

Cisco 라우터에서 IKEv2 경로 기반 터널용 HSRP를 사용하여 IPsec 이중화 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[기본/보조 라우터 컨피그레이션](#)

[HSRP를 사용하여 물리적 인터페이스 구성](#)

[IKEv2 제안 및 정책 구성](#)

[키구성](#)

[IKEv2 프로파일 구성](#)

[IPsec Transform-Set 구성](#)

[IPsec 프로필 구성](#)

[가상 터널 인터페이스 구성](#)

[동적 및/또는 정적 라우팅 구성](#)

[피어 라우터 컨피그레이션](#)

[IKEv2 제안 및 정책 구성](#)

[키구성](#)

[IKEv2 프로파일 구성](#)

[IPsec Transform-Set 구성](#)

[IPsec 프로필 구성](#)

[가상 터널 인터페이스 구성](#)

[동적 및/또는 정적 라우팅 구성](#)

[다음을 확인합니다.](#)

[시나리오 1. 기본 및 보조 라우터가 모두 활성 상태임](#)

[시나리오 2. 기본 라우터는 비활성 상태이고 보조 라우터는 활성 상태입니다.](#)

[시나리오 3. 기본 라우터가 다시 작동하고 보조 라우터가 대기 상태로 전환됨](#)

[문제 해결](#)

소개

이 문서에서는 Cisco 라우터에서 IKEv2 경로 기반 터널용 HSRP를 사용하여 IPsec 이중화를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 사이트 대 사이트 VPN
- HSRP(Hot Standby Router Protocol)
- IPsec 및 IKEv2에 대한 기본 지식

사용되는 구성 요소

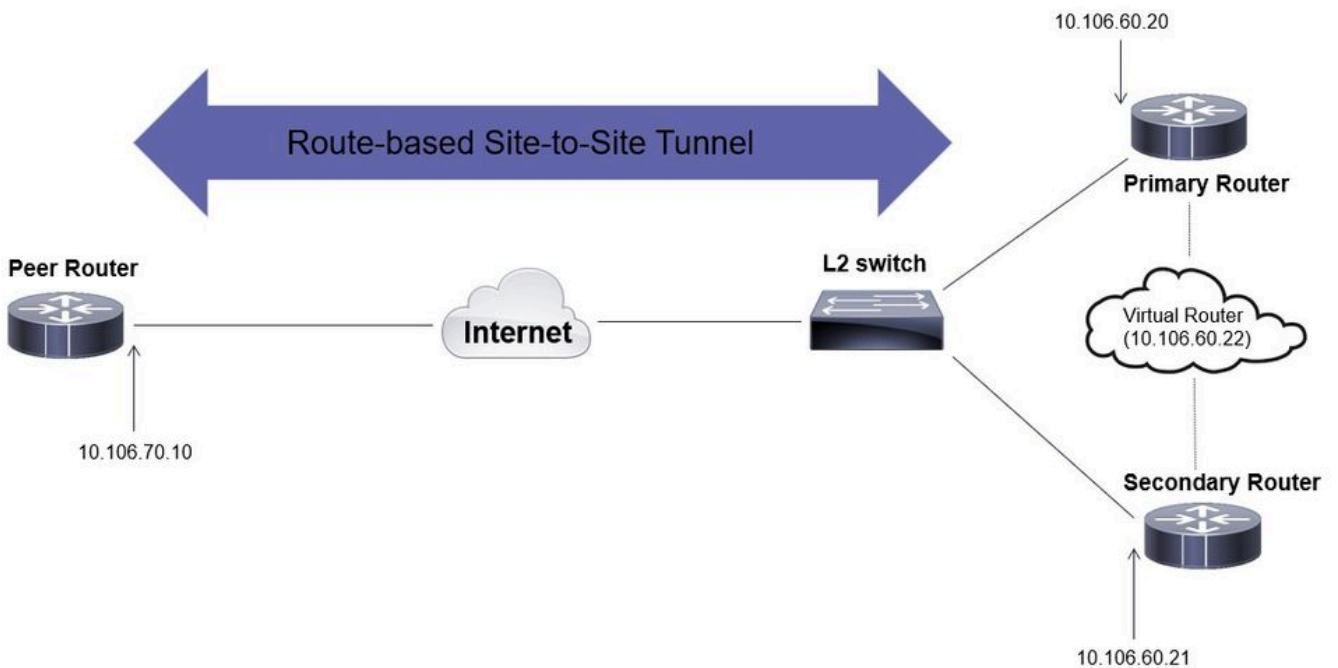
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS XE Software를 실행하는 Cisco CSR1000v 라우터, 버전 17.03.08a
- Cisco IOS Software, 버전 15.2를 실행하는 레이어 2 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



기본/보조 라우터 컨피그레이션

HSRP를 사용하여 물리적 인터페이스 구성

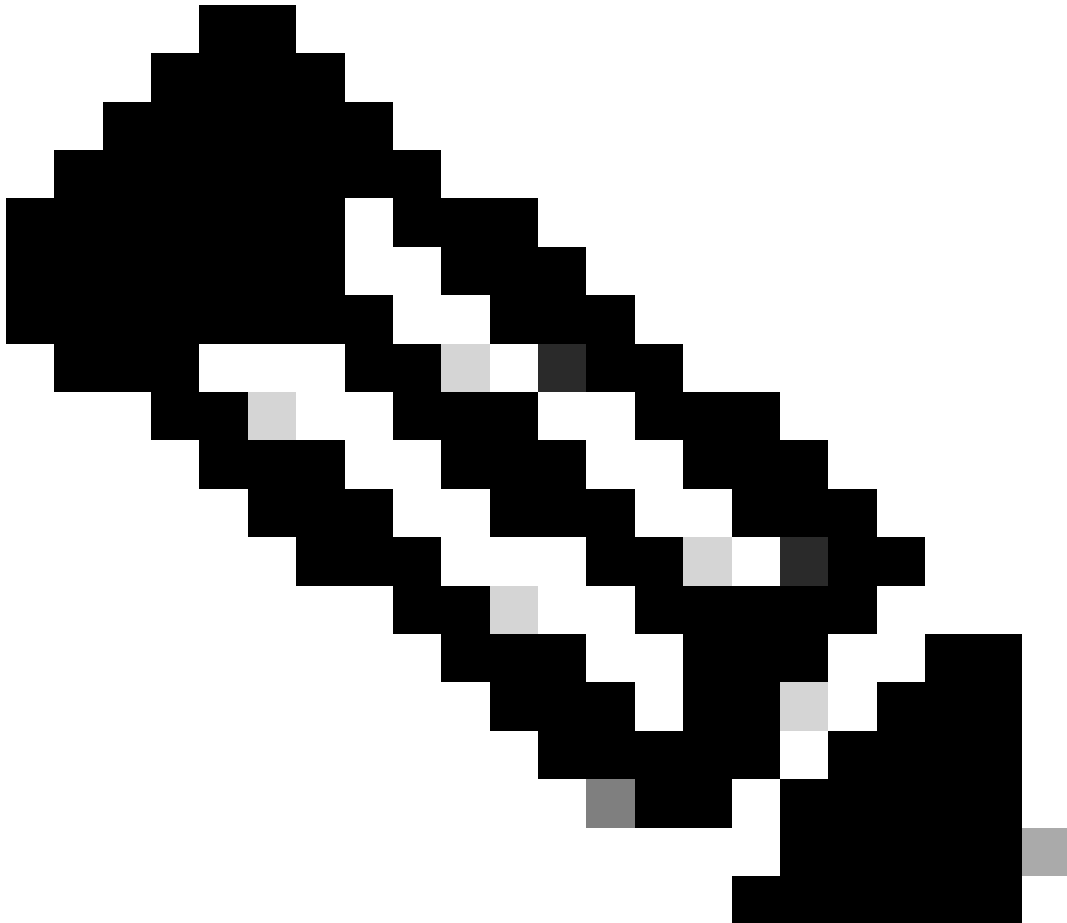
기본(우선 순위가 더 높음) 및 보조(기본 우선 순위가 100인) 라우터의 물리적 인터페이스를 구성합니다.

기본 라우터:

```
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
```

보조 라우터:

```
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
```



참고: 두 라우터가 모두 작동 및 실행 중일 때에도 활성 피어로 만들기 위해 기본 라우터가 더 높은 우선순위로 구성되어 있는지 확인하십시오. 이 예에서 기본 라우터는 우선순위 105로 구성된 반면 보조 라우터는 우선순위 100(HSRP의 기본값)입니다.

IKEv2 제안 및 정책 구성

선택한 암호화, 해싱 및 DH 그룹으로 IKEv2 제안서를 구성하고 IKEv2 정책에 매핑합니다.

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

crypto ikev2 policy IKEv2_POL
  proposal prop-1
```

키 구성

피어를 인증하는 데 사용할 사전 공유 키를 저장하도록 키를 구성합니다.

```
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
```

IKEv2 프로파일 구성

IKEv2 프로필을 구성하고 여기에 키를 연결합니다. 로컬 주소를 HSRP에 사용되는 가상 IP 주소로 설정하고 원격 주소를 라우터의 인터넷 연결 인터페이스의 IP로 설정합니다.

```
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
```

IPsec Transform-Set 구성

IPsec transform-set을 사용하여 암호화 및 해싱의 2단계 매개변수를 구성합니다.

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

IPsec 프로파일 구성

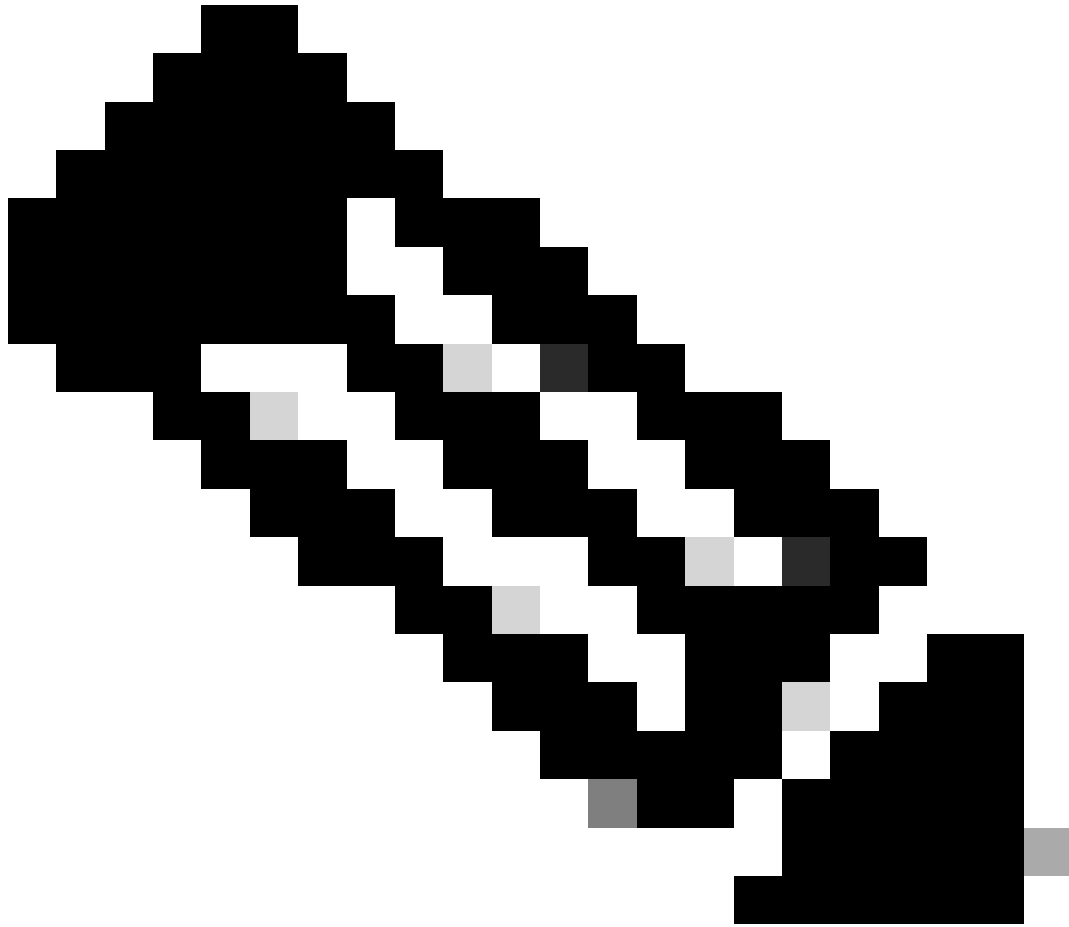
IKEv2 프로파일과 IPsec 변형 집합을 매핑하도록 IPsec 프로파일을 구성합니다. IPsec 프로파일이 터널 인터페이스에 적용됩니다.

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

가상 터널 인터페이스 구성

터널 소스 및 대상을 지정하도록 가상 터널 인터페이스를 구성합니다. 이러한 IP는 터널을 통해 트래픽을 암호화하는 데 사용됩니다. 아래에 표시된 대로 IPsec 프로파일도 이 인터페이스에 적용되어야 합니다.

```
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
```



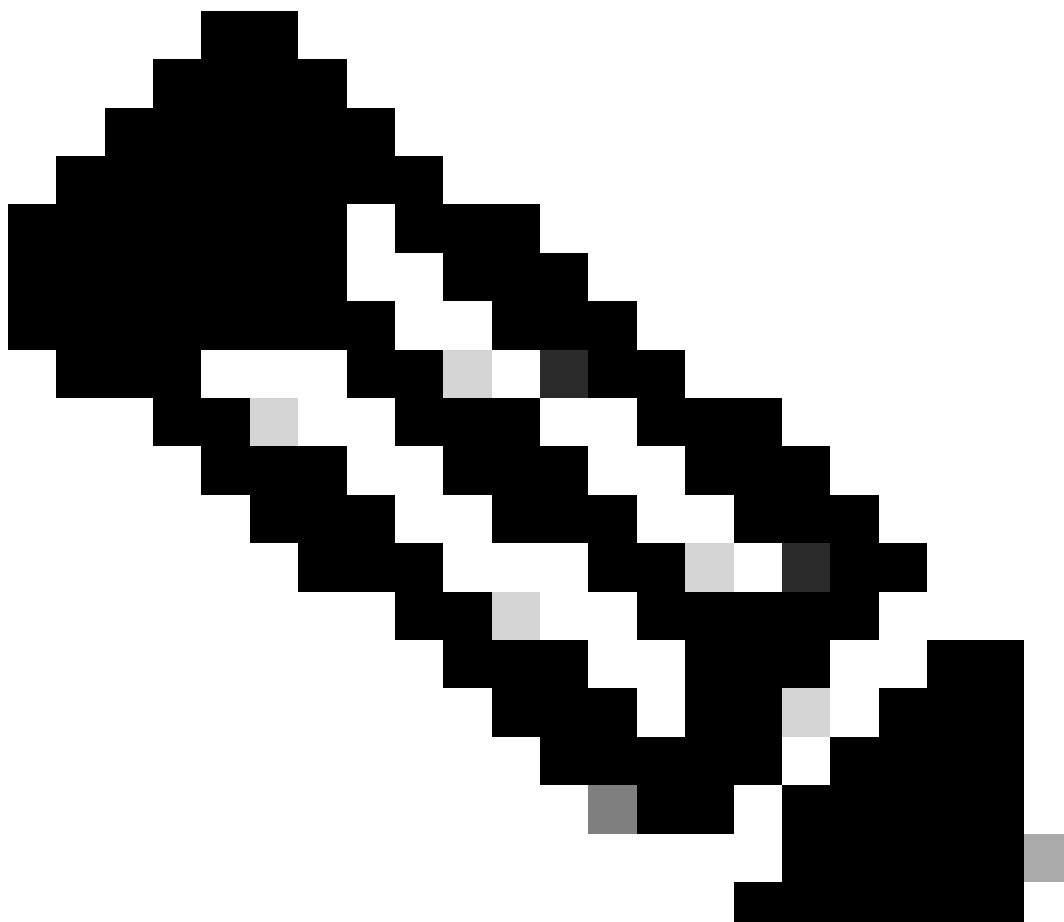
참고: 터널 소스로 HSRP에 사용 중인 가상 IP를 지정해야 합니다. 이 시나리오에서 GigabitEthernet1의 물리적 인터페이스를 사용하면 터널 협상이 실패합니다.

동적 및/또는 정적 라우팅 구성

요구 사항 및 네트워크 설계에 따라 동적 라우팅 프로토콜 및/또는 고정 경로를 사용하여 라우팅을 구성해야 합니다. 이 예에서는 EIGRP와 고정 경로의 조합을 사용하여 언더레이 통신 및 사이트 대 사이트 터널을 통한 오버레이 데이터 트래픽의 흐름을 설정합니다.

```
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 Tunne10
```



참고: 이 시나리오에서 10.10.10.0/24인 터널 인터페이스 서브넷이 알려지고 있는지 확인하십시오.

피어 라우터 컨피그레이션

IKEv2 제안 및 정책 구성

선택한 암호화, 해싱 및 DH 그룹으로 IKEv2 제안서를 구성하고 IKEv2 정책에 매핑합니다.

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

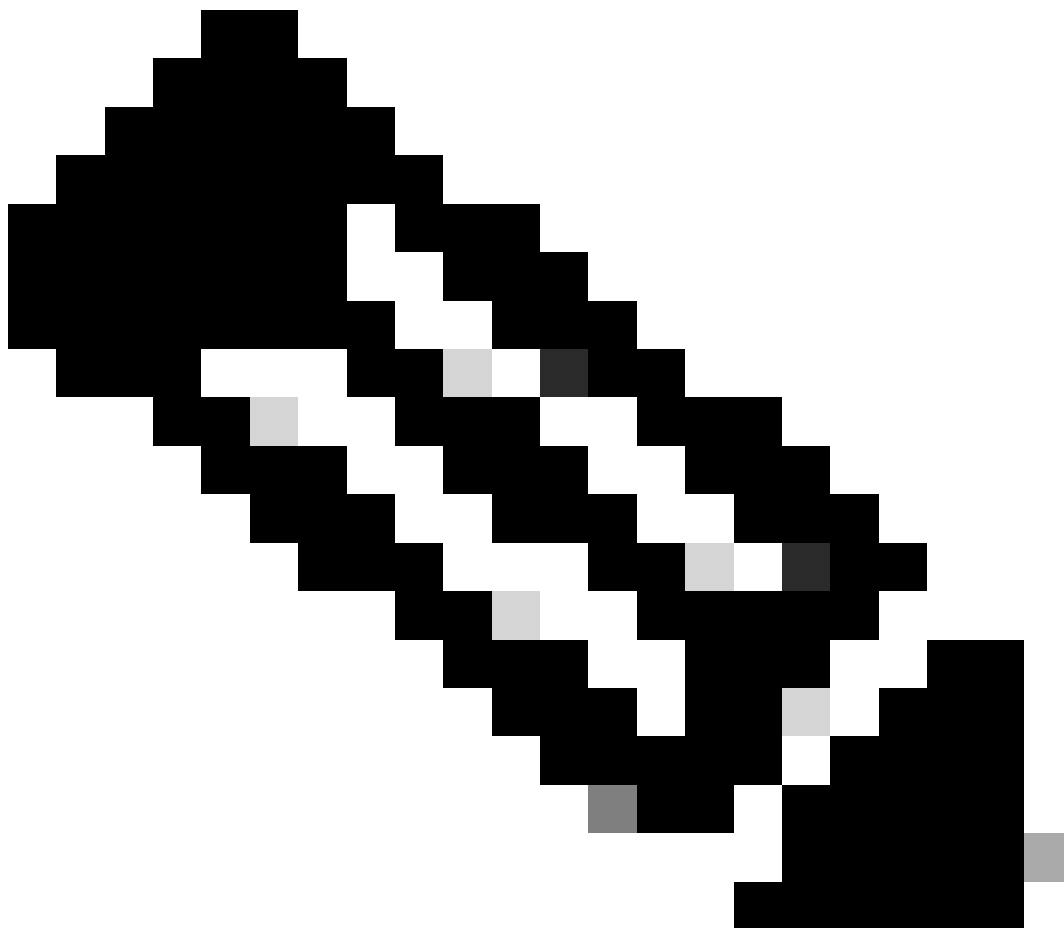
```
crypto ikev2 policy IKEv2_POL
```

proposal prop-1

키 구성

피어를 인증하는 데 사용할 사전 공유 키를 저장하도록 키를 구성합니다.

```
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
```



참고: 여기에서 사용되는 피어 IP 주소는 피어의 HSRP 컨피그레이션에 구성된 가상 IP 주소입니다. 기본/보조 피어의 물리적 인터페이스 IP에 대한 키링을 구성하지 않아야 합니다.

IKEv2 프로파일 구성

IKEv2 프로필을 구성하고 여기에 키를 연결합니다. 로컬 주소를 라우터의 인터넷 연결 인터페이스의 IP로 설정하고 원격 주소를 기본/보조 피어에서 HSRP에 사용되는 가상 IP 주소로 설정합니다.

```
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
```

IPsec Transform-Set 구성

IPsec transform-set을 사용하여 암호화 및 해싱의 2단계 매개변수를 구성합니다.

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

IPsec 프로파일 구성

IKEv2 프로파일과 IPsec 변형 집합을 매핑하도록 IPsec 프로필을 구성합니다. IPsec 프로필이 터널 인터페이스에 적용됩니다.

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

가상 터널 인터페이스 구성

터널 소스 및 대상을 지정하도록 가상 터널 인터페이스를 구성합니다. 터널 대상을 기본/보조 피어에서 HSRP에 사용되는 가상 IP로 설정해야 합니다. 그림과 같이 IPsec 프로필도 이 인터페이스에 적용되어야 합니다.

```
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
```

동적 및/또는 정적 라우팅 구성

동적 라우팅 프로토콜 또는 다른 엔드포인트와 유사한 고정 경로를 사용하여 필요한 경로를 구성합니다.

```
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
```

다음을 확인합니다.

예상되는 행동을 이해하기 위해 다음 세 가지 시나리오를 제시한다.

시나리오 1. 기본 및 보조 라우터가 모두 활성 상태임

기본 라우터가 더 높은 우선순위로 구성되었으므로 IPsec 터널이 협상되고 이 라우터에서 설정됩니다. 두 라우터의 상태를 확인하려면 명령을 사용할 수 `show standby` 있습니다.

<#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
```

터널에 대한 1단계(IKEv2) 및 2단계(IPsec) 보안 연결을 확인하려면 show crypto ikev2 sa 및 명령을 사용할 수 show crypto ipsec sa 있습니다.

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

Tunnel-id	Local	Remote	fvr/f/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:

시나리오 2. 기본 라우터는 비활성 상태이고 보조 라우터는 활성 상태입니다.

기본 라우터가 중단되거나 다운되는 시나리오에서 보조 라우터는 활성 라우터가 되고 사이트 간 터널은 이 라우터와 협상됩니다.

보조 라우터의 HSRP 상태는 명령을 사용하여 다시 확인할 수 show standby 있습니다.

<#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
```

또한 이 중단이 발생하면 다음 로그도 관찰할 수 있습니다. 이러한 로그는 보조 라우터가 현재 활성 상태이며 터널이 설정되었음을 보여줍니다.

```
*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
```

1단계 및 2단계 보안 연결을 확인하려면 여기 표시된 대로 show crypto ikev2 sa 및 show crypto ipsec sa를 다시 사용할 수 있습니다.

```
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:

시나리오 3. 기본 라우터가 다시 작동하고 보조 라우터가 대기 상태로 전환됨

기본 라우터가 복원되고 더 이상 다운되지 않으면 우선순위가 더 높게 구성되고 보조 라우터가 대기 모드로 전환되므로 다시 활성 라우터가 됩니다.

이 시나리오에서는 이러한 전환이 발생할 때 기본 및 보조 라우터에서 이러한 로그를 볼 수 있습니다.

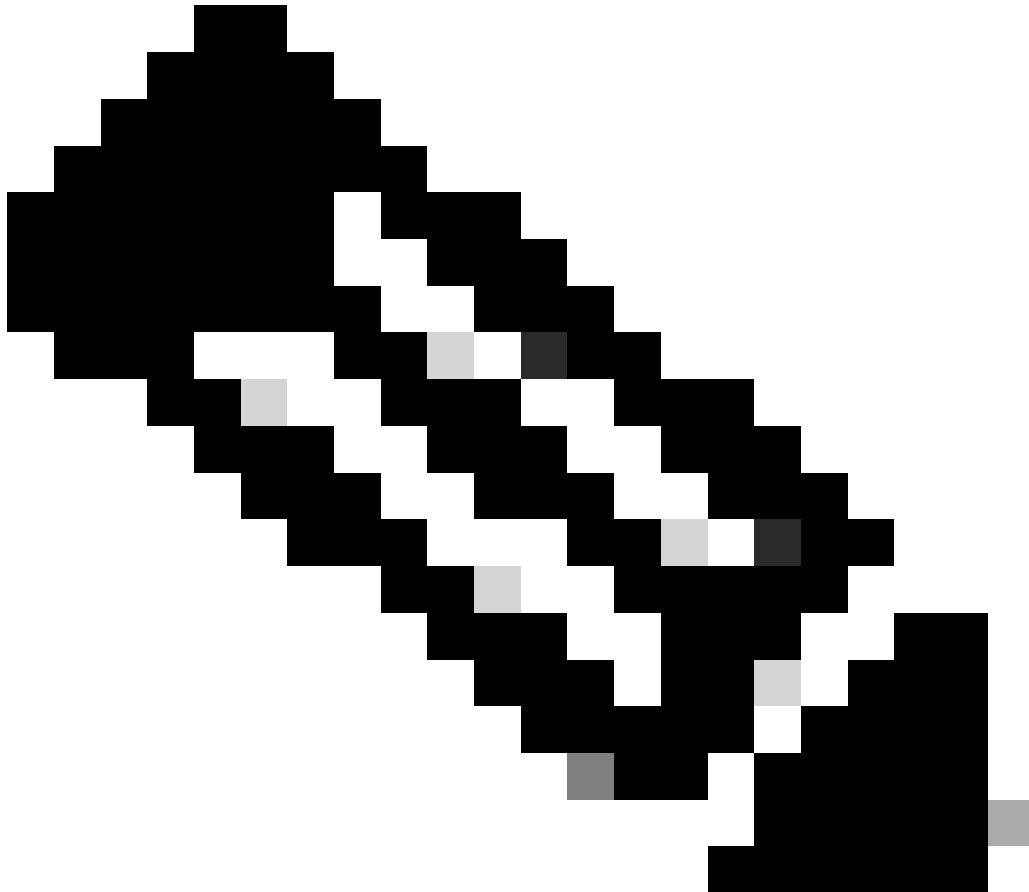
기본 라우터에는 다음 로그가 표시됩니다.

```
*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
```

보조 라우터에서 보조 라우터가 다시 대기 라우터가 되었음을 보여주는 다음 로그가 표시됩니다.

```
*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
```

1단계 및 2단계 보안 연결의 상태를 확인하려면 `show crypto ikev2 sa`를 사용하여 **show crypto ipsec sa** 확인할 수 있습니다.



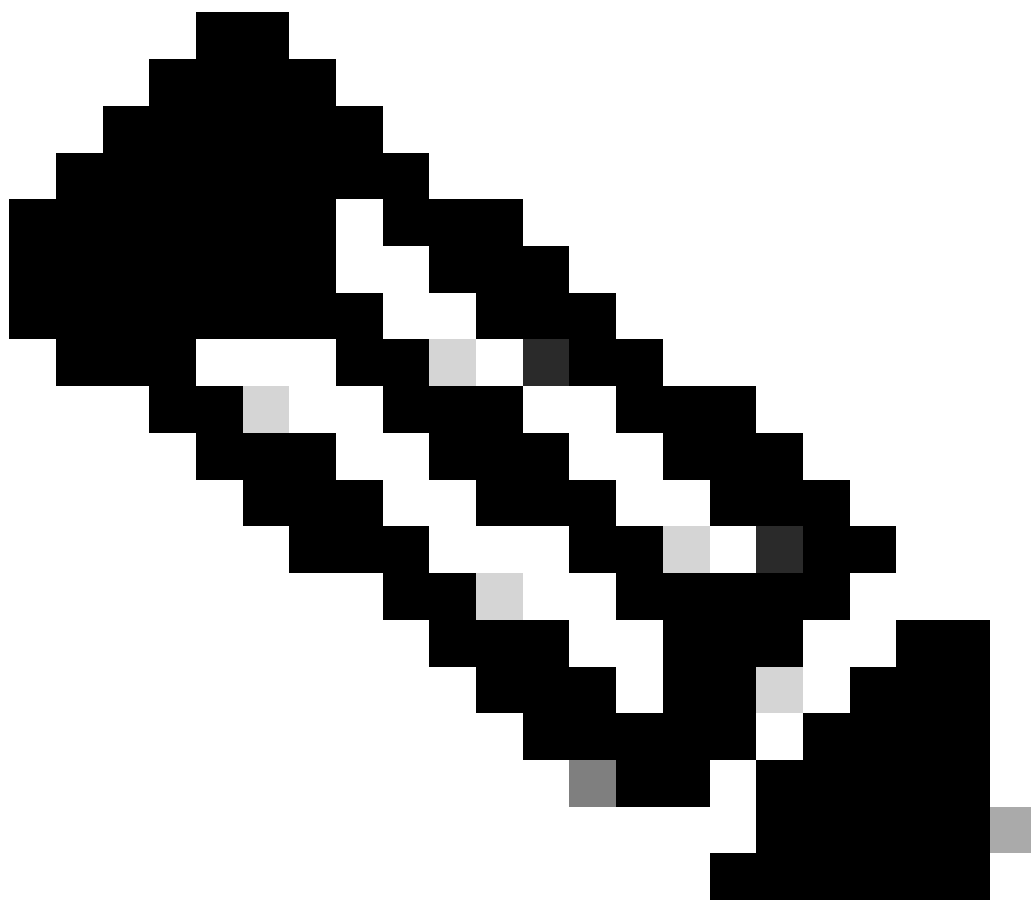
참고: 실행 중인 라우터에 여러 터널이 구성된 경우 `show crypto session remote X.X.X.X` 및 `show crypto ipsec sa peer X.X.X.X` 명령을 사용하여 터널의 1단계 및 2단계 상태를 확인할 수 있습니다.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

이러한 디버그는 IKEv2 터널의 문제를 해결하기 위해 활성화할 수 있습니다.

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



참고: 하나의 터널만 트러블슈팅하려면(디바이스가 프로덕션 중일 경우), 명령을 사용하여 조건부 디버그를 활성화해야 합니다. debug crypto condition peer ipv4 X.X.X.X.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.