Configuring IPSec with EIGRP and IPX Using GRE Tunneling

Document ID: 14136

Contents

Introduction

Normal IPSec configurations cannot transfer routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) or non−IP traffic such as Internetwork Packet Exchange (IPX), AppleTalk, and so forth. This document illustrates how to route between different networks using a routing protocol and non−IP traffic with IPSec. This technique uses generic routing encapsulation (GRE) as the method to accomplish this.

Prerequisites

Requirements

Before you attempt this configuration, ensure that you meet these requirements:

- Make sure the tunnel works before you apply the crypto maps.
- Crypto access list need to have GRE as the protocol to permit: 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>
- Use loopback IP addresses to identify Internet Key Exchange (IKE) peers and tunnel source and tunnel destination to improve availability.
- For a discussion of possible Maximum Transmission Unit (MTU) issues, refer to Adjusting IP MTU, TCP MSS, and PMTUD on Windows and Sun Systems.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS® Software Releases 12.1.8 and 12.2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions .

Configure

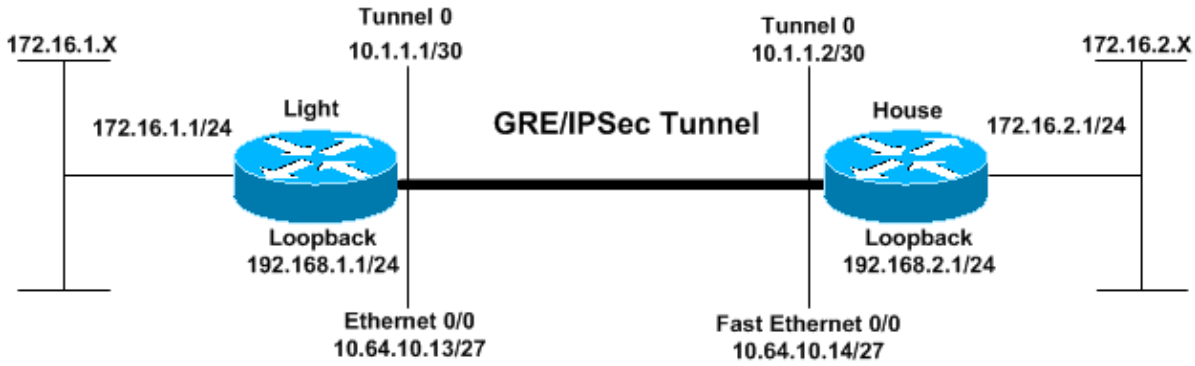
In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

IOS Configuration Note: With Cisco IOS Software Release 12.2(13)T and later codes (higher numbered T−train codes, Cisco IOS Software Release 12.3 and later codes) the configured IPSec "crypto map" only needs to be applied to the physical interface. It is no longer required to be applied on the GRE tunnel interface. Having the "crypto map" on the physical and tunnel interface when you use the Cisco IOS Software Release 12.2.(13)T and later codes still works. However, it is highly recommended to apply it only on the physical interface.

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

- Light
- House

Light

```
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#!
```

House

```
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#
```

Verify

This section provides information you can use to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show crypto engine connections active** Shows encrypted and decrypted packets between IPSec peers.
- **show crypto isakmp sa** Shows Phase 1 security associations.

- **show crypto ipsec sa** Shows Phase 2 security associations.
- **show ipx route [network] [default] [detailed]** Shows the contents of the IPX routing table.

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:
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

- **debug crypto isakmp** Displays errors during Phase 1.
- **debug crypto ipsec** Displays errors during Phase 2.
- **debug crypto engine** Displays information from the crypto engine.
- **debug ip** *your routing protocol* Displays information about your routing protocol's routing transactions.
- **clear crypto connection connection−id** *[slot | rsm | vip]* Terminates an encrypted session currently in progress. Encrypted sessions normally terminate when the session times out. Use the **show crypto cisco connections** command to learn the connection−id value.
- **clear crypto isakmp** Clears the Phase 1 security associations.
- **clear crypto sa** Clears the Phase 2 security associations.

Related Information

- **IPSec Support Page**
- **An Introduction to IP Security (IPSec) Encryption**
- **Configuring IPSec Network Security**
- **Configuring Internet Key Exchange Security Protocol**
- **Command Lookup Tool (registered customers only)**
- **Technical Support − Cisco Systems**

Updated: Jun 21, 2005 Document ID: 14136