Configurar a redundância de IPsec com HSRP para o túnel baseado em rota IKEv2 em roteadores Cisco

Contents

Introdução

Este documento descreve como configurar a redundância de IPsec com HSRP para túnel baseado em rota IKEv2 em roteadores Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN site a site
- Protocolo de Roteador Hot Standby [HSRP]
- Conhecimento básico de IPsec e IKEv2

Componentes Utilizados

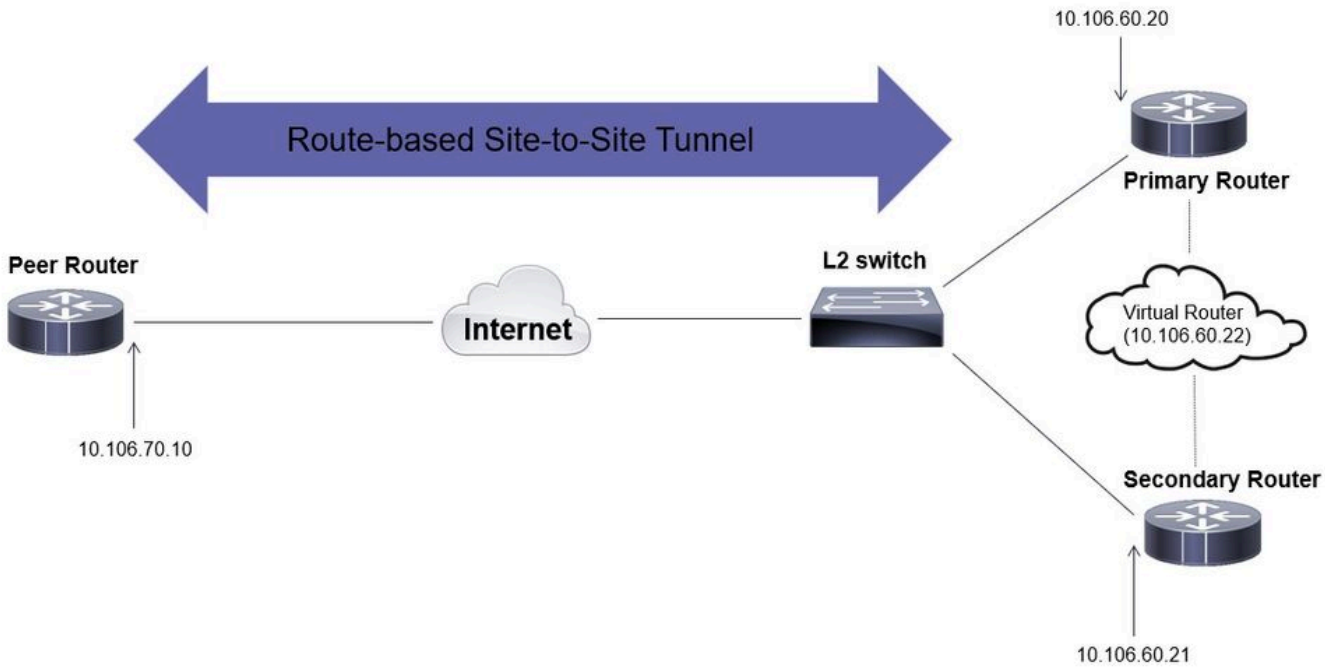
As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco CSR1000v executando o software IOS XE, versão 17.03.08a
- Switch de Camada 2 executando o Cisco IOS Software, versão 15.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurações do roteador primário/secundário

Configurar a interface física com HSRP

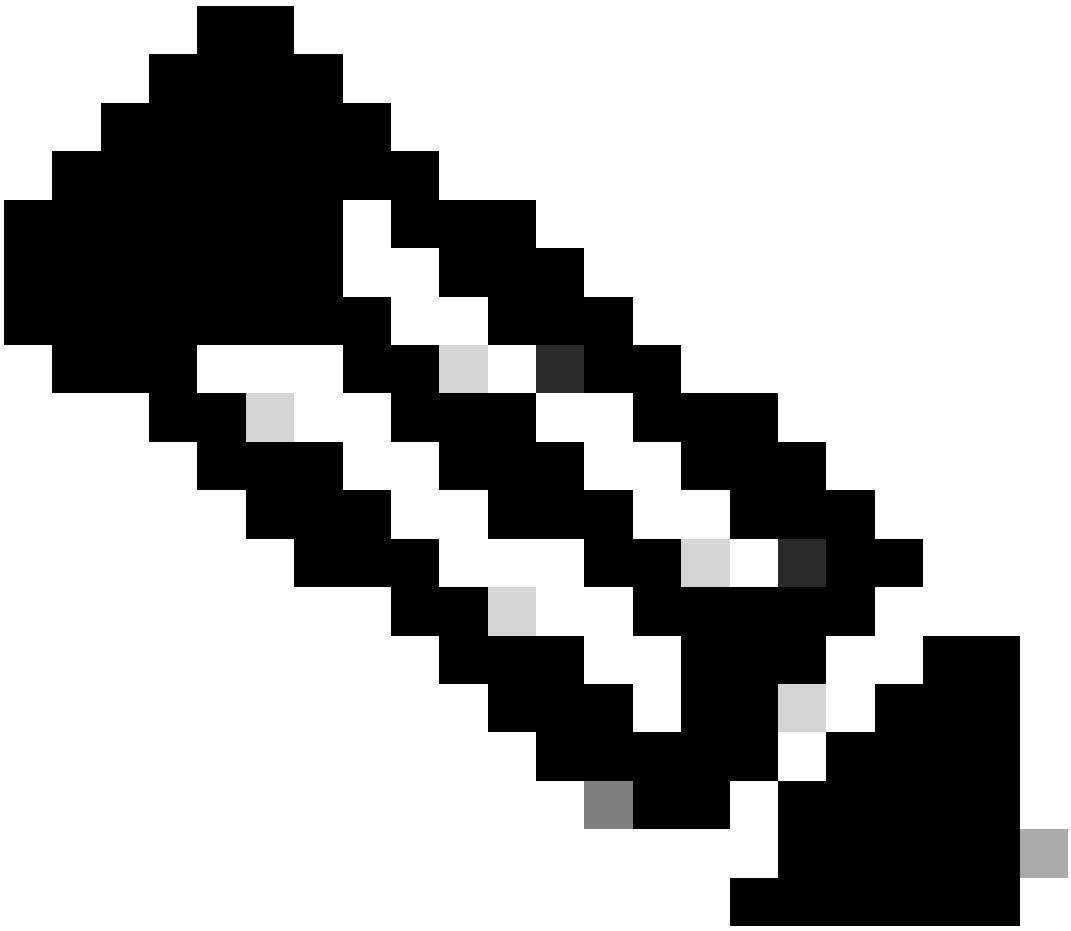
Configure as interfaces físicas dos roteadores primário (com uma prioridade mais alta) e secundário (com uma prioridade padrão de 100):

Roteador 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
```

Roteador secundário:

```
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
```



Observação: certifique-se de que o roteador principal padrão esteja configurado com uma

---

prioridade mais alta para torná-lo o peer ativo mesmo quando ambos os roteadores estiverem ativos e em execução sem nenhum problema. Para este exemplo, o principal foi configurado com uma prioridade de 105, enquanto o roteador secundário tem uma prioridade de 100 (que é o padrão para HSRP).

Configurar a proposta e a política de IKEv2

Configure uma proposta de IKEv2 com a criptografia, o hash e o grupo DH de sua escolha e mapeie-os para uma política de IKEv2.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configurar o porta- chaves

Configure o chaveiro para armazenar a chave pré-compartilhada que será usada para autenticar o 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
```

Configurar o perfil IKEv2

Configure o perfil IKEv2 e anexe o chaveiro a ele. Defina o endereço local para o endereço IP virtual que está sendo usado para HSRP e o endereço remoto como o IP da interface de Internet do roteador.

```
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
```

Configurar o conjunto de transformação IPsec

Configure os parâmetros da fase 2 de criptografia e hash usando o conjunto de transformação IPsec.

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

Configurar o perfil IPsec

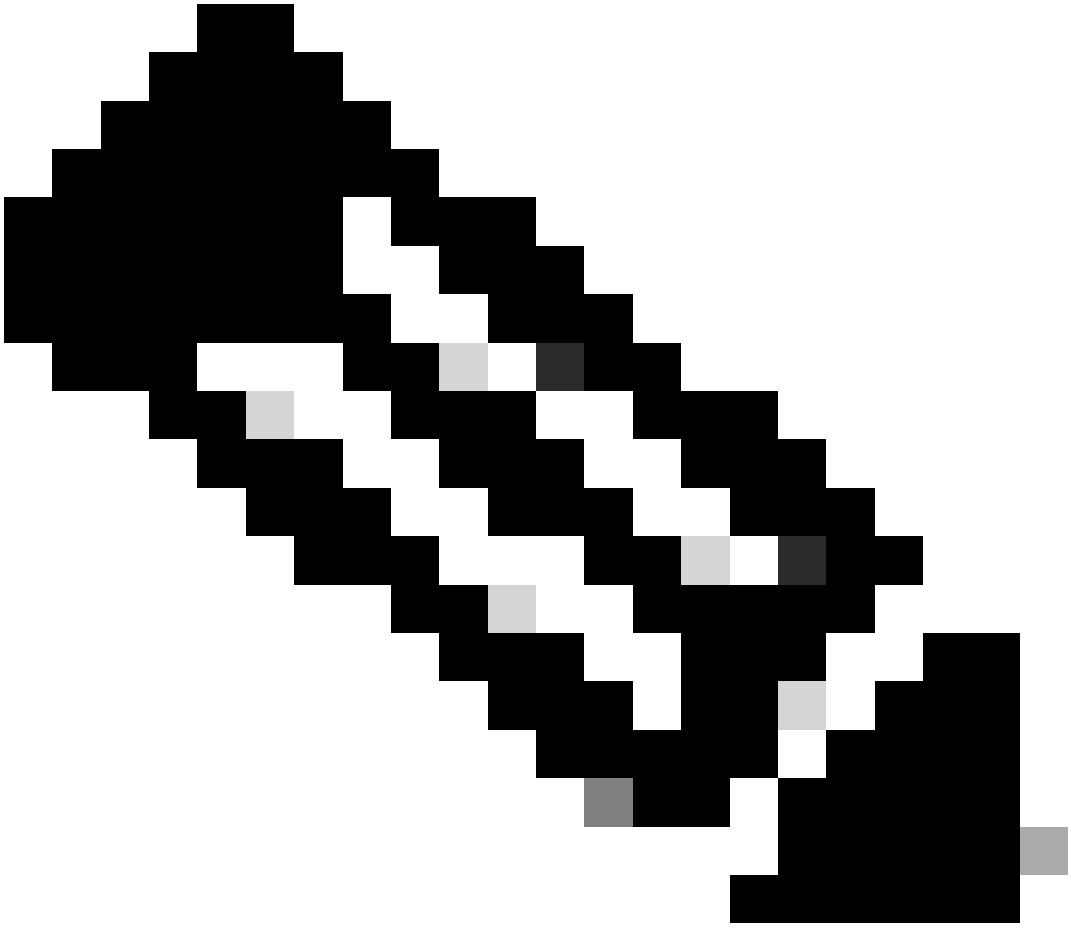
Configure o perfil IPsec para mapear o perfil IKEv2 e o conjunto de transformação IPsec. O perfil IPsec será aplicado à interface túnel.

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

Configurar a interface do túnel virtual

Configure a interface de túnel virtual para especificar a origem e o destino do túnel. Esses IPs serão usados para criptografar o tráfego pelo túnel. Certifique-se de que o perfil IPsec também seja aplicado a essa interface, como mostrado abaixo.

```
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
```



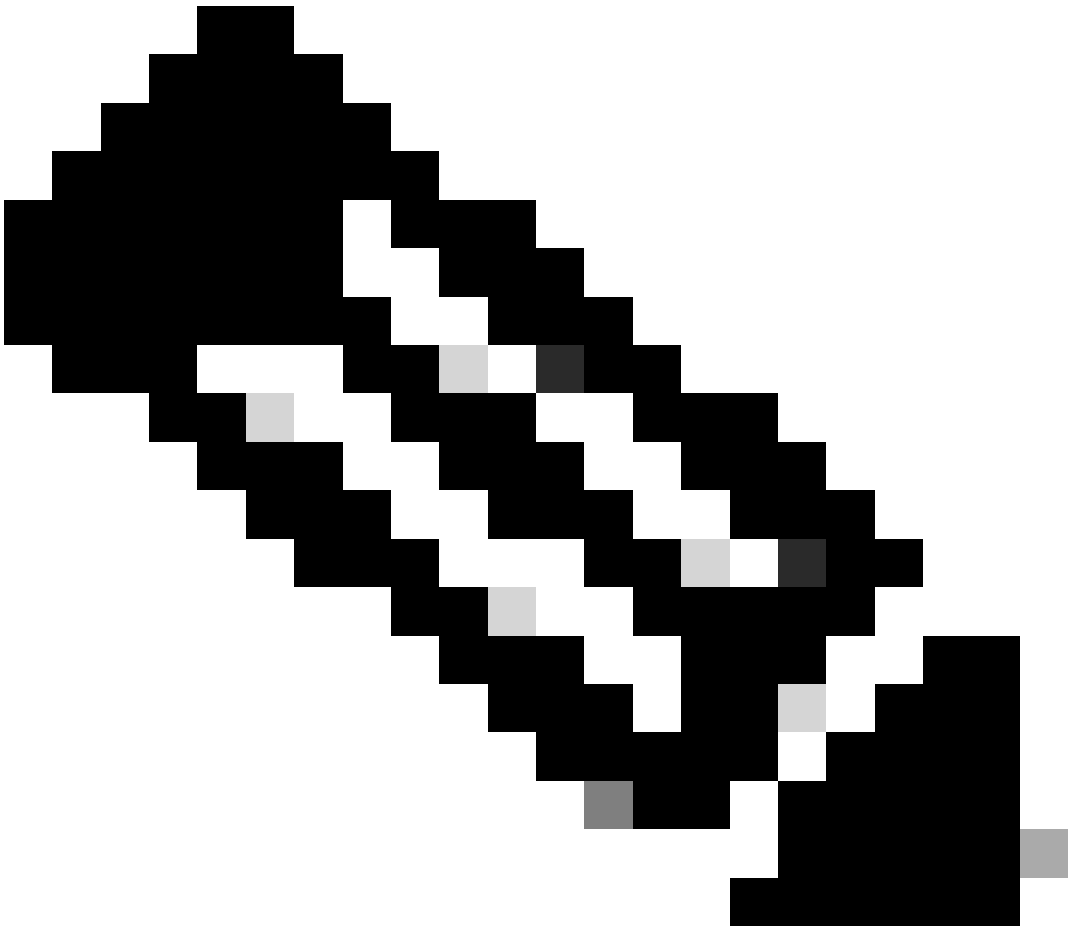
Observação: você precisará especificar o IP virtual que está sendo usado para HSRP como a origem do túnel. Usar a interface física, neste cenário GigabitEthernet1, fará com que a negociação do túnel falhe.

Configurar o roteamento dinâmico e/ou estático

Você precisa configurar o roteamento com protocolos de roteamento dinâmico e/ou rotas estáticas, dependendo do requisito e do projeto da rede. Para este exemplo, uma combinação de EIGRP e uma rota estática é usada para estabelecer a comunicação subjacente e o fluxo do tráfego de dados de sobreposição sobre o túnel site a site.

```
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
```



Observação: certifique-se de que a sub-rede da interface do túnel, que neste cenário é 10.10.10.0/24, esteja sendo anunciada.

Configurações do Roteador de Mesmo Nível

Configurar a proposta e a política de IKEv2

Configure uma proposta de IKEv2 com a criptografia, o hash e o grupo DH de sua escolha e mapeie-os para uma política de IKEv2.

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

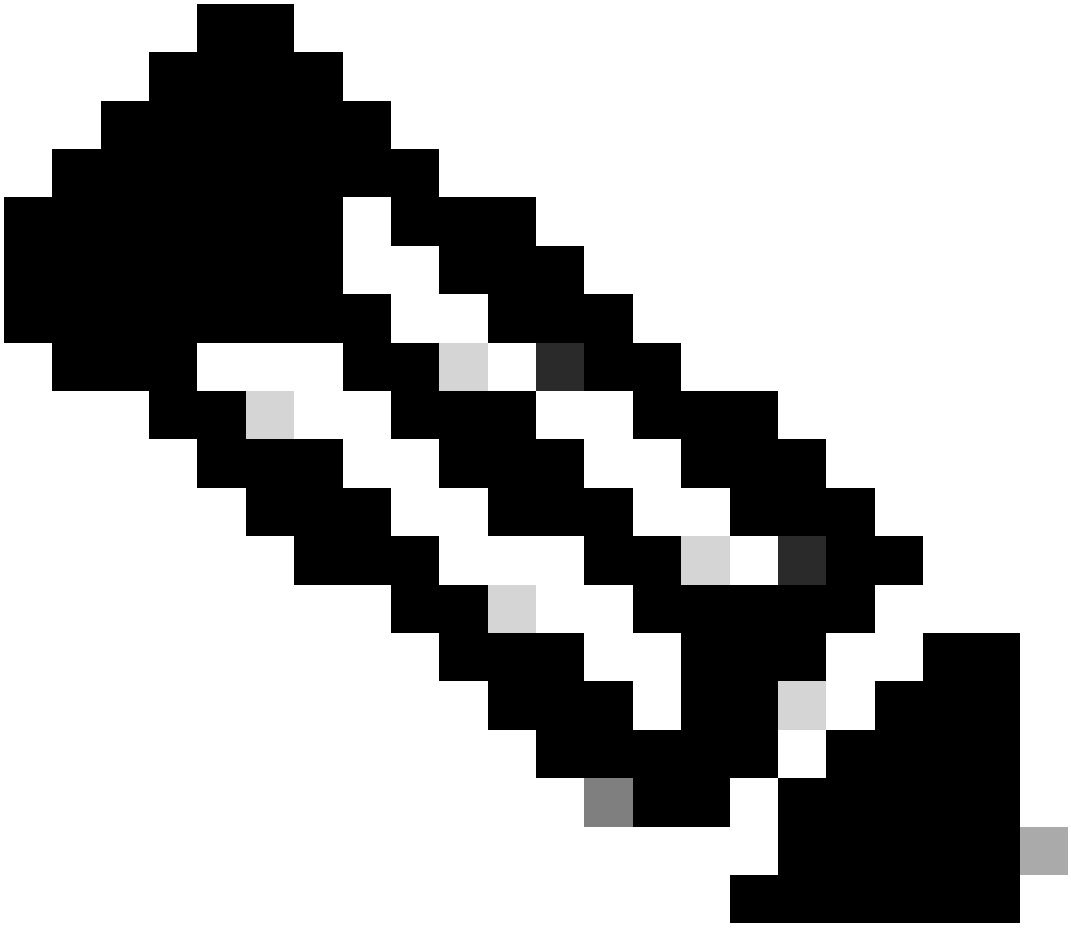
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configurar o porta- chaves

Configure o chaveiro para armazenar a chave pré-compartilhada que será usada para autenticar o 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
```



Observação: o endereço IP do peer usado aqui será o endereço IP virtual configurado na configuração HSRP do peer. Certifique-se de que você não esteja configurando o chaveiro para o IP da interface física do peer primário/secundário.

Configurar o perfil IKEv2

Configure o perfil IKEv2 e anexe o chaveiro a ele. Defina o endereço local como o IP da interface para a Internet do roteador e o endereço remoto como o endereço IP virtual que está sendo usado para HSRP no peer primário/secundário.

```
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
```

Configurar o conjunto de transformação IPsec

Configure os parâmetros da fase 2 de criptografia e hash usando o conjunto de transformação IPsec.

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

Configurar o perfil IPsec

Configure o perfil IPsec para mapear o perfil IKEv2 e o conjunto de transformação IPsec. O perfil IPsec será aplicado à interface túnel.

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

Configurar a interface do túnel virtual

Configure a interface de túnel virtual para especificar a origem e o destino do túnel. O destino do túnel deve ser definido como o IP virtual usado para HSRP no par primário/secundário. Certifique-se de que o perfil IPsec também seja aplicado a esta interface, como mostrado.

```
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
```

Configurar o roteamento dinâmico e/ou estático

Configure as rotas necessárias com protocolos de roteamento dinâmico ou rotas estáticas semelhantes às que você tem para o outro ponto final.

```
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
```

Verificar

Para entender o comportamento esperado, os três cenários a seguir são apresentados.

Cenário 1. Os roteadores principal e secundário estão ativos

Como o roteador primário está configurado com uma prioridade mais alta, o túnel IPsec é negociado e estabelecido nesse roteador. Para verificar o estado dos dois roteadores, você pode usar o 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 as associações de segurança da fase 1 (IKEv2) e da fase 2 (IPsec) para o túnel, você pode usar os comandos show crypto ikev2 saeshow crypto ipsec sa.

```
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:
```

Cenário 2. O roteador principal está inativo e o roteador secundário está ativo

Em um cenário em que o roteador primário sofre uma interrupção ou fica inativo, o roteador secundário se tornará o roteador ativo e o túnel de site para site será negociado com esse roteador.

O estado HSRP do roteador secundário pode ser verificado novamente usando o 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
```

Além disso, você também observará os seguintes registros quando essa interrupção ocorrer. Esses registros também mostram que o roteador secundário agora está ativo e o túnel foi estabelecido.

*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 verificar as associações de segurança das fases 1 e 2, você pode usar novamente o show crypto ikev2 sae show crypto ipsec sacomo mostrado aqui.

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:

Cenário 3. O roteador primário volta a funcionar e o secundário fica em espera

Quando o roteador principal for restaurado e não estiver mais inativo, ele se tornará o roteador ativo novamente, pois terá uma prioridade mais alta configurada e o roteador secundário entrará no modo de espera.

Durante esse cenário, você verá esses logs nos roteadores primário e secundário quando essa transição acontecer.

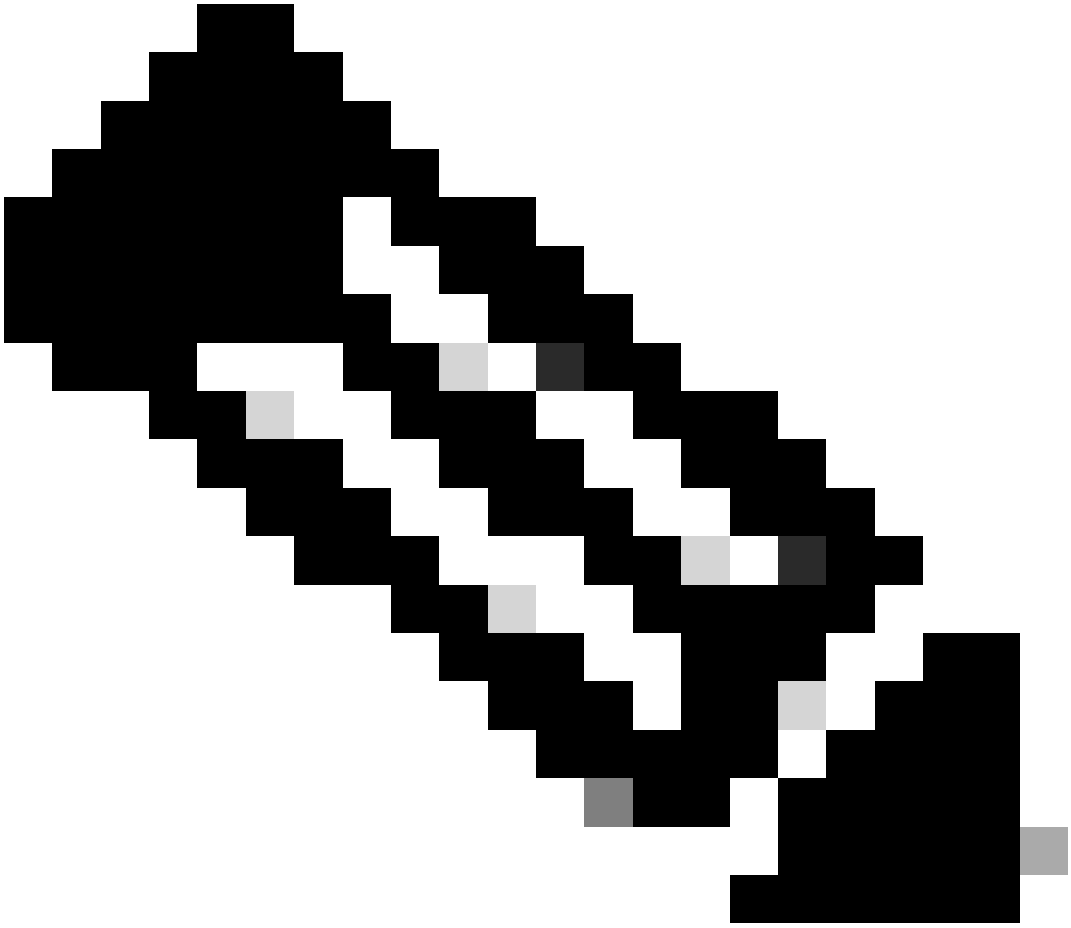
No roteador principal, os seguintes registros são exibidos:

*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

No roteador secundário, você verá estes registros que mostram que o roteador secundário se tornou novamente o roteador em standby:

*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 verificar o status das associações de segurança da Fase 1 e da Fase 2, você pode usar o show crypto ikev2 sae **show crypto ipsec sa**para verificar o mesmo.



Observação: se você tiver vários túneis configurados nos roteadores que estão ativos e em execução, poderá usar os comandos show crypto session remote X.X.X.X e show crypto ipsec sa peer X.X.X.X para verificar o status das fases 1 e 2 do túnel.

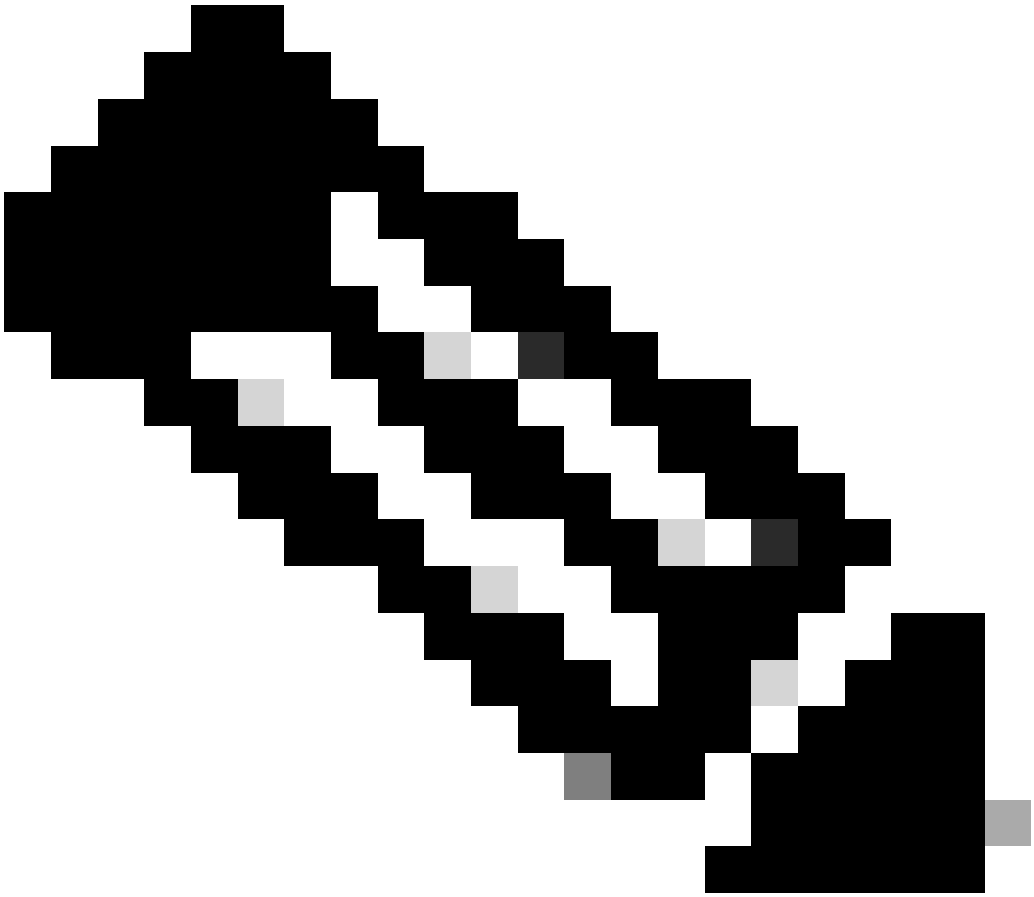
Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Essas depurações podem ser ativadas para solucionar problemas do túnel IKEv2.

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

debug crypto ipsec error
debug crypto ipsec message



Observação: se quiser solucionar problemas de apenas um túnel (que deve ser o caso se o dispositivo estiver em produção), você deve habilitar depurações condicionais usando o comando, debug crypto condition peer ipv4 X.X.X.X.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.