Configurazione della ridondanza IPsec con HSRP per il tunnel basato su route IKEv2 sui router Cisco

Sommario

Introduzione

In questo documento viene descritto come configurare la ridondanza IPsec con HSRP per il tunnel basato su route IKEv2 sui router Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN da sito a sito
- Protocollo HSRP (Hot Standby Router Protocol)
- Conoscenze base di IPsec e IKEv2

Componenti usati

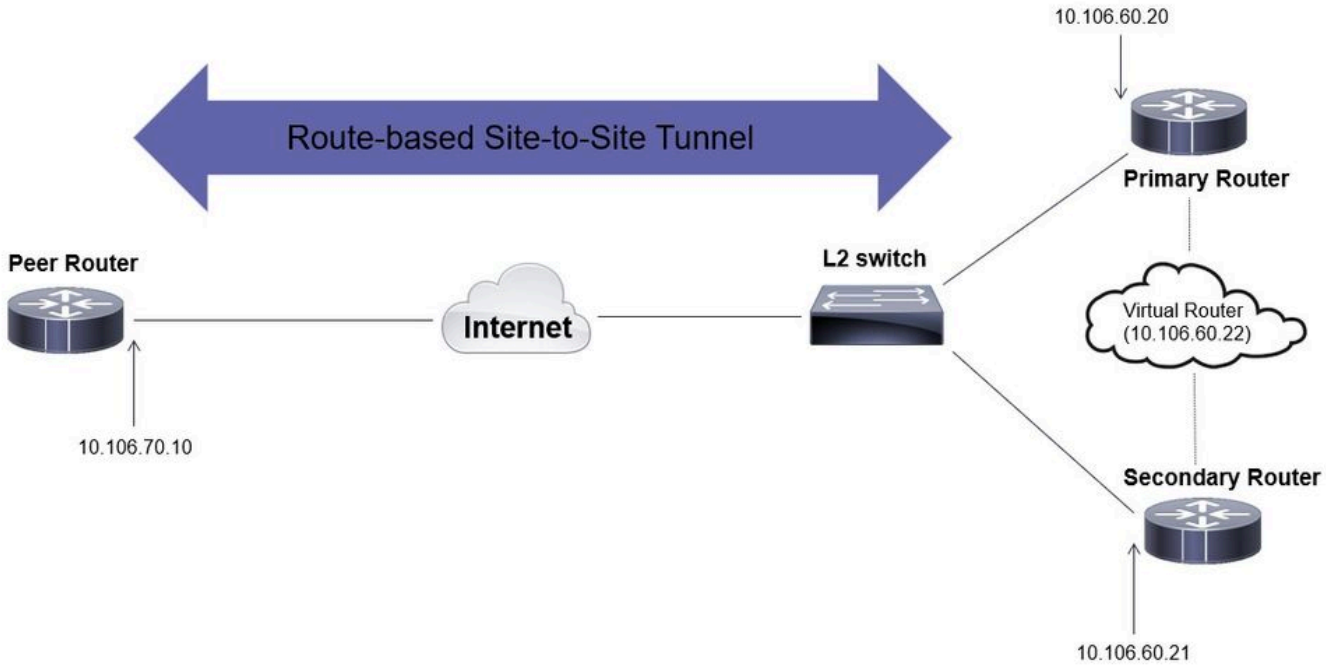
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco CSR1000v con software IOS XE, versione 17.03.08a
- Switch di layer 2 con software Cisco IOS, versione 15.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni router primario/secondario

Configurazione dell'interfaccia fisica con HSRP

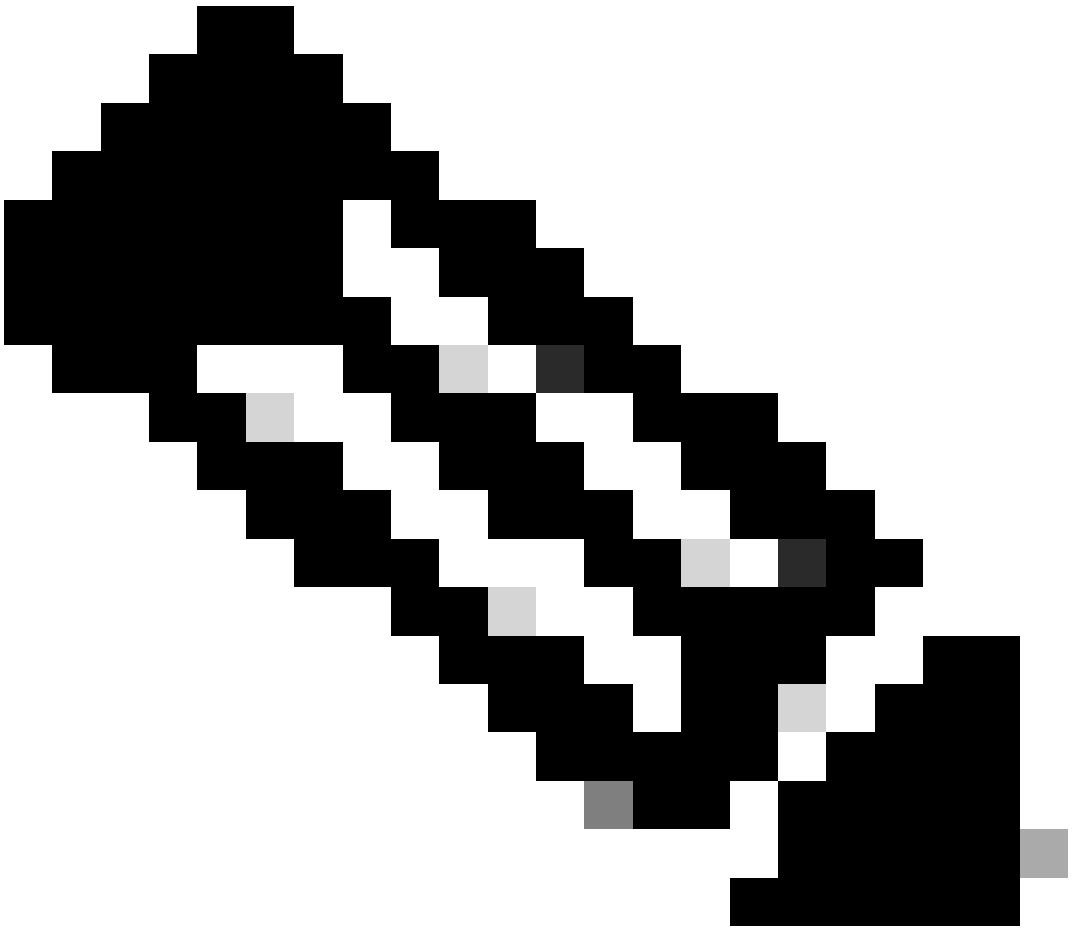
Configurare le interfacce fisiche dei router primario (con una priorità più alta) e secondario (con una priorità predefinita di 100):

Router primario:

```
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 secondario:

```
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: verificare che il router primario predefinito sia configurato con una priorità più alta in

modo da renderlo il peer attivo anche quando entrambi i router sono attivi e in esecuzione senza problemi. Nell'esempio, il router primario è stato configurato con una priorità di 105, mentre il router secondario ha una priorità di 100 (impostazione predefinita per HSRP).

Configurare la proposta e il criterio IKEv2

Configurare una proposta IKEv2 con il gruppo di crittografia, hashing e DH desiderato e mapparlo a un criterio IKEv2.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configurazione della sequenza di tasti

Configurare il keyring per archiviare la chiave già condivisa che verrà utilizzata per autenticare il peer.

```
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
```

Configurare il profilo IKEv2

Configurare il profilo IKEv2 e collegarvi il keyring. Impostare l'indirizzo locale sull'indirizzo IP virtuale utilizzato per HSRP e l'indirizzo remoto come IP dell'interfaccia con connessione 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
```

Configurare il set di trasformazioni IPSec

Configurare i parametri della fase 2 di crittografia e hashing utilizzando il set di trasformazioni IPsec.

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

Configurare il profilo IPSec

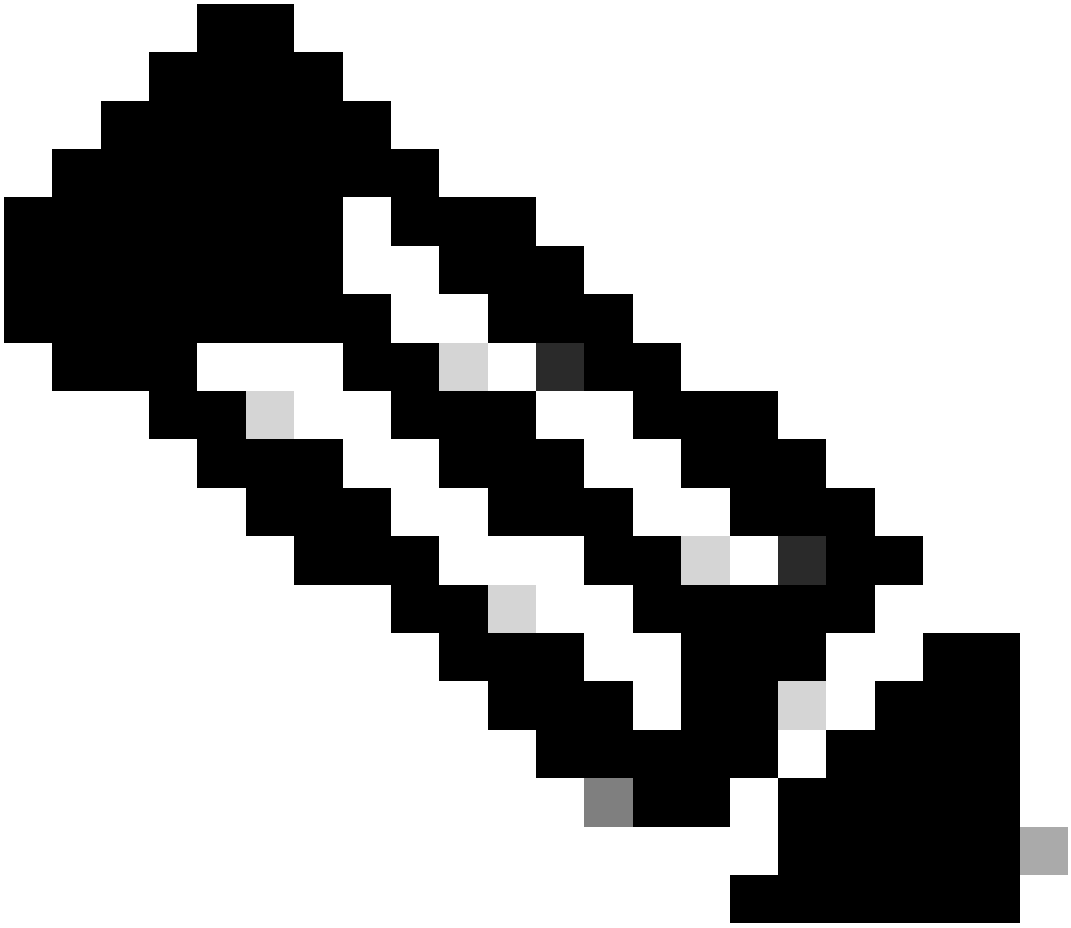
Configurare il profilo IPSec per eseguire il mapping del profilo IKEv2 e del set di trasformazioni IPSec. Il profilo IPsec verrà applicato all'interfaccia del tunnel.

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

Configurazione dell'interfaccia del tunnel virtuale

Configurare l'interfaccia del tunnel virtuale per specificare l'origine e la destinazione del tunnel. Questi IP verranno utilizzati per crittografare il traffico sul tunnel. Verificare che il profilo IPSec sia applicato anche a questa interfaccia, come mostrato di seguito.

```
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
```



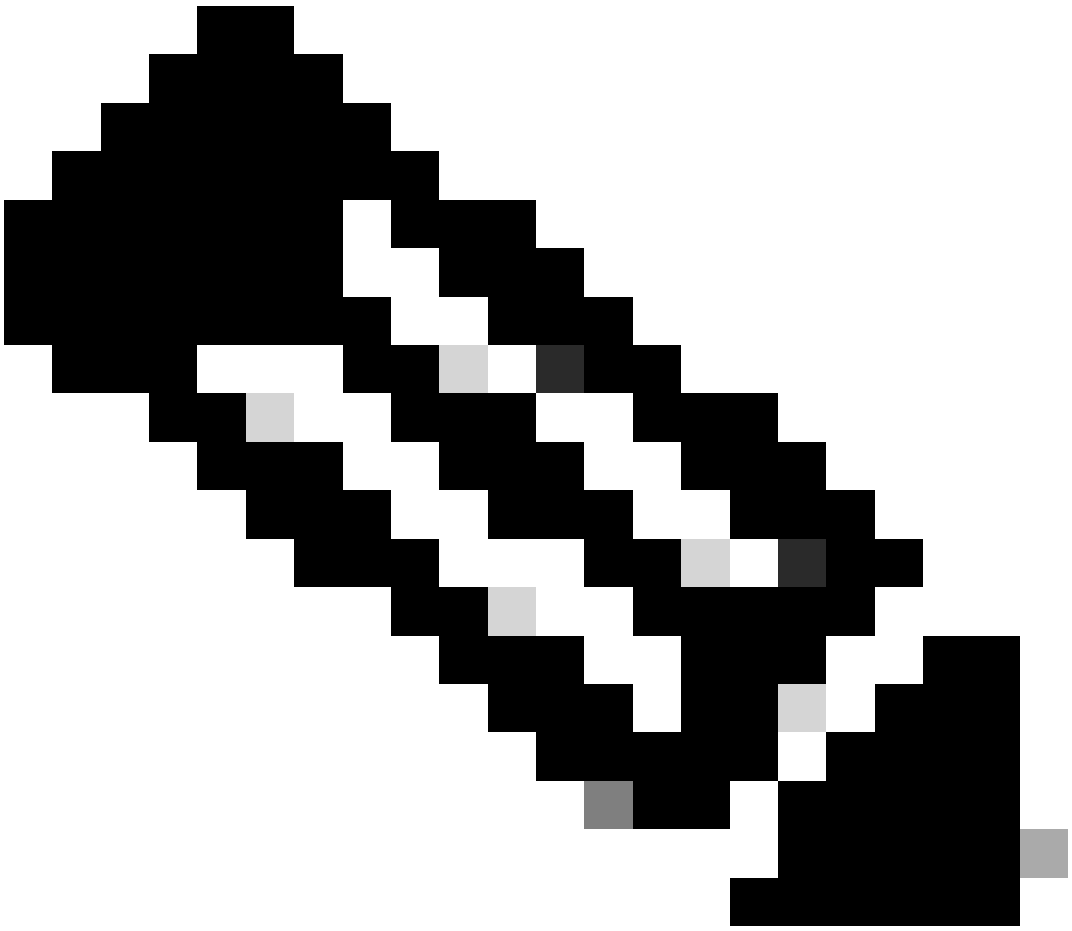
Nota: è necessario specificare l'IP virtuale utilizzato per HSRP come origine del tunnel. L'uso dell'interfaccia fisica, in questo scenario Gigabit Ethernet1, provocherà il fallimento della negoziazione del tunnel.

Configurazione del routing dinamico e/o statico

È necessario configurare il routing con protocolli di routing dinamico e/o route statiche a seconda dei requisiti e della progettazione della rete. Nell'esempio, viene usata una combinazione di EIGRP e un percorso statico per stabilire la comunicazione dell'underlay e il flusso del traffico di dati overlay sul tunnel da sito a sito.

```
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: verificare che la subnet dell'interfaccia del tunnel, che in questo scenario è 10.10.10.0/24, venga annunciata.

Configurazioni router peer

Configurare la proposta e il criterio IKEv2

Configurare una proposta IKEv2 con il gruppo di crittografia, hashing e DH desiderato e mapparlo a un criterio IKEv2.

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

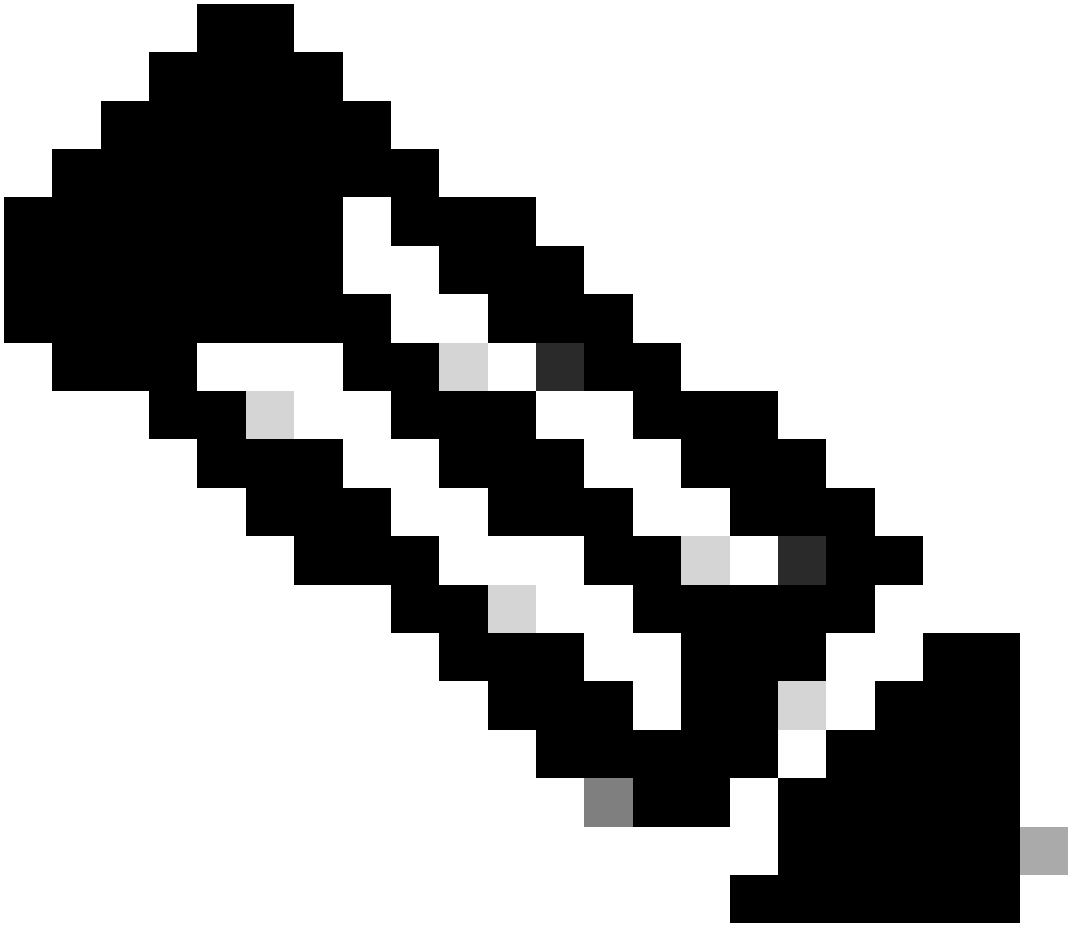
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configurazione della sequenza di tasti

Configurare il keyring per archiviare la chiave già condivisa che verrà utilizzata per autenticare il peer.

```
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: l'indirizzo IP del peer utilizzato in questo caso sarà l'indirizzo IP virtuale configurato nella configurazione HSRP del peer. Accertarsi di non configurare il keyring per l'IP dell'interfaccia fisica del peer primario/secondario.

Configurare il profilo IKEv2

Configurare il profilo IKEv2 e collegarvi il keyring. Impostare l'indirizzo locale come IP dell'interfaccia con connessione Internet del router e l'indirizzo remoto sull'indirizzo IP virtuale utilizzato per HSRP nel peer primario/secondario.

```
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
```

Configurare il set di trasformazioni IPSec

Configurare i parametri della fase 2 di crittografia e hashing utilizzando il set di trasformazioni IPsec.

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

Configurare il profilo IPSec

Configurare il profilo IPSec per eseguire il mapping del profilo IKEv2 e del set di trasformazioni IPSec. Il profilo IPsec verrà applicato all'interfaccia del tunnel.

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

Configurazione dell'interfaccia del tunnel virtuale

Configurare l'interfaccia del tunnel virtuale per specificare l'origine e la destinazione del tunnel. La destinazione del tunnel deve essere impostata come IP virtuale utilizzato per HSRP sul peer primario/secondario. Verificare che il profilo IPSec sia applicato anche all'interfaccia, come mostrato.

```
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
```

Configurazione del routing dinamico e/o statico

Configurare le route richieste con protocolli di routing dinamico o route statiche simili a quelle dell'altro endpoint.

```
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
```

Verifica

Per comprendere il comportamento previsto, vengono presentati i tre scenari seguenti.

Scenario 1. Router principale e secondario attivi

Poiché il router primario è configurato con una priorità più alta, il tunnel IPsec viene negoziato e stabilito su questo router. Per verificare lo stato dei due router, è possibile utilizzare il 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
```

Per verificare le associazioni di sicurezza per la fase 1 (IKEv2) e la fase 2 (IPsec) per il tunnel, è possibile utilizzare i comandi show crypto ikev2 sae show 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:
```

Scenario 2. Il router primario è inattivo e il router secondario è attivo

In uno scenario in cui il router primario sperimenta un'interruzione o si blocca, il router secondario diventa il router attivo e il tunnel da sito a sito viene negoziato con questo router.

È possibile verificare nuovamente lo stato HSRP del router secondario con il 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
```

Quando si verifica questa interruzione, è inoltre possibile osservare i seguenti registri. I log mostrano anche che il router secondario è ora attivo e che il tunnel è stato stabilito.

*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

Per controllare le associazioni di protezione della fase 1 e della fase 2, è possibile utilizzare di nuovo l'operatore show crypto ikev2 saand show crypto ipsec sacome mostrato di seguito.

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. Il router principale viene ripristinato e il router secondario entra in standby

Una volta ripristinato il router principale, che non è più inattivo, diventa nuovamente il router attivo perché ha una priorità più alta configurata e il router secondario passa alla modalità standby.

In questo scenario, quando si verifica questa transizione, vengono visualizzati questi registri sui router primario e secondario.

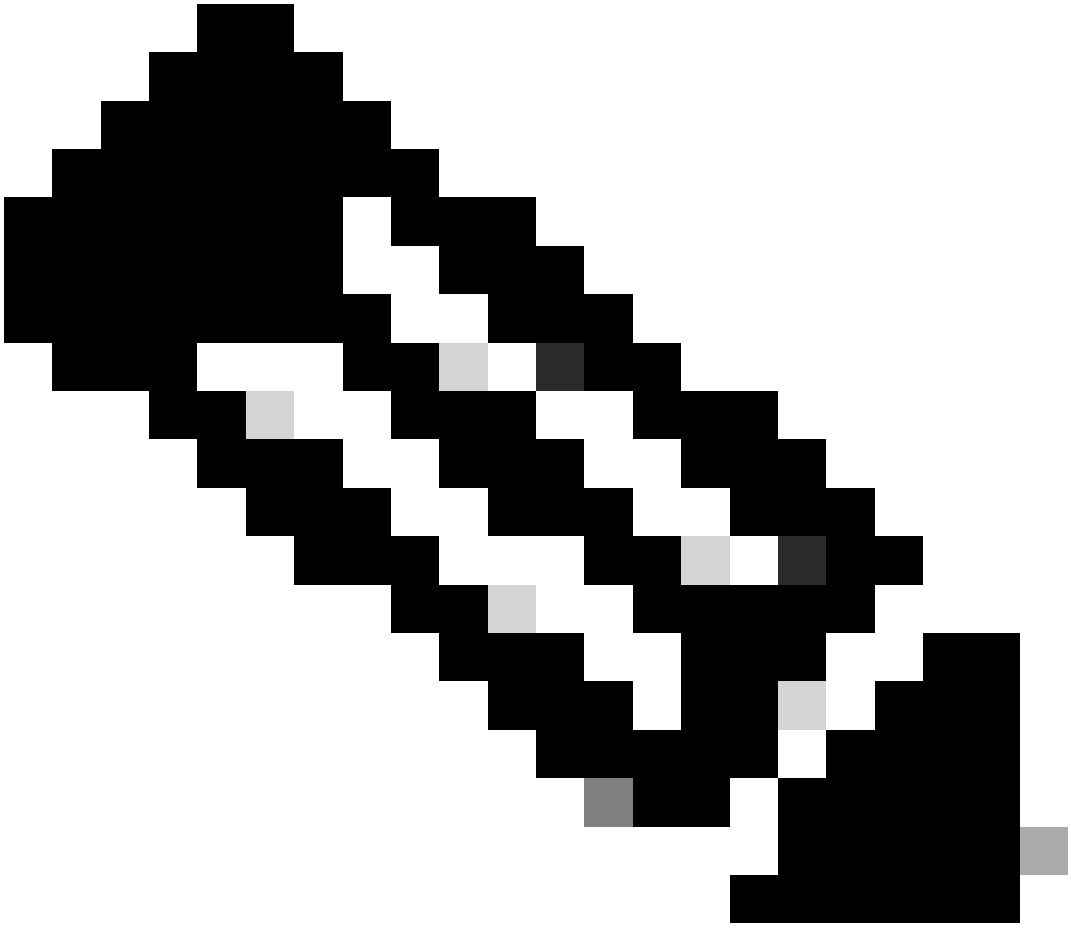
Sul router primario, vengono visualizzati i seguenti log:

*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

Sul router secondario, vengono visualizzati questi registri che mostrano che il router secondario è diventato nuovamente il router in 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

Per controllare lo stato delle associazioni di protezione di Fase 1 e Fase 2, è possibile utilizzare show crypto ikev2 sae **show crypto ipsec sa**per verificare lo stesso.



Nota: se sui router sono configurati più tunnel attivi e in esecuzione, è possibile usare i comandi show crypto session remote X.X.X e show crypto ipsec sa peer X.X.X.X per controllare lo stato del tunnel per la fase 1 e la fase 2.

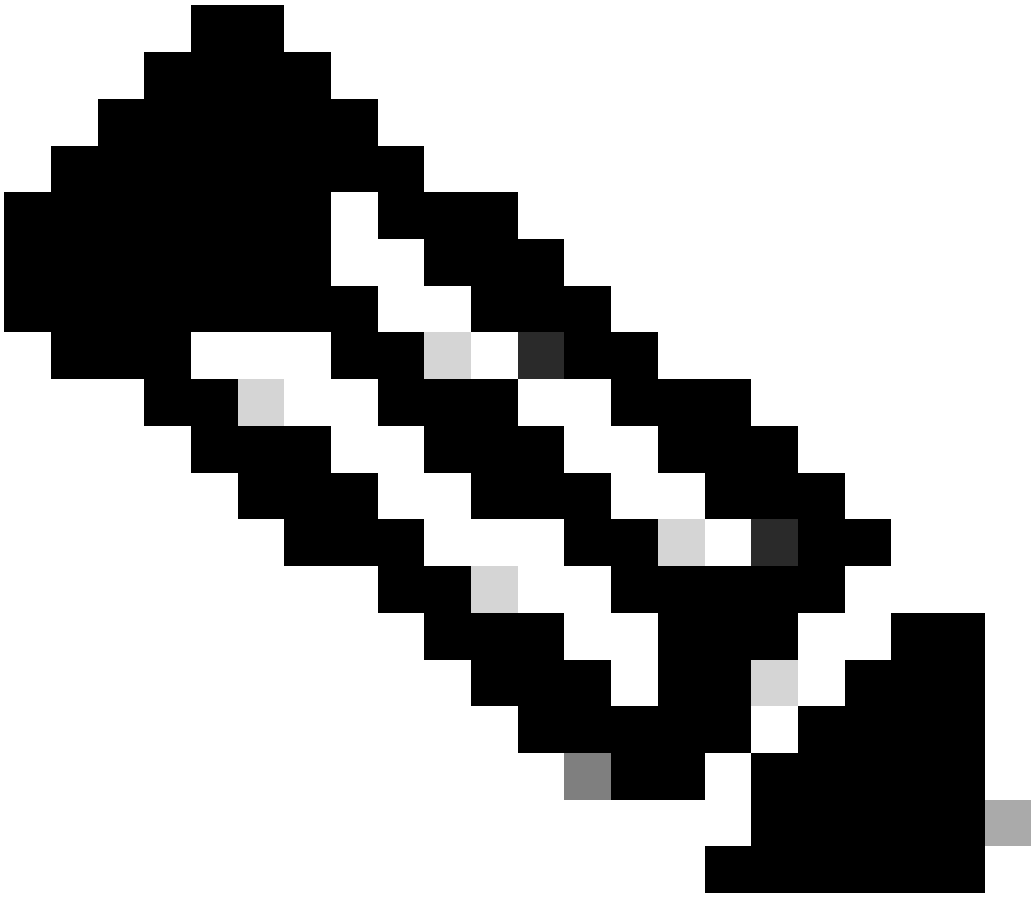
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

È possibile abilitare i debug per la risoluzione dei problemi del tunnel IKEv2.

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

debug crypto ipsec error
debug crypto ipsec message



Nota: se si desidera risolvere i problemi relativi a un solo tunnel (come nel caso del dispositivo in produzione), è necessario abilitare i debug condizionali utilizzando il comando, debug crypto condition peer ipv4 X.X.X.X.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).