CiscoルータでのIKEv2ルートベーストンネル用のHSRPを使用したIPsec冗長性の設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[設定](#)

- [ネットワーク図](#)
- [プライマリ/セカンダリルータの設定](#)
  - [HSRPを使用した物理インターフェイスの設定](#)
  - [IKEv2プロポーザルおよびポリシーの設定](#)
  - [キーリングの設定](#)
  - [IKEv2プロファイルの設定](#)
  - [IPSec トランスフォーム セットを設定します](#)
  - [IPSecプロファイルの設定](#)
  - [仮想トンネルインターフェイスの設定](#)
  - [ダイナミックルーティングとスタティックルーティングの設定](#)
- [ピアルータの設定](#)
  - [IKEv2プロポーザルおよびポリシーの設定](#)
  - [キーリングの設定](#)
  - [IKEv2プロファイルの設定](#)
  - [IPSec トランスフォーム セットを設定します](#)
  - [IPSecプロファイルの設定](#)
  - [仮想トンネルインターフェイスの設定](#)
  - [ダイナミックルーティングとスタティックルーティングの設定](#)

[確認](#)

- [シナリオ 1.プライマリとセカンダリの両方のルータがアクティブ](#)
- [シナリオ 2.プライマリルータが非アクティブで、セカンダリルータがアクティブ](#)
- [シナリオ 3.プライマリルータが復旧し、セカンダリルータがスタンバイになります。](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、CiscoルータでIKEv2ルートベースのトンネル用にHSRPを使用してIPSecの冗長性を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- サイト間 VPN
- ホットスタンバイルータプロトコル[HSRP]
- IPsecおよびIKEv2に関する基礎知識

使用するコンポーネント

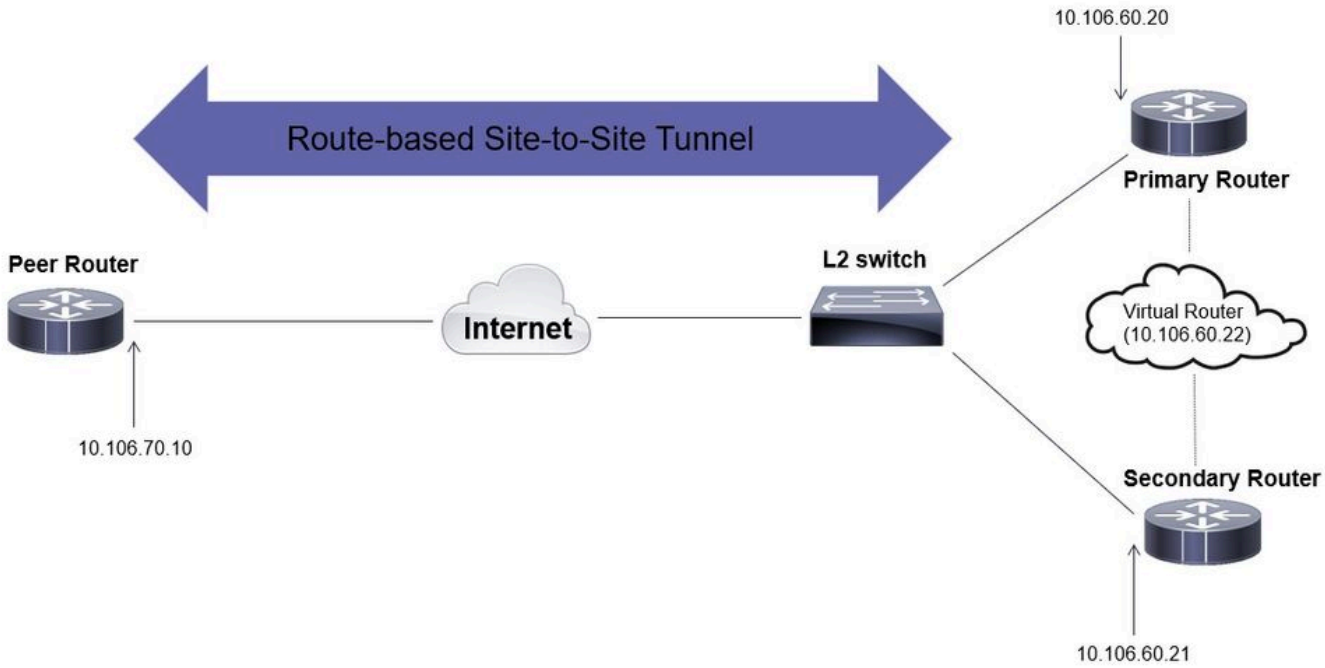
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS XEソフトウェアバージョン17.03.08aを実行するCisco CSR1000vルータ
- Cisco IOSソフトウェアバージョン15.2を実行するレイヤ2スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



プライマリ/セカンダリルータの設定

HSRPを使用した物理インターフェイスの設定

プライマリ（プライオリティが高い）ルータとセカンダリ（プライオリティがデフォルトの

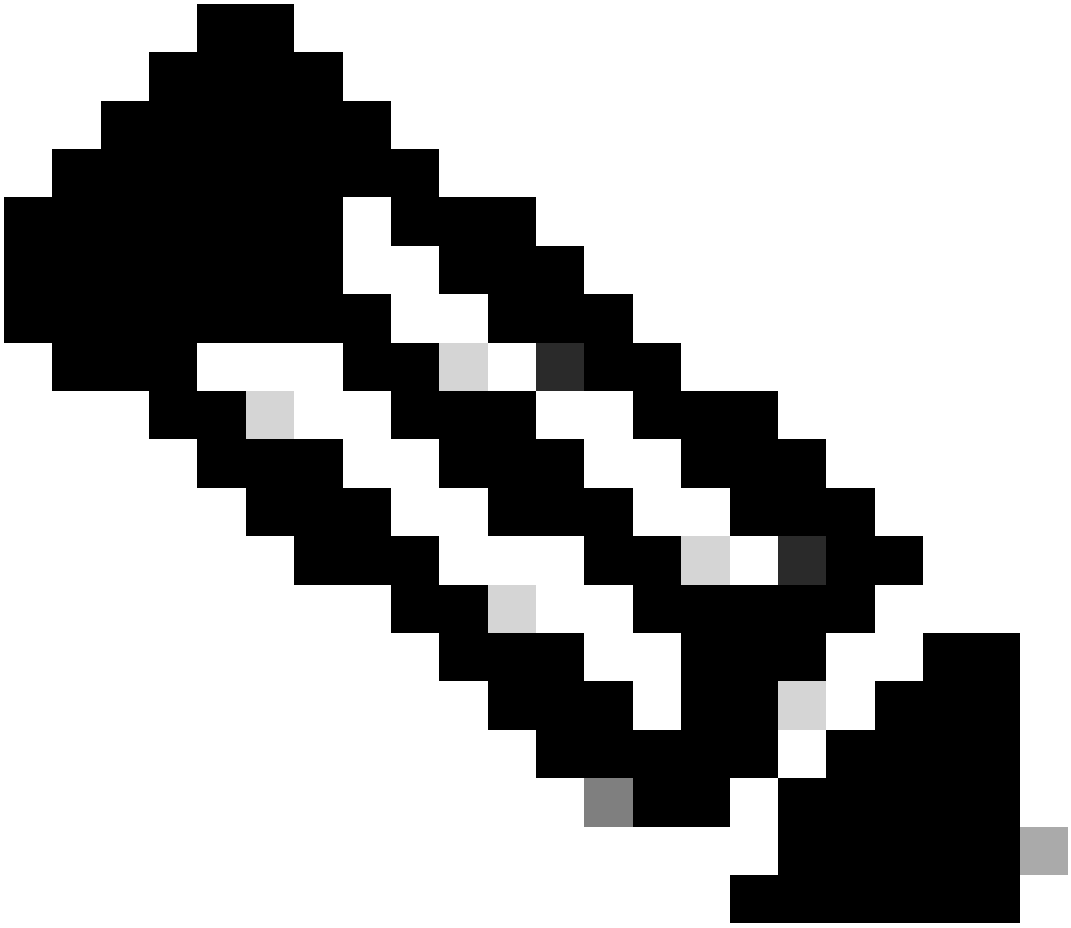
100）ルータの物理インターフェイスを設定します。

プライマリルータ：

```
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-HSRP
```

セカンダリルータ：

```
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
```



注：両方のルータが正常に起動して実行している場合でも、デフォルトプライマリルータをアクティブピアとするために、プライオリティがより高く設定されていることを確認します。この例では、プライマリにはプライオリティ105が設定されていますが、セカンダリルータにはプライオリティ100（HSRPのデフォルト）が設定されています。

IKEv2プロポーザルおよびポリシーの設定

選択した暗号化、ハッシュ、およびDHグループを使用してIKEv2プロポーザルを設定し、IKEv2ポリシーにマッピングします。

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

```
crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

キーリングの設定

ピアの認証に使用される事前共有キーを保存するようにキーリングを設定します。

```
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
```

IKEv2プロファイルの設定

IKEv2プロファイルを設定し、キーリングを接続します。ローカルアドレスをHSRPに使用されている仮想IPアドレスに設定し、リモートアドレスをルータのインターネット側インターフェイスのIPとして設定します。

```
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
```

IPSec トランスフォーム セットを設定します

IPSecトランスフォームセットを使用して、暗号化とハッシュのフェーズ2パラメータを設定します。

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

IPSecプロファイルの設定

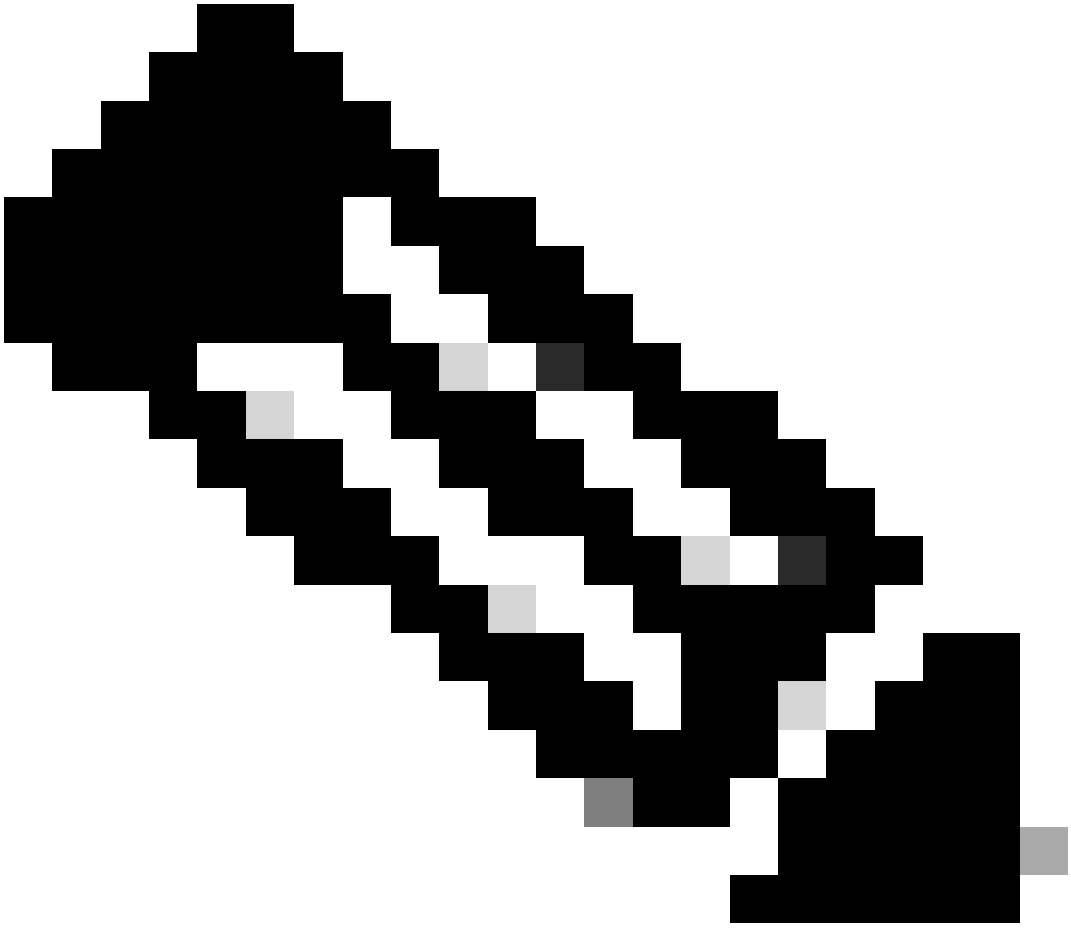
IKEv2プロファイルとIPsecトランスフォームセットをマッピングするようにIPsecプロファイルを設定します。IPsecプロファイルがトンネルインターフェイスに適用されます。

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

仮想トンネルインターフェイスの設定

仮想トンネルインターフェイスを設定して、トンネルの送信元と宛先を指定します。これらのIPは、トンネル上のトラフィックの暗号化に使用されます。次に示すように、IPsecプロファイルがこのインターフェイスにも適用されていることを確認します。

```
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
```



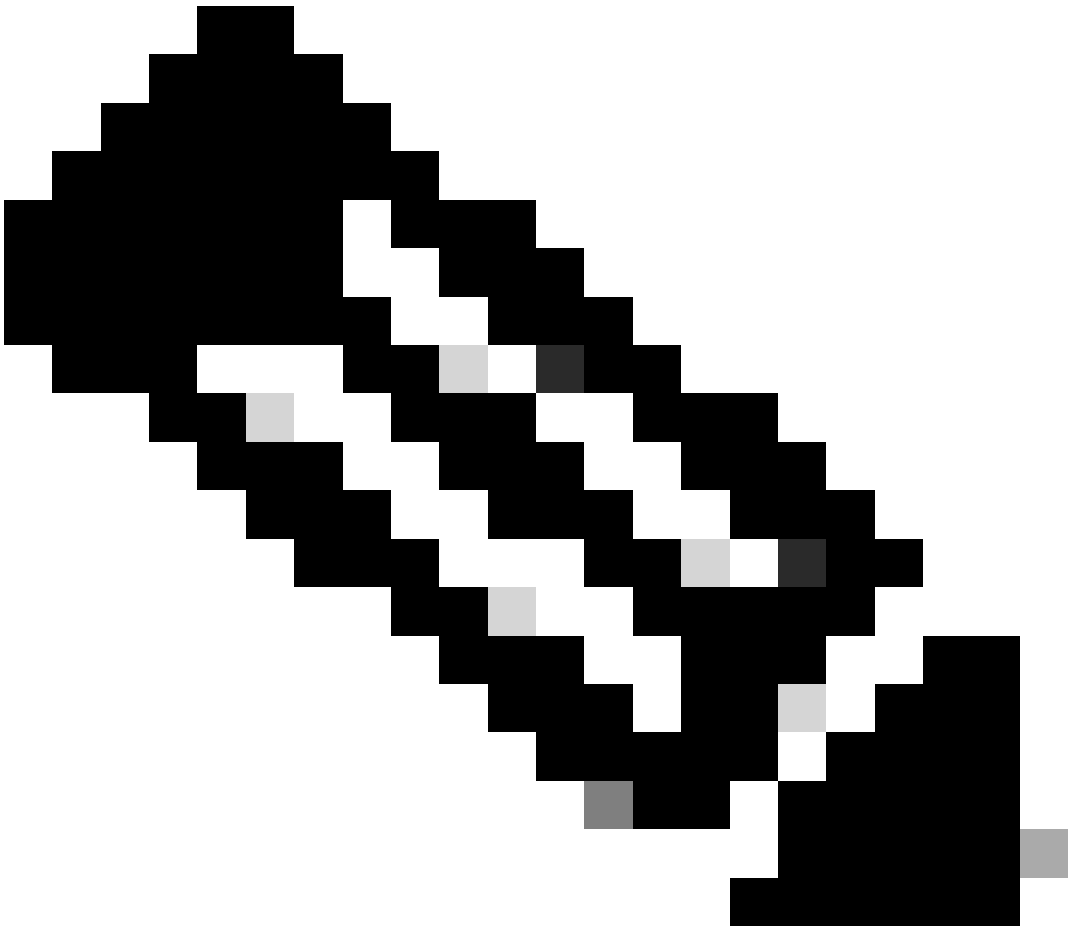
注:HSRPに使用される仮想IPをトンネル送信元として指定する必要があります。物理インターフェイス（このシナリオではGigabitEthernet1）を使用すると、トンネルネゴシエーションが失敗します。

ダイナミックルーティングとスタティックルーティングの設定

要件とネットワーク設計に応じて、ダイナミックルーティングプロトコルやスタティックルートを使用してルーティングを設定する必要があります。この例では、EIGRPとスタティックルートの組み合わせを使用して、サイト間トンネル上のオーバーレイデータトラフィックのアンダーレイ通信とフローを確立します。

```
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
```



注：トンネルインターフェイスサブネット(このシナリオでは10.10.10.0/24)がアドバタイズされていることを確認します。

ピアルータの設定

IKEv2プロポーザルおよびポリシーの設定

選択した暗号化、ハッシュ、およびDHグループを使用してIKEv2プロポーザルを設定し、IKEv2ポリシーにマッピングします。

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

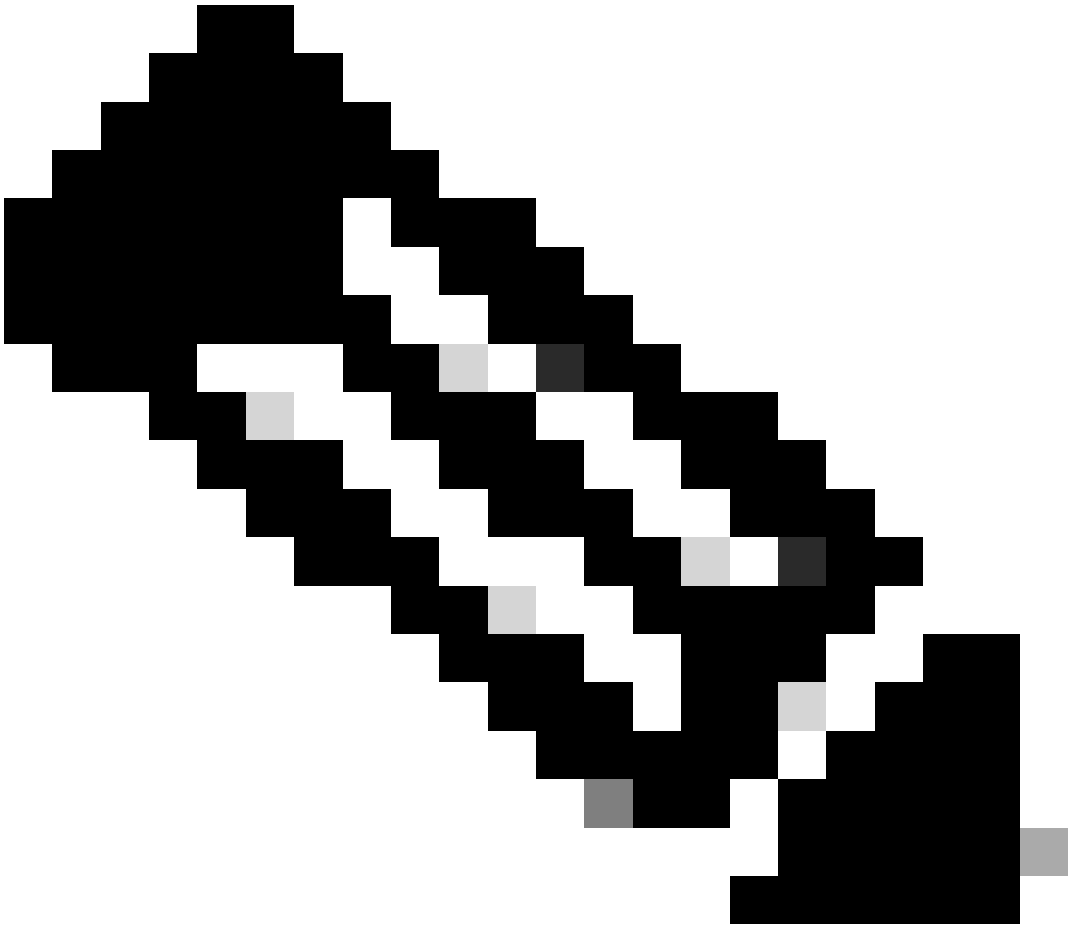
```
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

キーリングの設定

ピアの認証に使用される事前共有キーを保存するようにキーリングを設定します。

```
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
```



注：ここで使用されるピアIPアドレスは、ピアのHSRP設定で設定される仮想IPアドレスです。プライマリ/セカンダリピアの物理インターフェイスIPのキーリングを設定していないことを確認します。

IKEv2プロファイルの設定

IKEv2プロファイルを設定し、キーリングを接続します。ローカルアドレスをルータのインターネット側インターフェイスのIPとして設定し、リモートアドレスをプライマリ/セカンダリピアでHSRPに使用される仮想IPアドレスに設定します。

```
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
```

IPSec トランスフォーム セットを設定します

IPSecトランスフォームセットを使用して、暗号化とハッシュのフェーズ2パラメータを設定します。

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

IPSecプロファイルの設定

IKEv2プロファイルとIPsecトランスフォームセットをマッピングするようにIPsecプロファイルを設定します。IPsecプロファイルがトンネルインターフェイスに適用されます。

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

仮想トンネルインターフェイスの設定

仮想トンネルインターフェイスを設定して、トンネルの送信元と宛先を指定します。トンネルの宛先は、プライマリ/セカンダリピアでHSRPに使用される仮想IPとして設定する必要があります。次に示すように、IPsecプロファイルがこのインターフェイスにも適用されていることを確認します。

```
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
```

ダイナミックルーティングとスタティックルーティングの設定

他のエンドポイントと同様に、ダイナミックルーティングプロトコルまたはスタティックルートを使用して、必要なルートを設定します。

```
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
```

確認

予想される動作を理解するために、次の3つのシナリオを示します。

シナリオ 1.プライマリとセカンダリの両方のルータがアクティブ

プライマリルータは高いプライオリティで設定されているため、このルータではIPSecトンネルがネゴシエートされ、確立されます。2台のルータの状態を確認するには、show standbyコマンドを使用できます。

<#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
```

トンネルに対するフェーズ1(IKEv2)とフェーズ2(IPsec)のセキュリティアソシエーションを確認するには、show crypto ikev2 saコマンドとshow crypto ipsec saコマンドを使用します。

```
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:
```

シナリオ 2.プライマリルータが非アクティブで、セカンダリルータがアクティブ

プライマリルータが停止またはダウンした場合、セカンダリルータがアクティブルータになり、サイト間トンネルはこのルータとネゴシエートされます。

セカンダリルータのHSRP状態は、再度show standby コマンドを使用して確認できます。

<#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
```

さらに、この中断が発生すると、次のログも確認できます。これらのログは、セカンダリルータが現在アクティブであり、トンネルが確立されていることも示しています。

```
*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
```

フェーズ1とフェーズ2のセキュリティアソシエーションを確認するには、次に示すように show crypto ikev2 sa と show crypto ipsec sa を再度使用します。

```
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:
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:
```

シナリオ 3.プライマリルータが復旧し、セカンダリルータがスタンバイになります。

プライマリルータのプライオリティの方が高く設定されているため、プライマリルータが復旧してダウンしなくなった後は、再びアクティブルータになり、セカンダリルータはスタンバイモードになります。

このシナリオでは、この移行が発生したときに、プライマリルータとセカンダリルータでこれらの口グが表示されます。

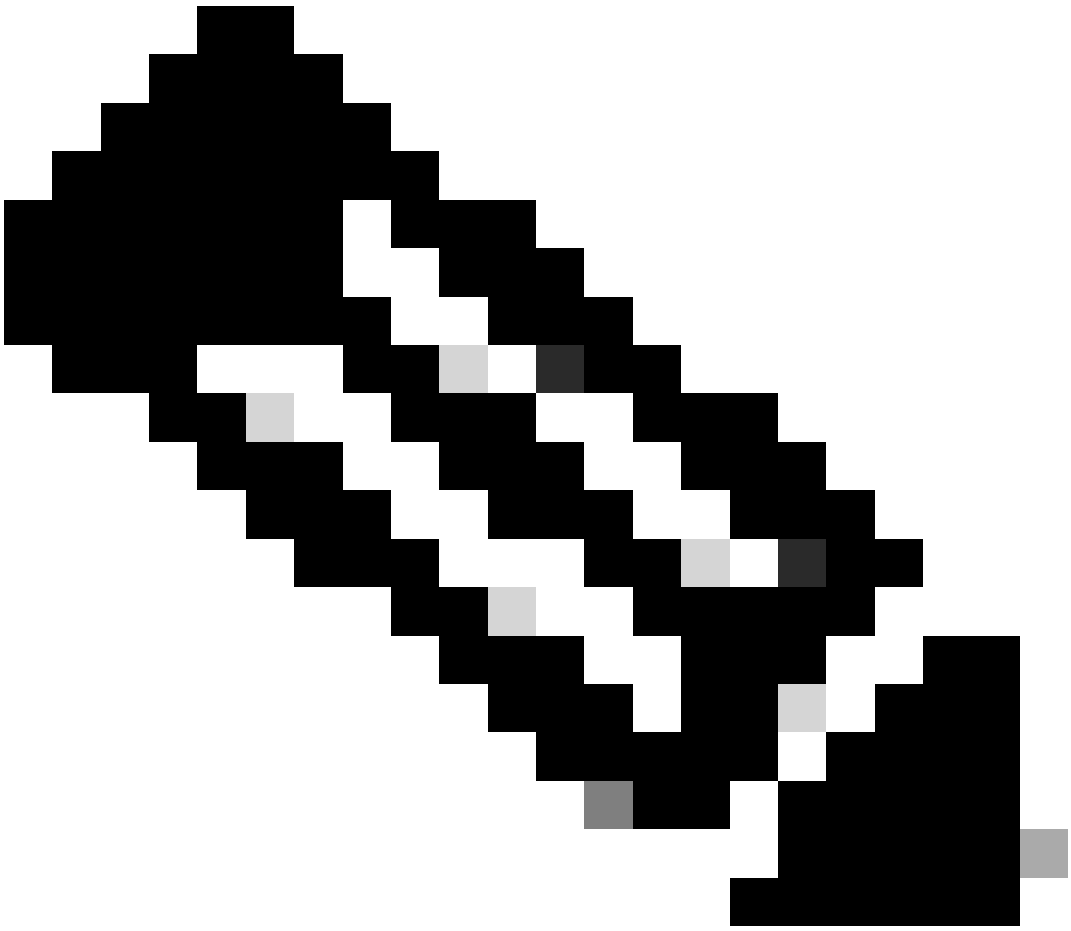
プライマリルータでは、次の口グが表示されます。

```
*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
```

セカンダリルータで、次のログが表示され、セカンダリルータが再びスタンバイルータになったことが示されます。

```
*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
*Jul 18 11:47:57.806: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Speak -> Standby
```

フェーズ1とフェーズ2のセキュリティアソシエーションのステータスを確認するには、show crypto ikev2 saと**show crypto ipsec sa**を使用して同じことを確認します。



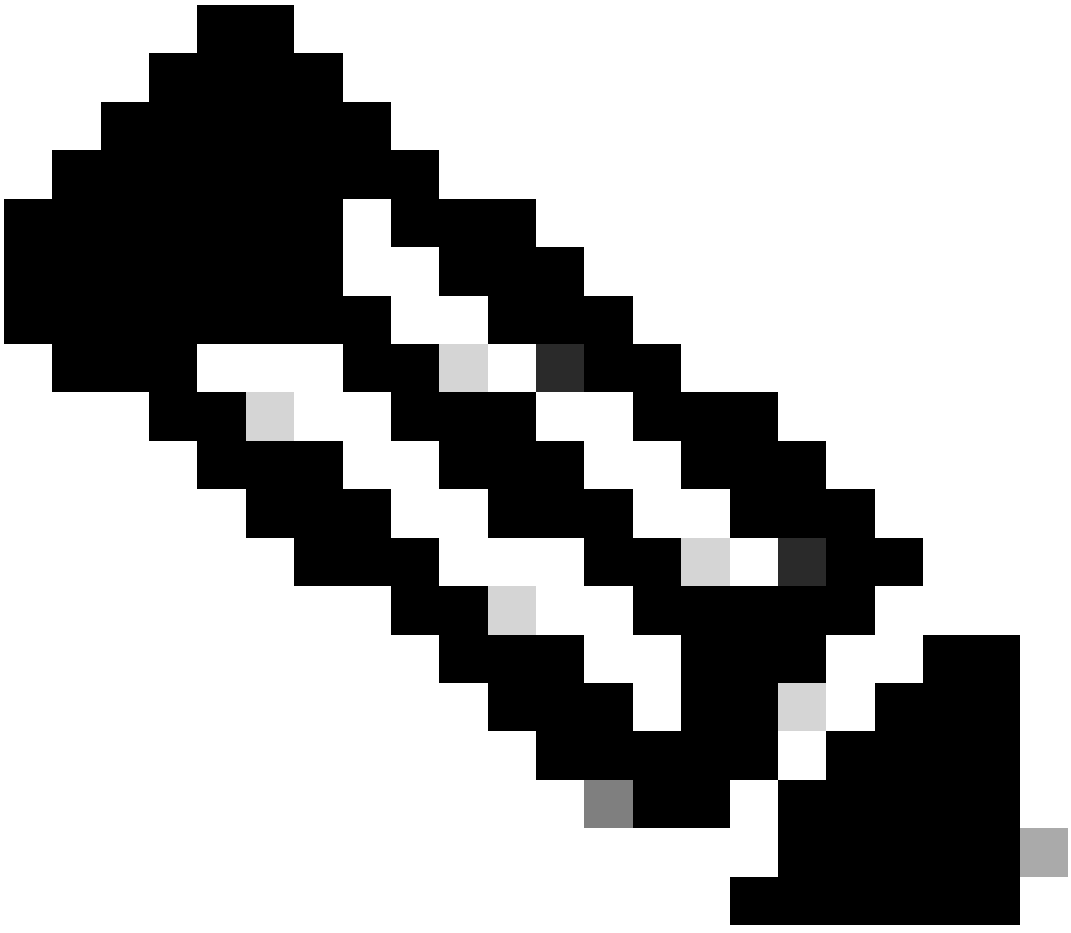
注：稼働しているルータに複数のトンネルが設定されている場合は、show crypto session remote X.X.X.Xコマンドとshow crypto ipsec sa peer X.X.X.Xコマンドを使用して、トンネルのフェーズ1とフェーズ2のステータスを確認できます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次のデバッグは、IKEv2トンネルのトラブルシューティングのために有効にできます。

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



注：トンネルを1つだけトラブルシューティングする場合（デバイスが実稼働中の場合など）は、次のコマンドを使用して条件付きデバッグを有効にする必要があります。 debug crypto condition peer ipv4 X.X.X.X.

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。