在Cisco路由器上为基于IKEv2路由的隧道配置HSRP的IPsec冗余

目录

简介

本文档介绍如何使用HSRP为Cisco路由器上的IKEv2基于路由的隧道配置IPsec冗余。

先决条件

要求

Cisco 建议您了解以下主题：

- 站点到站点 VPN
- 热备份路由器协议[HSRP]
- IPsec和IKEv2的基础知识

使用的组件

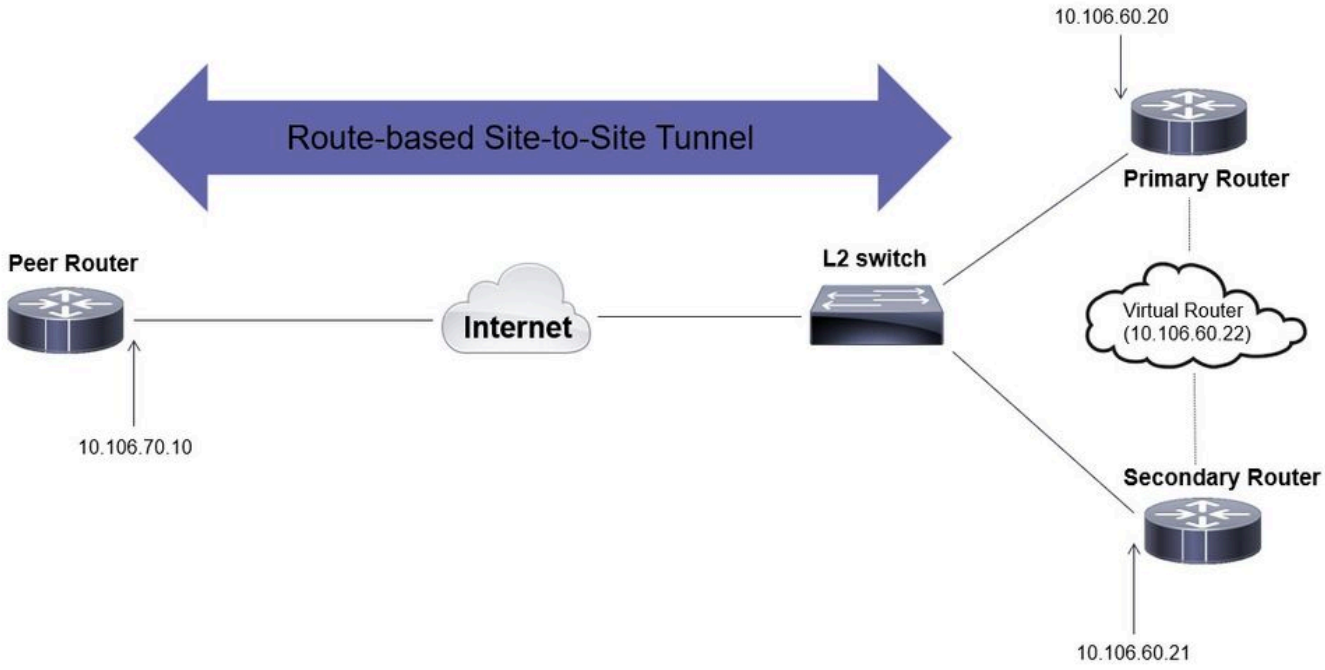
本文档中的信息基于以下软件和硬件版本：

- 运行IOS XE软件（版本17.03.08a）的思科CSR1000v路由器
- 运行Cisco IOS软件15.2版的第2层交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



主要/辅助路由器配置

使用HSRP配置物理接口

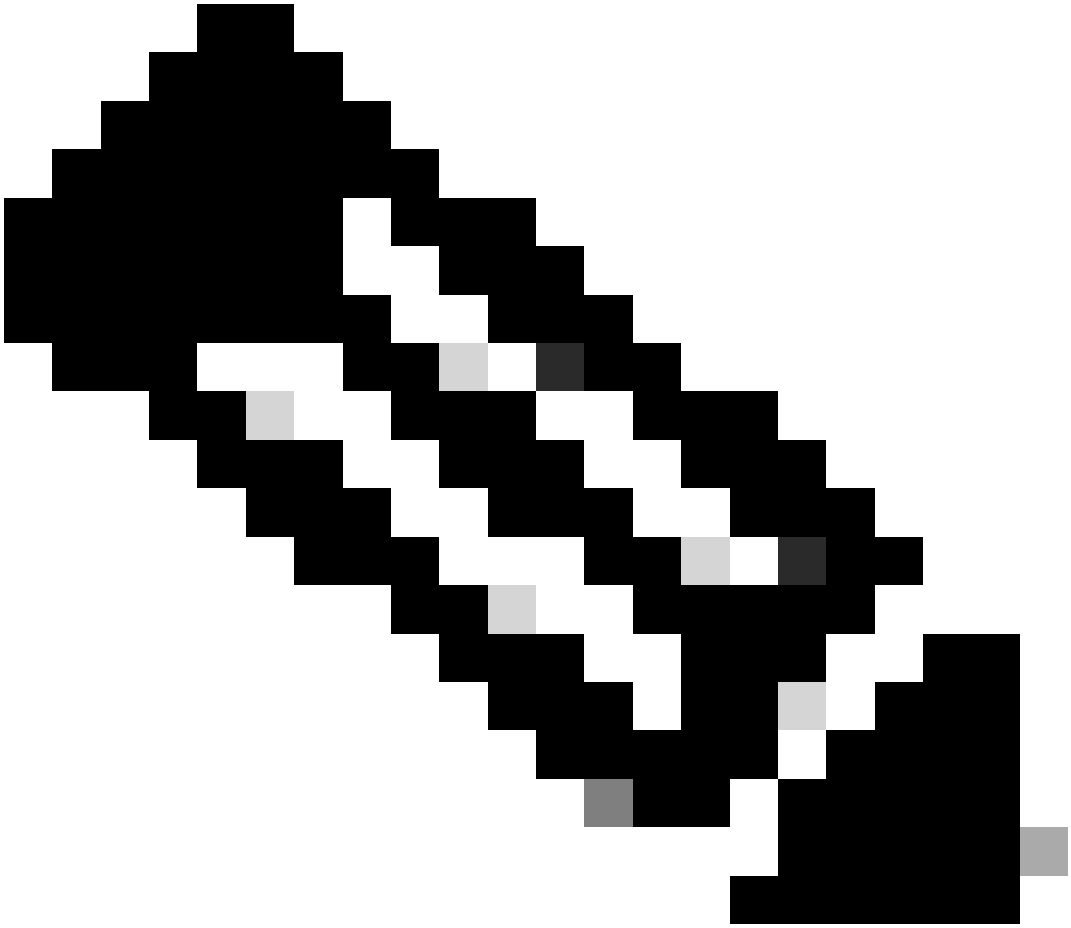
配置主要路由器（优先级较高）和辅助路由器（默认优先级为100）的物理接口：

主路由器：

```
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
```

辅助路由器：

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



注意：确保为默认主路由器配置了更高的优先级，以使其成为活动对等体（即使两台路由器都已启动并运行且没有任何问题）。在本示例中，主路由器的优先级配置为105，而辅助路由器的优先级配置为100（这是HSRP的默认设置）。

配置IKEv2建议和策略

使用您选择的加密、散列和DH组配置IKEv2提议，并将其映射到IKEv2策略。

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

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

配置密钥环

配置密钥环以存储将用于验证对等体的预共享密钥。

```
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
```

配置IKEv2配置文件

配置IKEv2配置文件并附加密钥环。将本地地址设置为用于HSRP的虚拟IP地址，并将远程地址设置为路由器面向互联网接口的IP地址。

```
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
```

配置IPsec转换集

使用IPsec转换集配置加密和散列的第2阶段参数。

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

配置IPSec配置文件

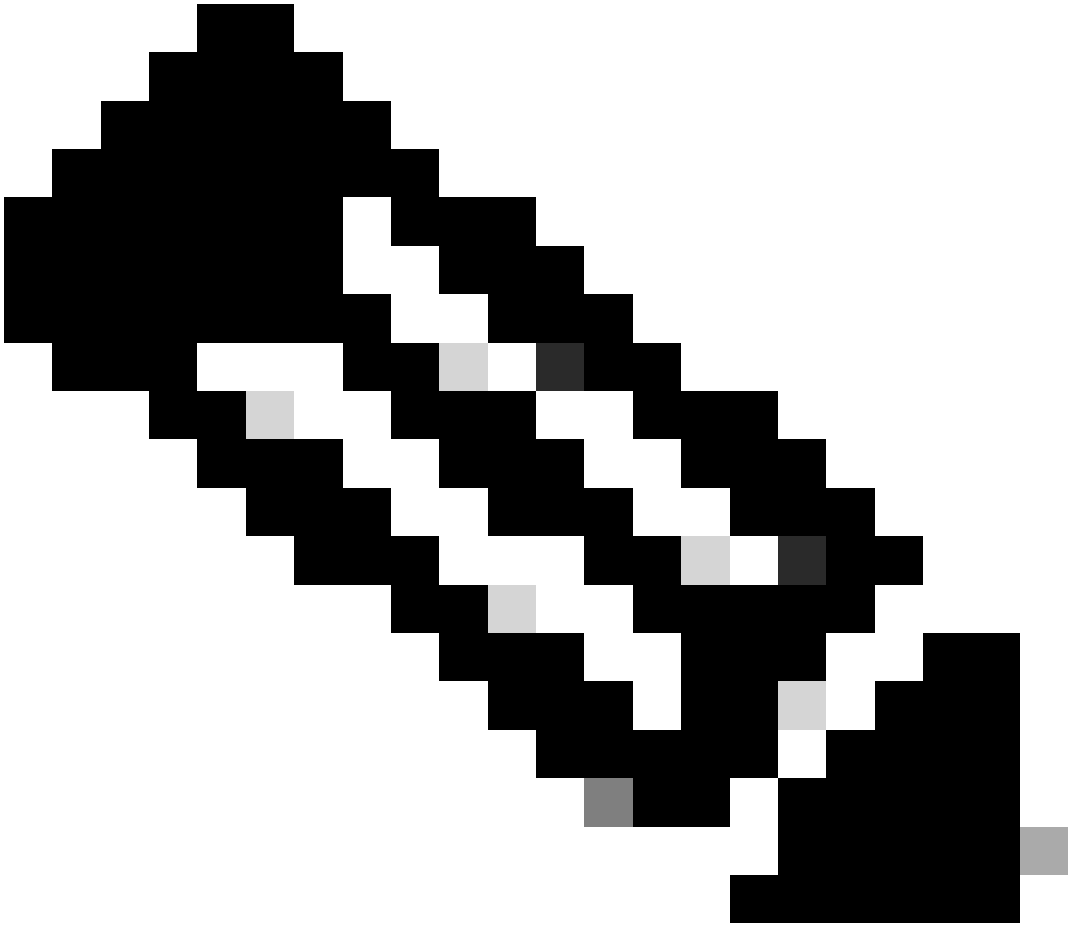
配置IPsec配置文件以映射IKEv2配置文件和IPsec转换集。IPsec配置文件将应用于隧道接口。

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

配置虚拟隧道接口

配置虚拟隧道接口以指定隧道源和目标。这些IP将用于加密通过隧道的流量。确保IPsec配置文件也应用于此接口，如下所示。

```
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
```



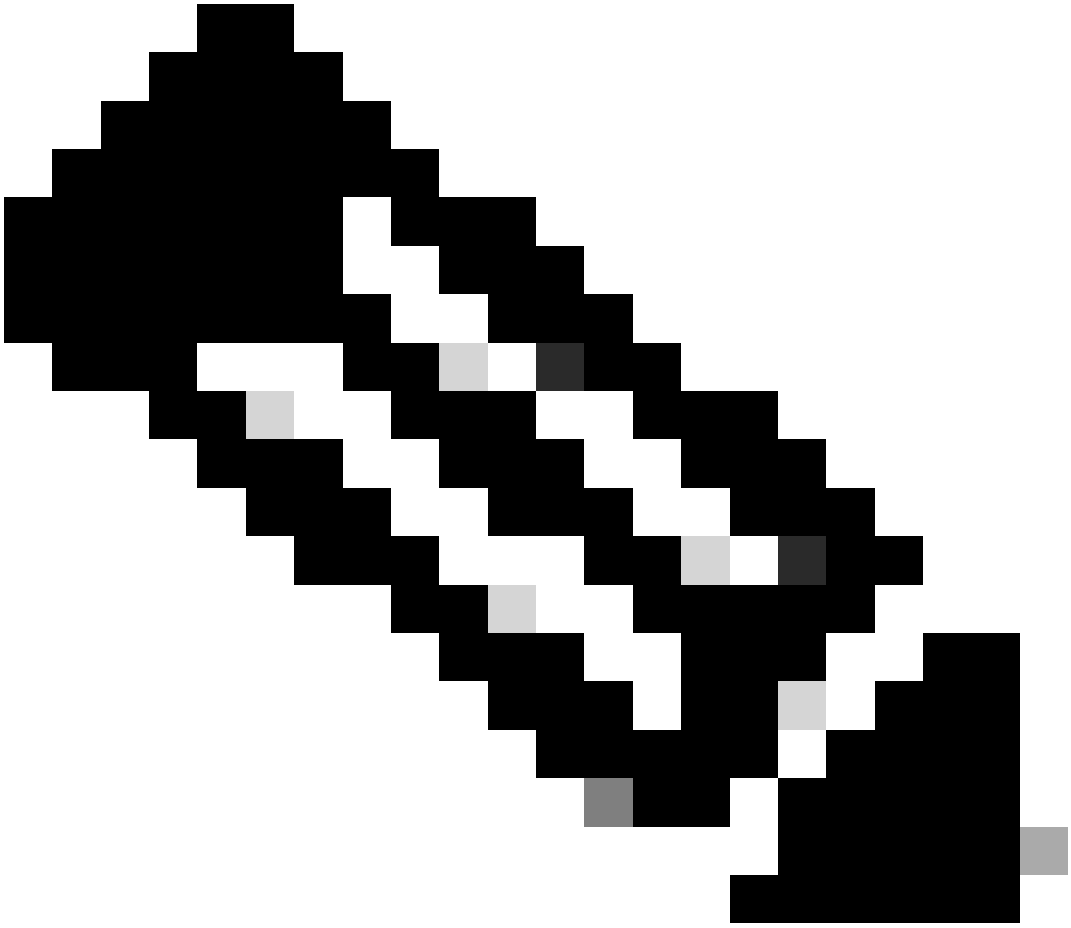
注意：您需要指定用于HSRP的虚拟IP作为隧道源。使用物理接口（在本场景中为GigabitEthernet1）将导致隧道协商失败。

配置动态和/或静态路由

您必须根据要求和网络设计使用动态路由协议和/或静态路由配置路由。在本示例中，结合使用EIGRP和静态路由来建立底层通信以及通过站点到站点隧道的重叠数据流量流。

```
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
```



注意：确保通告隧道接口子网(在此场景中为10.10.10.0/24)。

对等路由器配置

配置IKEv2建议和策略

使用您选择的加密、散列和DH组配置IKEv2提议，并将其映射到IKEv2策略。

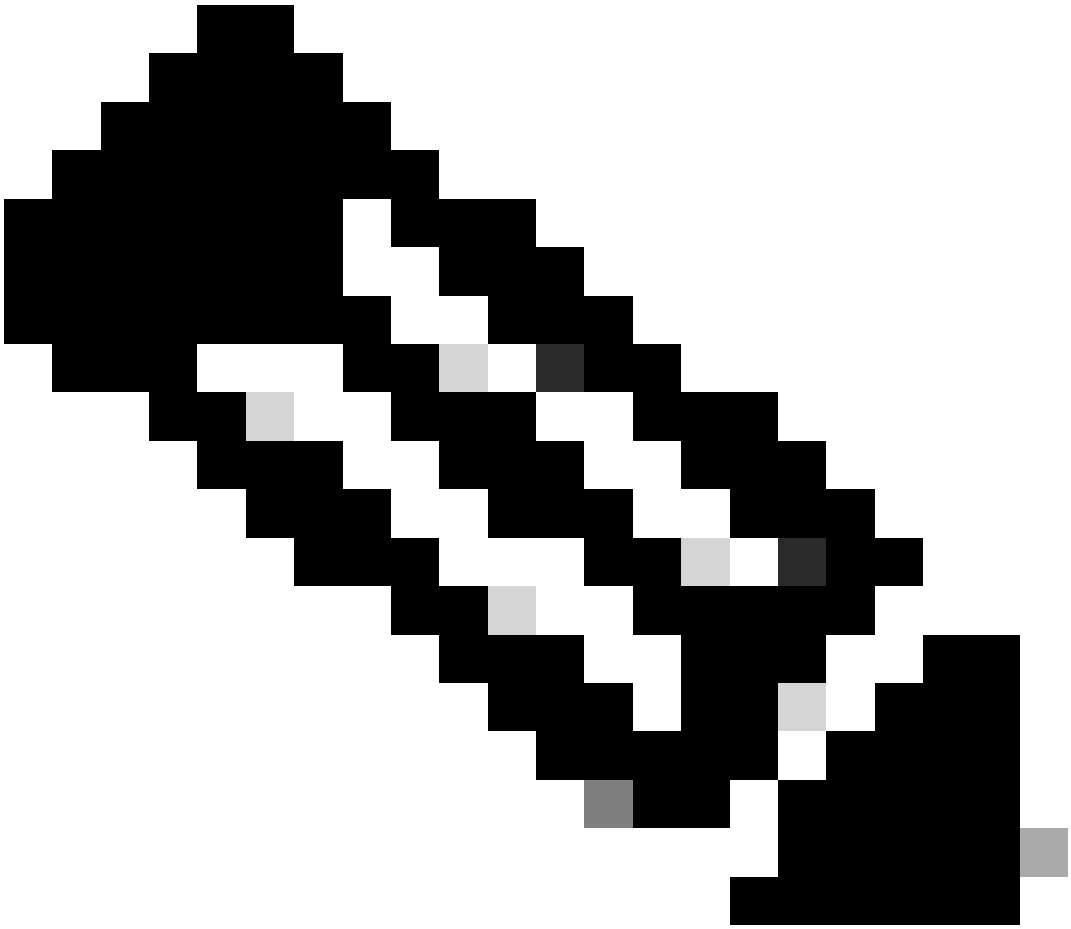
```
crypto ikev2 proposal prop-1
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2_POL
 proposal prop-1
```

配置密钥环

配置密钥环以存储将用于验证对等体的预共享密钥。

```
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
```



注意：此处使用的对等体IP地址是在对等体的HSRP配置中配置的虚拟IP地址。确保没有为主要/辅助对等体的物理接口IP配置密钥环。

配置IKEv2配置文件

配置IKEv2配置文件并附加密钥环。将本地地址设置为路由器面向互联网接口的IP地址，并将远程地址设置为主/辅助对等体上用于HSRP的虚拟IP地址。

```
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
```

配置IPsec转换集

使用IPsec转换集配置加密和散列的第2阶段参数。

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

配置IPSec配置文件

配置IPsec配置文件以映射IKEv2配置文件和IPsec转换集。IPsec配置文件将应用于隧道接口。

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

配置虚拟隧道接口

配置虚拟隧道接口以指定隧道源和目标。必须将隧道目标设置为主/辅助对等体上用于HSRP的虚拟IP。确保IPsec配置文件也应用于此接口，如下所示。

```
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
```

配置动态和/或静态路由

使用动态路由协议或静态路由配置所需的路由，就像您为其他终端配置路由一样。

```
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
```

验证

为了理解预期行为，提供了以下三个场景。

场景 1.主路由器和辅助路由器都处于活动状态

由于主路由器配置了更高的优先级，因此会在此路由器上协商并建立IPSec隧道。要检验两台路由器的状态，您可以使用show standby命令。

<#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
```

若要检验隧道的第1阶段(IKEv2)和第2阶段(IPsec)的安全关联，您可以使用show crypto ikev2 sa和show crypto ipsec sa命令。

```
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:
```

场景 2：主路由器处于非活动状态，辅助路由器处于活动状态

在主路由器出现故障或关闭的情况下，辅助路由器将成为活动路由器，并且站点到站点隧道将与此路由器协商。

可以使用show standby 命令再次验证辅助路由器的HSRP状态。

<#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

此外，当此中断发生时，您还将看到以下日志。这些日志还显示辅助路由器现在处于活动状态，并且已建立隧道。

*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

要检查第1阶段和第2阶段的安全关联，可以再次使用show crypto ikev2 sa和show crypto ipsec sa，如下所示。

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:

场景 3：主路由器恢复运行，辅助路由器进入备用状态

一旦主路由器恢复并且不再关闭，它将再次成为活动路由器，因为它配置了更高优先级，并且辅助路由器进入备用模式。

在此场景中，发生此转换时，您会在主路由器和辅助路由器上看到这些日志。

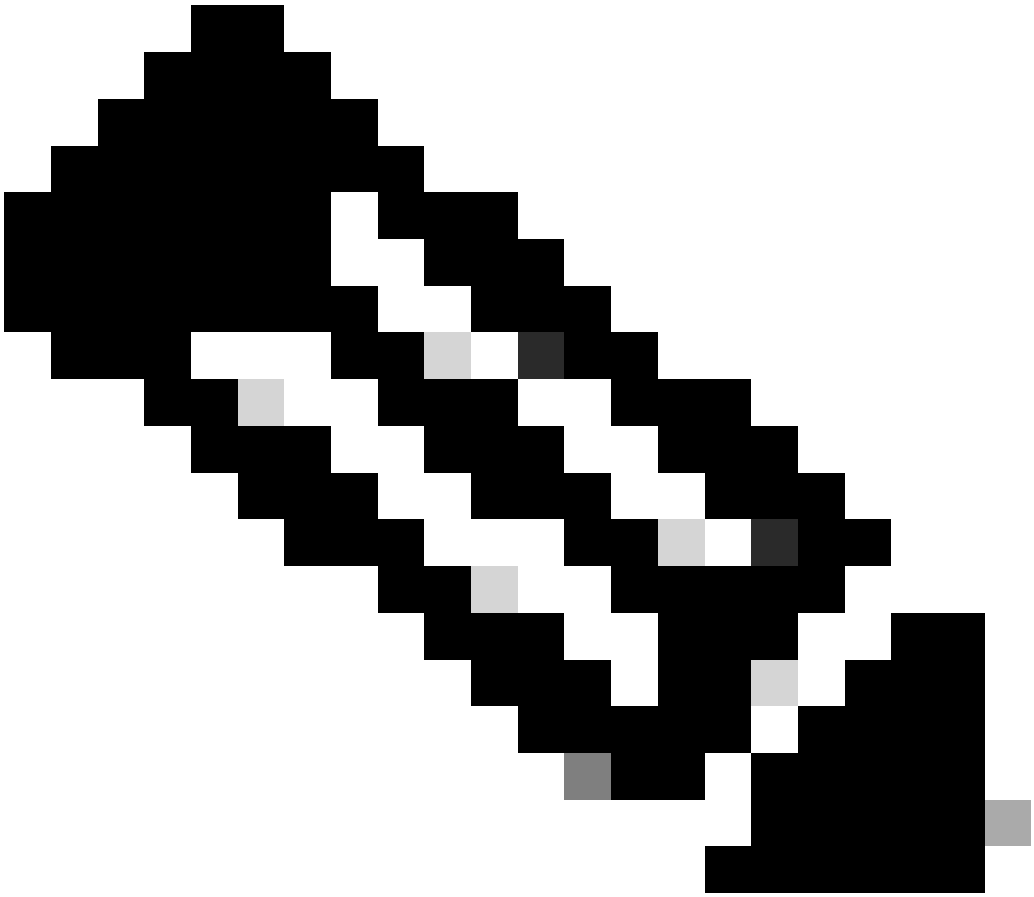
在主路由器上，会显示以下日志：

*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

在辅助路由器上，您会看到以下日志，表明辅助路由器再次成为备用路由器：

*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

要检查第1阶段和第2阶段安全关联的状态，您可以使用show crypto ikev2 sa和**show crypto ipsec sa**进行验证。



注意：如果在启动并运行的路由器上配置了多个隧道，则可以使用show crypto session remote X.X.X.X和show crypto ipsec sa peer X.X.X.X命令检查隧道第1阶段和第2阶段的状态。

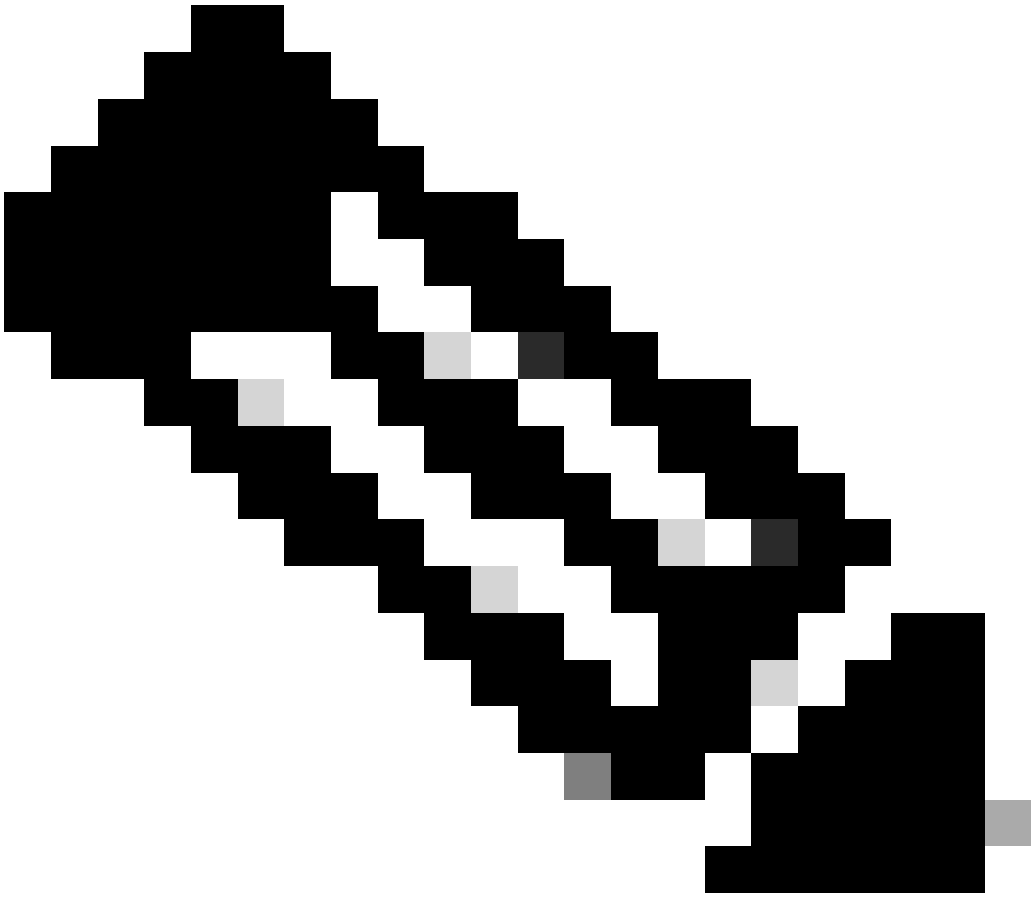
故障排除

本部分提供了可用于对配置进行故障排除的信息。

可以启用这些调试来排除IKEv2隧道故障。

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

debug crypto ipsec message



注意：如果您希望仅对一个隧道进行故障排除（如果设备处于生产状态则必须如此），则必须使用命令启用条件调试，debug crypto condition peer ipv4 X.X.X.X.

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。