使用GRE隧道配置EIGRP和IPX的IPSec

目錄

簡介

一般IPSec配置無法傳輸路由協定（如增強型內部網關路由協定[EIGRP]和開放最短路徑優先[OSPF]）或非IP流量（如網際網路資料包交換[IPX]、AppleTalk等）。本文檔說明如何使用IPSec使用路由協定在不同網路之間路由和非IP流量。此技術使用通用路由封裝(GRE)作為方法來完成此操作。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 應用密碼編譯對應之前，請確保通道正常運作。
- 加密訪問清單需要將GRE作為允許協定：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>
- 使用環回IP地址標識Internet金鑰交換(IKE)對等體以及隧道源和隧道目標，以提高可用性。
- 有關可能的最大傳輸單元(MTU)問題的討論，請參閱在Windows和Sun系統上調整IP MTU、TCP MSS和PMTUD。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.1.8和12.2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

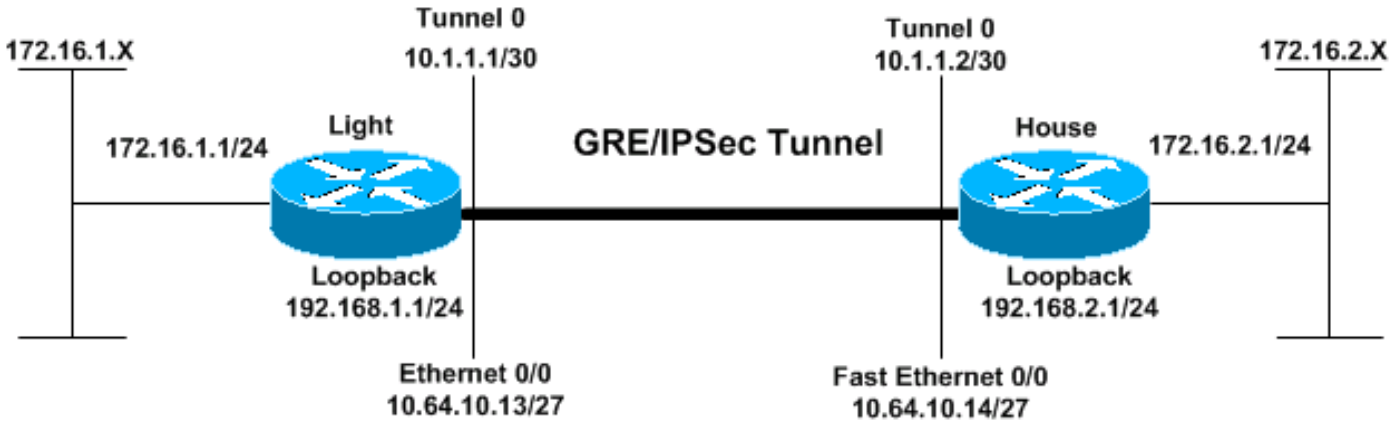
本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

IOS配置說明：對於Cisco IOS軟體版本12.2(13)T和更新版本的代碼（編號更高的T系列代碼、Cisco IOS軟體版本12.3和更新版本的代碼），配置的IPSec「加密對映」只需應用於物理介面。不再需要將其應用於GRE通道介面。使用Cisco IOS軟體版本12.2.(13)T和更新版本代碼時，在實體和通道介面上建立「密碼編譯對應」仍然有效。但是，強烈建議僅將其應用於物理介面。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

- 光
- 房子

光

```
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#!
```

房子

```
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#
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- show crypto engine connections active — 顯示IPSec對等體之間的加密和解密資料包。
- show crypto isakmp sa — 顯示第1階段安全關聯。
- show crypto ipsec sa — 顯示第2階段安全關聯。
- show ipx route [network] [default] [detailed] — 顯示IPX路由表的內容。

show Command Output With Tunnels Up

```
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 (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 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 (recv) 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 (recv) 0, #pkts verify failed: 0
 #pkts invalid identity (recv) 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 (recv) 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 (recv) 0, #pkts verify failed: 0
    #pkts invalid identity (recv) 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 (recv) 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 (recv) 0, #pkts verify failed: 0
 #pkts invalid identity (recv) 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 (recv) 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:
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug指令之前，請參閱有關Debug指令的重要資訊**。**

- debug crypto isakmp — 顯示階段1期間的錯誤。
- debug crypto ipsec — 顯示階段2期間的錯誤。
- debug crypto engine — 顯示來自加密引擎的資訊。
- debug ip *your routing protocol* — 顯示有關路由協定的路由事務的資訊。
- clear crypto connection connection-id *[slot | rsm | vip]* — 終止當前正在執行的加密會話。加密的作業階段通常會在作業階段逾時終止。使用show crypto cisco connections命令獲取connection-id值。
- clear crypto isakmp — 清除第1階段安全關聯。
- clear crypto sa — 清除第2階段安全關聯。

相關資訊

- IPSec支援頁面
- IP安全(IPSec)加密簡介
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定
- 命令查詢工具(僅限註冊客戶)
- 技術支援 - Cisco Systems