تكوين نفق IPsec باستخدام HSRP للتوجيه إلى مسار IKEv2 على موجهات Cisco

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق IPsec باستخدام HSRP للنفق المستند إلى مسار IKEv2 على موجهات Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة VPN من موقع إلى موقع
- بروتوكول الموجه الاحتياطي الفعال [HSRP]
- معرفة أساسية بـ IPsec و IKEv2

المكونات المستخدمة

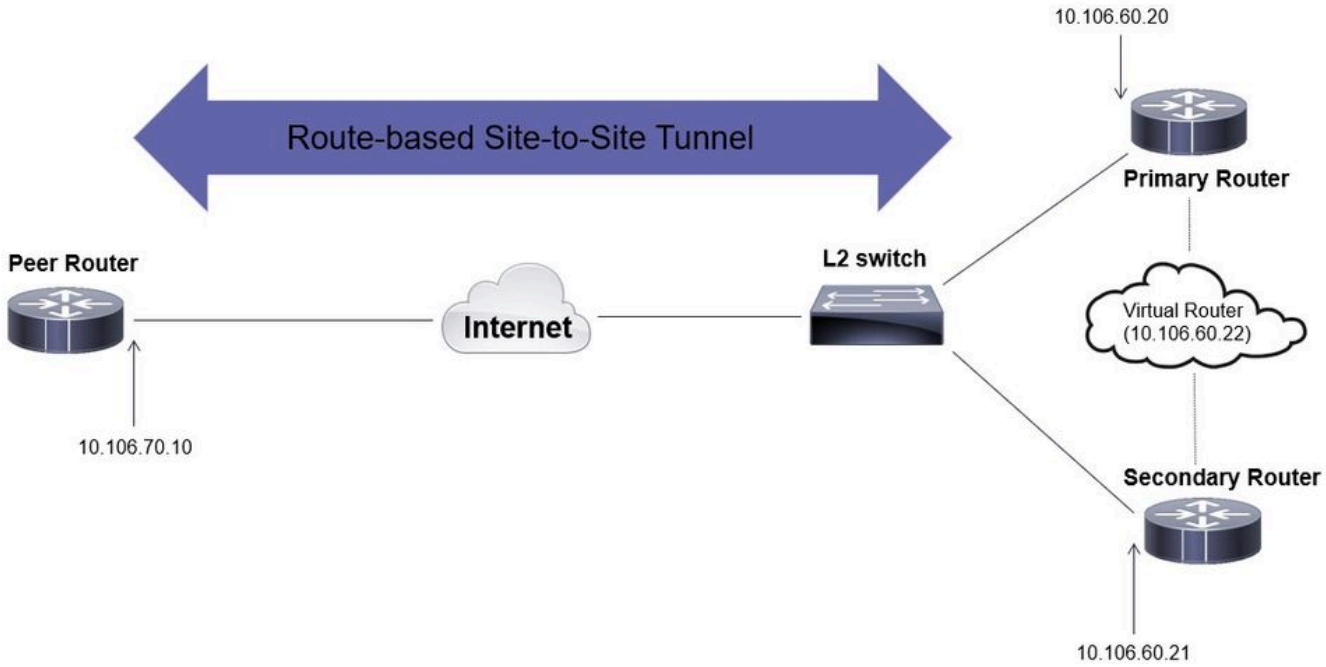
تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجه Cisco CSR1000V الذي يشغل برنامج IOS XE، الإصدار 17.03.08a
- محول الطبقة 2 الذي يشغل برنامج Cisco IOS Software، الإصدار 15.2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



تكوينات الموجه الأولي/الثانوي

تكوين الواجهة المادية باستخدام HSRP

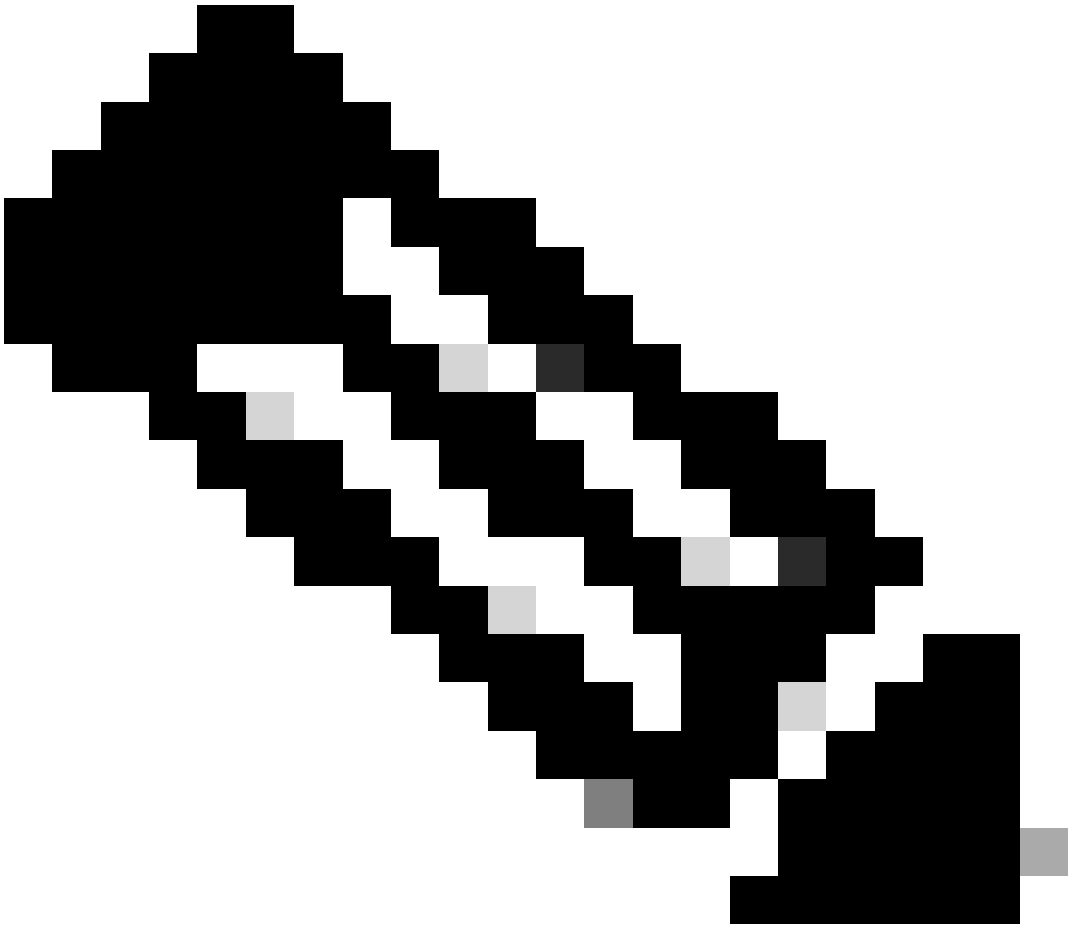
قم بتكوين الواجهات المادية للموجهات الأساسية (ذات الأولوية العليا) والثانوية (بأولوية افتراضية مقدارها 100):

الموجه الرئيسي:

```
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
```

الموجه الثانوي:

```
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
```



ملاحظة: تأكد من تكوين الموجه الأساسي الافتراضي بأولوية أعلى من أجل جعله النظير النشط حتى عندما يكون كلا الموجهين قيد التشغيل وقيد التشغيل دون أي مشاكل. على سبيل المثال، تم تكوين الأساسي بأولوية تبلغ 105 في حين أن الموجه الثانوي لديه أولوية تبلغ 100 (وهو الإعداد الافتراضي لـ HSRP).

تكوين مقترح IKEv2 ونهج

قم بتكوين اقتراح IKEv2 باستخدام التشفير والتجزئة ومجموعة DH التي تختارها وقم بتعيينها إلى سياسة IKEv2.

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

تكوين حلقة المفاتيح

قم بتكوين حلقة المفاتيح لتخزين المفتاح المشترك مسبقا الذي سيتم إستخدامه لمصادقة النظير.

```
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
```

تكوين ملف تعريف IKEv2

قم بتكوين ملف تعريف IKEv2 وربط حلقة المفاتيح به. قم بتعيين العنوان المحلي إلى عنوان IP الظاهري الذي يتم إستخدامه ل HSRP والعنوان البعيد كعنوان IP الخاص بواجهة الإنترنت للموجه.

```
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
```

تكوين مجموعة تحويل IPsec

تكوين معلمات المرحلة 2 للتشفير والتجزئة باستخدام مجموعة تحويل IPsec.

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

تكوين ملف تعريف IPsec

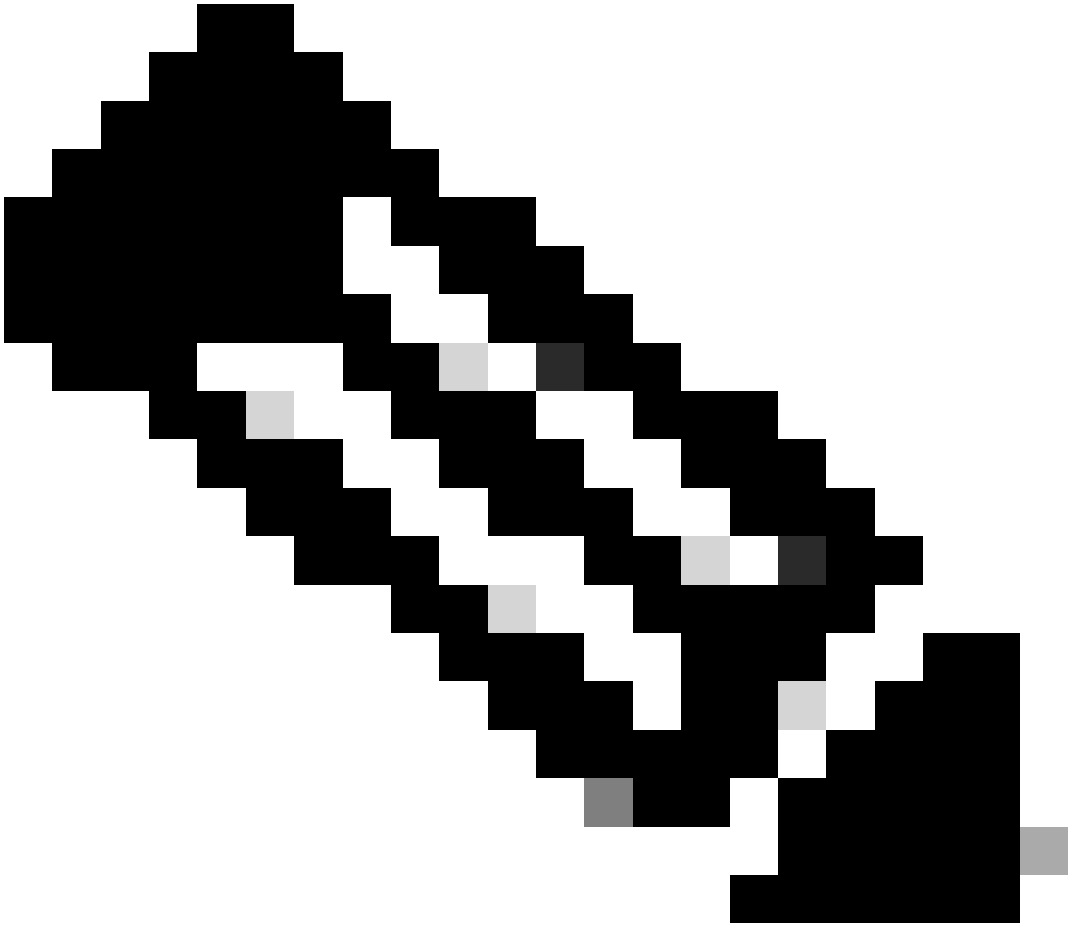
قم بتكوين ملف تعريف IPsec لتعيين ملف تعريف IKEv2 ومجموعة تحويل IPsec. سيتم تطبيق ملف تعريف IPsec على واجهة النفق.

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

تكوين واجهة النفق الظاهري

قم بتكوين واجهة النفق الظاهرية لتحديد مصدر النفق والوجهة. سيتم إستخدام عناوين IP هذه لتشفير حركة المرور عبر النفق. تأكد من تطبيق ملف تعريف IPsec أيضا على هذه الواجهة كما هو موضح أدناه.

```
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
```



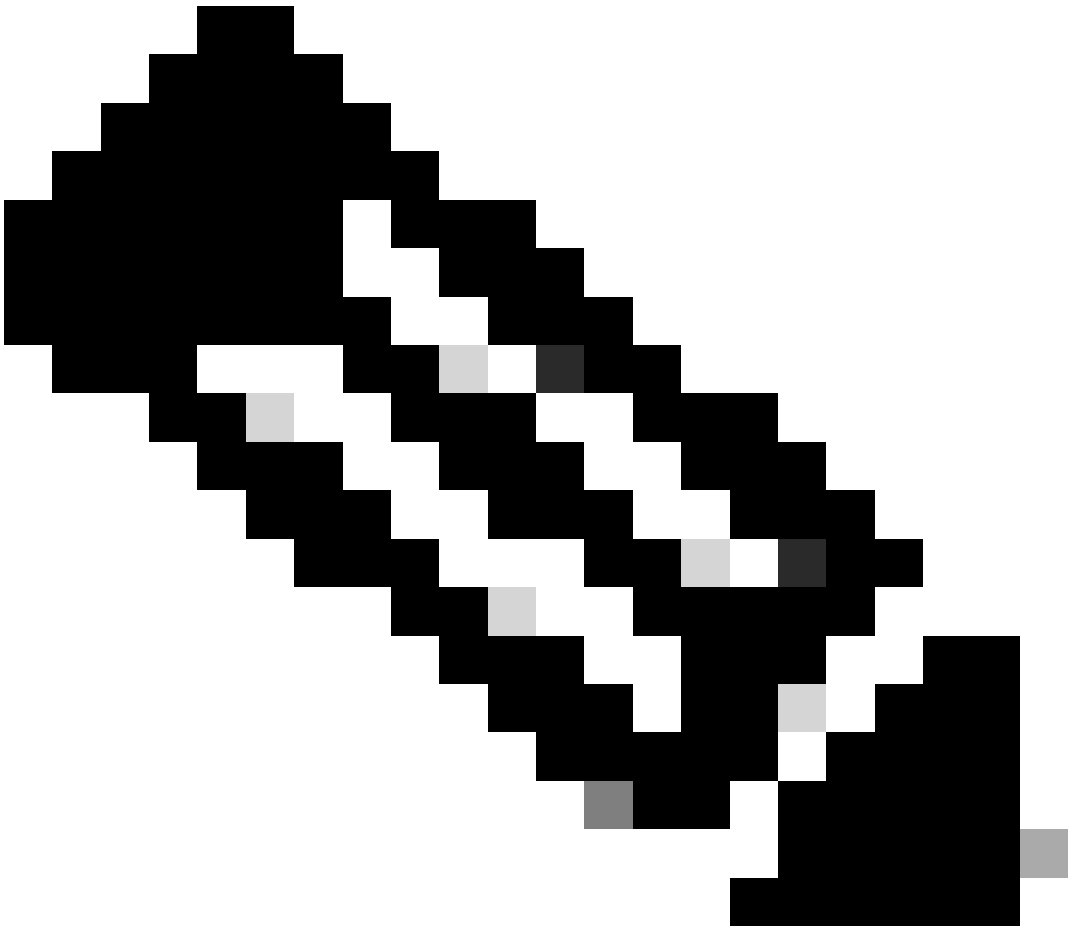
ملاحظة: ستحتاج إلى تحديد IP الظاهري الذي يتم إستخدامه ل HSRP كمصدر للنفق. سيؤدي إستخدام الواجهة المادية، في هذا السيناريو GigabitEthernet1، إلى فشل مفاوضات النفق.

تكوين التوجيه الديناميكي و/أو الثابت

يجب تكوين التوجيه باستخدام بروتوكولات التوجيه الديناميكية و/أو المسارات الثابتة وفقا للمتطلبات وتصميم الشبكة. على سبيل المثال، يتم إستخدام مجموعة من بروتوكول EIGRP ومسار ثابت لإنشاء الاتصال الأساسي وتدفق حركة مرور البيانات المتداخلة عبر نفق من موقع إلى موقع.

```
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
```



ملاحظة: تأكد من الإعلان عن الشبكة الفرعية لواجهة النفق، والتي تكون في هذا السيناريو 10.10.10.0/24.

تكوينات موجه النظير

تكوين مقترح IKEv2 ونهجه

قم بتكوين اقتراح IKEv2 باستخدام التشفير والتجزئة ومجموعة DH التي تختارها وقم بتعيينها إلى سياسة IKEv2.

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

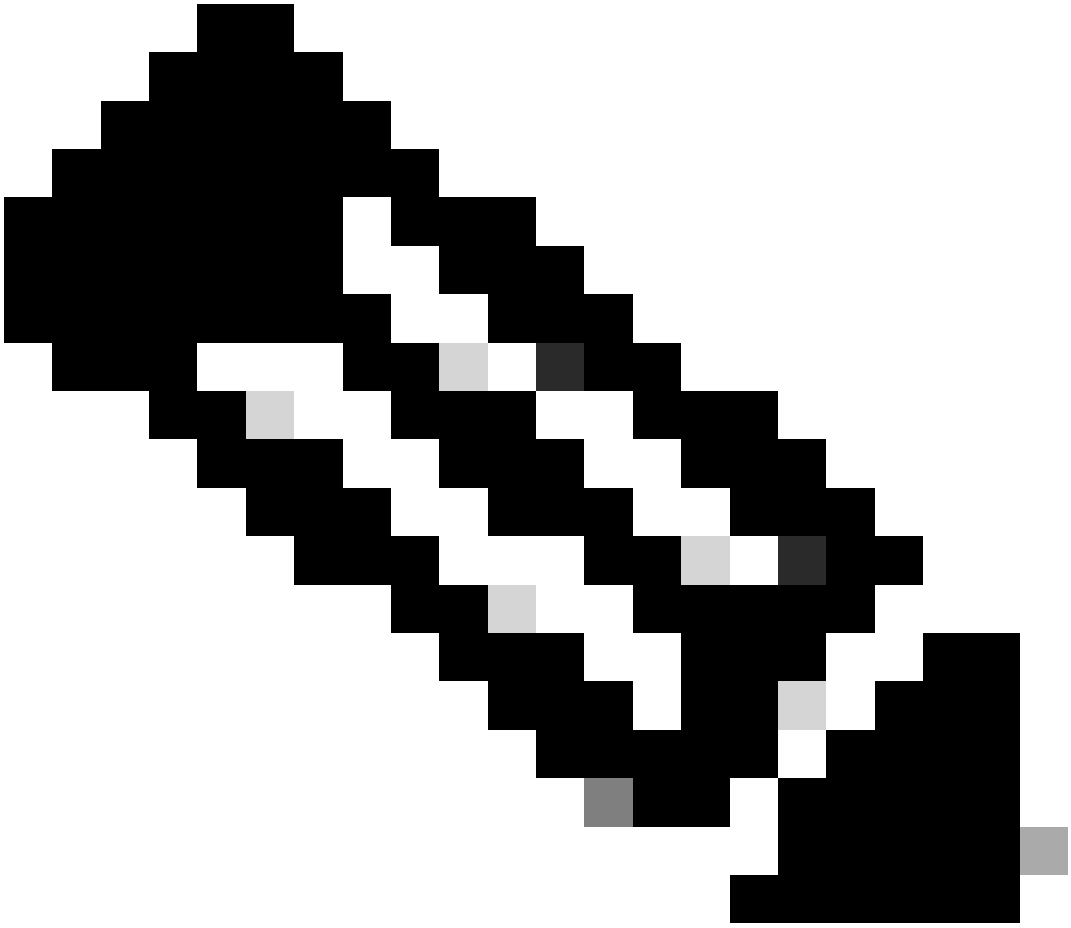
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

تكوين حلقة المفاتيح

قم بتكوين حلقة المفاتيح لتخزين المفتاح المشترك مسبقا الذي سيتم إستخدامه لمصادقة النظير.

```
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
```



ملاحظة: سيكون عنوان IP للنظير المستخدم هنا هو عنوان IP الظاهري الذي تم تكوينه في تكوين HSRP للنظير. تأكد من عدم تكوين حلقة المفاتيح لبروتوكول IP للواجهة المادية للنظير الأساسي/الثانوي.

تكوين ملف تعريف IKEv2

قم بتكوين ملف تعريف IKEv2 وربط حلقة المفاتيح به. قم بتعيين العنوان المحلي على أنه عنوان IP الخاص بواجهة الإنترنت للموجه والعنوان البعيد إلى عنوان IP الظاهري الذي يتم إستخدامه ل HSRP على النظير الأساسي/الثانوي.

```
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
```

تكوين مجموعة تحويل IPsec

تكوين معلمات المرحلة 2 للتشفير والتجزئة باستخدام مجموعة تحويل IPsec.

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

تكوين ملف تعريف IPsec

قم بتكوين ملف تعريف IPsec لتعيين ملف تعريف IKEv2 ومجموعة تحويل IPsec. سيتم تطبيق ملف تعريف IPsec على واجهة النفق.

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

تكوين واجهة النفق الظاهري

قم بتكوين واجهة النفق الظاهرية لتحديد مصدر النفق والوجهة. يجب تعيين وجهة النفق على أنها عنوان IP الظاهري المستخدم لـ HSRP على النظير الأساسي/الثانوي. تأكد من تطبيق ملف تعريف IPsec أيضا على هذه الواجهة كما هو موضح.

```
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
```

تكوين التوجيه الديناميكي و/أو الثابت

قم بتكوين الموجهات المطلوبة باستخدام بروتوكولات التوجيه الديناميكية أو الموجهات الثابتة المماثلة للكيفية التي دلك لنقطة النهاية الأخرى.

```
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
```

التحقق من الصحة

ولفهم السلوك المتوقع، يتم عرض السيناريوهات الثلاثة التالية.

السيناريو الأول. كل الموجهين الأساسي والثانوي نشط

ونظرا لأنه تم تكوين الموجه الرئيسي بأولوية أعلى، يتم التفاوض على نفق IPsec وإنشائه على هذا الموجه. للتحقق من حالة الموجهين، يمكنك إستخدام show standbyالأمر.

<#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
```

للتحقق من اقترانات أمان المرحلة 1 (IKEv2) والمرحلة 2 (IPsec) للنفق، يمكنك استخدام show crypto ipsec saأو show crypto ikev2 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:
```

السيناريو 2. الموجه الأساسي غير نشط والموجه الثانوي نشط

في سيناريو حيث يواجه الموجه الرئيسي انقطاع أو انخفاض، يصبح الموجه الثانوي الموجه النشط ويتم التفاوض حول نقل الموقع إلى الموقع مع هذه الموجه.

يمكن التحقق من حالة HSRP للموجه الثانوي مرة أخرى باستخدام show standby الأمر.

<#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
```

عوالة عل ذلك، سوف تالحظ أيضا السجالت التالية عند حدوث اذه التعطيل. تظهر هذه السجالت أيضا أن الموجه الثانوي نشط اآلن وأنه قد تم إنشاء النفق.

*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

للتحقق من اقترانات أمان المرحلة 1 والمرحلة 2، يمكنك مرة أخرى إستخدام show crypto ikev2 sashow crypto ipsec saوه كما موضح انه.

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:

السيناريو 3. يظهر الموجه الرئيسي مرة أخرى ويبدأ الموجه الثانوي في وضع الاستعداد

بمجرد إستعادة الموجه الأساسي وعدم تعطله بعد ذلك، يصبح الموجه النشط مرة أخرى لأنه يتمتع بأولوية أعلى تم تكوينها ويذهب الموجه الثانوي إلى وضع الاستعداد.

أثناء هذا السيناريو، ترى هذه السجلات على الموجهات الأساسية والثانوية عند حدوث هذا الانتقال.

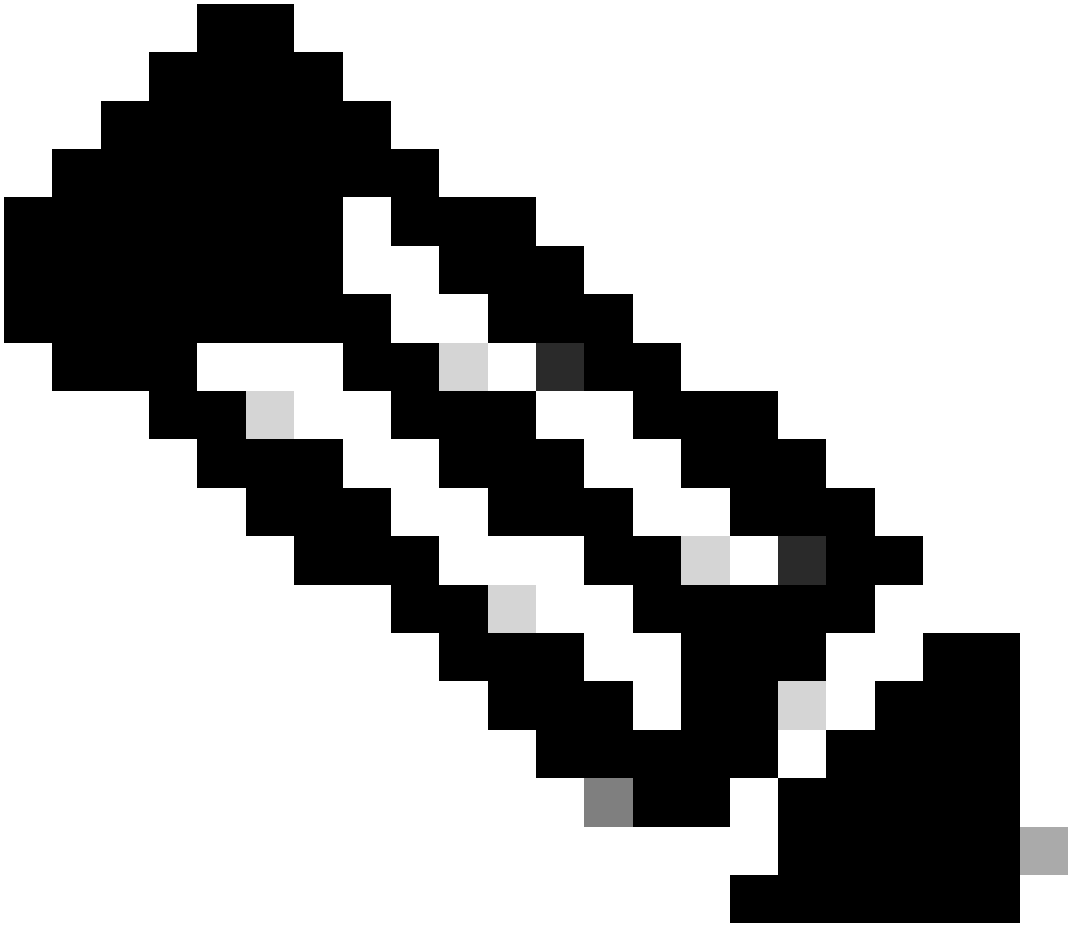
في الموجه الرئيسي، تظهر هذه السجلات:

*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

على الموجه الثانوي، ترى هذه السجلات التي تظهر أن الموجه الثانوي أصبح مرة أخرى الموجه الاحتياطي:

*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

للتحقق من حالة اقترانات أمان المرحلة 1 والمرحلة 2، يمكنك إستخدام show crypto ikev2 saوالتحقق **show crypto ipsec sa**من ذلك.



ملاحظة: إذا كان لديك أنفاق متعددة تم تكوينها على الموجهات قيد التشغيل والإعداد، فيمكنك إستخدام أوامر show crypto session remote x.x.x.x و show crypto ipSec sa peer x.x.x.x للتحقق من حالة المرحلة 1 والمرحلة 2 من النفق.

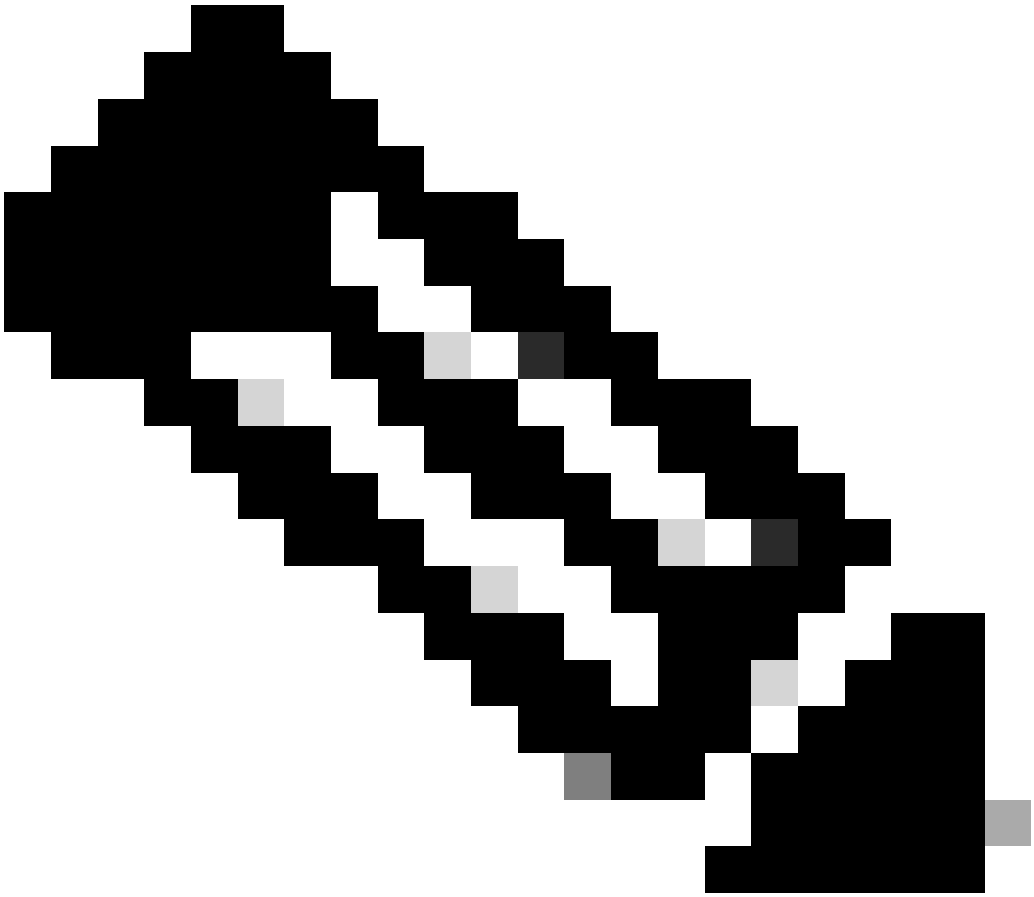
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يمكن تمكين عمليات تصحيح الأخطاء هذه لاستكشاف أخطاء نفق IKEv2 وإصلاحها.

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

debug crypto ipsec error
debug crypto ipsec message



ملاحظة: إذا كنت ترغب في أستكشاف أخطاء نفق واحد فقط وإصلاحها (والذي يجب أن يكون الحالة إذا كان الجهاز في مرحلة الإنتاج)، فيجب عليك تمكين تصحيح الأخطاء الشرطي باستخدام الأمر debug crypto condition peer ipv4 X.X.X.X.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).