IPsec-redundantie configureren met HSRP voor IKEv2 routegebaseerde tunnel op Cisco-routers

Inhoud

Inleiding

Dit document beschrijft hoe u IPsec-redundantie met HSRP voor IKEv2 op route gebaseerde tunnels op Cisco-routers kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Site-to-site VPN
- Hot Standby Router Protocol [HSRP]
- Basiskennis van IPsec en IKEv2

Gebruikte componenten

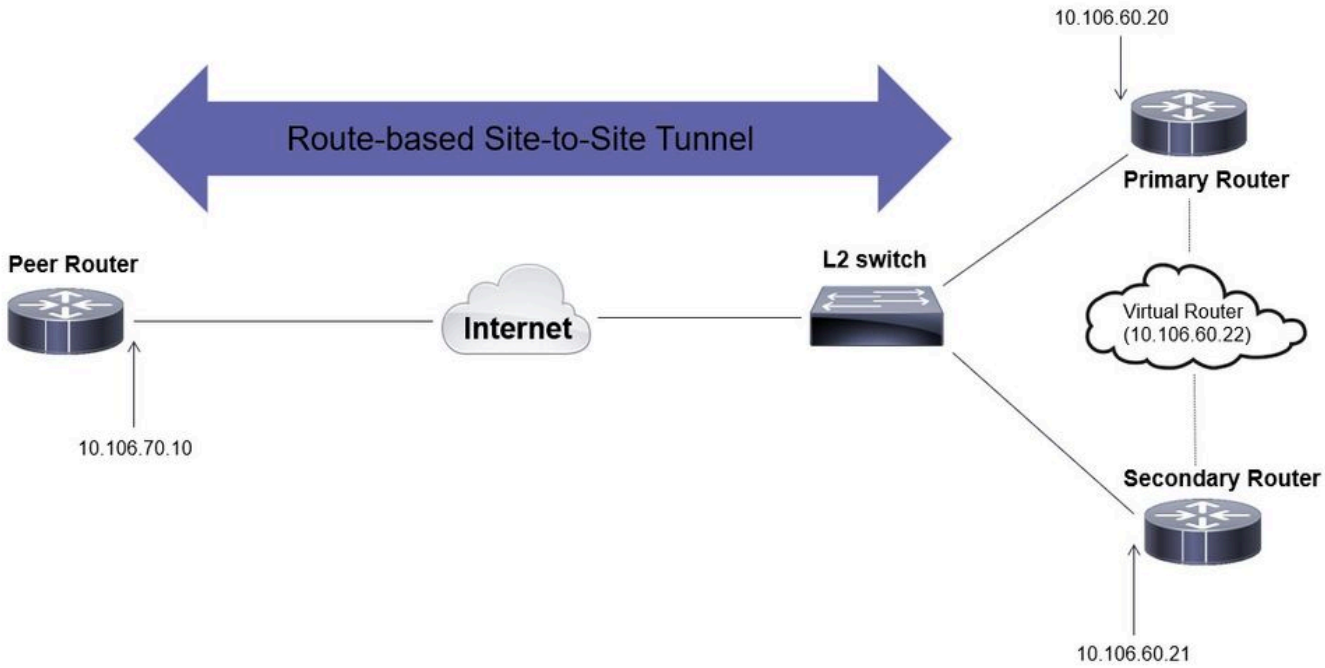
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco CSR1000v router met IOS XE-software, versie 17.03.08a
- Layer 2 switch met Cisco IOS-software, versie 15.2

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.

Configureren

Netwerkdiagram



Configuraties van primaire/secundaire router

De fysieke interface met HSRP configureren

Configureer de fysieke interfaces van de primaire (met een hogere prioriteit) en de secundaire

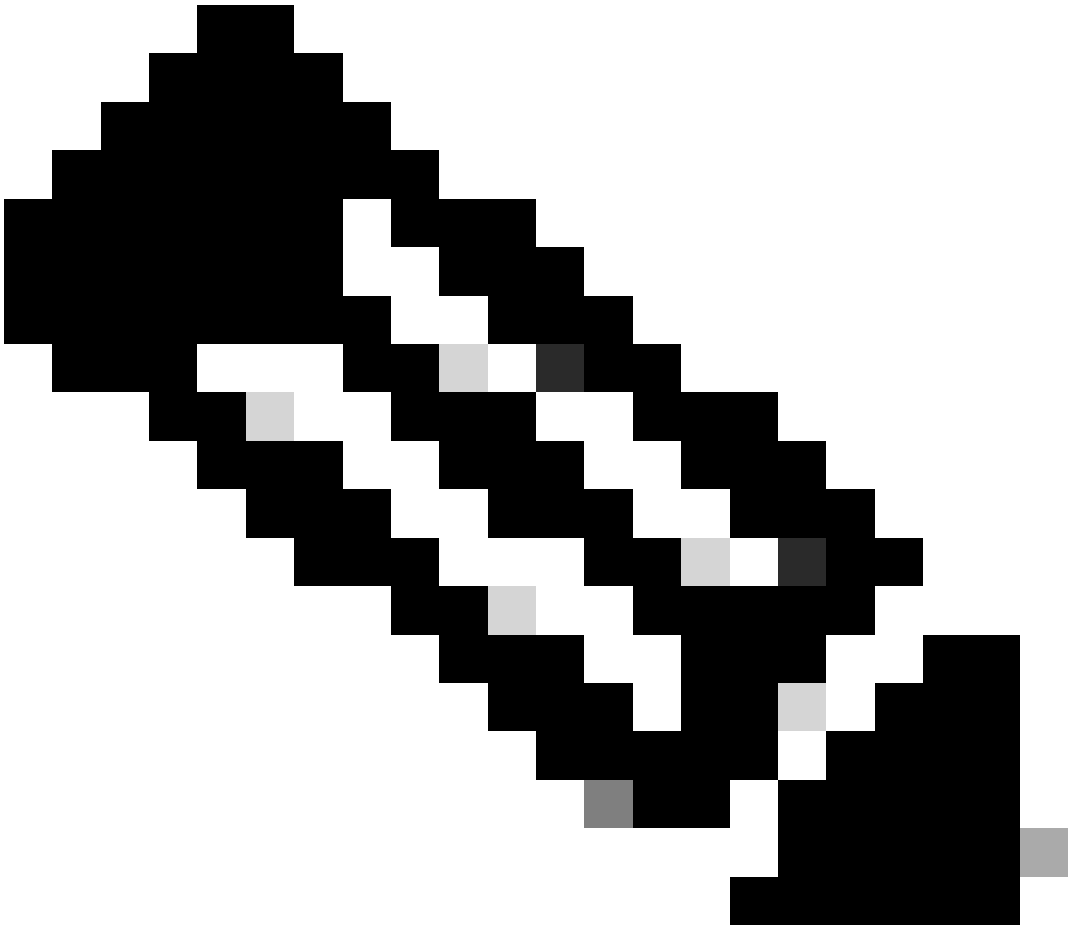
(met een standaardprioriteit van 100) routers:

primaire router:

```
interface GigabitEthernet1 ip address 10.106.60.20 255.255.255.0 standby 1 ip 10.106.60.22 standby 1 priority 105 standby 1 preempt standby 1 name VPN
```

Tweede router:

```
interface GigabitEthernet1 ip address 10.106.60.21 255.255.255.0 standby 1 ip 10.106.60.22 standby 1 preempt standby 1 name VPN-HSRP
```



Opmerking: Zorg ervoor dat de standaard primaire router is geconfigureerd met een hogere prioriteit om het de actieve peer te maken, zelfs wanneer beide routers zonder problemen actief zijn. Bij dit voorbeeld is de primaire router geconfigureerd met een

---

prioriteit van 105, terwijl de secundaire router een prioriteit van 100 heeft (wat het standaard is voor HSRP).

Het IKEv2-voorstel en -beleid configureren

Configureer een IKEv2 voorstel met de codering, hashing en DH groep van uw keuze en breng het in kaart met een IKEv2 beleid.

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

De sleutelhanger configureren

Configuratie van de sleutelring om de vooraf gedeelde sleutel op te slaan die zal worden gebruikt om de peer te verifiëren.

```
crypto ikev2 keyring keys
 peer 10.106.70.10
  address 10.106.70.10
  pre-shared-key local C!sco123
  pre-shared-key remote C!sco123
```

Het IKEv2-profiel configureren

Configureer het IKEv2-profiel en bevestig de toetsring eraan. Stel het lokale adres in op het virtuele IP-adres dat voor HSRP wordt gebruikt en het externe adres als IP van de interface met het internet van de router.

```
crypto ikev2 profile IKEv2_PROF
 match identity remote address 10.106.70.10 255.255.255.255
 identity local address 10.106.60.22
```

```
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
```

De IPsec-transformatie-set configureren

Configureer de parameters van fase 2 voor codering en hashing met de IPsec-transformatie.

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

Het IPsec-profiel configureren

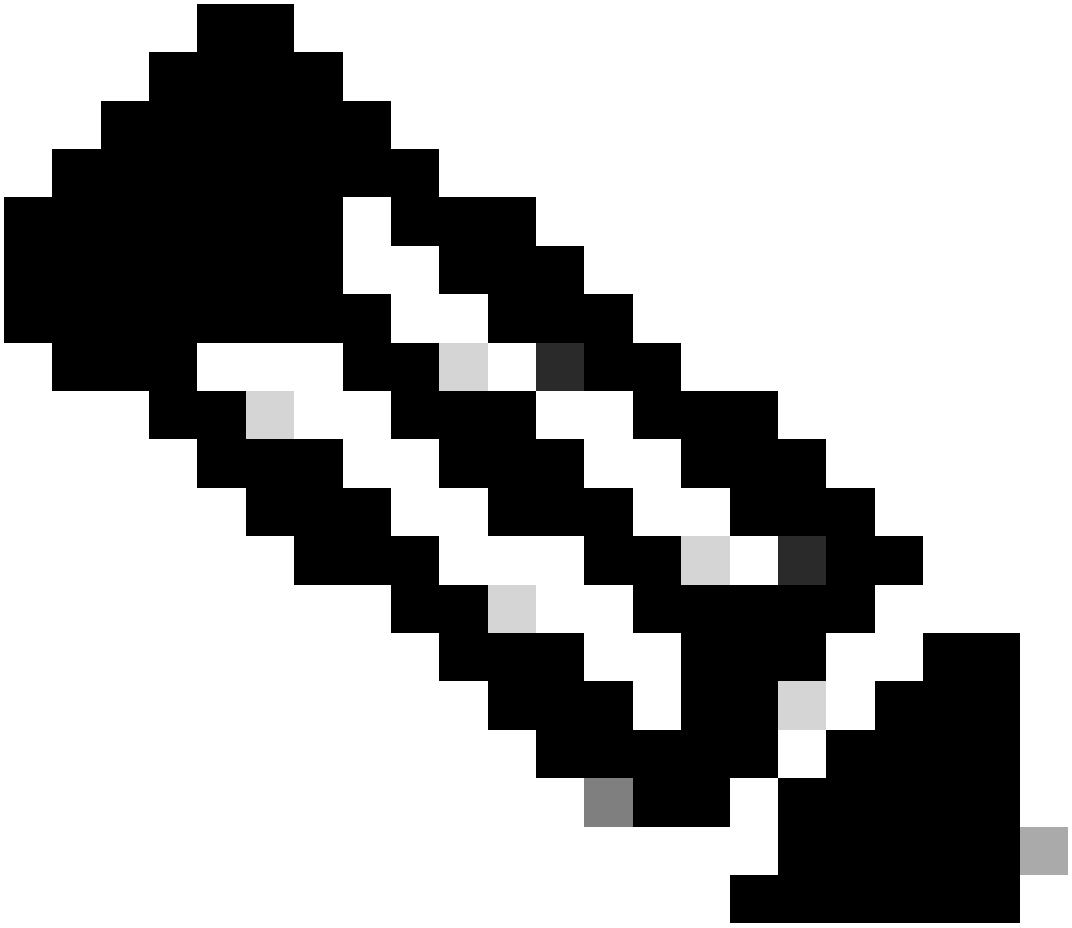
Configureer het IPsec-profiel om het IKEv2-profiel en de IPsec-transformatieset in kaart te brengen. Het IPsec-profiel wordt toegepast op de tunnelinterface.

```
crypto ipsec profile IPsec_PROF
 set transform-set ipsec-prop
 set ikev2-profile IKEv2_PROF
```

De virtuele tunnelinterface configureren

Configureer de virtuele tunnelinterface om de tunnelbron en de bestemming te specificeren. Deze IP's worden gebruikt om het verkeer via de tunnel te versleutelen. Zorg ervoor dat het IPsec-profiel ook op deze interface wordt toegepast, zoals hieronder wordt getoond.

```
interface Tunnel0
 ip address 10.10.10.10 255.255.255.0
 tunnel source 10.106.60.22
 tunnel mode ipsec ipv4
 tunnel destination 10.106.70.10
 tunnel protection ipsec profile IPsec_PROF
```



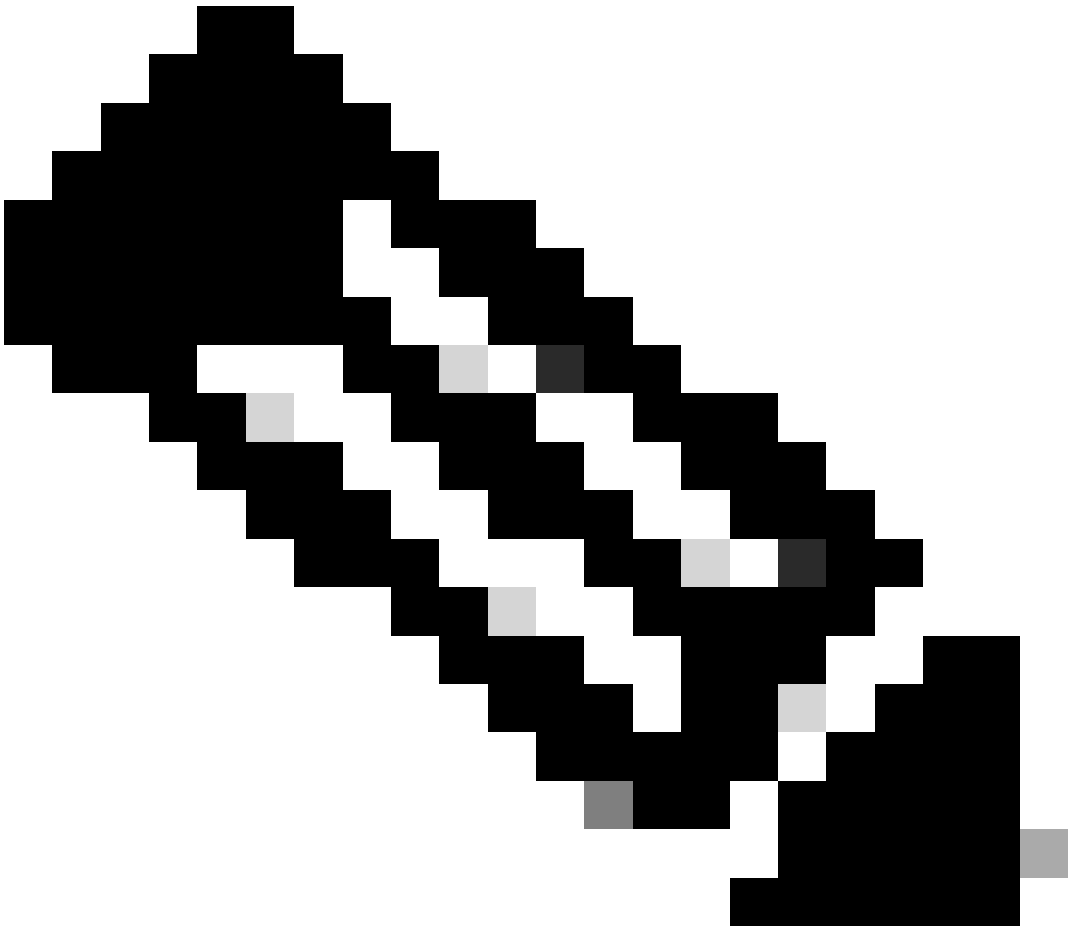
Opmerking: u moet de virtuele IP opgeven die voor HSRP als tunnelbron wordt gebruikt. Het gebruiken van de fysieke interface, in dit scenario Gigabit Ethernet1, zal de tunnelonderhandeling om veroorzaken te ontbreken.

Configureer de dynamische en/of statische routing

U moet de routing configureren met dynamische routeringsprotocollen en/of statische routes, afhankelijk van de vereisten en het netwerkontwerp. In dit voorbeeld wordt een combinatie van EIGRP en een statische route gebruikt om de onderliggende communicatie en de stroom van het verkeer van overlay-gegevens over de site-to-site tunnel tot stand te brengen.

```
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 10.106.60.0 0.0.0.255

ip route 192.168.30.0 255.255.255.0 Tunnel0
```



Opmerking: Zorg ervoor dat de tunnelinterfacesubnet, die in dit scenario 10.10.10.0/24 is, wordt geadverteerd.

Peer-routerconfiguraties

Het IKEv2-voorstel en -beleid configureren

Configureer een IKEv2 voorstel met de codering, hashing en DH groep van uw keuze en breng het in kaart met een IKEv2 beleid.

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha256
```

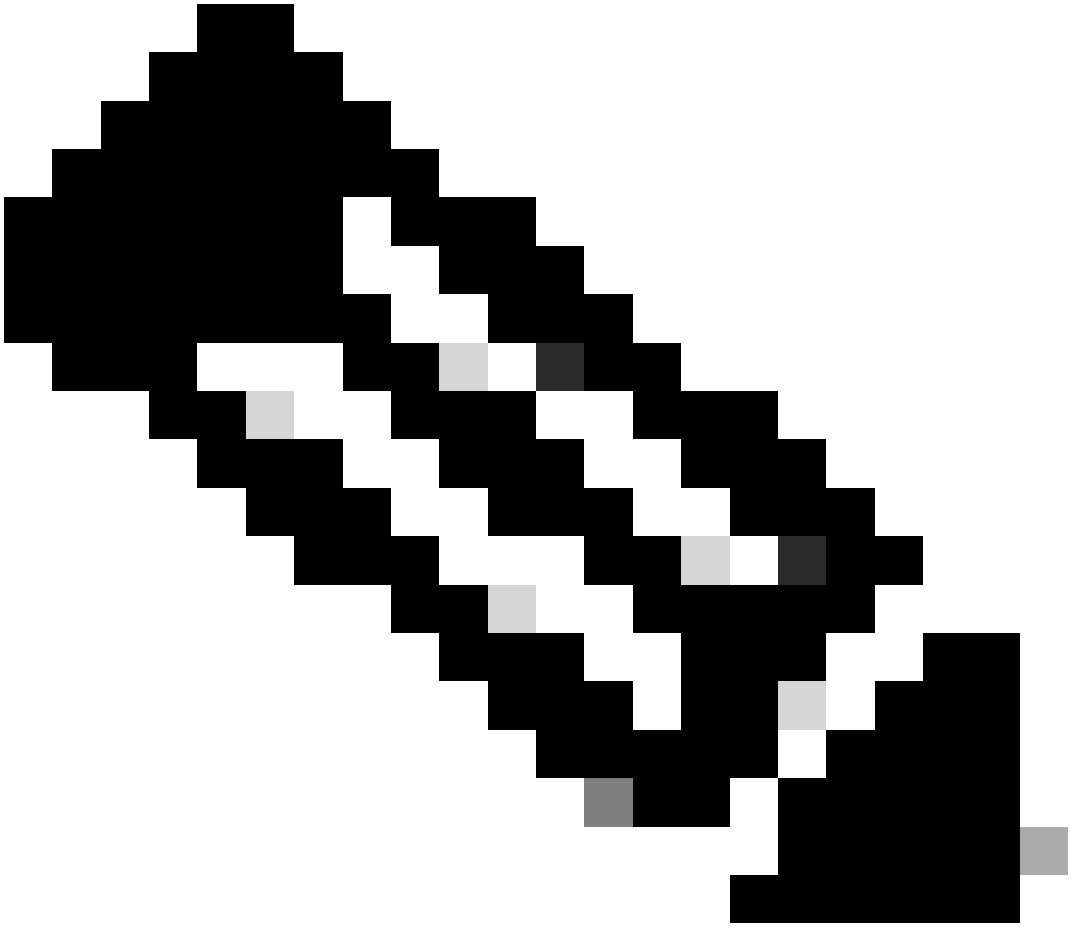
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

De sleutelhanger configureren

Configuratie van de sleutelring om de vooraf gedeelde sleutel op te slaan die zal worden gebruikt om de peer te verifiëren.

```
crypto ikev2 keyring keys
 peer 10.106.60.22
  address 10.106.60.22
  pre-shared-key local C!sco123
  pre-shared-key remote C!sco123
```



Opmerking: het peer IP-adres dat hier wordt gebruikt, is het virtuele IP-adres dat is ingesteld in de HSRP-configuratie van de peer. Zorg ervoor dat u de sleutelring voor de fysieke interface IP van de primaire/secundaire peer niet vormt.

Het IKEv2-profiel configureren

Configureer het IKEv2-profiel en bevestig de toetsring eraan. Stel het lokale adres in als IP van de interface met internet van de router en het externe adres naar het virtuele IP-adres dat voor HSRP wordt gebruikt op de primaire/secundaire peer.

```
crypto ikev2 profile IKEv2_PROF
 match identity remote address 10.106.60.22 255.255.255.255
 identity local address 10.106.70.10
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
```

De IPsec-transformatie-set configureren

Configureer de parameters van fase 2 voor codering en hashing met de IPsec-transformatie.

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

Het IPsec-profiel configureren

Configureer het IPsec-profiel om het IKEv2-profiel en de IPsec-transformatieset in kaart te brengen. Het IPsec-profiel wordt toegepast op de tunnelinterface.

```
crypto ipsec profile IPsec_PROF
 set transform-set ipsec-prop
 set ikev2-profile IKEv2_PROF
```

De virtuele tunnelinterface configureren

Configureer de virtuele tunnelinterface om de tunnelbron en de bestemming te specificeren. De tunnelbestemming moet worden ingesteld als het virtuele IP dat voor HSRP wordt gebruikt op de primaire/secundaire peer. Zorg ervoor dat het IPsec-profiel ook op deze interface wordt toegepast zoals aangegeven in de afbeelding.

```
interface Tunnel0
 ip address 10.10.10.11 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.106.60.22
 tunnel protection ipsec profile IPsec_PROF
```

Configureer de dynamische en/of statische routing

Configureer de gewenste routes met dynamische routeringsprotocollen of statische routes die vergelijkbaar zijn met de manier waarop u voor het andere eindpunt werkt.

```
router eigrp 10
```

```
network 10.10.10.0 0.0.0.255
network 10.106.70.0 0.0.0.255

ip route 192.168.10.0 255.255.255.0 Tunnel0
```

Verifiëren

Om inzicht te krijgen in het verwachte gedrag, worden de volgende drie scenario's gepresenteerd.

Scenario 1. Zowel primaire als secundaire routers zijn actief

Aangezien de primaire router met een hogere prioriteit wordt gevormd, wordt de IPsec-tunnel besproken en op deze router ingesteld. Om de staat van de twee routers te verifiëren, kunt u het show standbybevel gebruiken.

<#root>

pri-router#show standby
GigabitEthernet1 - Group 1

State is Active

7 state changes, last state change 00:00:21
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.864 secs
Preemption enabled

Active router is local

Standby router is 10.106.60.21, priority 100 (expires in 9.872 sec)

Priority 105 (configured 105)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 1/1

sec-router#show standby
GigabitEthernet1 - Group 1

State is Standby

11 state changes, last state change 00:00:49
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.888 secs
Preemption enabled

Active router is 10.106.60.20, priority 105 (expires in 8.768 sec)

Standby router is local

```
Priority 100 (default 100)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 0/1
```

Om de veiligheidsassociaties van fase 1 (IKEv2) en fase 2 (IPsec) voor de tunnel te verifiëren, kunt u de opdrachten show crypto ikev2 saen show crypto ipsec sagebruiken.

```
pri-router#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id            Local          Remote         fvrf/ivrf   Status
1              10.106.60.22/500 10.106.70.10/500   none/none   READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify:
Life/Active Time: 86400/444 sec

IPv6 Crypto IKEv2 SA

pri-router#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.106.70.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 36357, #pkts encrypt: 36357, #pkts digest: 36357
#pkts decaps: 36354, #pkts decrypt: 36354, #pkts verify: 36354
#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.: 10.106.60.22, remote crypto endpt.: 10.106.70.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x4967630D(1231512333)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xBA711B5E(3127974750)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2216, flow_id: CSR:216, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607986/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:
```

```
outbound esp sas:
spi: 0x4967630D(1231512333)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2215, flow_id: CSR:215, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607992/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Scenario 2. Primaire router is inactief en secundaire router is actief

In een scenario waar de primaire router een stroomonderbreking ervaart of daalt, zal de secundaire router de actieve router worden en de plaats-aan-plaats tunnel zal met deze router worden besproken.

De HSRP-status van de secundaire router kan opnieuw worden geverifieerd met behulp van de show standby opdracht.

<#root>

sec-router#show standby
GigabitEthernet1 - Group 1

State is Active

```
12 state changes, last state change 00:00:37
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.208 secs
Preemption enabled
```

Active router is local

```
Standby router is unknown
Priority 100 (default 100)
```

```
Group name is "VPN-HSRP" (cfgd)
FLAGS: 1/1
```

Bovendien zult u ook de volgende logbestanden observeren wanneer deze verstoring optreedt. Deze logboeken tonen ook aan dat de secundaire router nu actief is en de Tunnel is gevestigd.

*Jul 18 10:28:21.881: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Standby -> Active
*Jul 18 10:28:44.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Om de veiligheidsassociaties van fase 1 en fase 2 te controleren, kunt u de show crypto ikev2 saen show crypto ipsec sazoals hier getoond opnieuw gebruiken.

sec-router#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.106.60.22/500 10.106.70.10/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/480 sec

IPv6 Crypto IKEv2 SA

sec-router# show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.106.70.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 112, #pkts encrypt: 112, #pkts digest: 112
#pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112
#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.: 10.106.60.22, remote crypto endpt.: 10.106.70.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xFC4207BF(4232185791)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5F6EE796(1601103766)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2170, flow_id: CSR:170, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607988/3107)
IV size: 16 bytes

replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xFC4207BF(4232185791)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2169, flow_id: CSR:169, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607993/3107)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Scenario 3. De primaire router wordt back-up en de secundaire router wordt stand-by gezet

Zodra de primaire router wordt hersteld en niet meer neer is, wordt het opnieuw de actieve router aangezien het een hogere prioriteit gevormd heeft en de secundaire router gaat naar reservemodus.

Tijdens dit scenario ziet u deze logboeken op de primaire en secundaire routers wanneer deze overgang gebeurt.

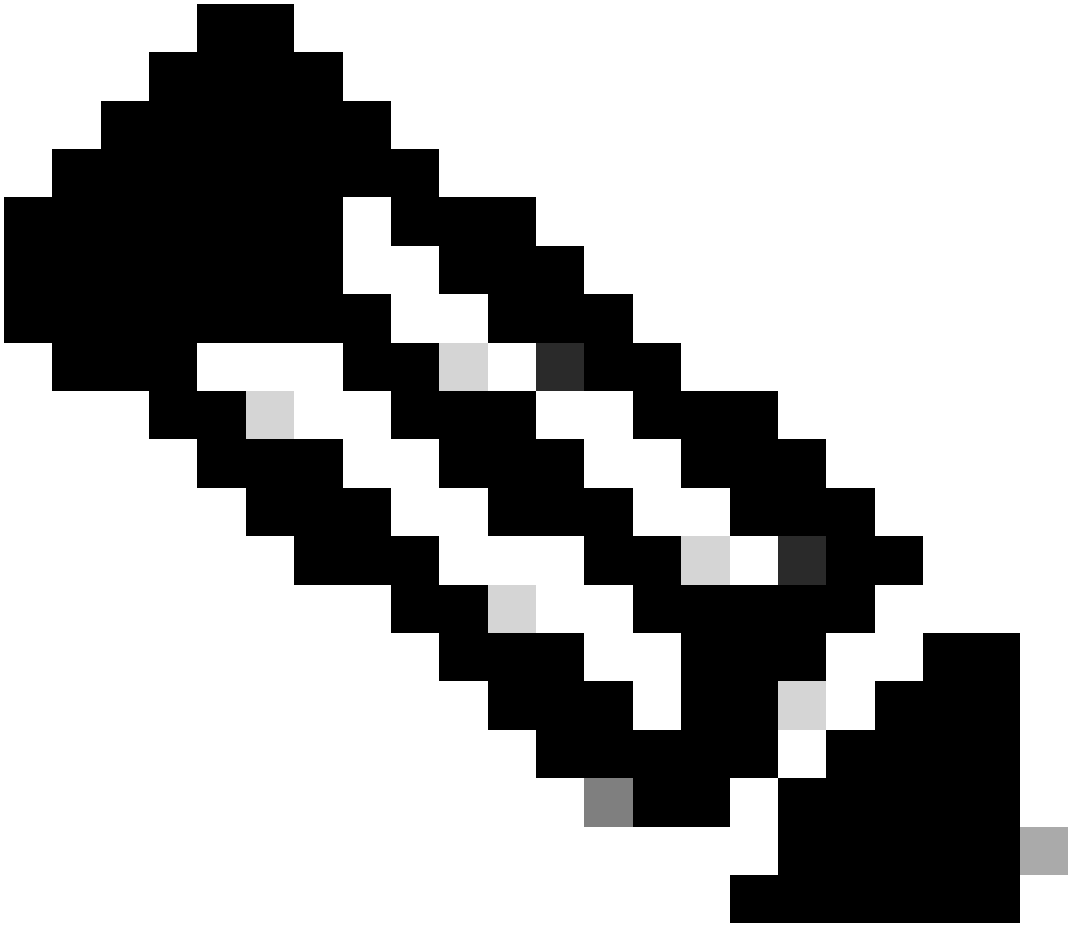
Op de primaire router, verschijnen deze logboeken:

*Jul 18 11:47:46.590: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Listen -> Active
*Jul 18 11:48:07.945: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Op de secundaire router, ziet u deze logboeken die aantonen dat de secundaire router opnieuw de standby router is geworden:

*Jul 18 11:47:46.370: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Active -> Speak
*Jul 18 11:47:52.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
*Jul 18 11:47:57.806: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Speak -> Standby

Om de status van de beveiligingsassociaties van fase 1 en fase 2 te controleren, kunt u de show crypto ikev2 saen **show crypto ipsec sa**de verificatie gebruiken.



Opmerking: Als u meerdere tunnels hebt geconfigureerd op de routers die actief zijn, kunt u de show crypto sessie externe X.X.X.X.X gebruiken en crypto ipsec tonen als peer X.X.X.X opdrachten om de fase 1 en fase 2 status van de tunnel te controleren.

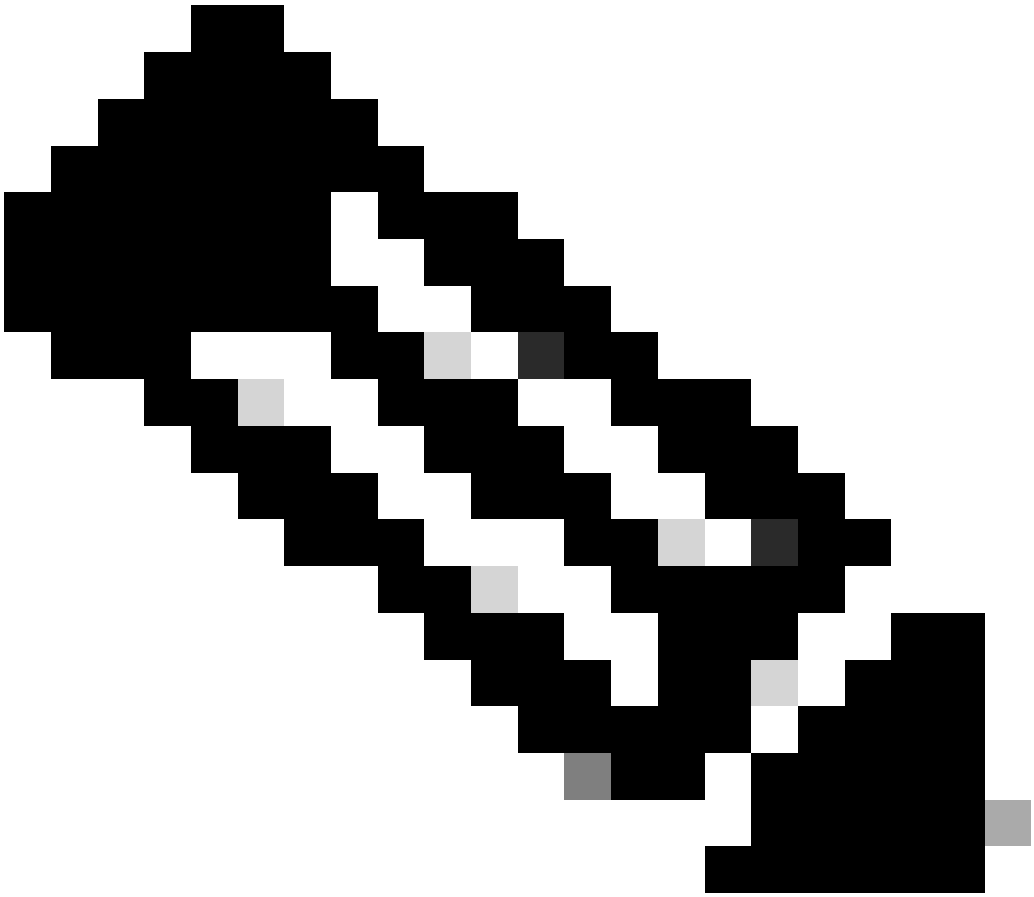
Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Deze debugs kunnen worden ingeschakeld om problemen op te lossen in de IKEv2-tunnel.

debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec

debug crypto ipsec error
debug crypto ipsec message



Opmerking: als u slechts één tunnel wilt oplossen (wat het geval moet zijn als het apparaat in productie is), moet u voorwaardelijke debugs inschakelen met de opdracht, debug crypto condition peer ipv4 X.X.X.X.

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.