

使用 GRE 通道配置带有 EIGRP 和 IPX 的 IPSec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[隧道开启时的 show 命令输出](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

普通的 IPSec 配置不能传输路由协议，例如 Enhanced Interior Gateway Routing Protocol (EIGRP) 和 Open Shortest Path First (OSPF)，也不能传输非 IP 数据流，例如互联网分组交换 (IPX)、AppleTalk 等。本文说明了如何使用路由协议和 IPSec，在不同网络之间路由非 IP 数据流。此技术使用通用路由封装 (GRE) 作为实现此功能的方法。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在应用加密映射之前，请确保隧道正常工作。
- 加密访问列表需要将 GRE 作为允许的协议：`access-list 101 permit gre host x.x.x.x host y.y.y.y`
`x.x.x.x = <tunnel_source> y.y.y.y = <tunnel_destination>`
- 使用回环 IP 地址识别互联网密钥交换 (IKE) 对等体及隧道源和隧道目的地，以改进其可用性。
- 有关可能的最大传输单元 (MTU) 问题的讨论，请参阅 [在 Windows 和 Sun 系统上调整 IP MTU、TCP MSS 和 PMTUD](#)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 软件版本 12.1.8 和 12.2.1

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“Cisco技术提示规则”。

配置

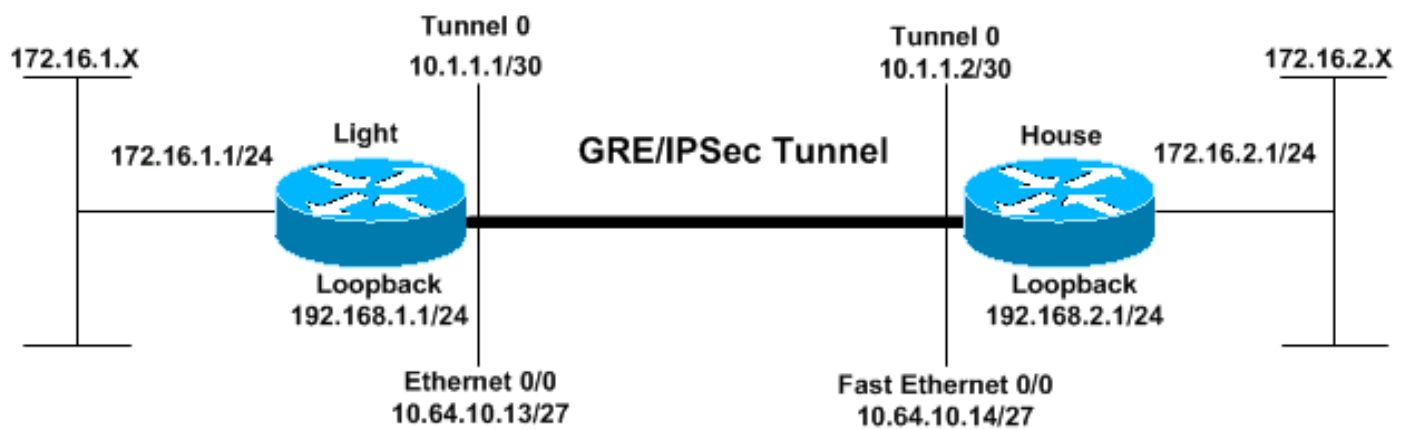
本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用[命令查找工具](#)([仅注册客户](#))。

IOS 配置说明：使用 Cisco IOS 软件版本 12.2(13)T 及更高版本代码（编号更高的 T 训练代码、Cisco IOS 软件版本 12.3 及更高版本代码），只需将配置的 IPSEC“加密映射”应用到物理接口，而不再需要将其应用到 GRE 隧道接口。使用 Cisco IOS 软件版本 12.2(13)T 及更高版本的代码仍能正常工作时，请在物理和隧道接口上应用“加密映射”。不过，强烈建议仅在物理接口上应用它。

网络图

本文档使用此图所示的网络设置。



配置

- [灯](#)
- [豪斯](#)

```

灯
Current configuration:
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Light

```

```
!  
logging rate-limit console 10 except errors  
!  
ip subnet-zero  
!  
!  
no ip finger  
!  
no ip dhcp-client network-discovery  
ipx routing 00e0.b06a.40fc  
!  
!--- IKE policies. crypto isakmp policy 25  
hash md5  
authentication pre-share  
crypto isakmp key cisco123 address 192.168.2.1  
!  
!--- IPsec policies. crypto ipsec transform-set WWW esp-  
des esp-md5-hmac  
mode transport  
!  
crypto map GRE local-address Loopback0  
crypto map GRE 50 ipsec-isakmp  
set peer 192.168.2.1  
set transform-set WWW  
!--- What to encrypt? match address 101  
!  
call rsvp-sync  
!  
fax interface-type modem  
mta receive maximum-recipients 0  
!  
interface Loopback0  
ip address 192.168.1.1 255.255.255.0  
!  
interface Tunnel0  
ip address 10.1.1.1 255.255.255.252  
ip mtu 1440  
ipx network CC  
tunnel source Loopback0  
tunnel destination 192.168.2.1  
crypto map GRE  
!  
interface FastEthernet0/0  
ip address 10.64.10.13 255.255.255.224  
no ip route-cache  
no ip mroute-cache  
duplex auto  
speed auto  
crypto map GRE  
!  
interface FastEthernet0/1  
ip address 172.16.1.1 255.255.255.0  
duplex auto  
speed auto  
ipx network AA  
!  
router eigrp 10  
network 10.1.1.0 0.0.0.3  
network 172.16.1.0 0.0.0.255  
network 192.168.1.0  
no auto-summary  
no eigrp log-neighbor-changes  
!  
ip kerberos source-interface any
```

```
ip classless
ip route 192.168.2.0 255.255.255.0 10.64.10.14
ip http server
!
!--- What to encrypt? access-list 101 permit gre host
192.168.1.1 host 192.168.2.1
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

Light#!
```

豪斯

```
Current configuration:
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname House
!
ip subnet-zero
!
ipx routing 00e0.b06a.4114
!
!--- IKE policies. crypto isakmp policy 25
hash md5
authentication pre-share
crypto isakmp key cisco123 address 192.168.1.1
!
!--- IPSec policies. crypto ipsec transform-set WWW esp-
des esp-md5-hmac
mode transport
!
crypto map GRE local-address Loopback0
crypto map GRE 50 ipsec-isakmp
set peer 192.168.1.1
set transform-set WWW
!--- What to encrypt? match address 101
!
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface Tunnel0
ip address 10.1.1.2 255.255.255.252
ip mtu 1440
ipx network CC
tunnel source Loopback0
tunnel destination 192.168.1.1
crypto map GRE
!
interface FastEthernet0/0
ip address 10.64.10.14 255.255.255.224
no ip route-cache
```

```

no ip mroute-cache
duplex auto
speed auto
crypto map GRE
!
interface FastEthernet0/1
ip address 172.16.2.1 255.255.255.0
duplex auto
speed auto
ipx network BB
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 10
network 10.1.1.0 0.0.0.3
network 172.16.2.0 0.0.0.255
network 192.168.2.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.64.10.13
ip http server
!--- What to encrypt? access-list 101 permit gre host
192.168.2.1 host 192.168.1.1
!
line con 0
line aux 0
line vty 0 4
login
!
end

House#

```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

[命令输出解释程序工具 \(仅限注册用户 \) 支持某些 show 命令](#)，使用此工具可以查看对 show 命令输出的分析。

- **show crypto engine connections active** - 显示 IPsec 对等体之间的加密和解密数据包。
- **show crypto isakmp sa** - 显示第 1 阶段的安全连接。
- **show crypto ipsec sa** - 显示第 2 阶段的安全连接。
- **show ipx route [network] [default] [detailed]** - 显示 IPX 路由表的内容。

隧道开启时的 show 命令输出

```
Light#show ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

```

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
172.16.0.0/24 is subnetted, 2 subnets
C    172.16.1.0 is directly connected, FastEthernet0/1
D    172.16.2.0 [90/297246976] via 10.1.1.2, 00:00:31, Tunnel0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Tunnel0
C    10.64.10.0/27 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Loopback0
S    192.168.2.0/24 [1/0] via 10.64.10.14
```

Light#**ping**

```
Protocol [ip]:
Target IP address: 172.16.2.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Light#
```

House#**show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.16.0.0/24 is subnetted, 2 subnets
D    172.16.1.0 [90/297246976] via 10.1.1.1, 00:00:36, Tunnel0
C    172.16.2.0 is directly connected, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Tunnel0
C    10.64.10.0/27 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 10.64.10.13
C    192.168.2.0/24 is directly connected, Loopback0
```

House#**ping**

```
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.2.1
Type of service [0]:
Set DF bit in IP header? [no]:
```

Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Light#**show ipx route**

Codes: C - Connected primary network, c - Connected secondary network
S - Static, F - Floating static, L - Local (internal), W - IPXWAN
R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
s - seconds, u - uses, U - Per-user static

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C AA (NOVELL-ETHER), Fa0/1
C CC (TUNNEL), Tu0
R BB [151/01] via CC.00e0.b06a.4114, 17s, Tu0

House#**show ipx route**

Codes: C - Connected primary network, c - Connected secondary network
S - Static, F - Floating static, L - Local (internal), W - IPXWAN
R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
s - seconds, u - uses, U - Per-user static

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C BB (NOVELL-ETHER), Fa0/1
C CC (TUNNEL), Tu0
R AA [151/01] via CC.00e0.b06a.40fc, 59s, Tu0

Light#**ping ipx BB.0004.9af2.8261**

Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to BB.0004.9af2.8261, timeout is 2 second:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

House#**ping ipx AA.0004.9af2.8181**

Type escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to AA.0004.9af2.8181, timeout is 2 second:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Light#**show crypto isa sa**

dst	src	state	conn-id	slot
192.168.2.1	192.168.1.1	QM_IDLE	1	0
192.168.1.1	192.168.2.1	QM_IDLE	2	0

House#**show crypto isa sa**

dst	src	state	conn-id	slot
192.168.1.1	192.168.2.1	QM_IDLE	1	0
192.168.2.1	192.168.1.1	QM_IDLE	2	0

Light#**show crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_MD5+DES_56_CB	0	0
2	<none>	<none>	set	HMAC_MD5+DES_56_CB	0	0
2000	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	0	161
2001	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	161	0
2002	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	0	0
2003	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	0	0
2004	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	0	0
2005	FastEthernet0/0	10.64.10.13	set	HMAC_MD5+DES_56_CB	0	0

House#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_MD5+DES_56_CB	0	0
2	<none>	<none>	set	HMAC_MD5+DES_56_CB	0	0
2000	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	0	159
2001	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	159	0
2002	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	0	0
2003	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	0	0
2004	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	0	0
2005	FastEthernet0/0	10.64.10.14	set	HMAC_MD5+DES_56_CB	0	0

House#show crypto ipsec sa detail

interface: Tunnel0

Crypto map tag: GRE, local addr. 192.168.2.1

local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)

current_peer: 192.168.1.1

PERMIT, flags={origin_is_acl,transport_parent,}

#pkts encaps: 192, #pkts encrypt: 192, #pkts digest 192

#pkts decaps: 190, #pkts decrypt: 190, #pkts verify 190

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#pkts no sa (send) 12, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1

path mtu 1514, media mtu 1514

current outbound spi: 1FA721CA

inbound esp sas:

spi: 0xEE52531(249898289)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4607961/2797)

IV size: 8 bytes

replay detection support: Y

spi: 0xFEE24F3(267265267)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4608000/2826)

IV size: 8 bytes

replay detection support: Y

spi: 0x19240817(421791767)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }
slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2759)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x1FA721CA(531046858)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4607972/2797)
IV size: 8 bytes
replay detection support: Y

spi: 0x12B10EB0(313593520)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2826)
IV size: 8 bytes
replay detection support: Y

spi: 0x1A700242(443548226)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2759)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 192.168.1.1

PERMIT, flags={transport_parent,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
path mtu 1514, media mtu 1514
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

interface: FastEthernet0/0

Crypto map tag: GRE, local addr. 192.168.2.1

local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)

current_peer: 192.168.1.1

PERMIT, flags={origin_is_acl,transport_parent,}

#pkts encaps: 193, #pkts encrypt: 193, #pkts digest 193

#pkts decaps: 192, #pkts decrypt: 192, #pkts verify 192

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0

#pkts no sa (send) 12, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1

path mtu 1514, media mtu 1514

current outbound spi: 1FA721CA

inbound esp sas:

spi: 0xEE52531(249898289)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4607961/2789)

IV size: 8 bytes

replay detection support: Y

spi: 0xFEE24F3(267265267)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2002, flow_id: 3, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4608000/2817)

IV size: 8 bytes

replay detection support: Y

spi: 0x19240817(421791767)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2004, flow_id: 5, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4608000/2750)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x1FA721CA(531046858)

transform: esp-des esp-md5-hmac ,

in use settings ={Transport, }

slot: 0, conn id: 2001, flow_id: 2, crypto map: GRE

sa timing: remaining key lifetime (k/sec): (4607972/2789)

```
IV size: 8 bytes
replay detection support: Y
spi: 0x12B10EB0(313593520)
transform: esp-des esp-md5-hmac ,
in use settings =(Transport, )
slot: 0, conn id: 2003, flow_id: 4, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2817)
IV size: 8 bytes
replay detection support: Y
spi: 0x1A700242(443548226)
transform: esp-des esp-md5-hmac ,
in use settings =(Transport, )
slot: 0, conn id: 2005, flow_id: 6, crypto map: GRE
sa timing: remaining key lifetime (k/sec): (4608000/2750)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

```
local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
current_peer: 192.168.1.1
  PERMIT, flags={transport_parent,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
path mtu 1514, media mtu 1514
current outbound spi: 0
```

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

[命令输出解释程序工具 \(仅限注册用户 \) 支持某些 show 命令](#)，使用此工具可以查看对 show 命令

输出的分析。

注意：在发出debug命令之前，请参阅[有关debug命令的重要信息](#)。

- debug crypto isakmp -显示在阶段1期间的错误。
- debug crypto ipsec -显示在阶段2期间的错误。
- debug crypto engine - 显示来自加密引擎的信息。
- debug ip your routing protocol - 显示与路由协议的路由事务相关的信息。
- clear crypto connection connection-id [slot / rsm / vip] — 终止当前正在进行的加密会话。当会话超时时，加密会话通常会终止。使用 show crypto cisco connections 命令可获得连接 ID 值。
- clear crypto isakmp - 清除第 1 阶段的安全连接。
- clear crypto sa - 清除第 2 阶段的安全连接。

[相关信息](#)

- [IPSec 支持页面](#)
- [IP 安全 \(IPsec\) 加密简介](#)
- [配置 IPSec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [命令查找工具 \(仅限注册用户 \)](#)
- [技术支持 - Cisco Systems](#)