Konfigurieren der IPsec-Redundanz mit HSRP für einen routenbasierten IKEv2-Tunnel auf Cisco Routern

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Konfigurieren
  - Netzwerkdiagramm
  - Primäre/sekundäre Router-Konfigurationen
    - Konfigurieren der physischen Schnittstelle mit HSRP
    - Konfigurieren des IKEv2-Angebots und der IKE-Richtlinie
    - Konfigurieren des Keyrings
    - Konfigurieren des IKEv2-Profils
    - Konfigurieren des IPsec-Transformationssatzes
    - Konfigurieren des IPsec-Profils
    - Konfigurieren der virtuellen Tunnelschnittstelle
    - Konfigurieren des dynamischen und/oder statischen Routings
  - Peer-Router-Konfigurationen
    - Konfigurieren des IKEv2-Angebots und der IKE-Richtlinie
    - Konfigurieren des Keyrings
    - Konfigurieren des IKEv2-Profils
    - Konfigurieren des IPsec-Transformationssatzes
    - Konfigurieren des IPsec-Profils
    - Konfigurieren der virtuellen Tunnelschnittstelle
    - Konfigurieren des dynamischen und/oder statischen Routings
- Überprüfung
  - Szenario 1. Sowohl primäre als auch sekundäre Router sind aktiv
  - Szenario 2. Der primäre Router ist inaktiv, und der sekundäre Router ist aktiv.
  - Szenario 3. Primärer Router wird wieder aktiviert und der sekundäre Router wird in den Standby-Modus versetzt
- Fehlerbehebung

Einleitung

In diesem Dokument wird die Konfiguration der IPsec-Redundanz mit HSRP für einen routenbasierten IKEv2-Tunnel auf Cisco Routern beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Standortübergreifendes VPN
- Hot Standby Router Protocol [HSRP]
- Grundkenntnisse von IPsec und IKEv2

Verwendete Komponenten

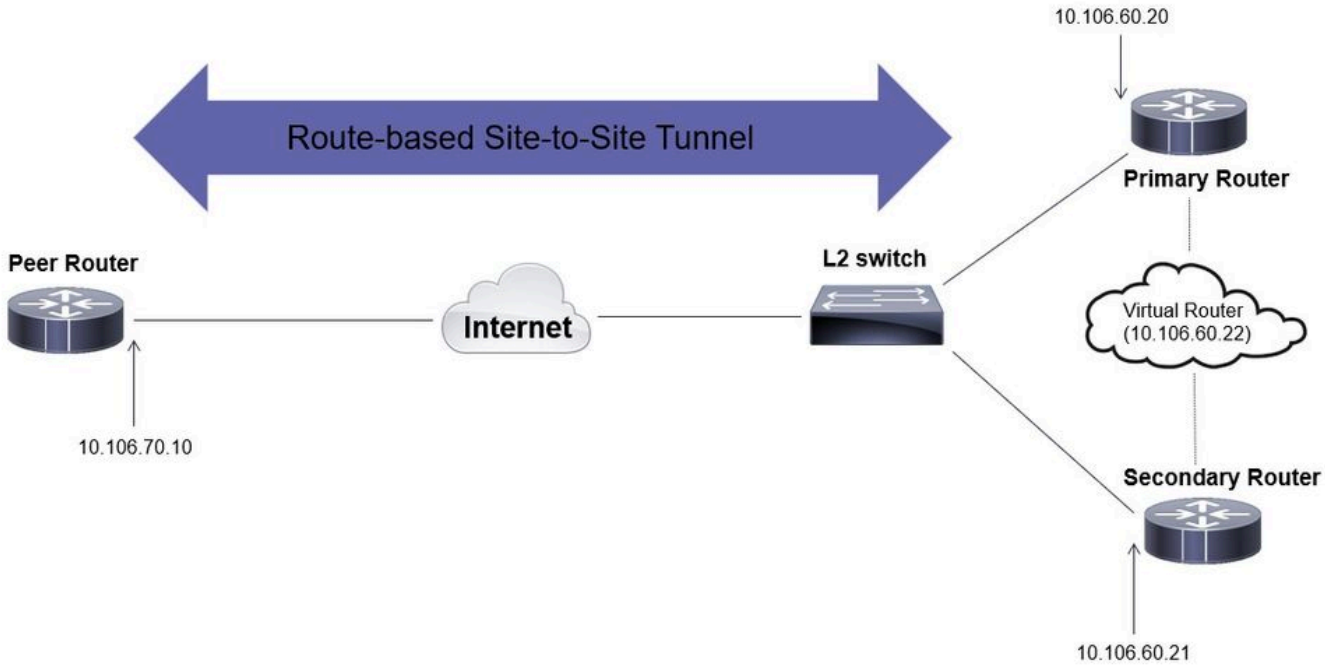
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco CSR1000v-Router mit IOS XE Software, Version 17.03.08a
- Layer-2-Switch mit Cisco IOS-Software, Version 15.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Primäre/sekundäre Router-Konfigurationen

Konfigurieren der physischen Schnittstelle mit HSRP

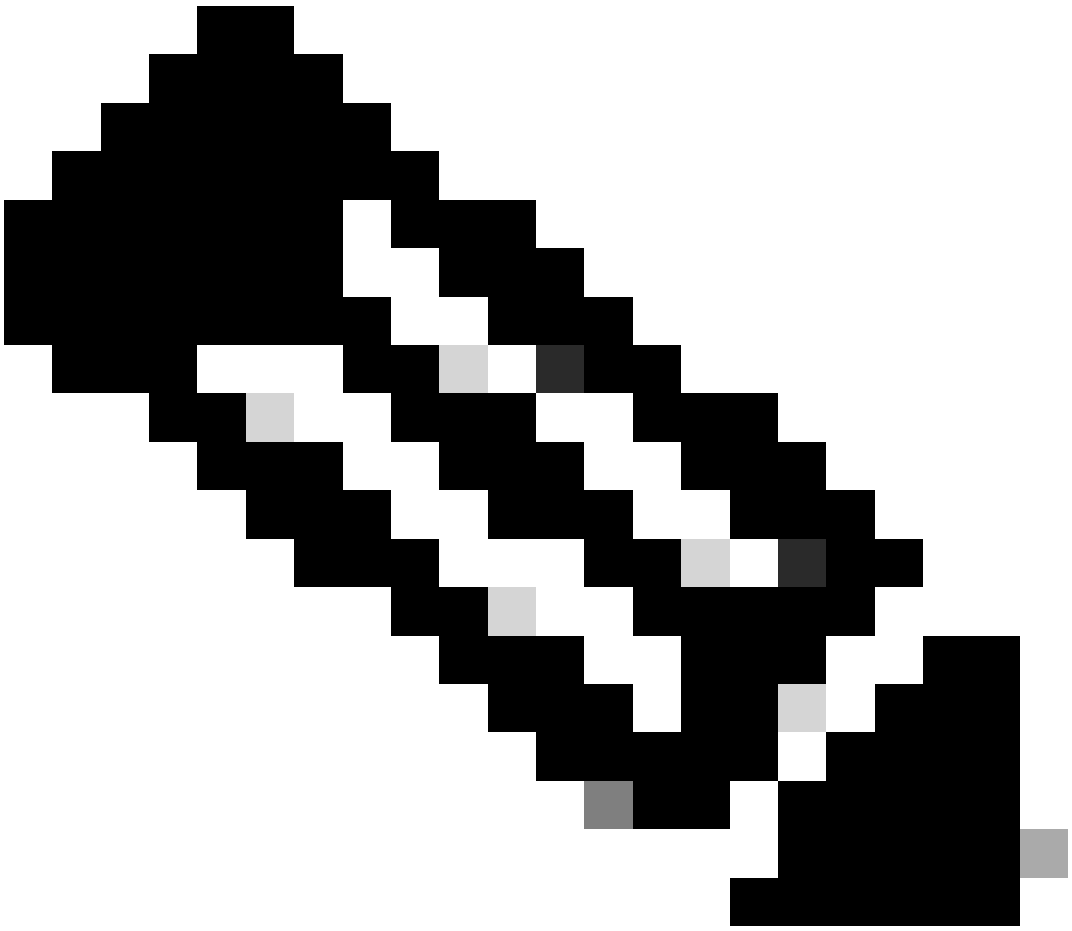
Konfigurieren Sie die physischen Schnittstellen der primären (mit einer höheren Priorität) und sekundären (mit einer Standardpriorität von 100) Router:

Primärer 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
```

Sekundärer 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
```



Hinweis: Stellen Sie sicher, dass der primäre Standardrouter mit einer höheren Priorität

---

konfiguriert ist, damit er selbst dann als aktiver Peer fungieren kann, wenn beide Router problemlos funktionieren. In diesem Beispiel wurde für den primären Router die Priorität 105 konfiguriert, während der sekundäre Router die Priorität 100 hat (dies ist der Standard für HSRP).

Konfigurieren des IKEv2-Angebots und der IKE-Richtlinie

Konfigurieren Sie ein IKEv2-Angebot mit der Verschlüsselungs-, Hashing- und DH-Gruppe Ihrer Wahl, und ordnen Sie es einer IKEv2-Richtlinie zu.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Konfigurieren des Keyrings

Konfigurieren Sie den Keyring, um den vorinstallierten Schlüssel zu speichern, der zur Authentifizierung des Peers verwendet wird.

```
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
```

Konfigurieren des IKEv2-Profils

Konfigurieren Sie das IKEv2-Profil, und schließen Sie den Keyring daran an. Legen Sie die lokale Adresse auf die virtuelle IP-Adresse fest, die für HSRP verwendet wird, und die Remote-Adresse auf die IP-Adresse der Internetschnittstelle des Routers.

```
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
```

Konfigurieren des IPsec-Transformationssatzes

Konfigurieren Sie die Phase-2-Parameter für Verschlüsselung und Hashing mit dem IPsec-Transformationssatz.

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

Konfigurieren des IPsec-Profils

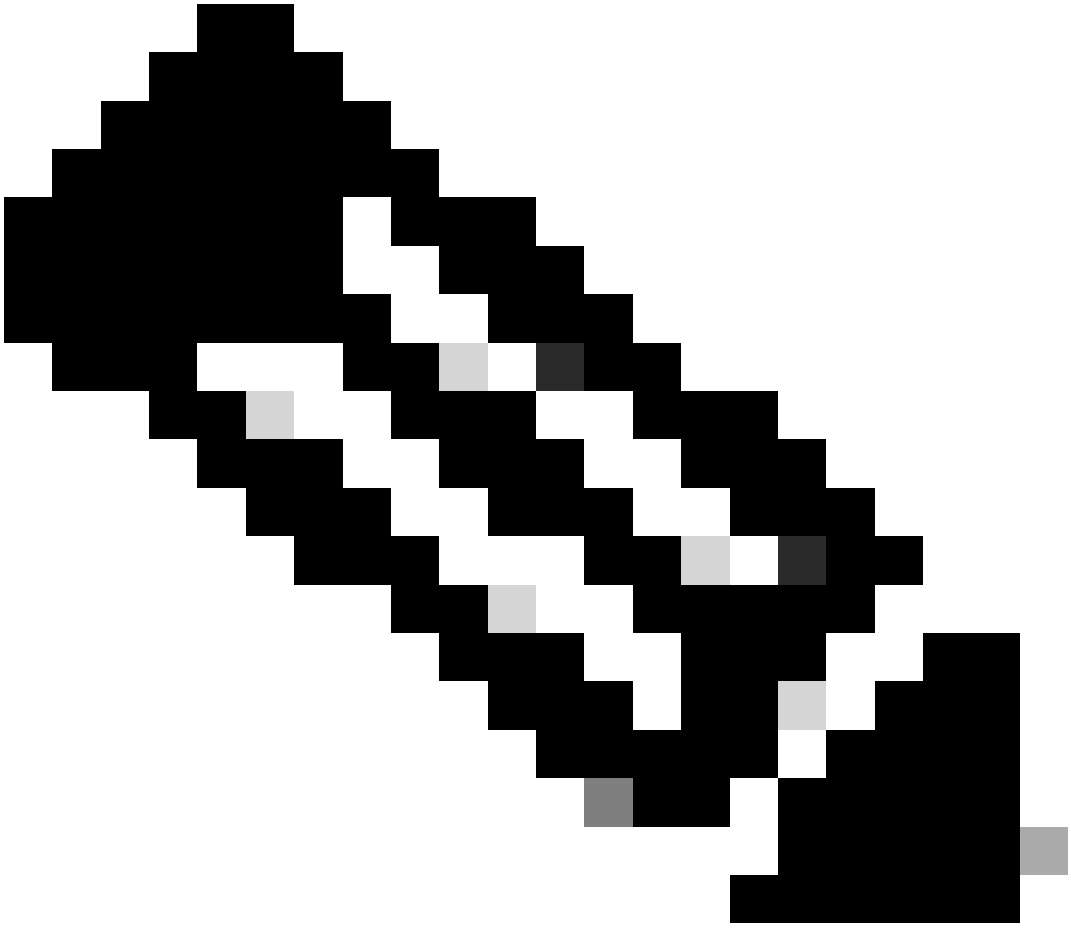
Konfigurieren Sie das IPsec-Profil, um das IKEv2-Profil und den IPsec-Transformationssatz zuzuordnen. Das IPsec-Profil wird auf die Tunnelschnittstelle angewendet.

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

Konfigurieren der virtuellen Tunnelschnittstelle

Konfigurieren Sie die virtuelle Tunnelschnittstelle, um die Tunnelquelle und das Tunnelziel anzugeben. Diese IPs werden verwendet, um den Datenverkehr über den Tunnel zu verschlüsseln. Stellen Sie sicher, dass das IPsec-Profil auch auf diese Schnittstelle angewendet wird, wie unten gezeigt.

```
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
```



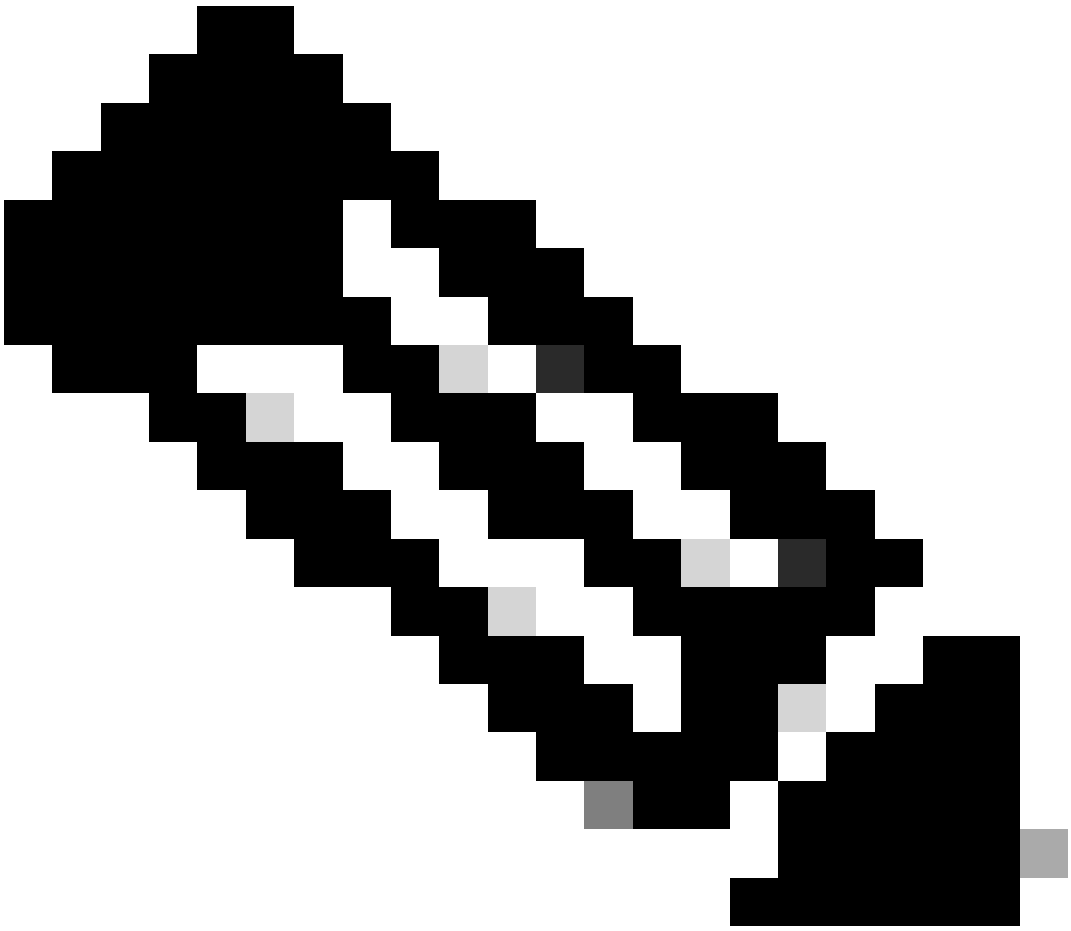
Hinweis: Sie müssen die virtuelle IP angeben, die für HSRP als Tunnelquelle verwendet wird. Bei Verwendung der physischen Schnittstelle GigabitEthernet1 schlägt die Tunnelaushandlung fehl.

Konfigurieren des dynamischen und/oder statischen Routings

Sie müssen das Routing je nach Anforderung und Netzwerkdesign mit dynamischen Routing-Protokollen und/oder statischen Routen konfigurieren. In diesem Beispiel wird eine Kombination aus EIGRP und einer statischen Route verwendet, um die Underlay-Kommunikation und den Fluss des Overlay-Datenverkehrs über den Site-to-Site-Tunnel einzurichten.

```
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
```



Hinweis: Stellen Sie sicher, dass das Subnetz der Tunnelschnittstelle, in diesem Szenario 10.10.10.0/24, angekündigt wird.

Peer-Router-Konfigurationen

Konfigurieren des IKEv2-Angebots und der IKE-Richtlinie

Konfigurieren Sie ein IKEv2-Angebot mit der Verschlüsselungs-, Hashing- und DH-Gruppe Ihrer Wahl, und ordnen Sie es einer IKEv2-Richtlinie zu.

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

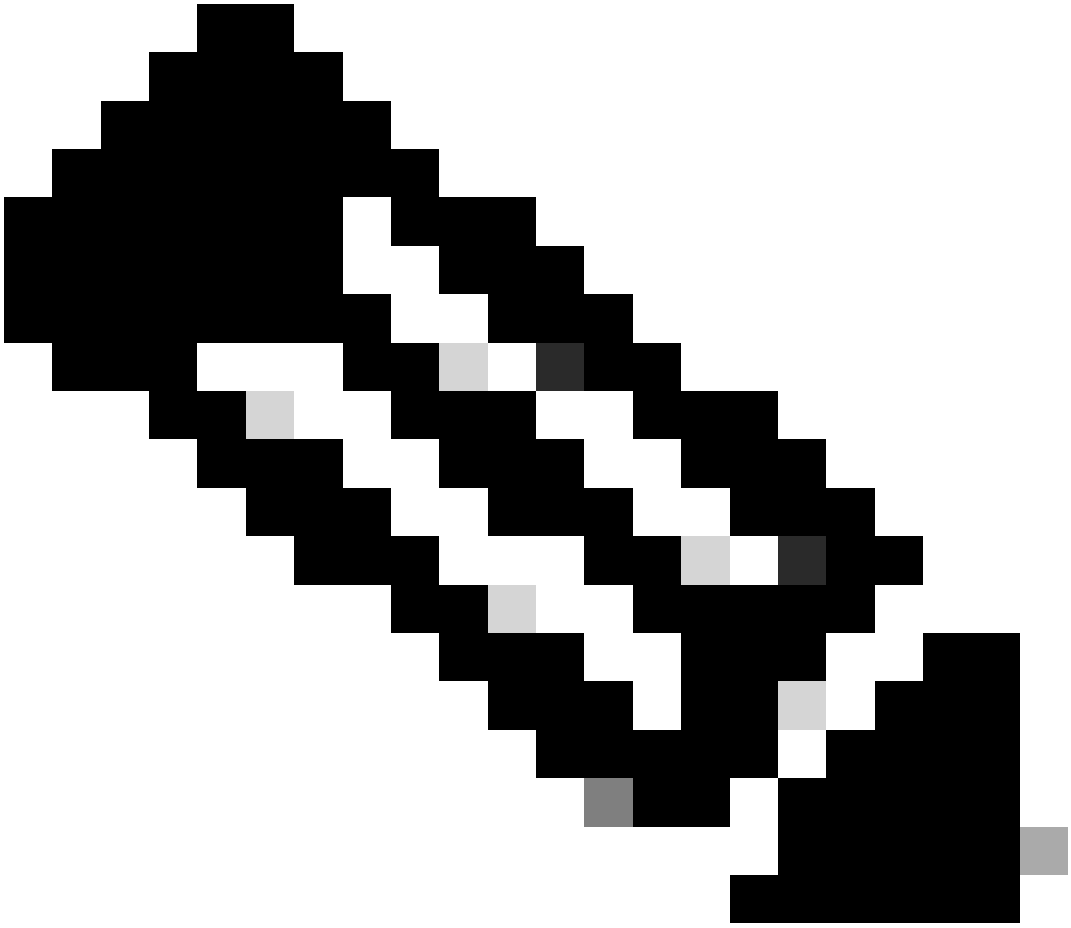
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Konfigurieren des Keyrings

Konfigurieren Sie den Keyring, um den vorinstallierten Schlüssel zu speichern, der zur Authentifizierung des Peers verwendet wird.

```
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
```



Hinweis: Die hier verwendete Peer-IP-Adresse ist die virtuelle IP-Adresse, die in der HSRP-Konfiguration des Peers konfiguriert ist. Stellen Sie sicher, dass Sie den Keyring nicht für die IP-Adresse der physischen Schnittstelle des primären/sekundären Peers konfigurieren.

Konfigurieren des IKEv2-Profils

Konfigurieren Sie das IKEv2-Profil, und schließen Sie den Keyring daran an. Legen Sie die lokale Adresse als IP der zum Internet gerichteten Schnittstelle des Routers und die Remote-Adresse als virtuelle IP-Adresse fest, die für HSRP auf dem primären/sekundären Peer verwendet wird.

```
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
```

Konfigurieren des IPsec-Transformationssatzes

Konfigurieren Sie die Phase-2-Parameter für Verschlüsselung und Hashing mit dem IPsec-Transformationssatz.

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

Konfigurieren des IPsec-Profils

Konfigurieren Sie das IPsec-Profil, um das IKEv2-Profil und den IPsec-Transformationssatz zuzuordnen. Das IPsec-Profil wird auf die Tunnelschnittstelle angewendet.

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

Konfigurieren der virtuellen Tunnelschnittstelle

Konfigurieren Sie die virtuelle Tunnelschnittstelle, um die Tunnelquelle und das Tunnelziel anzugeben. Das Tunnelziel muss als virtuelle IP festgelegt werden, die für HSRP auf dem primären/sekundären Peer verwendet wird. Stellen Sie sicher, dass das IPsec-Profil auch auf diese Schnittstelle angewendet wird, wie dargestellt.

```
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
```

Konfigurieren des dynamischen und/oder statischen Routings

Konfigurieren Sie die erforderlichen Routen mit dynamischen Routing-Protokollen oder statischen Routen, ähnlich wie beim anderen Endpunkt.

```
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
```

Überprüfung

Um das erwartete Verhalten zu verstehen, werden die folgenden drei Szenarien vorgestellt.

Szenario 1. Sowohl primäre als auch sekundäre Router sind aktiv

Da der primäre Router mit einer höheren Priorität konfiguriert ist, wird der IPsec-Tunnel auf diesem Router ausgehandelt und eingerichtet. Mit dem show standbyBefehl können Sie den Status der beiden Router überprüfen.

<#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
```

Um die Sicherheitszuordnungen für Phase 1 (IKEv2) und Phase 2 (IPsec) für den Tunnel zu überprüfen, können Sie die show crypto ikev2 saund-show crypto ipsec saBefehle verwenden.

```
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:
```

Szenario 2. Der primäre Router ist inaktiv, und der sekundäre Router ist aktiv.

In einem Szenario, in dem der primäre Router ausfällt oder ausfällt, wird der sekundäre Router zum aktiven Router, und der Site-to-Site-Tunnel wird mit diesem Router ausgehandelt.

Der HSRP-Status des sekundären Routers kann mithilfe des show standby Befehls erneut überprüft werden.

<#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
```

Darüber hinaus beobachten Sie bei dieser Unterbrechung auch die folgenden Protokolle. Diese Protokolle zeigen auch, dass der sekundäre Router jetzt aktiv ist und der Tunnel eingerichtet wurde.

*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

Um die Sicherheitszuordnungen für Phase 1 und Phase 2 zu überprüfen, können Sie erneut das show crypto ikev2 saund verwenden, show crypto ipsec sawie hier gezeigt.

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:

Szenario 3. Primärer Router wird wieder aktiviert und der sekundäre Router wird in den Standby-Modus versetzt

Sobald der primäre Router wiederhergestellt und nicht mehr ausgefallen ist, wird er wieder zum aktiven Router, da eine höhere Priorität konfiguriert wurde und der sekundäre Router in den Standby-Modus wechselt.

In diesem Szenario werden diese Protokolle beim Übergang auf dem primären und sekundären Router angezeigt.

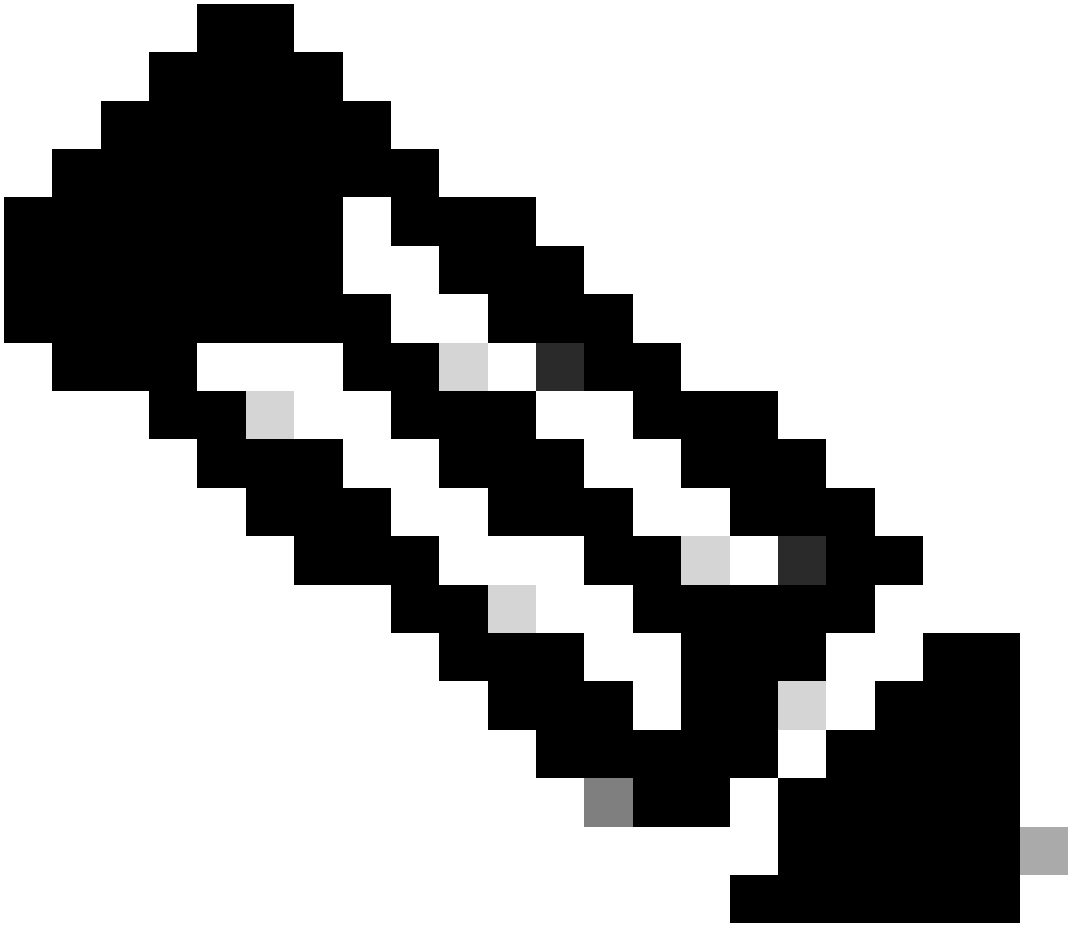
Auf dem primären Router werden folgende Protokolle angezeigt:

*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

Auf dem sekundären Router sehen Sie diese Protokolle, die zeigen, dass der sekundäre Router wieder zum Standby-Router geworden ist:

*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

Um den Status der Sicherheitszuordnungen für Phase 1 und Phase 2 zu überprüfen, können Sie show crypto ikev2 saund **show crypto ipsec sa**verwenden.



Hinweis: Wenn auf den aktiven Routern mehrere Tunnel konfiguriert sind, können Sie die Befehle show crypto session remote X.X.X.X und show crypto ipsec als X.X.X.X-Befehle für Peers verwenden, um den Status von Phase 1 und Phase 2 des Tunnels zu überprüfen.

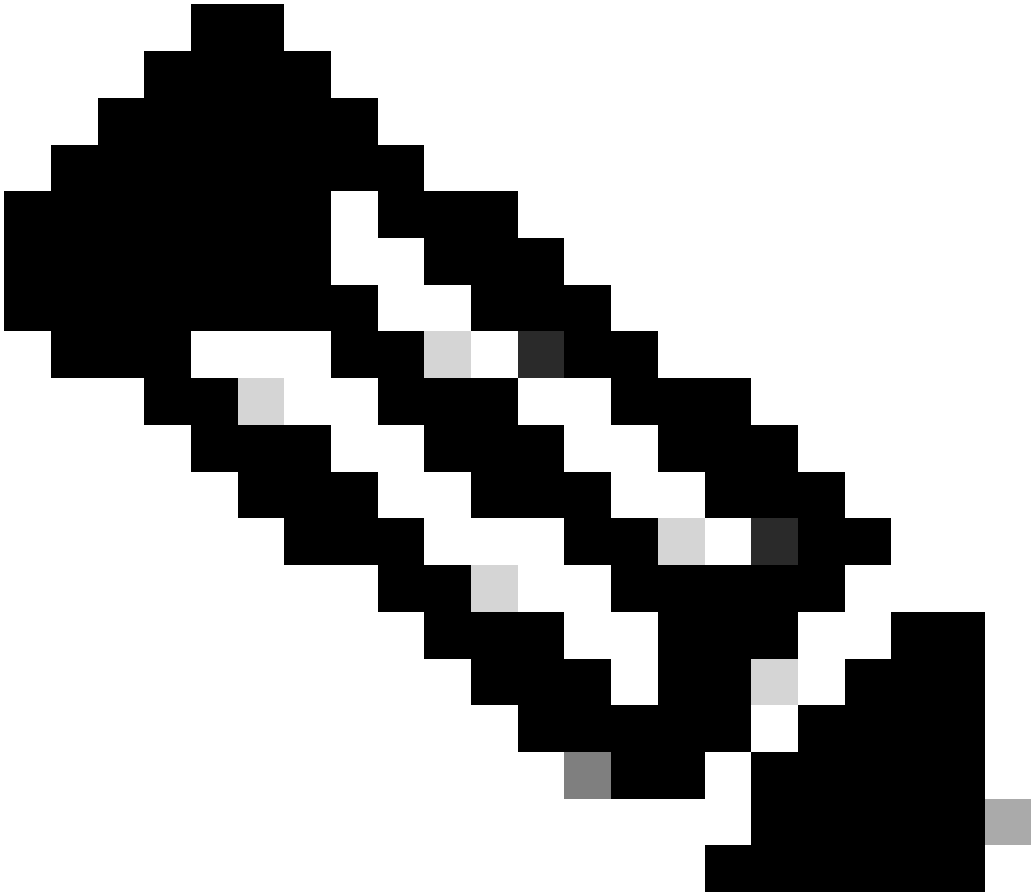
Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Diese Debug-Funktionen können aktiviert werden, um Fehler im IKEv2-Tunnel zu beheben.

debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 internal

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message



Hinweis: Wenn Sie nur einen Tunnel (was der Fall sein muss, wenn sich das Gerät in der Produktion befindet) beheben möchten, müssen Sie bedingtes Debuggen mit dem Befehl debug crypto condition peer ipv4 X.X.X.X.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.