie zijn ingesteld, wordt het voorstel aanvaard en wordt het omhulsel van een IPSec SA gecreëerd. Aangezien er nog geen waarden van de Security Parameter Index (SPI) met deze worden geassocieerd, is dit slechts een schaal van een SA die nog niet	**ISAKMP (1002): Ontvangen pakket van 172.16.1.1 poorts 500 sport 500 Global (R) QM_IDLE** **ISAKMP: nieuw knooppunt -830593317 instellen op QM_IDLE** ISAKMP:(1002) HASH-lading verwerken. bericht-ID = 3464373979 ISAKMP:(1002) verwerking van SA-lading. bericht-ID = 3464373979 **ISAKMP:(1002):Controle van het IPSec-voorstel 1** **ISAKMP: transformatie 1, ESP_3DES** **ISAKMP: eigenschappen bij transformatie:** **ISAKMP: Encaps is 2 (Vervoer)** **ISAKMP: Levenstype SA in seconden** **ISAKMP: Leven SA (basiswaarde) van 3600** **ISAKMP: SA-levenstype in kilobytes** **ISAKMP: SA-levensduur (VPI) van 0x00x46 0x50 0x0** **ISAKMP: voor authentiek middel is HMAC-SHA** **ISAKMP:(1002):atts zijn acceptabel.** IPSEC(validering_request_request): deel 1 van het voorstel IPSEC(validering_request_request): deel 1 van het voorstel, **(key eng. msg) INBOUND Local= 172.16.10.1:0, Remote= 172.16.1.1:0,** **local_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),** **Remote_proxy= 172.16.1.1/255.255.255.255/47/0**	De snelle Mode (Fas IPSec)-uitwisseling b en de toespraak stuu eerste QM-bericht na knooppunt.

kan worden gebruikt om verkeer over te gaan.	**(type=1),** **protocol= ESP, transformatie= NONE (transport),** **lifedur= 0s en 0kb,** **spi= 0x0(0), conn_id= 0, keysize= 128, vlaggen= 0x0**
Dit zijn slechts algemene IPSec service berichten die zeggen dat het goed werkt.	IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): terugblik op verbinding 0 IPSEC-IFC MGRE/TU0: reeds luisteren naar crypto_ss_call_start **IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Een socket met profiel, DMVPN-IPSEC openen** IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): terugblik op verbinding 0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Tandtunnel meteen. IPSEC-IFC MGRE/TU0: Tunnel0-tunnelinterface toevoegen aan gedeelde lijst IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnelbescherming_start_nog-niet-bestaande_timer 8C9388 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Aanvraag goed luisteren
Pseudo-crypto map entry moet worden gecreëerd voor IP protocol 47 (GRE) van 172.16.10.1 (hub public address) tot 172.16.1.1 (speerpunt). Er wordt een IPSec SA/SPI gecreëerd voor zowel het inkomende als het uitgaande verkeer met waarden uit het geaccepteerde voorstel.	kaart in kaart brengen AVL mislukt, kaart + ace-paar bestaat al op de kaart CRYPTO_SS (TUNNEL SEC): Passive open, socket informatie: lokaal 172.16.10.1 172.16.10.1/255.255.255.255/0, op afstand 172.16.1.1 172.16.1.1/255.255.255.255/0, poort 47, ifc Tu0 Crypto-kaart: proxy_match **src - adres : 172.16.10.1** **addr : 172.16.1.1** **protocol : 47** src - poort : 0 Startpoort: 0 ISAKMP:(1002) verwerking NONCE-lading. bericht-ID = 3464373979 ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 3464373979 ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 3464373979 ISAKMP:(1002):QM Responder krijgt spi ISAKMP:(1002):Node 3464373979, Invoer = IKE_MESG_VAN_PEER, IKE_QM_EXCH **ISAKMP:(1002):Oude staat = IKE_QM_READY New State = IKE_QM_SPI_STARVE** **ISAKMP:(1002) IPsec SAs maken** **inkomende SA van 172.16.1.1 t/m 172.16.10.1 (f/i) 0/0** **(proxy 172.16.1.1 tot 172.16.10.1)** **heeft spi 0xDD2AC2B3 en conn_id 0** **levensduur van 3600 seconden** **levensduur van 4608000 kg** **uitgaande SA van 172.16.10.1 t/m 172.16.1.1 (f/i)**

	0/0 (volmacht 172.16.10.1 t/m 172.16.1.1) heeft spi 0x82C3E0C4 en conn_id 0 levensduur van 3600 seconden levensduur van 4608000 kg
Het tweede QM-bericht verzonden door de hub. Bericht gegenereerd door IPSec service die bevestigt dat tunnelbescherming zich op Tunnel0 bevindt. Er wordt een ander SA creatiebericht gezien dat de bestemming IPs, SPIs, set eigenschappen en levensduur in kilobytes en seconden resteert.	ISAKMP:(1002) pakketten verzenden naar 172.16.1.1 mijn_poort 500 peer_port 500 (R) QM_IDLE ISAKMP:(1002):verzenden van een IKE IPv4-pakket. ISAKMP:(1002):Node 3464373979, Invoer = IKE_MESG_INTERNAL, IKE_GOT_SPI ISAKMP:(1002):Oude staat = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 CRYPTO_SS (TUNNEL SEC): Volledige binding van toepassing op socket IPSEC(key_engine): heeft een rijgebeurtenis met 1 KMI-bericht(en) Crypto-kaart: proxy_match src - adres : 172.16.10.1 addr : 172.16.1.1 protocol : 47 src - poort : 0 Startpoort: 0 IPSEC (crypto_ipsec_sa_Find_ident_head): opnieuw aansluiten op dezelfde proxy's en peer 172.16.1.1 IPSEC (policy_db_add_ident): src 172.16.10.1, dest 172.16.1.1, dest_poort 0 IPSEC(aangemaakt_sa): als opgericht, sa_dest= 172.16.10.1, sa_proto= 50, sa_spi= 0xDD2AC2B3(3710567091), sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3 sa_leven(k/sec)= (4536779/3600) IPSEC(aangemaakt_sa): als opgericht, sa_dest= 172.16.1.1, sa_proto= 50, sa_spi= 0x82C3E0C4(2193875140), sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4 sa_leven(k/sec)= (4536779/3600) IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): Tunnel0-moment 8B6A0E8 met tun_decap_oce 6A648F0 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): 8 C9388 terugblik op de aansluiting IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): boodschap van kant IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): 8 C9388 terugblik op de aansluiting IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnelbescherming_socket_up IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): NHRP voor signalering IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Mtu 1.458, via MTU IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): 8

C9388 terugblik op de aansluiting

ISAKMP (1002): Ontvangen pakket van 172.16.10.1 poorts 500 sport 500 Global (I) QM_IDLE

ISAKMP:(1002) HASH-lading verwerken. bericht-ID = 3464373979

ISAKMP:(1002) verwerking van SA-lading. bericht-ID = 3464373979

ISAKMP:(1002):Controle van het IPSec-voorstel 1

ISAKMP: transformatie 1, ESP_3DES

ISAKMP: eigenschappen bij transformatie:

ISAKMP: Encaps is 2 (Vervoer)

ISAKMP: Levenstype SA in seconden

ISAKMP: Leven SA (basiswaarde) van 3600

ISAKMP: SA-levenstype in kilobytes

ISAKMP: SA-levensduur (VPI) van 0x00x46 0x50 0x0

ISAKMP: voor authentiek middel is HMAC-SHA

ISAKMP:(1002):atts zijn acceptabel.

IPSEC(validering_request_request): deel 1 van het voorstel

IPSEC(validering_request_request): deel 1 van het voorstel,

(key eng. msg) INBOUND Local= 172.16.1.1:0, Remote= 172.16.10.1:0,

local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),

Remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),

protocol= ESP, transformatie= NONE (transport),

lifedur= 0s en 0kb,

spi= 0x0(0), conn_id= 0, keysize= 128, vlaggen= 0x0

Crypto-kaart: proxy_match

src - adres : 172.16.1.1

addr : 172.16.10.1

protocol : 47

src - poort : 0

Startpoort: 0

ISAKMP:(1002) verwerking NONCE-lading. bericht-ID = 3464373979

ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 3464373979

ISAKMP:(1002) verwerkings-ID-lading. bericht-ID = 3464373979

ISAKMP:(1002) IPsec SAs maken

inkomende SA van 172.16.10.1 t/m 172.16.1.1 (f/i) 0/0

(volmacht 172.16.10.1 t/m 172.16.1.1)

heeft spi 0x82C3E0C4 en conn_id 0

levensduur van 3600 seconden

levensduur van 4608000 kg

uitgaande SA van 172.16.1.1 t/m 172.16.10.1 (f/i) 0/0

Hij ontvangt het twee
QM-pakket met het IP
voorstel. Dit bevestig
QM1 door de hub we
ontvangen. De ontva
eigenschappen
specificeren dat: Enc
flag ingesteld op 2
(transport mode, vlag
zou tunnelmodus zijn
standaard SA-levens
van 3600 seconden e
4608000 kilobytes
(0x465000 in hex), H
SHA voor verificatie e
DES voor encryptie.
dit dezelfde eigensch
zijn die in de lokale
configuratie zijn inges
wordt het voorstel
aanvaard en wordt he
omhulsel van een IPS
SA gecreëerd. Aange
er nog geen waarden
de Security Paramete
Index (SPI) met deze
worden geassocieerd
slechts een schaal va
SA die nog niet kan w
gebruikt om verkeer d
gaan.
De pseudo-crypto ma
entry moet worden
gecreëerd voor IP pro
47 (GRE) van 172.16
(hub public address)
172.16.1.1 (speerpun
Er wordt een IPSec S
gecreëerd voor zowe
inkomende als het
uitgaande verkeer me
waarden uit het
geaccepteerde voors

(proxy 172.16.1.1 tot 172.16.10.1)
heeft spi 0xDD2AC2B3 en conn_id 0
levensduur van 3600 seconden
levensduur van 4608000 kg

ISAKMP:(1002) pakje verzenden naar 172.16.10.1 mijn_poorts 500 per poort 500 (I) QM_IDLE
ISAKMP:(1002):verzenden van een IKE IPv4-pakket.
ISAKMP:(1002):schrappen van fout FALSE-reden "geen fout": fout-83059317 fout
ISAKMP:(1002):Node 3464373979, Invoer = IKE_MESG_VAN_PEER, IKE_QM_EXCH
ISAKMP:(1002):Oude staat = IKE_QM_I_QM1 Nieuwe staat = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): heeft een rijgebeurtenis met 1 KMI-bericht(en)
Crypto-kaart: proxy_match
src - adres : 172.16.1.1
addr : 172.16.10.1
protocol : 47
src - poort : 0
Startpoort: 0
IPSEC (crypto_ipsec_sa_Find_ident_head): opnieuw aansluiten op dezelfde proxy's en peer 172.16.10.1
IPSEC (policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_poort 0

IPSEC(aangemaakt_sa): als opgericht,
sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 3
sa_leven(k/sec)= (4499172/3600)
IPSEC(aangemaakt_sa): als opgericht,
sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac, sa_conn_id= 4
sa_leven(k/sec)= (4499172/3600)
IPSEC(update_huidige_outbound_sa): Schakel SA peer 172.16.10.1 stroom in als naar SPI D2AC2B3
IPSEC(update_huidige_outbound_sa): geactualiseerd peer-172.16.10.1-stroom zoals naar SPI DD2AC2B3
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): Tunnel knooppunt 94F2740 met tun_decap_oce 794ED30
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): tunnelbescherming_socket_up
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): NHRP voor signalering
NHRP: NCS 10.1.1.254 Tunnel 0Vrf 0 Cluster 0 Priority 0 Transioveren naar "E" van "

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):

Het woord heeft het c
en laatste QM-berich
het knooppunt gestu
dat de QM-uitwisselir
voltooit. In tegenstelli
ISAKMP, waar elke p
door elke staat gaat (
tot MM6/P1_COMPL
is IPSec een beetje a
omdat er slechts drie
berichten in plaats va
zijn. Het Initiator (onz
stem in dit geval, zoa
aangegeven door "I"
IKE_QM_I_QM1 beric
gaat van QM_READY
QM_I_QM1 direct naa
QM_PHASE2_COMP
Responder (hub) gaa
QM_READY,
QM_SPI_STARVE,
QM_R_QM2,
QM_PHASE2_COMP
Er wordt een ander S
creatiebericht gezien
bestemming IPs, SPI
eigenschappen en
levensduur in kilobyte
seconden resteert.

verbindingsraadpleging teruggegeven 961D220
NHRP: Proberen pakketjes via DEST 10.1.1.254 te verzenden

Deze laatste QM-berichten bevestigen dat de Quick Mode is voltooid en IPSec aan beide zijden van de tunnel is geïnstalleerd. In tegenstelling tot ISAKMP, waar elke peer door elke staat gaat (MM1 tot MM6/P1_COMPLETE), is IPSec een beetje anders omdat er slechts drie berichten in plaats van zes zijn. Responder (onze hub in dit geval, zoals aangeduid door "R" in het bericht IKE_QM_R_QM1) gaat QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. De Initiator (wordt gesproken) gaat van QM_READY en vervolgens direct van QM_I_QM1 naar QM_PHASE2_COMPLETE.

ISAKMP (1002): Ontvangen pakket van 172.16.1.1 poorts 500 sport 500 Global (R) QM_IDLE
ISAKMP:(1002):verwijderen van fout-830/593/317 FALSE reden "QM klaar (wacht)"
ISAKMP:(1002):Node 3464373979, Invoer = IKE_MESG_VAN_PEER, IKE_QM_EXCH
ISAKMP:(1002):Oude staat = IKE_QM_R_QM2 Nieuwe staat = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): heeft een rijgebeurtenis met 1 KMI-bericht(en)
IPSEC (key_engine_enabled_outbound): rec kan kennisgeving bij ISAKMP mogelijk maken
IPSEC (key_engine_enabled_outbound): S.A. mogelijk maken met spi 2193875140/50
IPSEC(update_huidige_outbound_sa): Schakel SA peer 172.16.1.1 stroom in als naar SPI 82C3E0C4
IPSEC(update_huidige_outbound_sa): geactualiseerd peer-172.16.1.1 stroomuitval naar SPI 82C3E0C4

NHRP: Registratieaanvraag via Tunnel0 vrf 0, pakketgrootte: 108
src : 10.1.1.1, dst: 10.1.1.254
F) na: IPv4(1), type: IP (800), hop: 255, af: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz : 108 extoff: 52
M) vlaggen: " unieke nat " , vraagt u : 65540
src NBMA: 172.16.1.1
src - protocol : 10.1.1.1, protocol bij het dst: 10.1.1.254
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, voorf: 0
Uitbreiding responder-adres (3):
Uitbreiding van de NHS-gegevens voor voorwaartse verzending(4):
Omgekeerde doorgifte NHS-record-uitbreiding(5):
Verificatieuitbreiding(7):
type:Cleartext(1), data:NHRPAUTH
NAT-adresuitbreiding(9):
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0

Dit zijn de NHRP-registratieverzoeken naar de hub worden gestuurd in een pogin zich te registreren bij NHS (de hub). Het is normaal om hier mee van te zien, omdat he woord blijft proberen bij de NHS te registre totdat het een "registratierelease."
src,dst: Tunnel bron (gesproken) en bestemming (hub) IP adressen. Dit zijn de en de bestemming va GRE-pakket dat door router wordt verzond
src NBMA: het NBMA (internet)-adres van h sprekende bedrijf dat pakket heeft verzond probeert zich te regis bij het NHS

	cliënt NBMA: 172.16.10.1 **clientprotocol: 10.1.1.254**	**src - protocol** : tunnel van de sprak die zich probeert te registrere **protocol dst** : tunnela van de NHS/hub **Verificatieuitbreiding**, gegevens en kolomm NHRP-verificatietoes **cliënt NBMA**: NBMA- van de NHS/hub **clientprotocol**: tunnela van de NHS/hub
	NHRP-RATE: Verzenden van het eerste registratieverzoek voor 10.1.1.254, vereist 65540 **%LINK-3-UPDOWN: Interface Tunnel0, veranderde status in omhoog** NHRP: if_up: Tunnel 0-poorten 0 **NHRP: Tunnel0: Cache update voor target 10.1.1.254/32 next-hop met 10.1.1.254 172.16.10.1** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220 NHRP: Proberen pakketjes via DEST 10.1.1.254 te verzenden	Meer NHRP-servicesberichten die aangeven dat het aanvankelijke Registratieverzoek op 10.1.1.254 naar de N verstuurd. Er is ook e bevestiging dat een c ingang werd toegevo voor tunnels IP 10.1.1.254/24 die op 172.16.10.1 leeft. De vertraagde boodscha dat de Tunnel "niet di is.
	IPSEC-IFC GRE/TU0: tunnel IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220 IPSEC-IFC GRE/TU0: reeds luisteren naar crypto_ss_call_start IPSEC-IFC GRE/TU0: reeds luisteren naar crypto_ss_call_start **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Een socket met profiel, DMVPN-IPSEC openen** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): verbindingsraadpleging teruggegeven 961D220 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket is al open. Negeren. %LINEPROTO-5-UPDOWN: Het protocol van de lijn op Interface Tunnel0, veranderde staat in omhoog	Dit zijn algemene IPS service berichten die zeggen dat het goed Hier zie je eindelijk h Tunnelprotocol in opk is.
Dit is de NHRP-registratieverzoeken die van de gesproken worden ontvangen in een poging zich te registreren bij het NHS (de hub). Het is normaal om hier meerdere van te zien, omdat het woord blijft proberen zich bij de NHS te registreren totdat het een	**NHRP: Ontvang Registratieaanvraag via Tunnel0 vrf 0, pakketgrootte: 108** F) na: IPv4(1), type: IP (800), hop: 255, af: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz : 108 extoff: 52 M) vlaggen: " unieke nat " , vraagt u : 65540 **src NBMA: 172.16.1.1** **src - protocol : 10.1.1.1, protocol bij het dst: 10.1.1.254** (C-1) code: geen fout(0) voorvoegsel: 32 mtu: 17912, hd_time: 7200	

"registratierelease." **src NBMA**: het NBMA (internet)-adres van het sprekende bedrijf dat dit pakket heeft verzonden en probeert zich te registreren bij het NHS **src - protocol** : tunneladres van de sprak die zich probeert te registreren **protocol dst** : tunneladres van de NHS/hub **Verificatieuitbreiding**, gegevens en kolommen; NHRP-verificatietoestel **cliënt NBMA**: NBMA-adres van de NHS/hub **clientprotocol**: tunneladres van de NHS/hub	addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, voorf: 0 Uitbreiding responder-adres (3): Uitbreiding van de NHS-gegevens voor voorwaartse verzending(4): Omgekeerde doorgifte NHS-record-uitbreiding(5): **Verificatieuitbreiding(7):** **type:Cleartext(1), data:NHRPAUTH** NAT-adresuitbreiding(9): (C-1) code: geen fout(0) voorvoegsel: 32 mtu: 17912, hd_time: 0 addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0 **cliënt NBMA: 172.16.10.1** **clientprotocol: 10.1.1.254**
NHRP debug-pakketten met een doelnetwerk van 10.1.1.1/32 bij volgende hop van 10.1.1.1 bij NHRP van 172.16.1.1. 172.16.1.1 wordt ook toegevoegd aan de lijst met adressen waaraan de hub multicast-verkeer doorgeeft. Deze berichten bevestigen dat de registratie een succes was, evenals een resolutie voor het woordvoersTunneladres.	NHRP: netid_in = 1, to_us = 1 **NHRP: Tunnel0: Cache add voor target 10.1.1.1/32 next-hop 10.1.1.1** **172.16.1.1** **NHRP: Tunnel endpoints toevoegen (VPN): 10.1.1.1, NBMA: 172.16.1.1)** **NHRP: succesvol verbonden NHRP-subblok voor Tunnel Endpoints (VPN) 10.1.1.1, NBMA: 172.16.1.1)** NHRP: Ingesloten subblokknooppunt voor cache: Doel geplaatst subblokknooppunt voor cache: Target 10.1.1.1/32nhop 10.1.1.1 NHRP: Omgeconvergeerde interne dynamische cache voor 10.1.1.1/32 interface Tunnel0 naar extern **NHRP: Tu0: Het maken van dynamische multicast mapping NBMA: 172.16.1.1** **NHRP: Toegevoegde dynamische multicast mapping voor NBMA: 172.16.1.1** NHRP: Het updaten van onze cache met NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1 NHRP: Nieuwe verplichte lengte: 32 NHRP: Probeert pakketjes te verzenden via DEST 10.1.1.1 **NHRP: NHRP is met succes opgelost 10.1.1.1 tot NBMA 172.16.1.1** **NHRP: Encapsulation succesvol. Tunnel IP-adres 172.16.1.1**
Dit is het NHRP-registratieantwoord dat door de hub naar de spits is gestuurd in antwoord op het eerder ontvangen "NHRP-registratieverzoek". Net als de andere registratiepakketten stuurt	**NHRP: Verzend het antwoord van de registratie via Tunnel 0 vrf 0, pakketgrootte: 128** **src : 10.1.1.254, dst: 10.1.1.1** F) na: IPv4(1), type: IP (800), hop: 255, af: 1 shtl: 4(NSAP), sstl: 0(NSAP) pktsz : extoff: 52 M) vlaggen: " unieke nat " , vraagt u : 65540 **src NBMA: 172.16.1.1**

de hub meerdere van deze pakketten in antwoord op de meerdere aanvragen.
src,dst: Tunnel bron (hub) en bestemmings (gesproken) IP-adressen. Dit zijn de bron en de bestemming van het GRE-pakket dat door de router wordt verzonden
src NBMA: NBMA (internet)-adres van het sprekende
src - protocol : tunneladres van de sprak die zich probeert te registreren
protocol dst : tunneladres van de NHS/hub
cliënt NBMA: NBMA-adres van de NHS/hub
clientprotocol: tunneladres van de NHS/hub
Verificatieuitbreiding, gegevens en kolommen; NHRP-verificatietoestel

src - protocol : 10.1.1.1, protocol bij het dst: 10.1.1.254
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, voorf: 0
Uitbreiding responder-adres (3):
C) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0
cliënt NBMA: 172.16.10.1
clientprotocol: 10.1.1.254
Uitbreiding van de NHS-gegevens voor voorwaartse verzending(4):
Omgekeerde doorgifte NHS-record-uitbreiding(5):
Verificatieuitbreiding(7):
type:Cleartext(1), data:NHRPAUTH
NAT-adresuitbreiding(9):
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0
cliënt NBMA: 172.16.10.1
clientprotocol: 10.1.1.254
NHRP: Ontvang het antwoord van de Registratie via Tunnel0 vrf 0, pakketgrootte: 128
F) na: IPv4(1), type: IP (800), hop: 255, af: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz : extoff: 52
M) vlaggen: " unieke nat " , vraagt u : 65541
src NBMA: 172.16.1.1
src - protocol : 10.1.1.1, protocol bij het dst: 10.1.1.254
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, voorf: 0
Uitbreiding responder-adres (3):
C) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0
cliënt NBMA: 172.16.10.1
clientprotocol: 10.1.1.254
Uitbreiding van de NHS-gegevens voor voorwaartse verzending(4):
Omgekeerde doorgifte NHS-record-uitbreiding(5):
Verificatieuitbreiding(7):
type:Cleartext(1), data:NHRPAUTH
NAT-adresuitbreiding(9):
(C-1) code: geen fout(0)
voorvoegsel: 32 mtu: 17912, hd_time: 0

Dit is het NHRP-registratieantwoord d
door de hub naar de
is gestuurd in antwoo
het eerder ontvanger
"NHRP-registratiever
Net als de andere registratiepakketten s
de hub meerdere var
pakketten in antwoor
de meerdere aanvrag
src NBMA: NBMA (internet)-adres van h
sprekende
src - protocol : tunnel
van de sprak die zich
probeert te registrere
protocol dst : tunnela
van de NHS/hub
cliënt NBMA: NBMA-
van de NHS/hub
clientprotocol: tunnela
van de NHS/hub
Verificatieuitbreiding,
gegevens en kolomm
NHRP-verificatietoes

	addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4 , pref : 0 **cliënt NBMA: 172.16.10.1** **clientprotocol: 10.1.1.254** NHRP: netid_in = 0, to_us = 1	
Meer algemene IPSec service berichten die zeggen dat het goed werkt.	IPSEC-IFC MGRE/TU0: reeds luisteren naar crypto_ss_call_start IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Een socket met profiel, DMVPN-IPSEC openen IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): 8C9388 terugblik op de aansluiting IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Socket is al open. Negeren. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnelbescherming_stop_wait_timer 8C9388	
	NHRP: NHS-UP: 10.1.1.254	NHRP-servicebericht de NHS op 10.1.1.25 aangeven, zijn omho
Het bericht van het systeem dat verklaart de nabijheid Eur is omhoog met de buur gesproken op 10.1.1.1.	%DUAL-5-NBRCHANGE: DHCP-IPv4 1: Buurland 10.1.1.1 (Tunnel0) staat op: nieuwe nabijheid	
	%DUAL-5-NBRCHANGE: DHCP-IPv4 1: Buurland 10.1.1.254 (Tunnel0) is omhoog: nieuwe nabijheid	Het bericht van het systeem dat verklaar nabijheid Eur is omh met het buurhub op 10.1.1.254.
Systeembericht dat een succesvolle NHRP-resolutie bevestigt.	NHRP: NHRP is met succes opgelost 10.1.1.1 tot NBMA 172.16.1.1	

Functionaliteit en probleemoplossing bevestigen

Deze sectie heeft een aantal van de meest nuttige **tonen** opdrachten die worden gebruikt om zowel de hub als de toespraak problemen op te lossen. Gebruik deze debug-conditionalen om meer specifieke uitwerpselen mogelijk te maken:

- debug dmvpn conditie peer nbma *NBMA_ADDRESS*
- debug van VPN-conditie per tunnel *TUNNEL_ADDRESS*
- debug van crypto conditie peer ipv4 *NBMA_ADDRESS*

spuitbussen

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
```

```
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"

Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

sessiedetails tonen

```
Spoke1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

crypto isakmp als detail tonen

```
Spoke1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

Hub#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption IPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

crypto ipsec als detail weergeven

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

tonen van IP-telefoon

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1

Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

ip nhs tonen

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0

Hub#show ip nhrp nhs (As the hub is the only NHS for this DMVPN cloud,
it does not have any servers configured)
```

dmvpn [details] tonen

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S

Spoke1#show dmvpn detail
```

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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 Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:

Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# 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: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket # 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 Tunnel0 is up/up, Addr. is 10.1.1.254, VRF "" Tunnel Src./Dest. addr:
172.16.10.1/MGRE, Tunnel VRF "" Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network ----- --------------- --
------------ ----- -------- ----- ----------------- 1 172.16.1.1 10.1.1.1 UP 00:01:32 D
10.1.1.1/32
```

```
Crypto Session Details:
-------------------------------------------------------------------------------- Interface:
Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

Gerelateerde informatie

- IPsec-probleemoplossing: Opdrachten begrijpen en gebruiken
- Encryptie van de volgende generatie
- RFC3706: IKE-detectie van dode peers
- RFC3947: IKE NAT-verplaatsing
- Technische ondersteuning en documentatie – Cisco Systems