Configurer la redondance IPsec avec HSRP pour le tunnel basé sur la route IKEv2 sur les routeurs Cisco

Table des matières

Introduction

Ce document décrit comment configurer la redondance IPsec avec HSRP pour le tunnel basé sur la route IKEv2 sur les routeurs Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN de site à site
- Protocole HSRP (Hot Standby Router Protocol)
- Connaissances de base sur IPsec et IKEv2

Composants utilisés

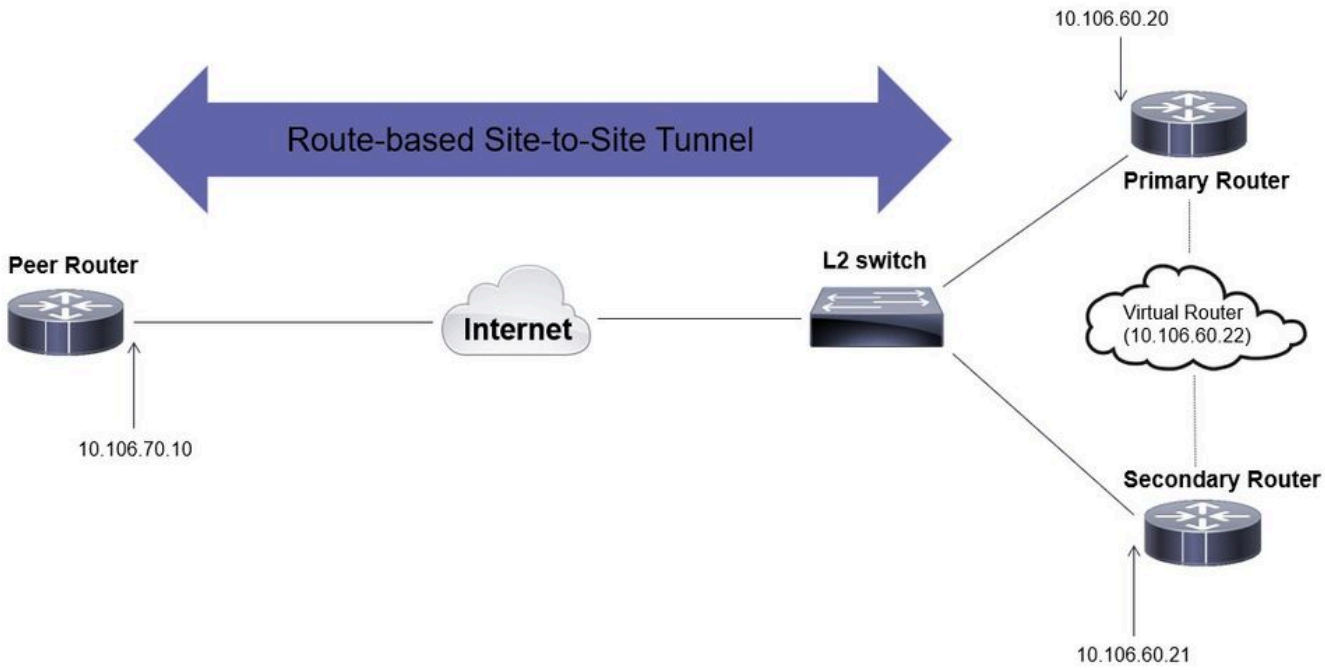
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco CSR1000v exécutant le logiciel IOS XE, version 17.03.08a
- Commutateur de couche 2 exécutant le logiciel Cisco IOS, version 15.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Configurations du routeur principal/secondaire

Configuration de l'interface physique avec HSRP

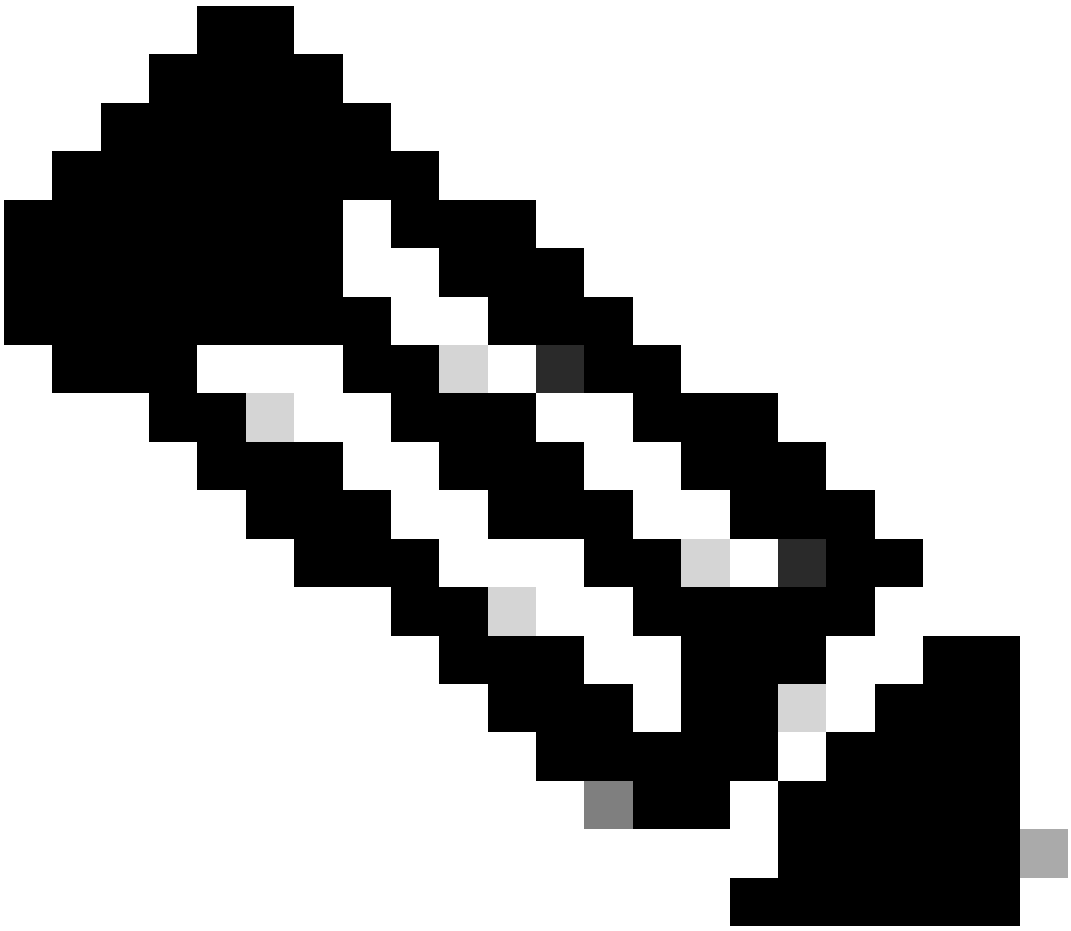
Configurez les interfaces physiques des routeurs principal (avec une priorité plus élevée) et secondaire (avec une priorité par défaut de 100) :

Routeur 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
```

Routeur secondaire :

```
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
```



Remarque : assurez-vous que le routeur principal par défaut est configuré avec une

---

priorité plus élevée afin d'en faire l'homologue actif même lorsque les deux routeurs sont opérationnels sans aucun problème. Dans cet exemple, le routeur principal a été configuré avec une priorité de 105 tandis que le routeur secondaire a une priorité de 100 (qui est la priorité par défaut pour HSRP).

Configuration de la proposition et de la politique IKEv2

Configurez une proposition IKEv2 avec le groupe de cryptage, de hachage et DH de votre choix et mappez-la à une stratégie IKEv2.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configuration du porte-clés

Configurez le porte-clés pour stocker la clé pré-partagée qui sera utilisée pour authentifier l'homologue.

```
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
```

Configuration du profil IKEv2

Configurez le profil IKEv2 et attachez-y le porte-clés. Définissez l'adresse locale sur l'adresse IP virtuelle utilisée pour HSRP et l'adresse distante comme adresse IP de l'interface Internet du routeur.

```
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
```

Configuration du Transform-Set IPsec

Configurez les paramètres de phase 2 du chiffrement et du hachage à l'aide du jeu de transformation IPsec.

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

Configurer le profil IPsec

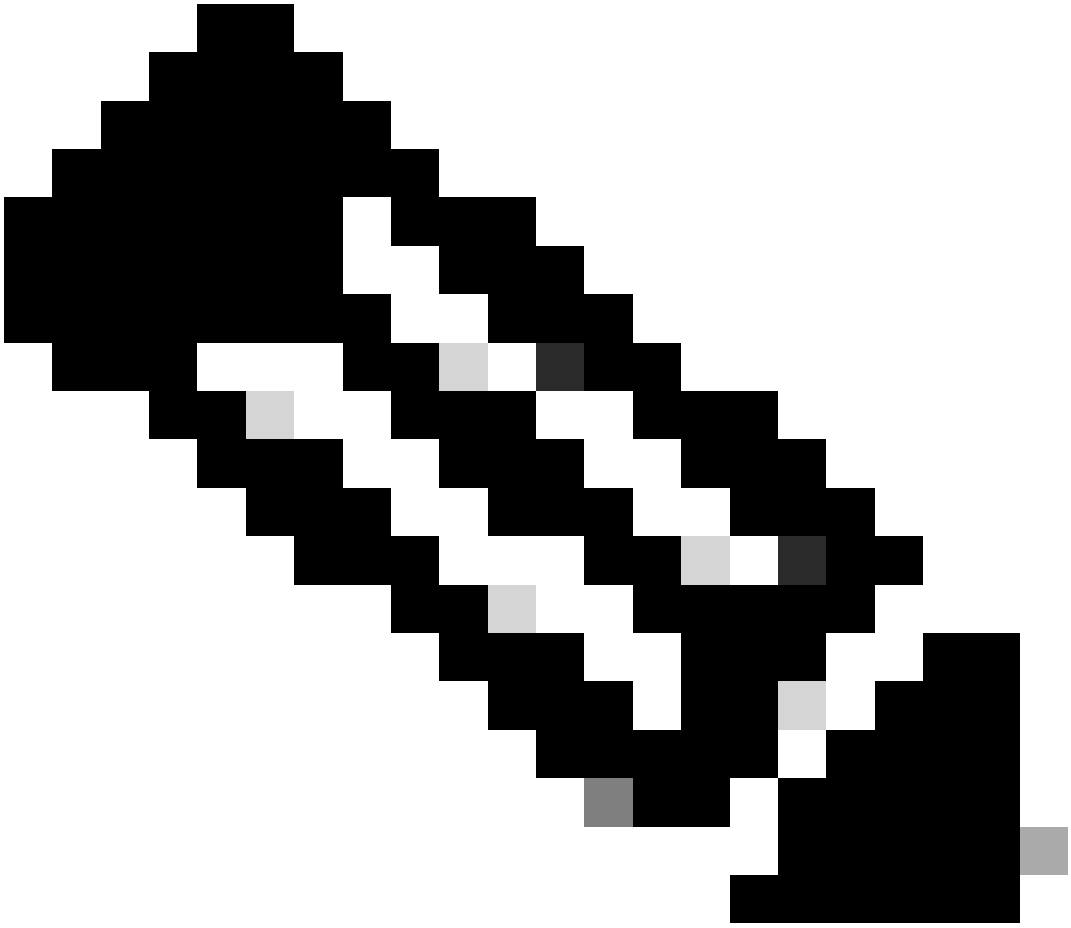
Configurez le profil IPsec pour mapper le profil IKEv2 et le jeu de transformation IPsec. Le profil IPsec sera appliqué à l'interface du tunnel.

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

Configuration de l'interface de tunnel virtuel

Configurez l'interface de tunnel virtuel pour spécifier la source et la destination du tunnel. Ces adresses IP seront utilisées pour chiffrer le trafic sur le tunnel. Assurez-vous que le profil IPsec est également appliqué à cette interface, comme indiqué ci-dessous.

```
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
```



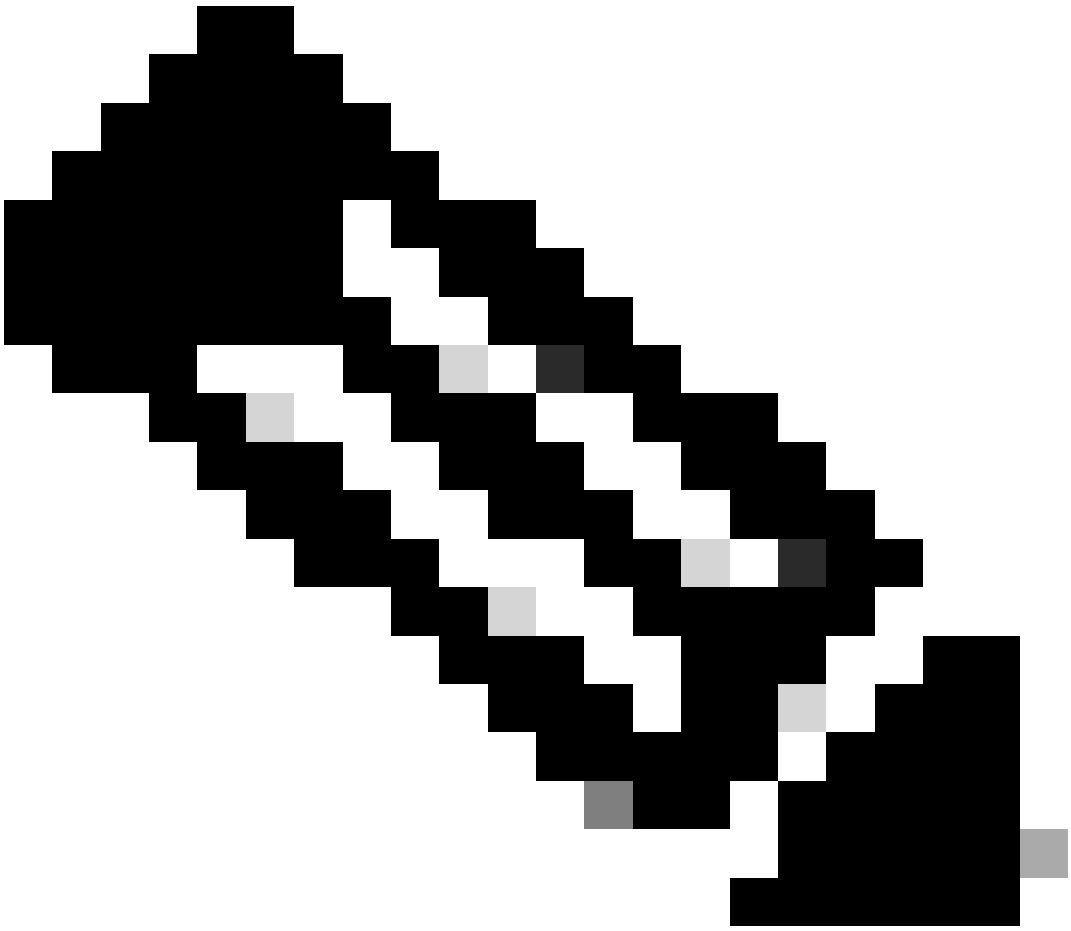
Remarque : vous devrez spécifier l'IP virtuelle qui est utilisée pour HSRP comme source du tunnel. L'utilisation de l'interface physique, dans ce scénario GigabitEthernet1, entraînera l'échec de la négociation du tunnel.

Configuration du routage dynamique et/ou statique

Vous devez configurer le routage avec des protocoles de routage dynamique et/ou des routes statiques en fonction des besoins et de la conception du réseau. Dans cet exemple, une combinaison du protocole EIGRP et d'une route statique est utilisée pour établir la communication sous-jacente et le flux du trafic de données de superposition sur le tunnel site à 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
```



Remarque : assurez-vous que le sous-réseau de l'interface du tunnel, qui dans ce scénario est 10.10.10.0/24, est annoncé.

Configurations des routeurs homologues

Configuration de la proposition et de la politique IKEv2

Configurez une proposition IKEv2 avec le groupe de cryptage, de hachage et DH de votre choix et mappez-la à une stratégie IKEv2.

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

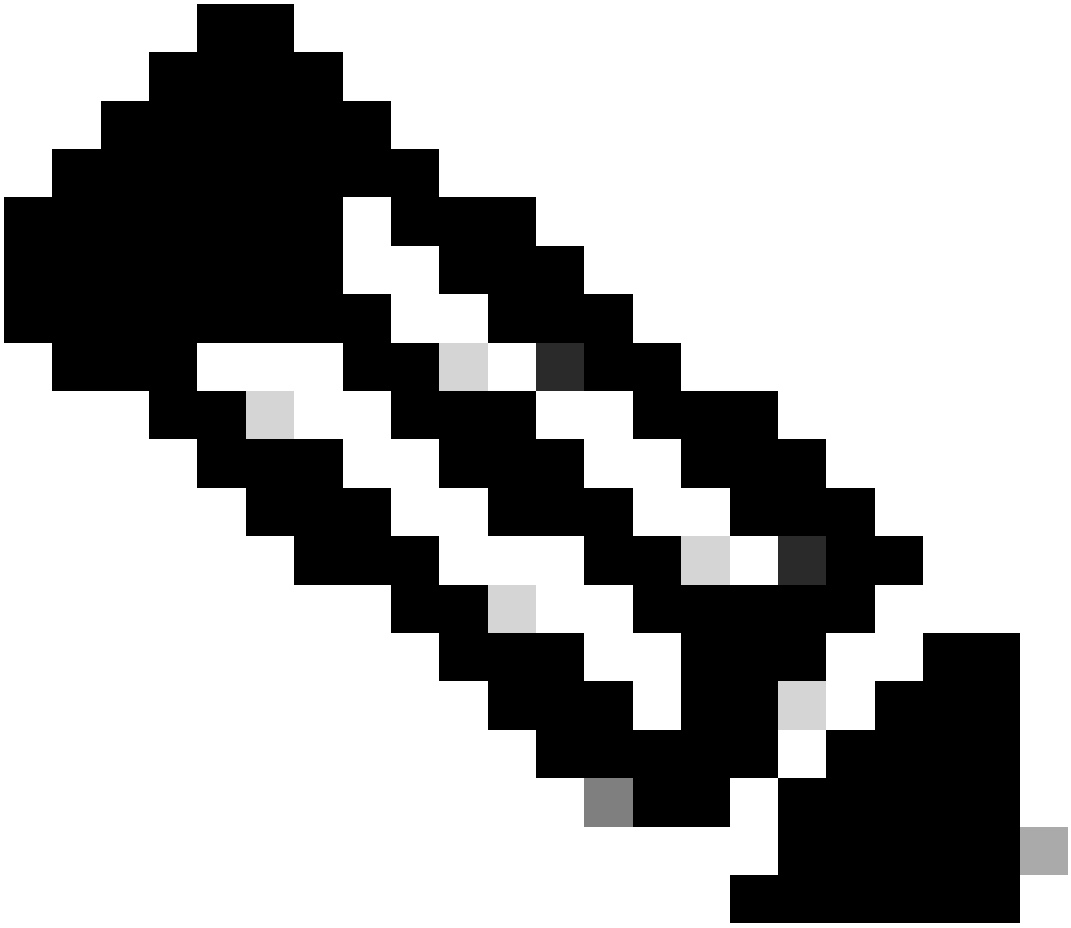
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

Configuration du porte-clés

Configurez le porte-clés pour stocker la clé pré-partagée qui sera utilisée pour authentifier l'homologue.

```
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
```



Remarque : l'adresse IP de l'homologue utilisée ici sera l'adresse IP virtuelle qui est configurée dans la configuration HSRP de l'homologue. Assurez-vous que vous ne configurez pas le trousseau de clés pour l'adresse IP de l'interface physique de l'homologue principal/secondaire.

Configuration du profil IKEv2

Configurez le profil IKEv2 et attachez-y le porte-clés. Définissez l'adresse locale comme adresse IP de l'interface Internet du routeur et l'adresse distante comme adresse IP virtuelle utilisée pour HSRP sur l'homologue principal/secondaire.

```
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
```

Configuration du Transform-Set IPsec

Configurez les paramètres de phase 2 du chiffrement et du hachage à l'aide du jeu de transformation IPsec.

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

Configurer le profil IPsec

Configurez le profil IPsec pour mapper le profil IKEv2 et le jeu de transformation IPsec. Le profil IPsec sera appliqué à l'interface du tunnel.

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

Configuration de l'interface de tunnel virtuel

Configurez l'interface de tunnel virtuel pour spécifier la source et la destination du tunnel. La destination du tunnel doit être définie comme l'IP virtuelle utilisée pour HSRP sur l'homologue principal/secondaire. Assurez-vous que le profil IPsec est également appliqué à cette interface, comme indiqué.

```
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
```

Configuration du routage dynamique et/ou statique

Configurez les routes requises avec des protocoles de routage dynamique ou des routes statiques similaires à celles dont vous disposez pour l’autre point d’extrémité.

```
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
```

Vérifier

Pour comprendre le comportement attendu, les trois scénarios suivants sont présentés.

Scénario 1. Les routeurs principal et secondaire sont actifs

Comme le routeur principal est configuré avec une priorité plus élevée, le tunnel IPsec est négocié et établi sur ce routeur. Pour vérifier l'état des deux routeurs, vous pouvez utiliser la show standbycommande.

<#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
```

Pour vérifier les associations de sécurité de phase 1 (IKEv2) et de phase 2 (IPsec) pour le tunnel, vous pouvez utiliser les commandes show crypto ikev2 saet 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:
```

Scénario 2. Le routeur principal est inactif et le routeur secondaire est actif

Dans un scénario où le routeur principal subit une panne ou tombe en panne, le routeur secondaire devient le routeur actif et le tunnel site à site est négocié avec ce routeur.

L'état HSRP du routeur secondaire peut à nouveau être vérifié à l'aide de la show standby commande.

<#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
```

En outre, vous observerez également les journaux suivants lorsque cette interruption se produit. Ces journaux indiquent également que le routeur secondaire est maintenant actif et que le tunnel a été établi.

*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

Pour vérifier les associations de sécurité de phase 1 et de phase 2, vous pouvez à nouveau utiliser le show crypto ikev2 saet show crypto ipsec sacomme indiqué ici.

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:

Scénario 3. Le routeur principal redémarre et le routeur secondaire est mis en veille

Une fois que le routeur principal est restauré et n'est plus arrêté, il redevient le routeur actif car sa priorité est configurée plus élevée et le routeur secondaire passe en mode veille.

Au cours de ce scénario, vous voyez ces journaux sur les routeurs principal et secondaire lorsque cette transition se produit.

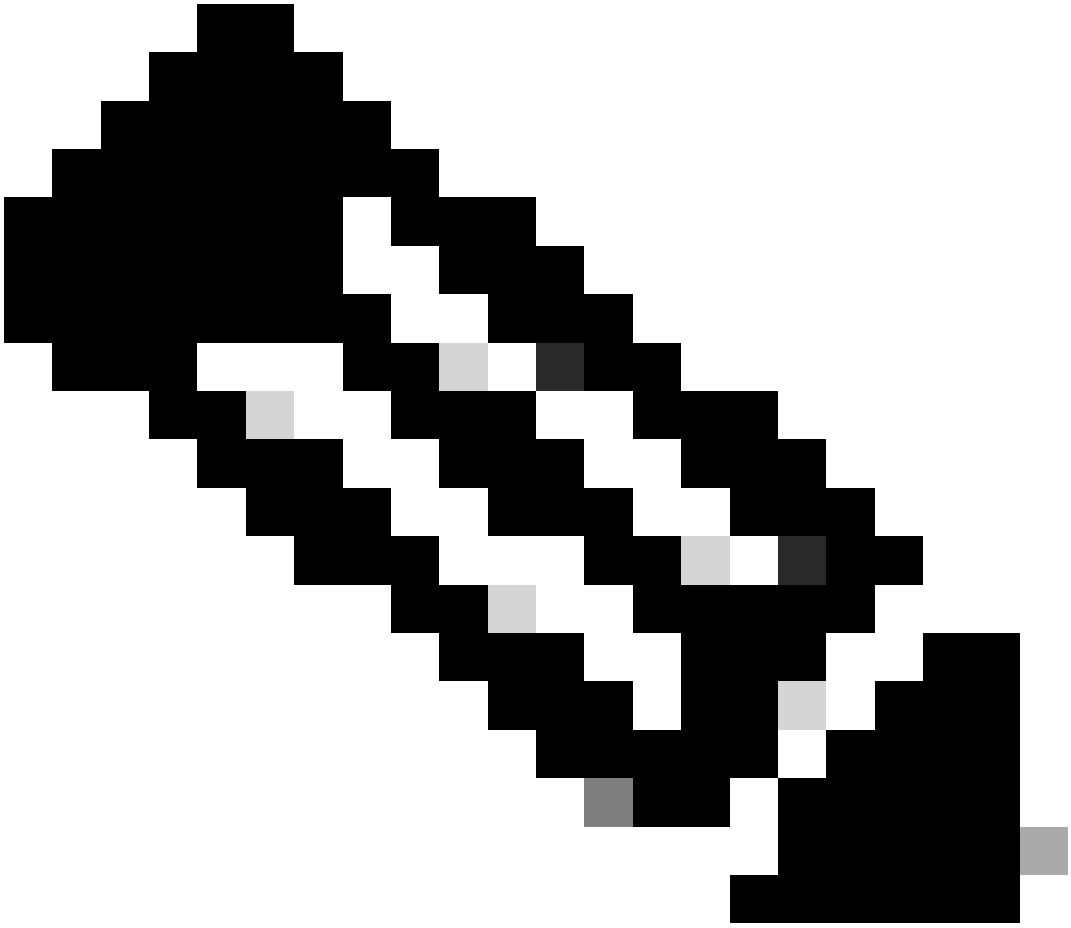
Sur le routeur principal, ces journaux apparaissent :

*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

Sur le routeur secondaire, vous voyez ces journaux qui montrent que le routeur secondaire est redevenu le routeur de secours :

*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

Pour vérifier l'état des associations de sécurité de Phase 1 et de Phase 2, vous pouvez utiliser l' show crypto ikev2 saet **show crypto ipsec sa**l'.



Remarque : si plusieurs tunnels sont configurés sur les routeurs qui sont opérationnels, vous pouvez utiliser les commandes show crypto session remote X.X.X.X et show crypto ipsec sa peer X.X.X.X pour vérifier l'état des phases 1 et 2 du tunnel.

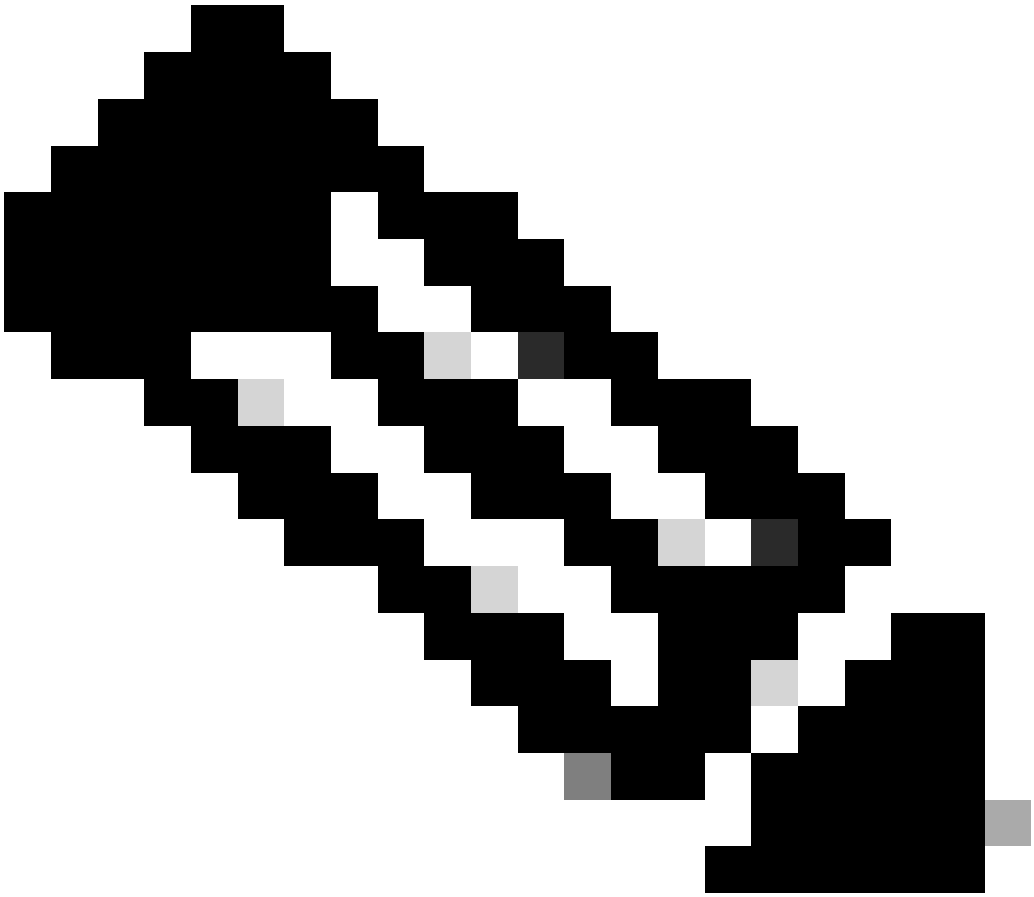
Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ces débogages peuvent être activés pour dépanner le tunnel IKEv2.

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

debug crypto ipsec error
debug crypto ipsec message



Remarque : si vous souhaitez dépanner un seul tunnel (ce qui doit être le cas si le périphérique est en production), vous devez activer les débogages conditionnels à l'aide de la commande, debug crypto condition peer ipv4 X.X.X.X.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.