Configuración de la Redundancia IPsec con HSRP para el Túnel Basado en Rutas IKEv2 en Routers Cisco

Contenido

Introducción

Este documento describe cómo configurar la redundancia IPsec con HSRP para el túnel basado en rutas IKEv2 en routers Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de sitio a sitio
- Protocolo de router con espera en caliente [HSRP]
- Conocimientos básicos de IPsec e IKEv2

Componentes Utilizados

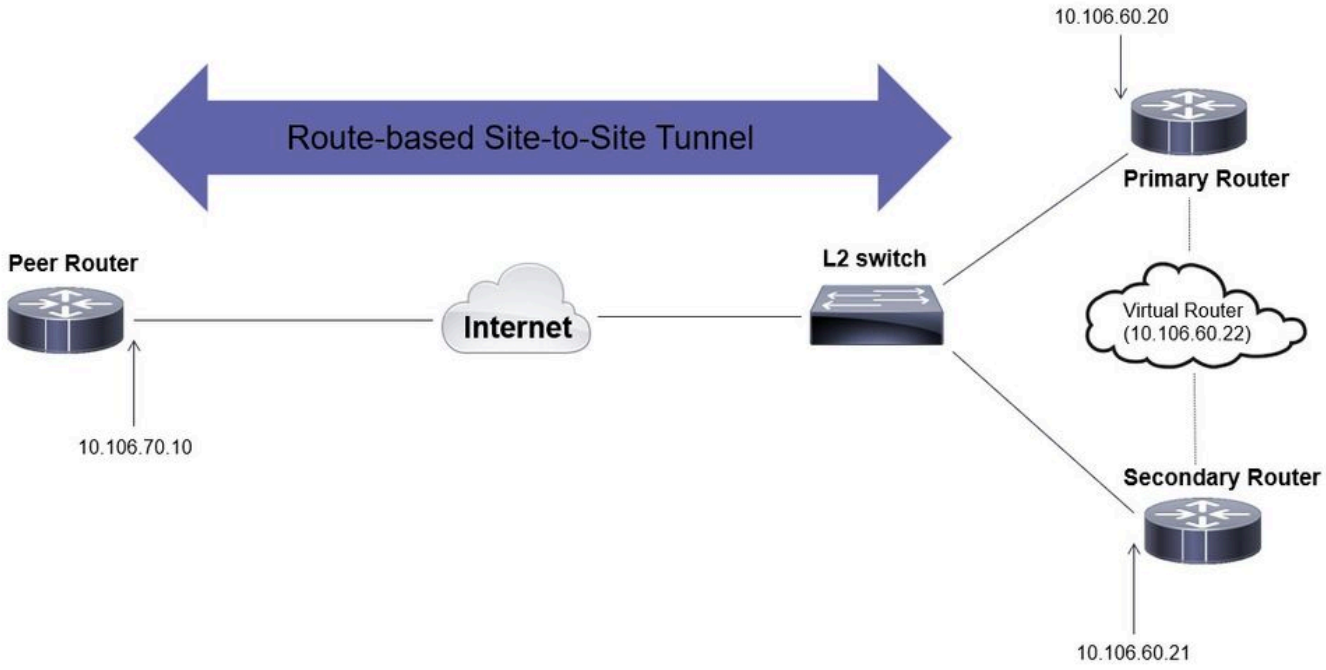
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco CSR1000v con software IOS XE, versión 17.03.08a
- Switch de capa 2 que ejecuta Cisco IOS Software, versión 15.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuraciones de router principal/secundario

Configuración de la Interfaz Física con HSRP

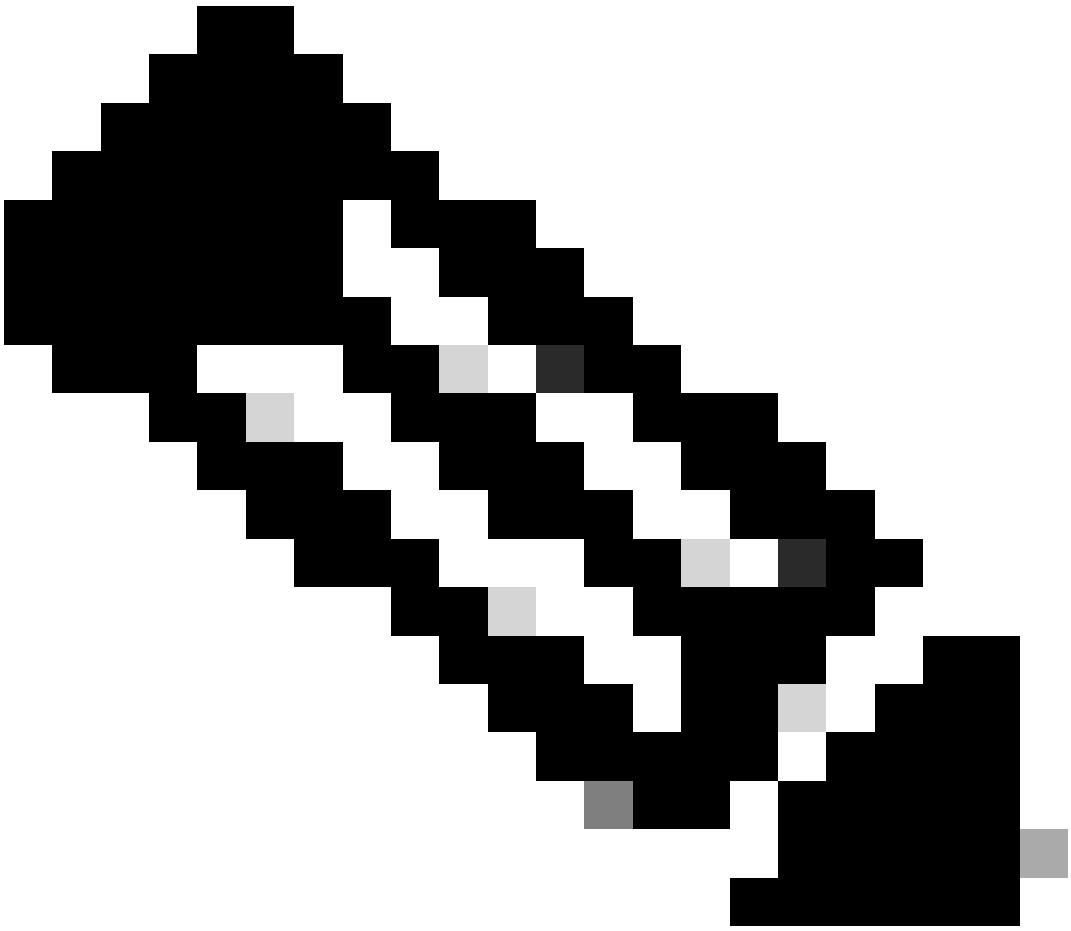
Configure las interfaces físicas de los routers primario (con una prioridad más alta) y secundario (con una prioridad predeterminada de 100):

Router principal:

```
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
```

Router secundario:

```
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
```



Nota: Asegúrese de que el router principal predeterminado esté configurado con una

---

prioridad más alta para convertirlo en el par activo incluso cuando ambos routers estén activos y funcionando sin ningún problema. Para este ejemplo, el router primario se ha configurado con una prioridad de 105, mientras que el router secundario tiene una prioridad de 100 (que es el valor predeterminado para HSRP).

Configurar la propuesta y la directiva IKEv2

Configure una propuesta IKEv2 con el grupo de cifrado, hash y DH que desee y asígnela a una política IKEv2.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configuración del anillo de claves

Configure el anillo de claves para almacenar la clave previamente compartida que se utilizará para autenticar el par.

```
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
```

Configuración del perfil IKEv2

Configure el perfil IKEv2 y adjúntele el anillo de claves. Establezca la dirección local en la dirección IP virtual que se utiliza para HSRP y la dirección remota como la IP de la interfaz de cara a Internet del 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
```

Configuración del conjunto de transformación IPsec

Configure los parámetros de fase 2 de cifrado y hash mediante IPsec transform-set.

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

Configuración del perfil IPsec

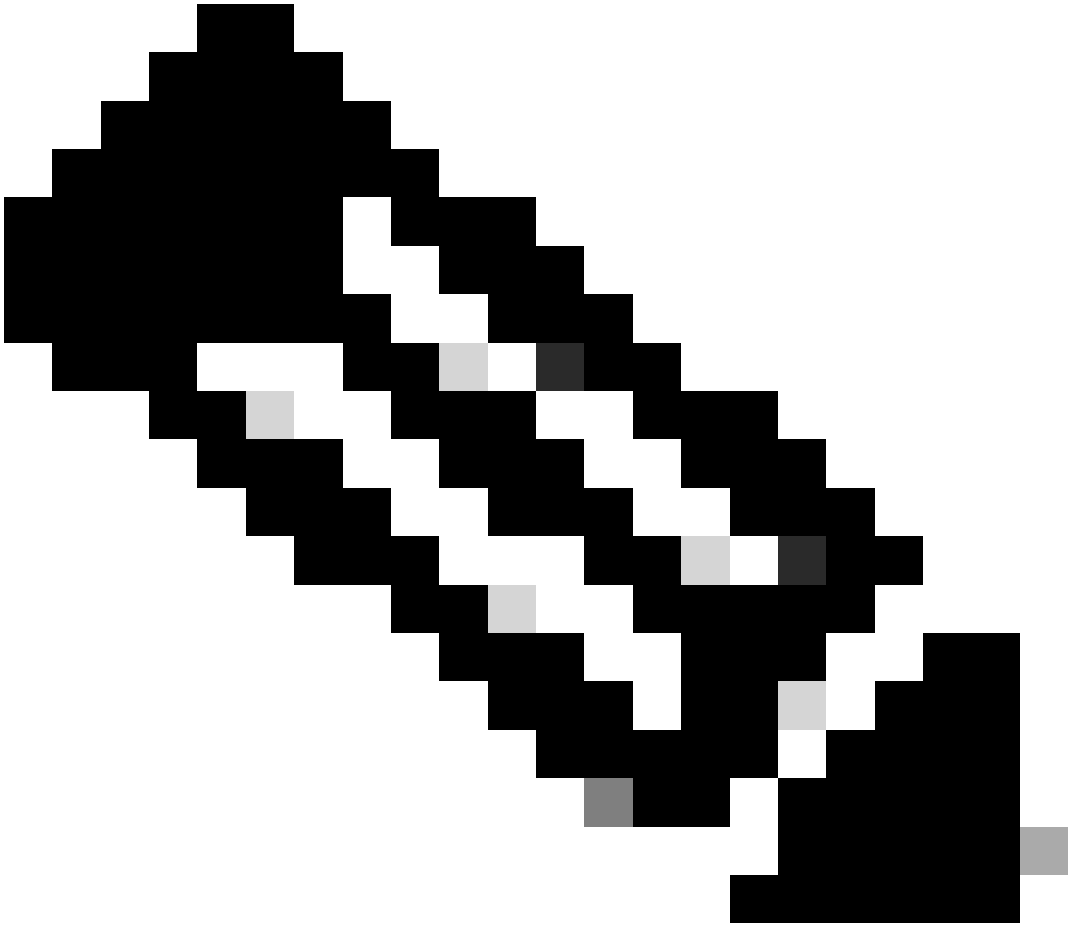
Configure el perfil IPsec para asignar el perfil IKEv2 y el conjunto de transformación IPsec. El perfil IPsec se aplicará a la interfaz de túnel.

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

Configuración de la Interfaz de Túnel Virtual

Configure la interfaz de túnel virtual para especificar el origen y el destino del túnel. Estas IP se utilizarán para cifrar el tráfico a través del túnel. Asegúrese de que el perfil IPsec también se aplique a esta interfaz como se muestra a continuación.

```
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
```



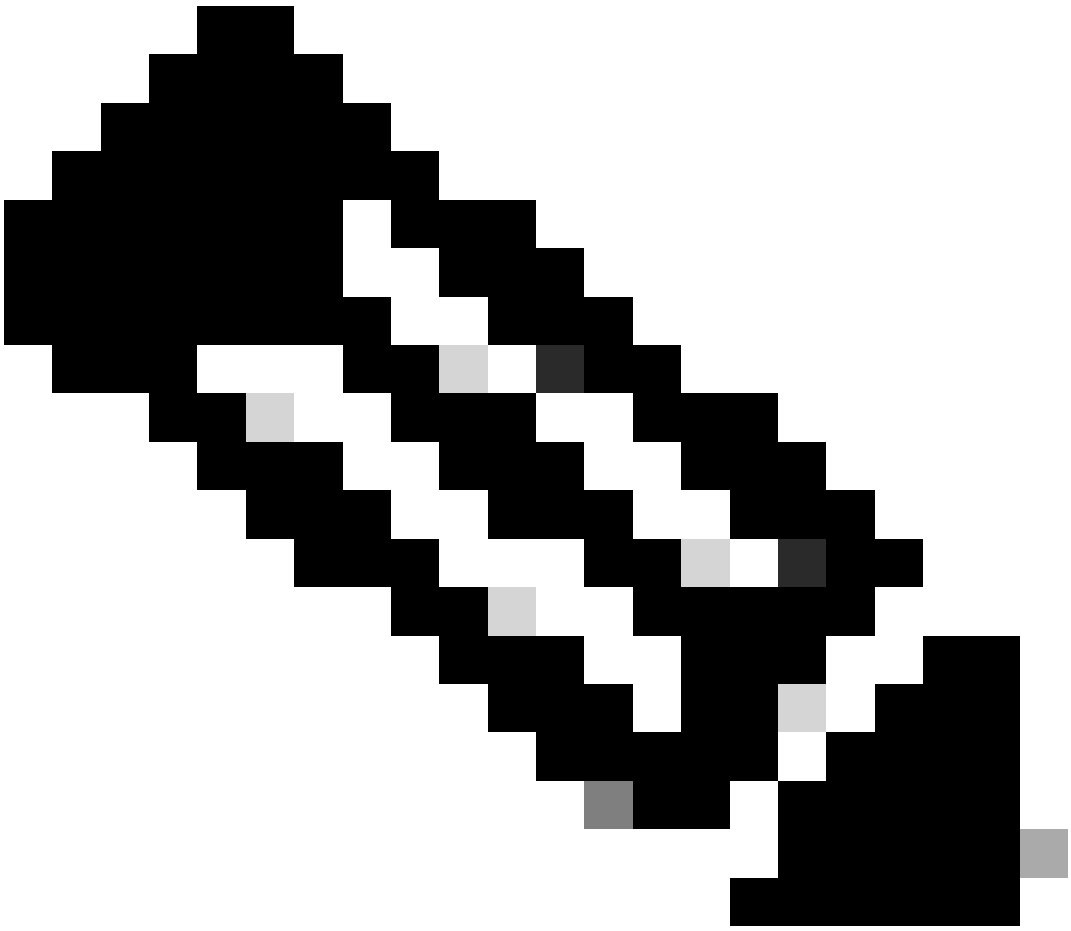
Nota: Deberá especificar la IP virtual que se está utilizando para HSRP como origen del túnel. El uso de la interfaz física, en este escenario GigabitEthernet1, hará que la negociación del túnel falle.

Configuración del enrutamiento dinámico o estático

Tiene que configurar el ruteo con protocolos de ruteo dinámicos y/o rutas estáticas según los requisitos y el diseño de la red. En este ejemplo, se utiliza una combinación de EIGRP y una ruta estática para establecer la comunicación subyacente y el flujo del tráfico de datos de superposición a través del túnel de sitio a sitio.

```
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
```



Nota: Asegúrese de que la subred de la interfaz de túnel, que en este escenario es 10.10.10.0/24, se está anunciando.

Configuraciones de router de peer

Configurar la propuesta y la directiva IKEv2

Configure una propuesta IKEv2 con el grupo de cifrado, hash y DH que desee y asígnela a una política IKEv2.

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

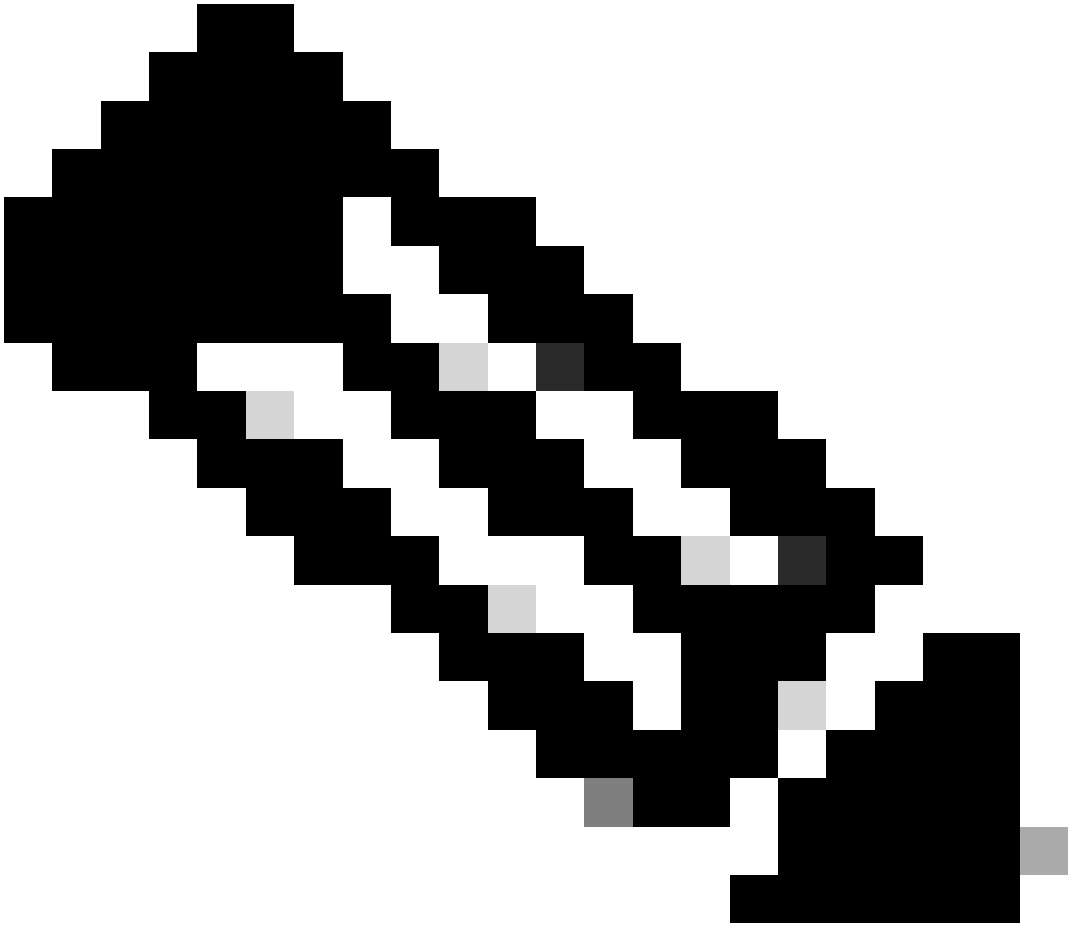
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configuración del anillo de claves

Configure el anillo de claves para almacenar la clave previamente compartida que se utilizará para autenticar el par.

```
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
```



Nota: La dirección IP del par utilizada aquí será la dirección IP virtual que se configura en la configuración HSRP del par. Asegúrese de que no está configurando el anillo de claves para la IP de la interfaz física del peer primario/secundario.

Configuración del perfil IKEv2

Configure el perfil IKEv2 y adjúntele el anillo de claves. Establezca la dirección local como la IP de la interfaz de cara a Internet del router y la dirección remota como la dirección IP virtual que se está utilizando para HSRP en el par principal/secundario.

```
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
```

Configuración del conjunto de transformación IPsec

Configure los parámetros de fase 2 de cifrado y hash mediante IPsec transform-set.

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

Configuración del perfil IPsec

Configure el perfil IPsec para asignar el perfil IKEv2 y el conjunto de transformación IPsec. El perfil IPsec se aplicará a la interfaz de túnel.

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

Configuración de la Interfaz de Túnel Virtual

Configure la interfaz de túnel virtual para especificar el origen y el destino del túnel. El destino del túnel debe configurarse como la IP virtual utilizada para HSRP en el peer primario/secundario. Asegúrese de que el perfil IPsec también se aplique a esta interfaz como se muestra.

```
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
```

Configuración del enrutamiento dinámico o estático

Configure las rutas requeridas con protocolos de ruteo dinámico o rutas estáticas similares a las que tiene para el otro terminal.

```
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
```

Verificación

Para comprender el comportamiento esperado, se presentan los tres escenarios siguientes.

Escenario 1. Los routers primario y secundario están activos

Dado que el router principal está configurado con una prioridad más alta, el túnel IPsec se negocia y establece en este router. Para verificar el estado de los dos routers, puede utilizar el show standbycomando.

<#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
```

Para verificar las asociaciones de seguridad de fase 1 (IKEv2) y fase 2 (IPsec) para el túnel, puede utilizar los comandos show crypto ikev2 say show crypto ipsec sae.

```
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:
```

Situación hipotética 2. El router principal está inactivo y el secundario activo

En un escenario donde el router primario experimenta una interrupción o se cae, el router secundario se convertirá en el router activo y el túnel de sitio a sitio se negociará con este router.

El estado HSRP del router secundario se puede verificar nuevamente con el show standby comando.

<#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
```

Además, también observará los siguientes registros cuando se produzca esta interrupción. Estos registros también muestran que el router secundario está ahora activo y que se ha establecido el túnel.

*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

Para comprobar las asociaciones de seguridad de fase 1 y fase 2, puede utilizar de nuevo el show crypto ikev2 say show crypto ipsec sacomo se muestra aquí.

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:

Situación hipotética 3. El router principal vuelve a estar activo y el secundario en espera

Una vez que se restaura el router primario y ya no está inactivo, se convierte nuevamente en el router activo ya que tiene una prioridad más alta configurada y el router secundario pasa al modo de espera.

Durante este escenario, verá estos registros en los routers primario y secundario cuando ocurra esta transición.

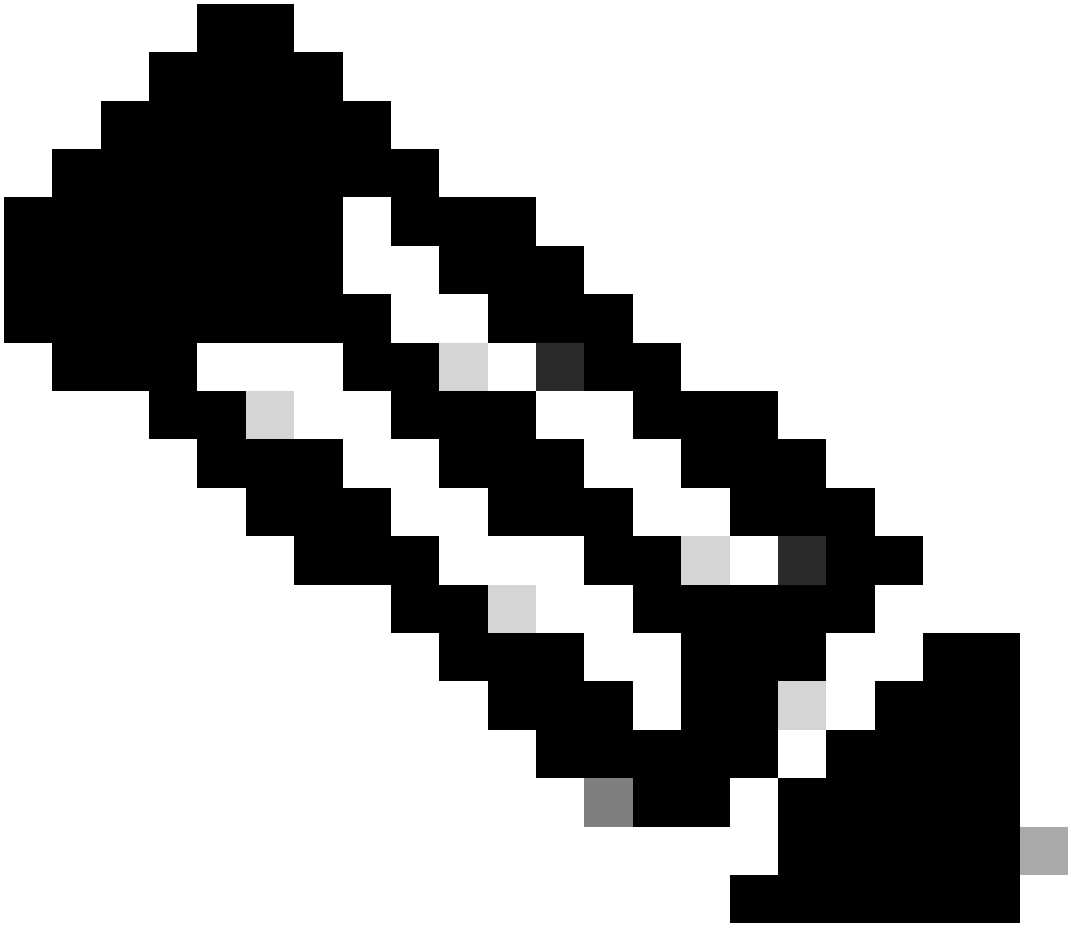
En el router primario, aparecen estos registros:

*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

En el router secundario, verá estos registros que muestran que el router secundario se ha convertido nuevamente en el router en espera:

*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

Para comprobar el estado de las asociaciones de seguridad de fase 1 y fase 2, puede utilizar show crypto ikev2 say **show crypto ipsec sa**para verificar el mismo.



Nota: Si tiene varios túneles configurados en los routers que están en funcionamiento, puede utilizar los comandos show crypto session remote X.X.X.X y show crypto ipsec sa peer X.X.X.X para verificar el estado de fase 1 y fase 2 del túnel.

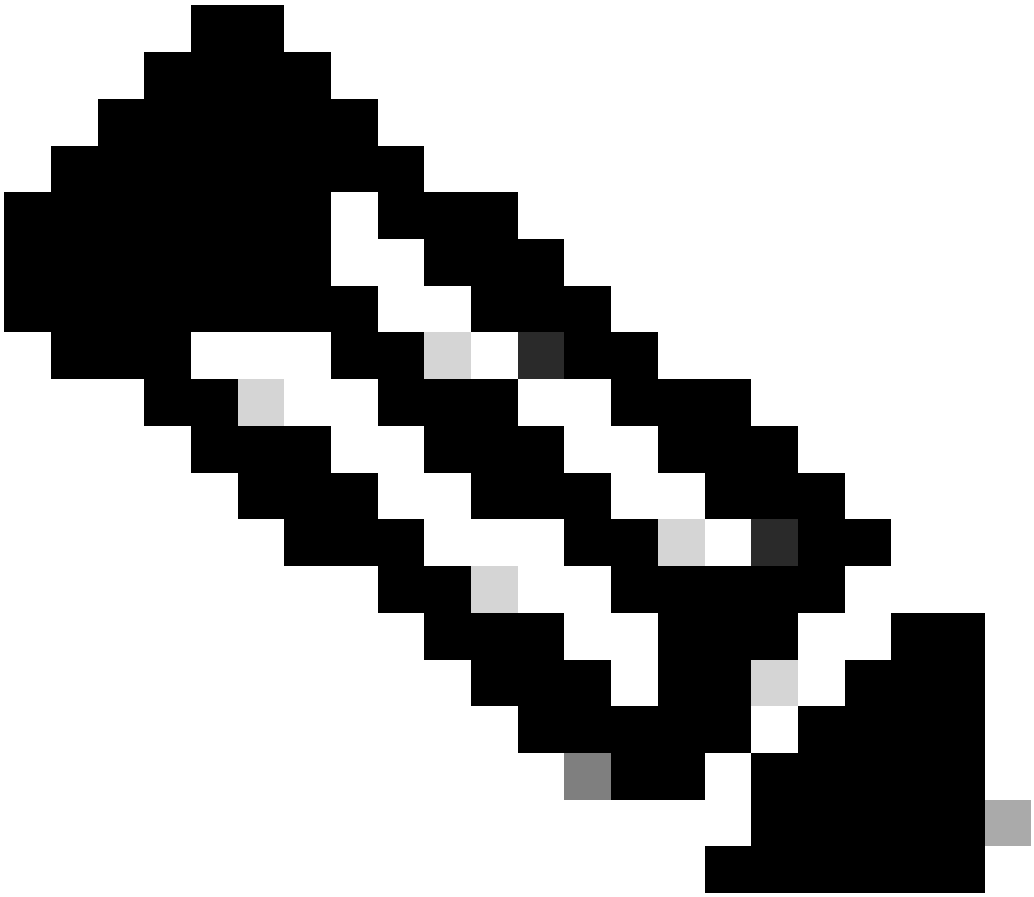
Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Estas depuraciones se pueden habilitar para solucionar problemas del túnel IKEv2.

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

debug crypto ipsec error
debug crypto ipsec message



Nota: Si desea resolver problemas de un solo túnel (lo que debe ocurrir si el dispositivo está en producción), debe habilitar las depuraciones condicionales mediante el comando, debug crypto condition peer ipv4 X.X.X.X.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).