

# GRE 터널링을 사용하여 EIGRP 및 IPX로 IPSec 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[show 명령 출력\(터널 위로\)](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

## 소개

일반 IPSec 컨피그레이션은 EIGRP(Enhanced Interior Gateway Routing Protocol) 및 OSPF(Open Shortest Path First) 등의 라우팅 프로토콜 또는 IPX(Internet Packet Exchange), AppleTalk 등의 비 IP 트래픽을 전송할 수 없습니다. 이 문서에서는 IPSec을 사용하여 라우팅 프로토콜과 비 IP 트래픽을 사용하여 서로 다른 네트워크 간에 라우팅하는 방법을 설명합니다. 이 기법은 일반 GRE(라우팅 캡슐화)를 사용하여 이를 수행합니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 암호화 맵을 적용하기 전에 터널이 작동하는지 확인합니다.
- 암호화 액세스 목록은 GRE를 프로토콜로 허용해야 합니다. `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>`
- 루프백 IP 주소를 사용하여 IKE(Internet Key Exchange) 피어 및 터널 소스 및 터널 대상을 식별하여 가용성을 향상시킵니다.
- 가능한 MTU(Maximum Transmission Unit) 문제에 대한 자세한 내용은 [Windows 및 Sun 시스템에서 IP MTU, TCP MSS 및 PMTUD 조정을 참조하십시오.](#)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.1.8 및 12.2.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

## 구성

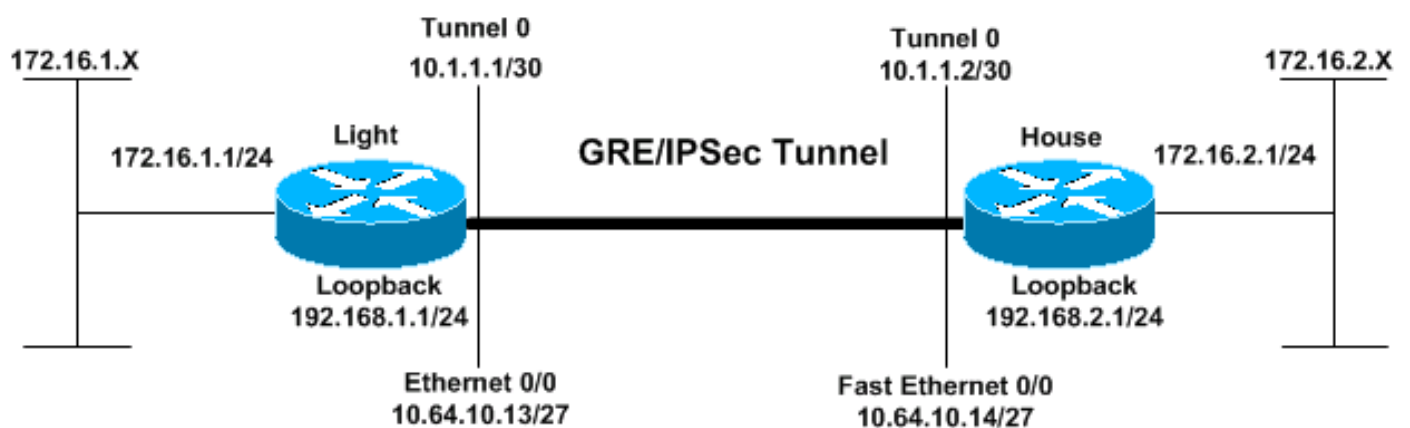
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)([등록된 고객만 해당](#))를 사용합니다.

**IOS 구성 참고:** Cisco IOS Software Release 12.2(13)T 및 이후 코드(번호가 높은 T-트레인 코드, Cisco IOS Software Release 12.3 이상 코드)를 사용하면 구성된 IPsec "crypto map"만 물리적인 인터페이스에 적용해야 합니다. 더 이상 GRE 터널 인터페이스에 적용할 필요가 없습니다. Cisco IOS Software Release 12.2(13)T 및 이후 코드를 사용할 때 물리적 및 터널 인터페이스에 "crypto map"이 있는 것은 여전히 작동합니다. 그러나 물리적 인터페이스에만 적용하는 것이 좋습니다.

## 네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



## 구성

- [조명](#)
- [하우스](#)

조명

```
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#!
```

## 하우스

```
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#

```

## 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터](#) 를에서 지원되는데(등록된 고객만), 이 틀을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show crypto engine connections active**(암호화 엔진 연결 활성 표시) - IPSec 피어 간 암호화 및 암호 해독된 패킷을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.
- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.

- **show ipx route [network] [default] [detailed]**—IPX 라우팅 테이블의 내용을 표시합니다.

## show 명령 출력(터널 위로)

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:

## [문제 해결](#)

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

### [문제 해결 명령](#)

일부 show 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오](#).

- debug crypto isakmp - 1단계 중 오류를 표시합니다.
- debug crypto ipsec - 2단계 중 오류를 표시합니다.
- debug crypto engine - 암호화 엔진의 정보를 표시합니다.
- debug ip *your routing protocol* - 라우팅 프로토콜의 라우팅 트랜잭션에 대한 정보를 표시합니다.
- 암호화 연결 연결 id 지우기 [[슬롯](#) / rsm / vip]—현재 진행 중인 암호화된 세션을 종료합니다. 암호화 세션은 세션이 시간 초과되면 일반적으로 종료됩니다. show crypto cisco connections 명령을 사용하여 connection-id 값을 확인합니다.
- clear crypto isakmp - 1단계 보안 연결을 지웁니다.
- clear crypto sa - 2단계 보안 연결을 지웁니다.

## [관련 정보](#)

- [IPSec 지원 페이지](#)
- [IPSec\(IP Security\) 암호화 소개](#)
- [IPSec 네트워크 보안 구성](#)
- [인터넷 키 교환 보안 프로토콜 구성](#)
- [명령 조회 도구\(등록된 고객만 해당\)](#)
- [Technical Support - Cisco Systems](#)