# IPsec 터널 구성 - Cisco 라우터에서 Checkpoint 방화벽 4.1

## 목차



## 소개

이 문서에서는 두 개의 프라이빗 네트워크에 연결하기 위해 사전 공유 키를 사용하여 IPsec 터널을 구성하는 방법을 설명합니다. Cisco 라우터 내의 192.168.1.x 프라이빗 네트워크와 Checkpoint 방화벽 내의 10.32.50.x 프라이빗 네트워크.

## 사전 요구 사항

### 요구 사항

이 샘플 컨피그레이션에서는 컨피그레이션을 시작하기 전에 라우터 내부 및 Checkpoint 내에서 인터넷(172.18.124.x 네트워크로 표시)으로 이동하는 트래픽이 플로우된다고 가정합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 3600 라우터
- Cisco IOS® 소프트웨어(C3640-JO3S56I-M), 릴리스 12.1(5)T, 릴리스 소프트웨어(fc1)
- Checkpoint 방화벽 4.1

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 규칙을 참고하십시오.

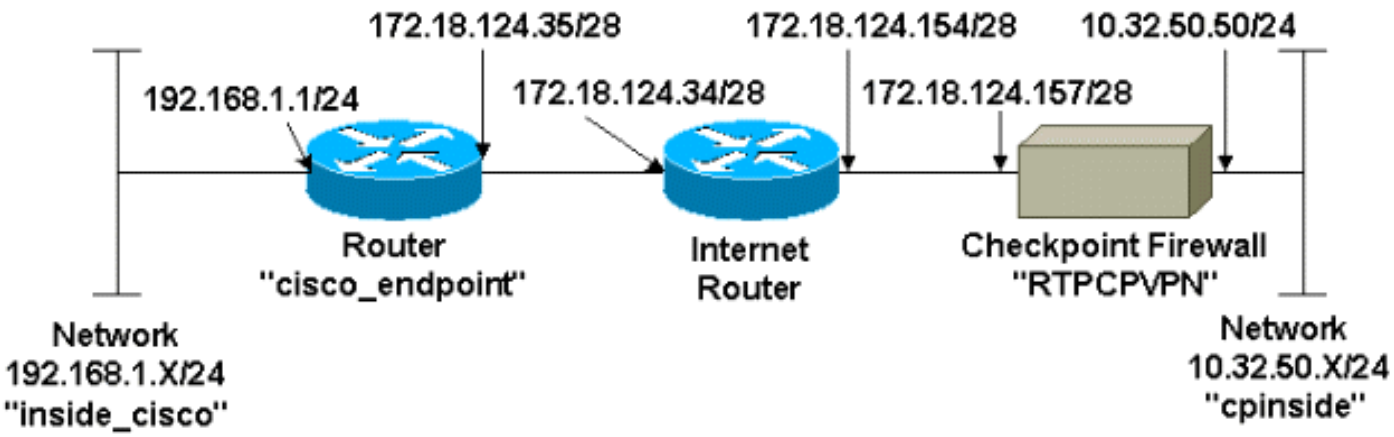
# 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.




## 구성

이 문서에서는 이러한 구성을 사용합니다.

- 라우터 컨피그레이션
- 검사점 방화벽 구성

### 라우터 컨피그레이션

| Cisco 3600 라우터 컨피그레이션 |
| --- |
| Current configuration : 1608 bytes<br>!<br>version 12.1<br>no service single-slot-reload-enable<br>service timestamps debug uptime<br>service timestamps log uptime<br>no service password-encryption<br>! |

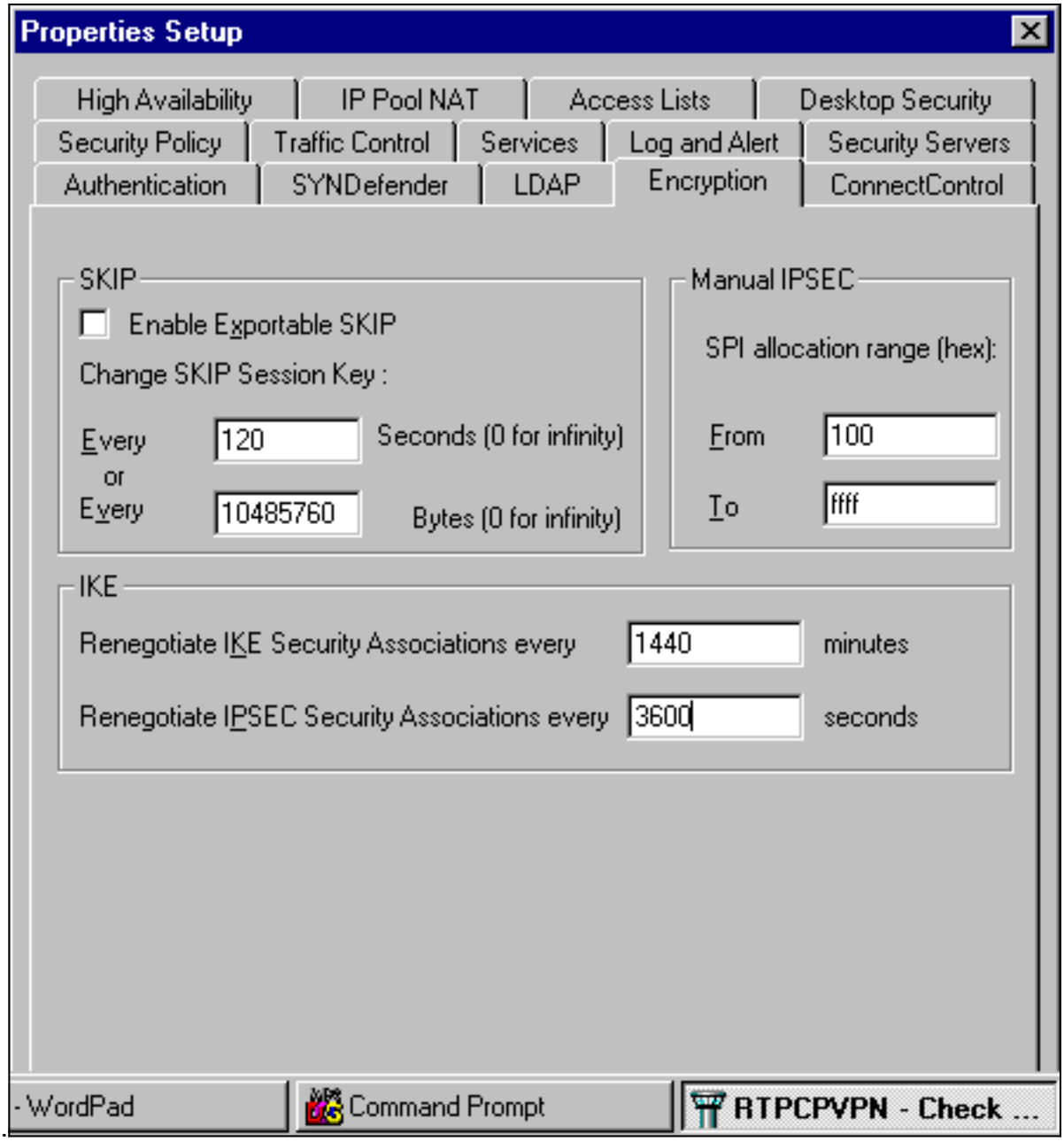
```
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
```

```
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

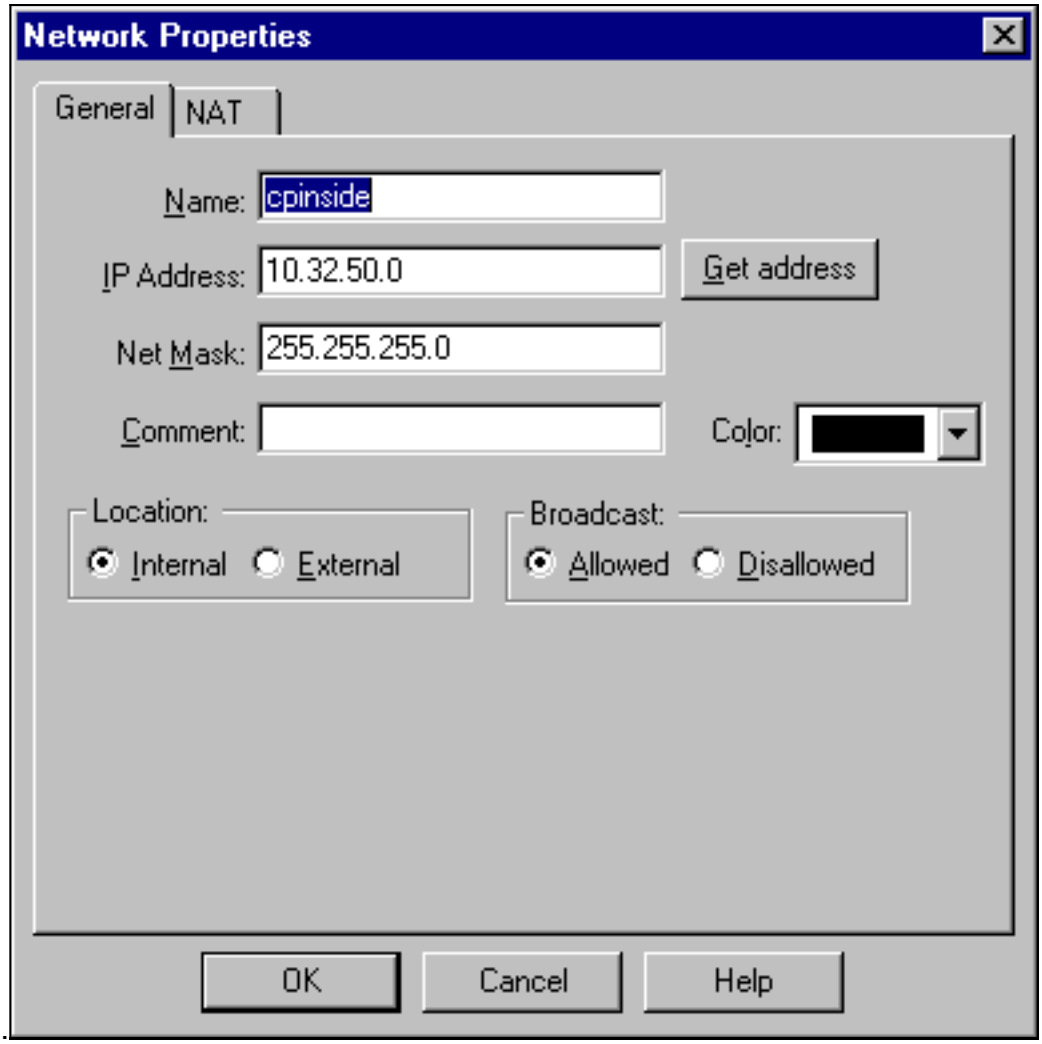
## 검사점 방화벽 구성

체크포인트 방화벽을 구성하려면 다음 단계를 완료합니다.

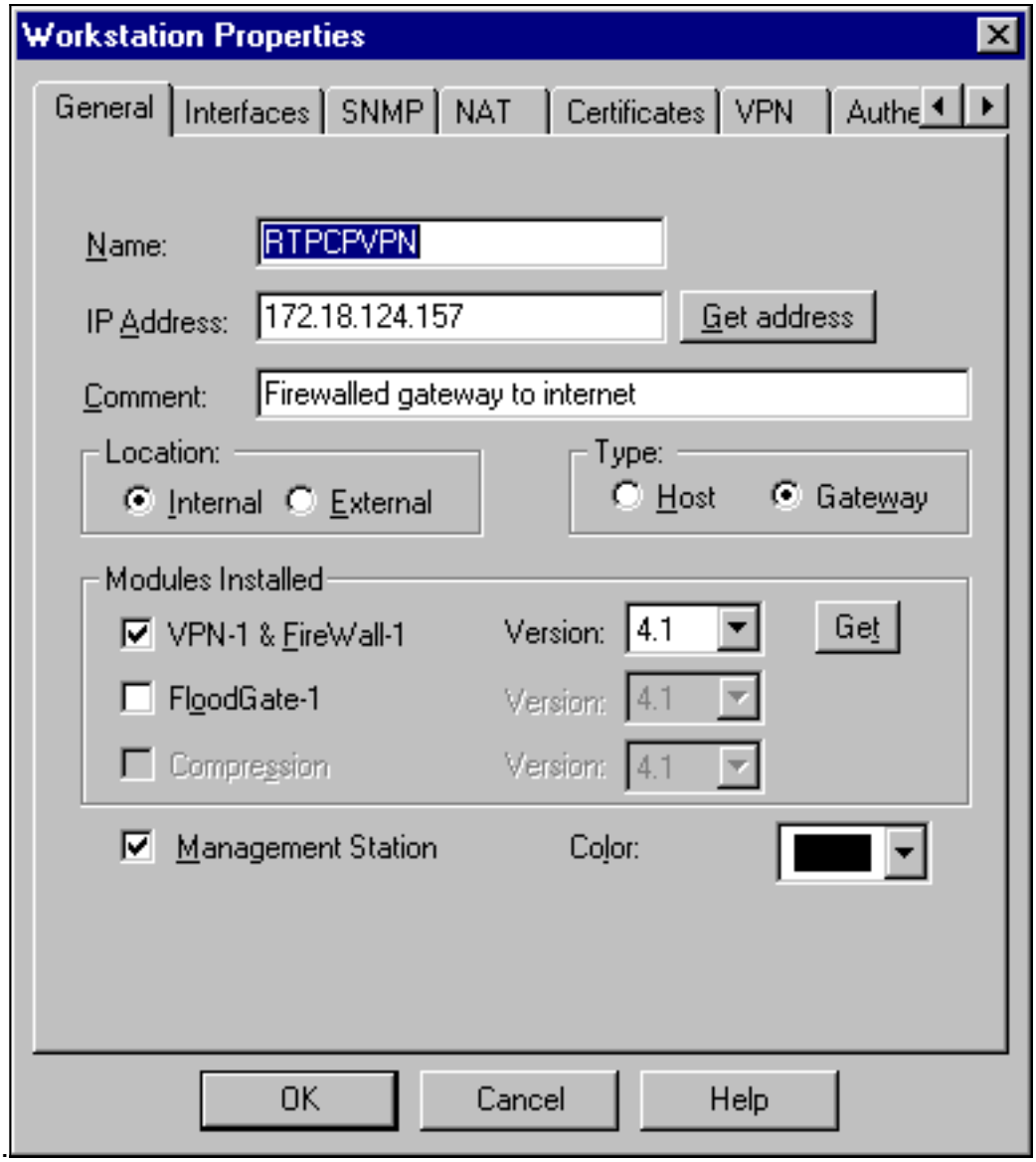
1. IKE 및 IPsec 기본 수명은 벤더 간에 다르므로 **Properties > Encryption**을 선택하여 Checkpoint 수명을 Cisco 기본값에 맞게 설정합니다.Cisco 기본 IKE 수명은 86400초(1440분)이며 다음 명령으로 수정할 수 있습니다.**crypto isakmp policy #수명 #**구성 가능한 Cisco IKE 수명은 60~86400초입니다. Cisco 기본 IPsec 수명은 3600초이며, crypto ipsec **security-association lifetime seconds** 명령으로 수정할 수 있습니다.구성 가능한 Cisco IPsec 수명은 120~86400초입니다



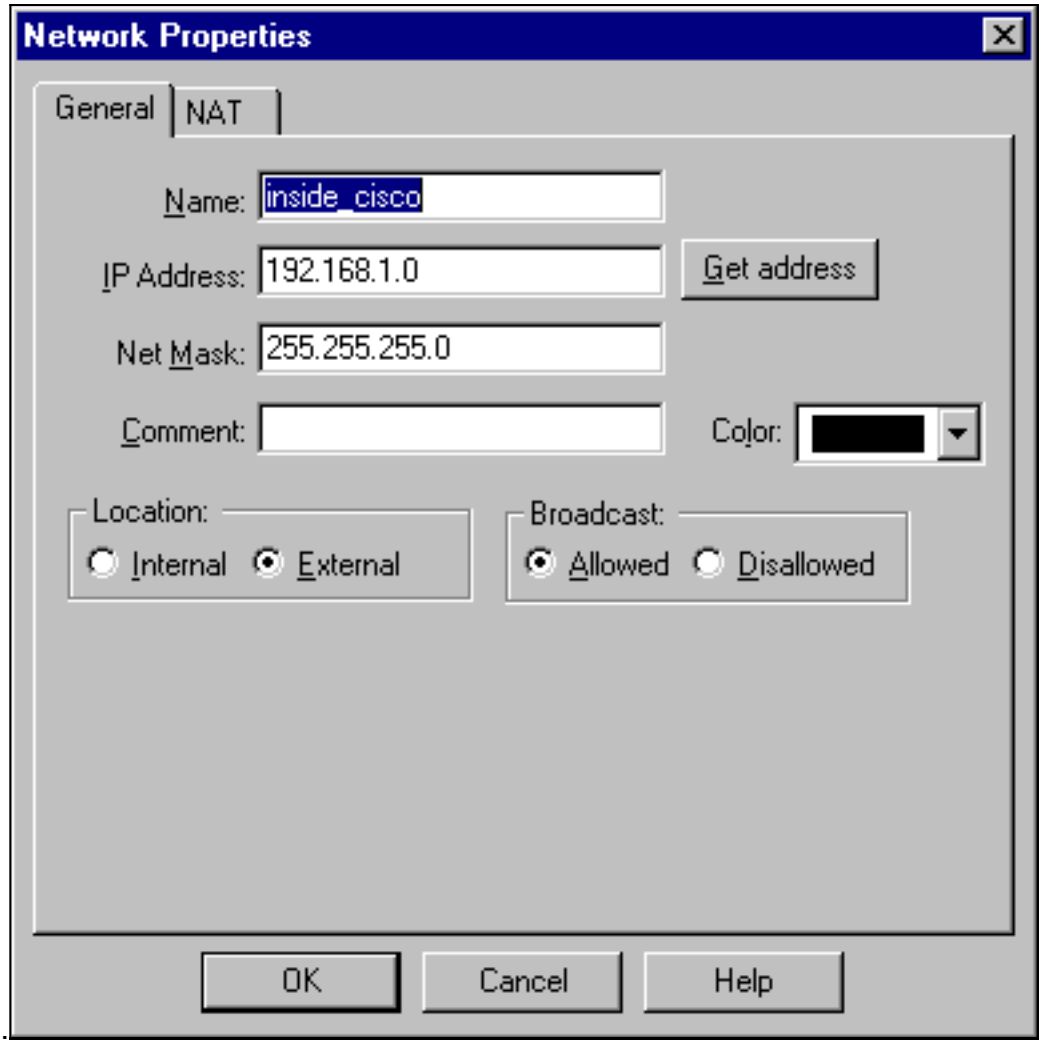

2. Manage(**관리**) > **Network objects(네트워크 개체)** > **New(또는 Edit)** > **Network(네트워크)를 선택하여** 체크포인트 뒤에 있는 내부 네트워크에 대한 개체(일명 "cpinside")를 구성합니다.이는 Cisco **access-list 115 permit ip 192.168.1.0 10.32.50.0 0.0.0.255** 명령의 대상(두 번째) 네트워크**와** 일치해야 합니다.위치(Location)에서 **내부**를 선택합니다



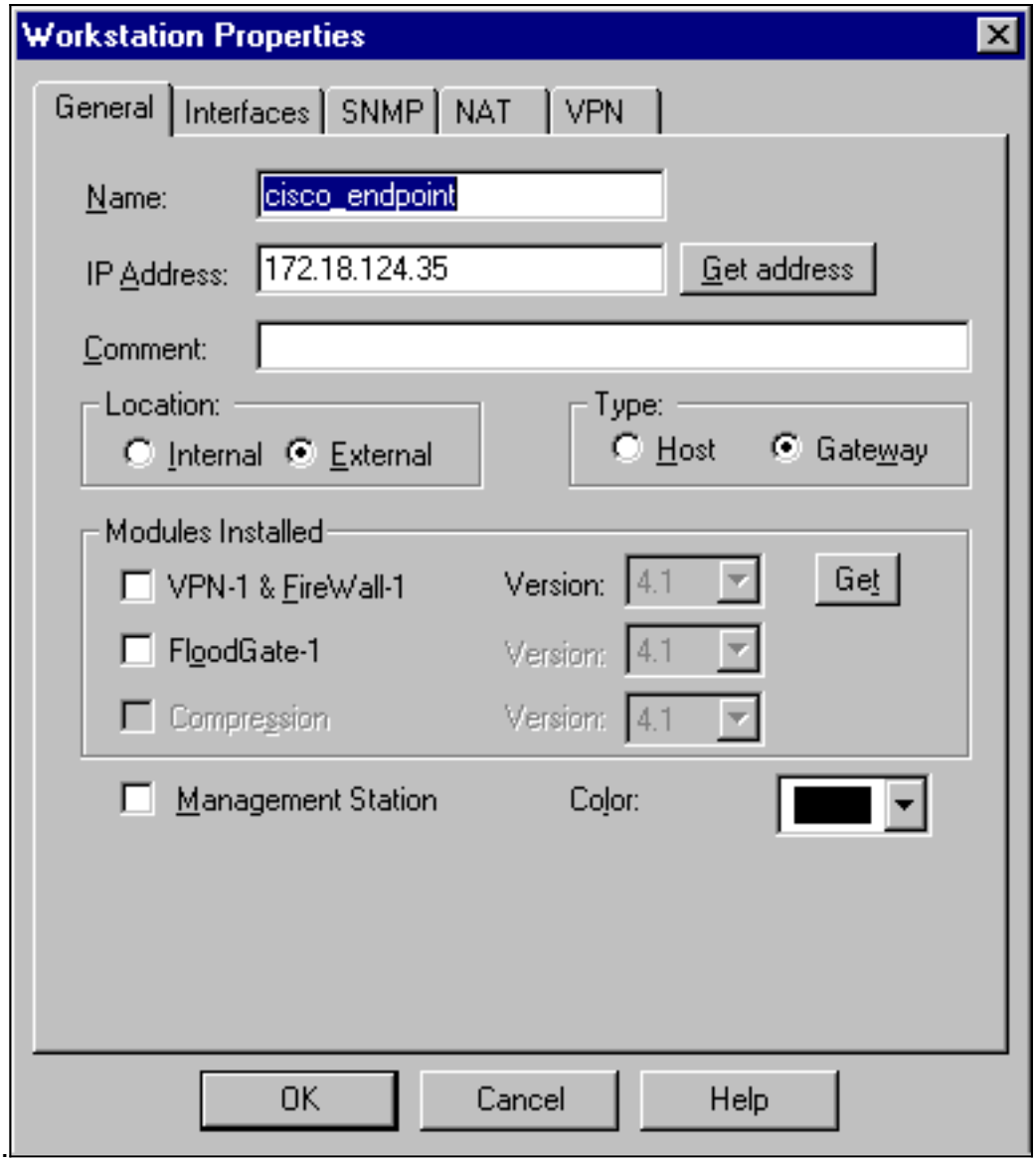

3. Manage(**관리) > Network objects(네트워크 개체) > Edit(편집)**를 선택하여 Cisco 라우터가 **set peer 172.18.124.157** 명령에서 가리키는 RTPCPVPN Checkpoint(게이트웨이) 엔드포인트의 개체를 편집합니다.위치(Location)에서 **내부**를 선택합니다. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다. Modules Installed(설치된 모듈)에서 **VPN-1 & FireWall-1** 확인란을 선택하고 **Management Station(관리 스테이션)** 확인란을 선택합니다



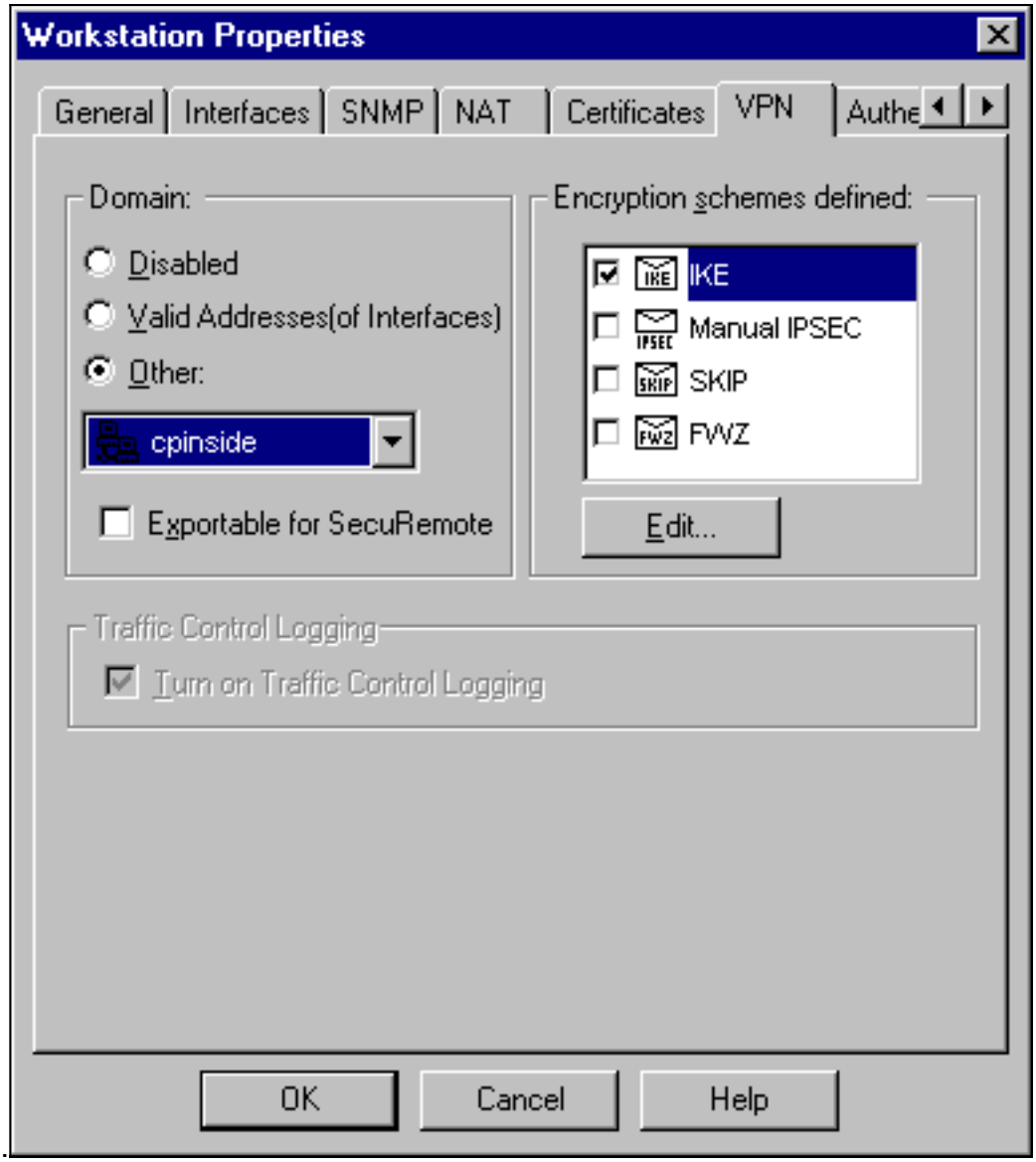

4. Manage(**관리**) > **Network objects(네트워크 개체)** > **New(새로 만들기)** > **Network(네트워크)를 선택하여** Cisco 라우터 뒤에 있는 외부 네트워크(일명 "inside_cisco")에 대한 개체를 구성합니다.이는 Cisco **access-list 115 permit ip 192.168.1.0 10.32.50.0 0.0.0.255** 명령의 소스(첫 번째) 네트워크**와** 일치해야 합니다.위치(Location)에서 **외부**를 선택합니다




5. Manage(**관리) > Network objects(네트워크 개체) > New(새로 만들기) > Workstation(워크스테이션)을 선택하여** 외부 Cisco 라우터 게이트웨이("cisco_endpoint"라고 함)에 대한 객체를 추가합니다. 이는 crypto **map *name* 명령**이 적용되는 Cisco 인터페이스입니다.위치(Location)에서 **외부**를 선택합니다. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다.**참고:** VPN-1/FireWall-1 확인란을 선택하지 마십시오

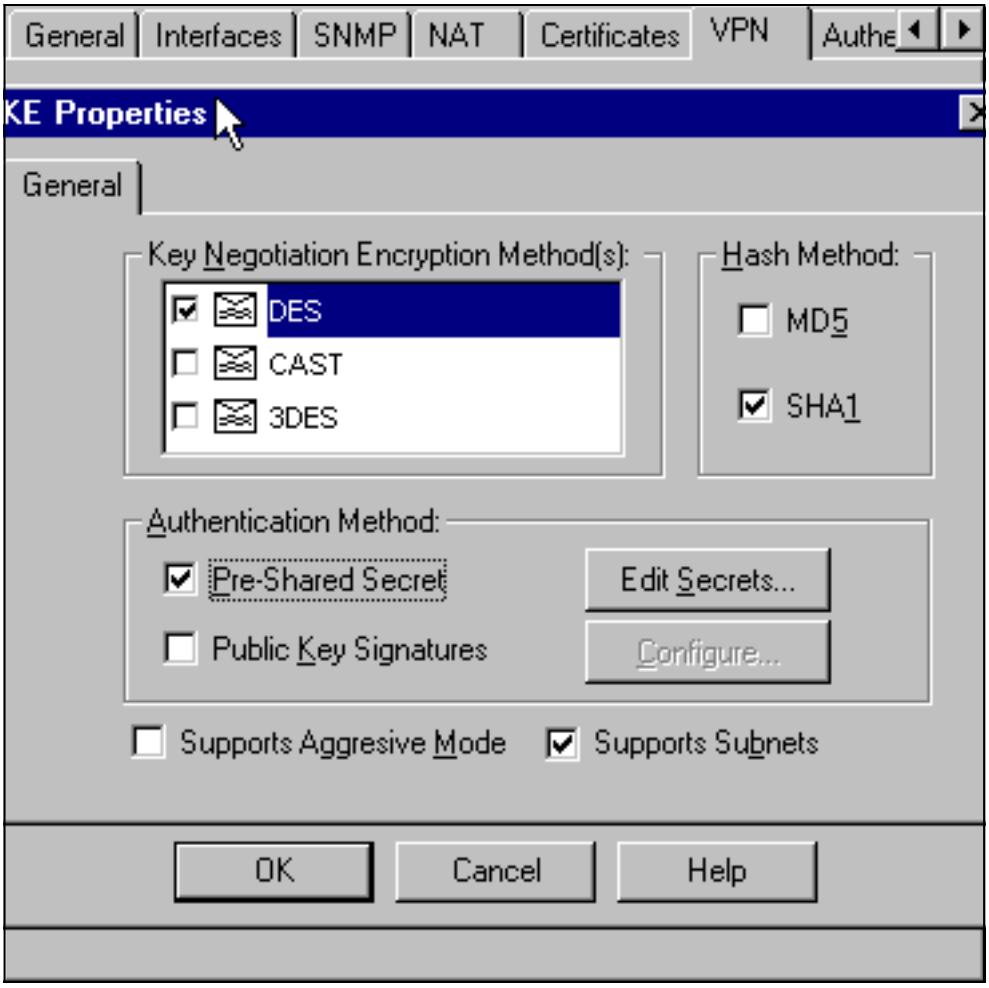



6. Manage(**관리) > Network objects(네트워크 개체) > Edit(편집)**를 선택하여 Checkpoint gateway endpoint(일명 "RTPCPVPN") VPN 탭을 편집합니다. Domain(도메인)에서 **Other(기타)**를 선택한 다음 드롭다운 목록에서 Checkpoint 네트워크의 내부("cpinside")를 선택합니다. Encryption schemes defined(정의된 암호화 체계)에서 **IKE**를 선택한 다음 Edit(수정)를 **클릭합**

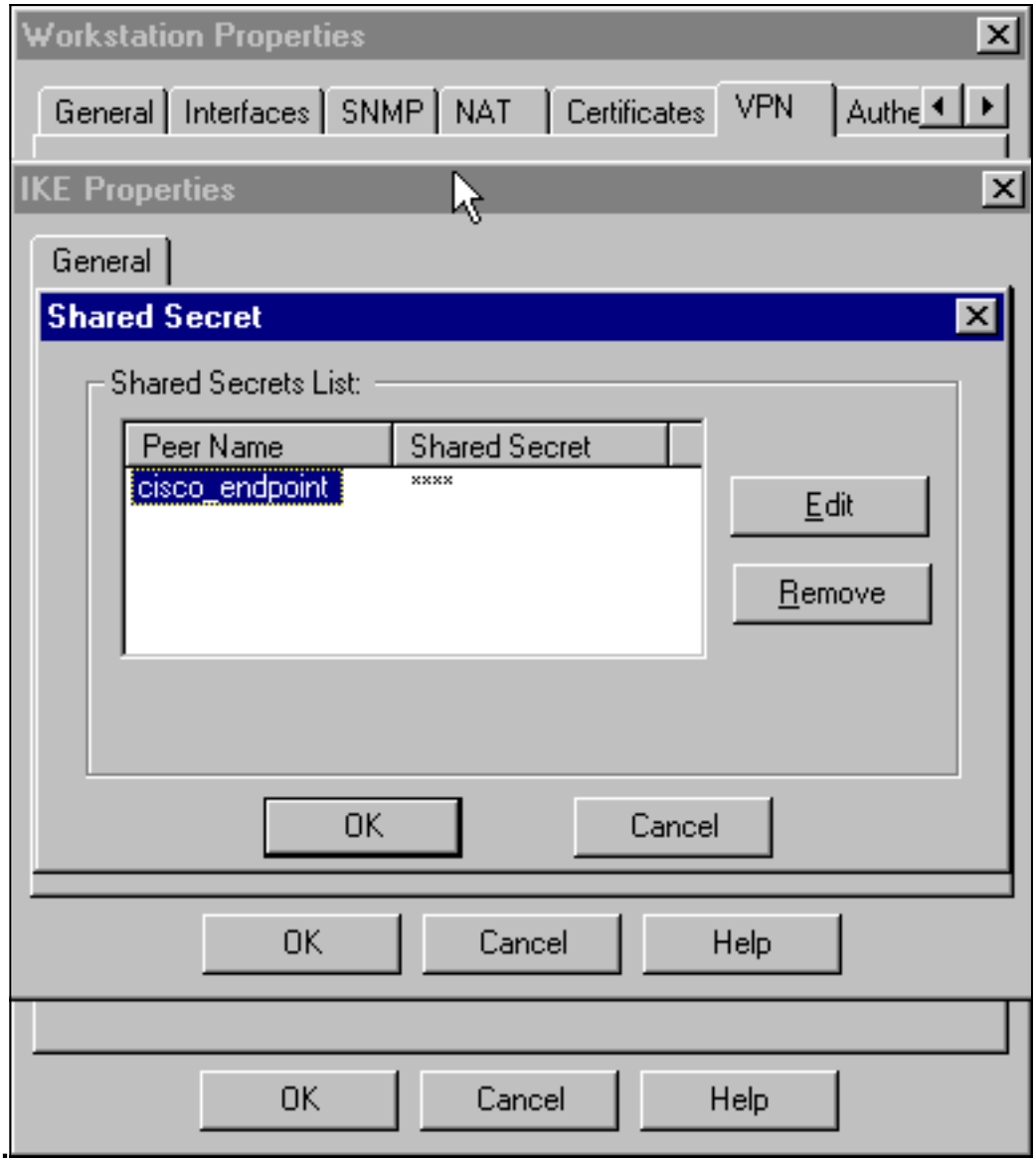



니다.

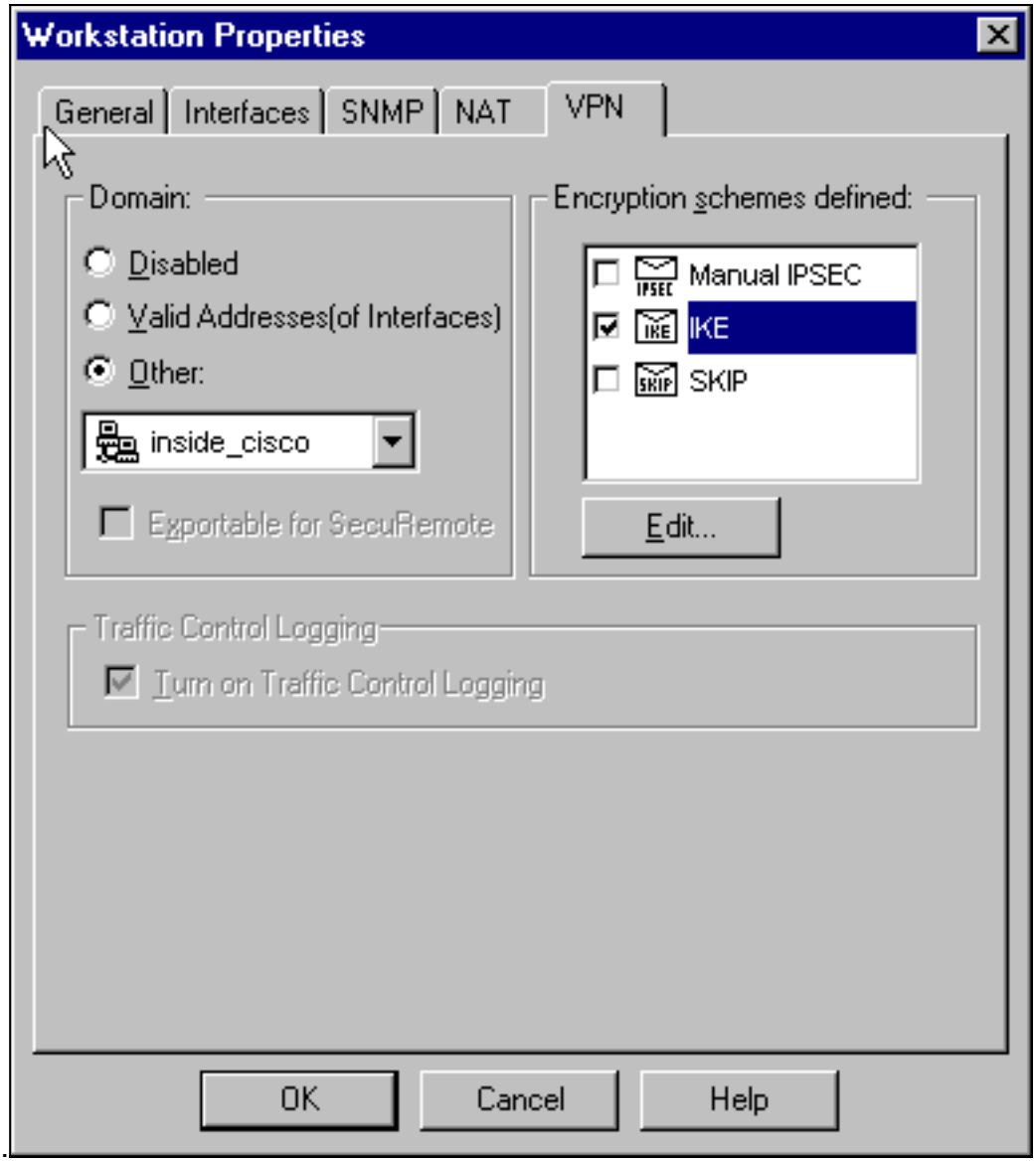
7. DES 암호화의 IKE 속성을 변경하여 다음 명령에 동의합니다.**crypto isakmp policy #암호화 des참고:** DES 암호화는 기본값이므로 Cisco 컨피그레이션에 표시되지 않습니다.
8. 다음 명령에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.**crypto isakmp policy #해시 sha참고:** SHA 해싱 알고리즘이 기본값이므로 Cisco 컨피그레이션에 표시되지 않습니다.다음 설정을 변경합니다.Aggressive **Mode를 선택 취소합니다**.Supports Subnets(**서브넷 지원)를** 선택합니다.Authentication **Method(인증 방법)** 아래에서 Pre-Shared Secret(사전 공유 암호)을 선택합니다. 이 명령은 다음 명령과 동일합니다.**crypto isakmp policy #인증 사전 공유**



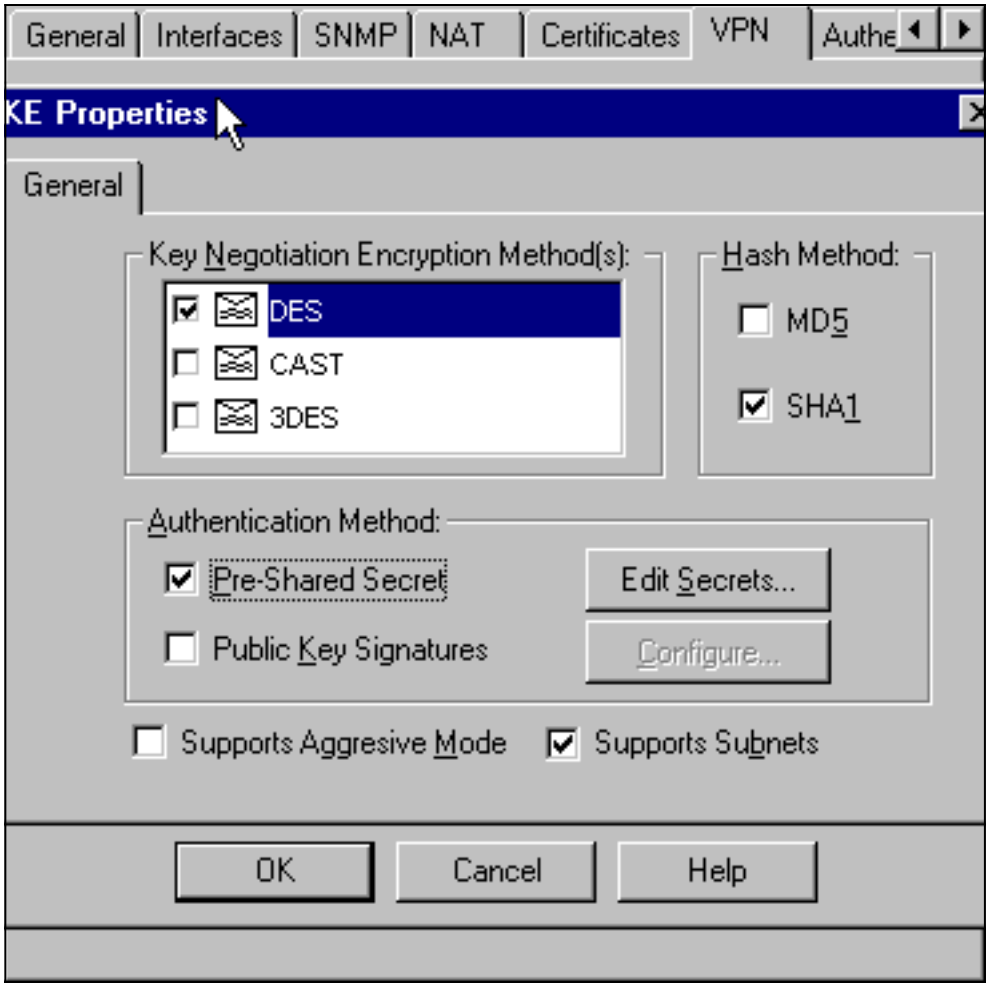

9. Edit **Secrets**를 클릭하여 Cisco crypto isakmp key **address *address* 명령**에 동의하도록 사전 공유 키를 **설정합니다**



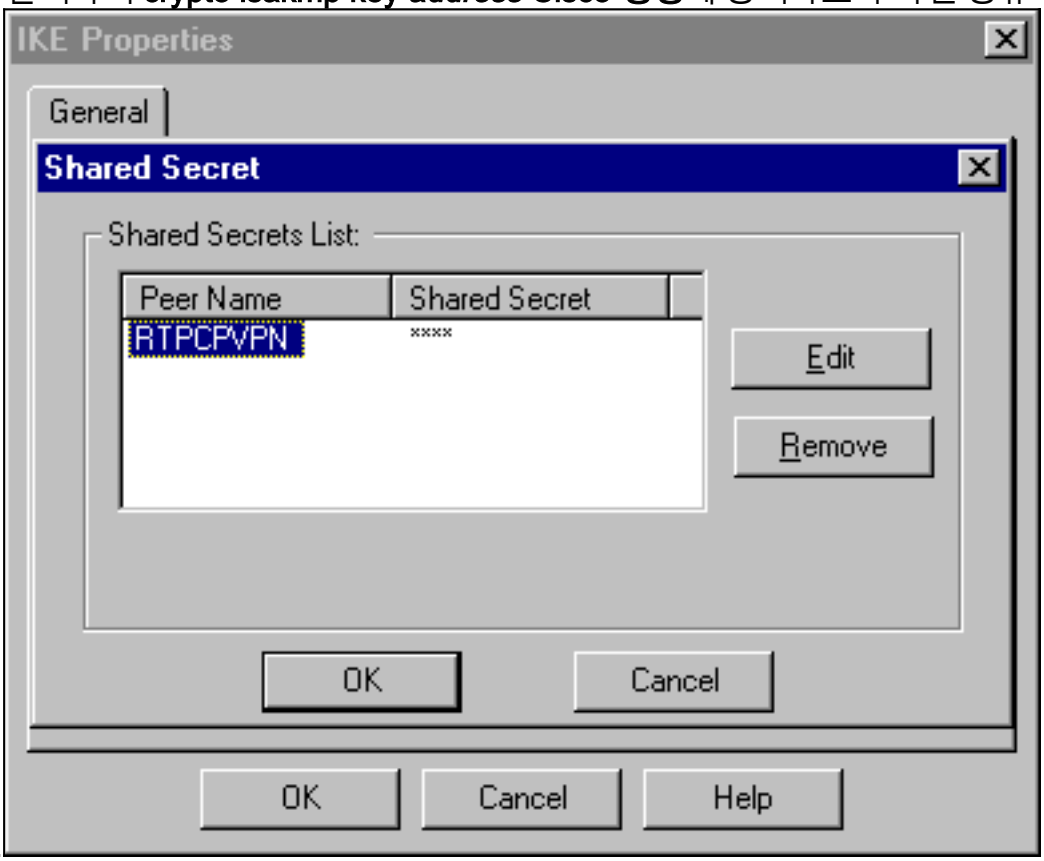

10. Manage(**관리) > Network objects(네트워크 개체) > Edit(편집)를 선택하여** "cisco_endpoint" VPN 탭을 편집합니다. Domain(도메인)에서 **Other(기타)**를 선택한 다음 Cisco 네트워크의 내부("inside_cisco"라고 함)를 선택합니다. Encryption schemes defined(정의된 암호화 체계)에서 **IKE**를 선택한 다음 Edit(수정)를 **클릭합니다**




11. 다음 명령에 동의하도록 IKE 속성 DES 암호화를 변경합니다.**crypto isakmp policy #암호화 des참고:** DES 암호화는 기본값이므로 Cisco 컨피그레이션에 표시되지 않습니다.
12. 다음 명령에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.**crypto isakmp policy #해시 sha참고:** SHA 해싱 알고리즘이 기본값이므로 Cisco 컨피그레이션에 표시되지 않습니다.다음 설정을 변경합니다.Aggressive **Mode를 선택 취소합니다**.Supports Subnets(**서브넷 지원)를** 선택합니다.Authentication **Method(인증 방법)** 아래에서 Pre-Shared Secret(사전 공유 암호)을 선택합니다. 이 명령은 다음 명령과 동일합니다.**crypto isakmp policy #인증 사전 공유**



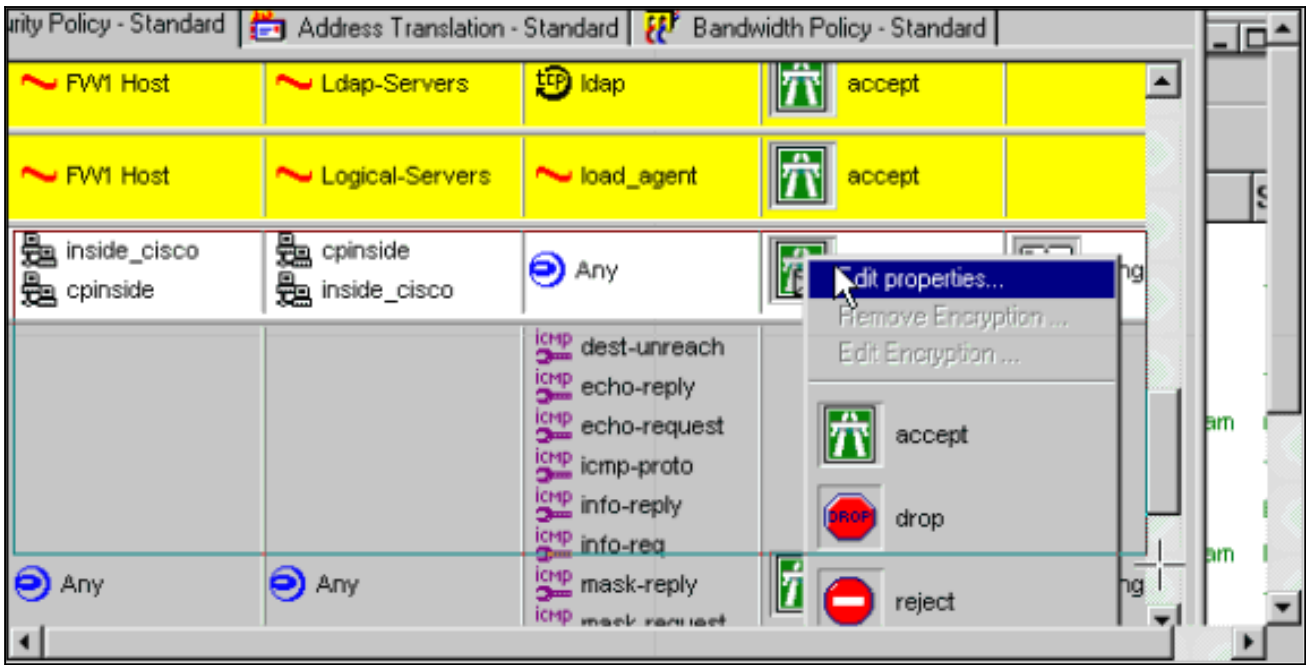

13. Edit **Secrets**를 클릭하여 **crypto isakmp key *address* Cisco 명령**에 동의하도록 사전 공유 키를 **설정합니다**.



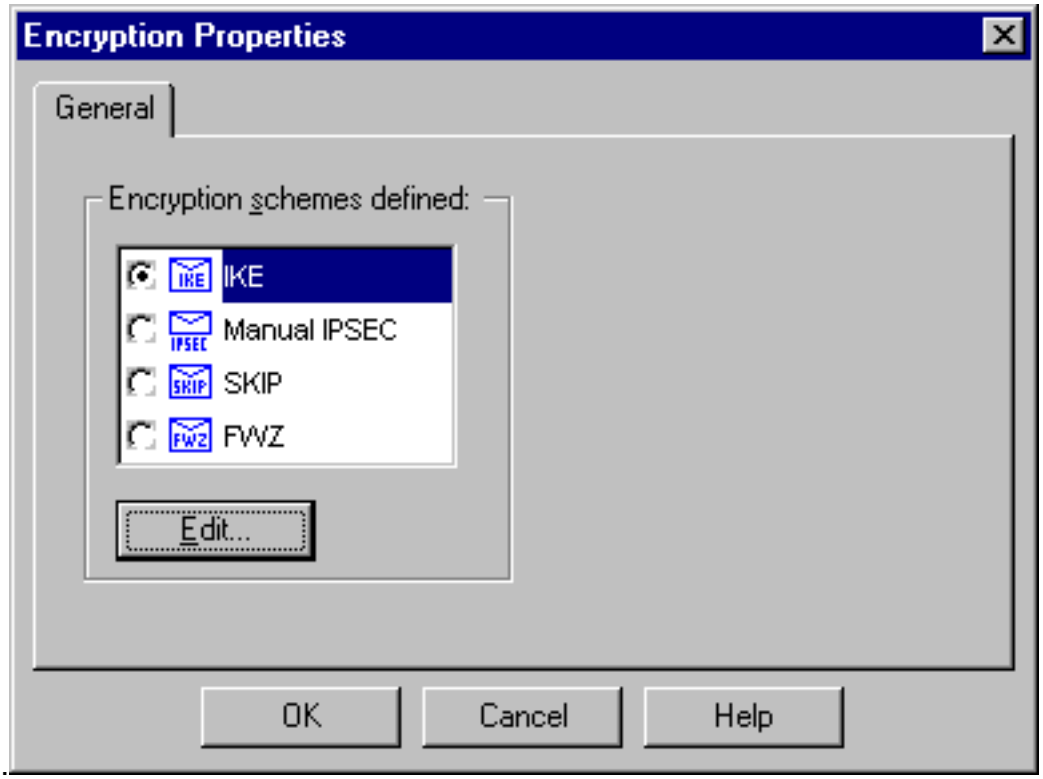

14. Policy Editor(정책 편집기) 창에서 Source(소스)와 Destination(대상)을 모두 "inside_cisco" 및 "cpinside"(양방향)로 포함하는 규칙을 삽입합니다. Set **Service=Any**, **Action=Encrypt** 및 **Track=Long**.


15. 녹색 **암호화** 아이콘을 클릭하고 **Edit properties**를 선택하여 Action 제목 아래에서 암호화 정책을 구성합니다

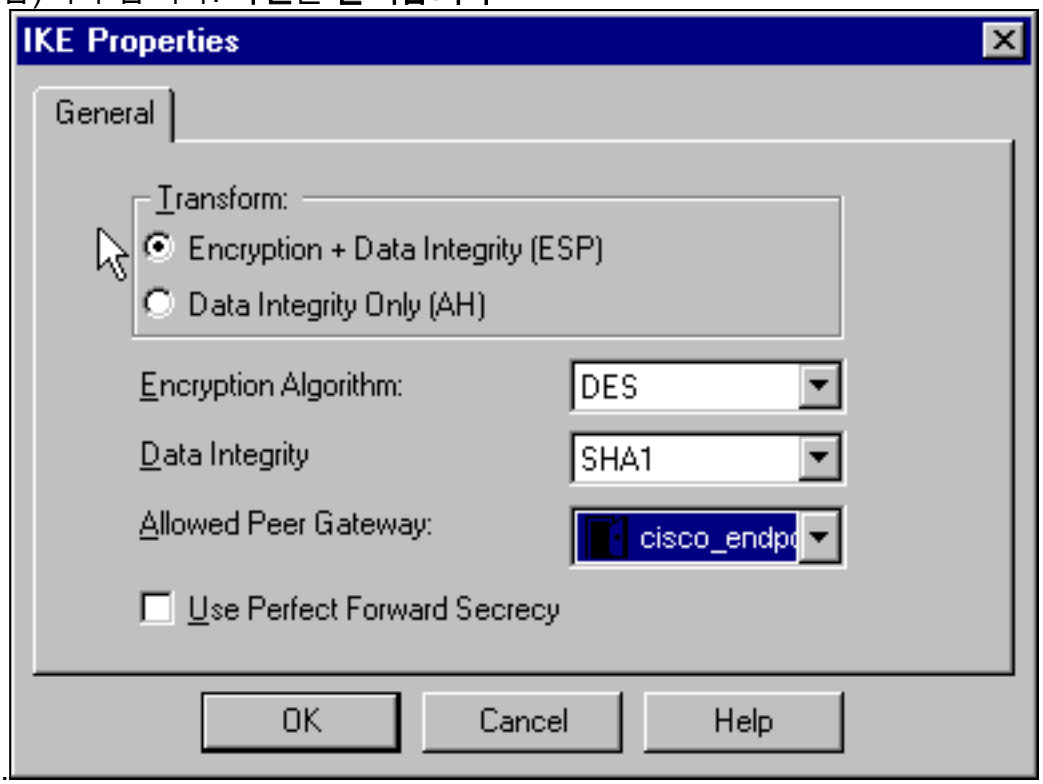
.




16. IKE를 선택한 다음 Edit를 **클릭합니다**




17. IKE Properties(IKE 속성) 창에서 crypto ipsec transform-set rtpset esp-des esp-sha-hmac 명령의 Cisco IPsec 변환**에** 동의하도록 이러한 속성을 변경합니다.Transform(변형)에서 **Encryption + Data Integrity (ESP)를** 선택합니다. 암호화 알고리즘은 **DES**, 데이터 무결성은 **SHA1**이어야 하며, 허용된 피어 게이트웨이는 외부 라우터 게이트웨이("cisco_endpoint"라고 함)여야 합니다. **확인**을 **클릭합니다**




18. Checkpoint를 구성한 후 Checkpoint 메뉴**에서 Policy > Install**을 선택하여 변경 사항을 적용합니다.

## 다음을 확인합니다.

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

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto isakmp sa** - 피어에서 현재 IKE SA(Security Association)를 모두 봅니다.
- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 봅니다.

# 문제 해결

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

## 문제 해결 명령

**참고:** debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto engine** - 암호화 및 해독을 수행하는 암호화 엔진에 대한 디버그 메시지를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug crypto ipsec** - IPsec 이벤트를 표시합니다.
- **clear crypto isakmp** - 모든 활성 IKE 연결을 지웁니다.
- **clear crypto sa** - 모든 IPsec SA를 지웁니다.

## 네트워크 요약

Checkpoint의 암호화 도메인에 인접한 여러 내부 네트워크가 구성된 경우, 해당 디바이스는 흥미로운 트래픽과 관련하여 이를 자동으로 요약할 수 있습니다. 라우터가 일치하도록 구성되지 않은 경우 터널이 실패할 가능성이 높습니다. 예를 들어 10.0.0.0 /24 및 10.0.1.0 /24의 내부 네트워크가 터널에 포함되도록 구성된 경우 10.0.0.0 /23으로 요약될 수 있습니다.

## 체크포인트

Policy Editor(정책 편집기) 창에서 Tracking(추적)이 Long으로 설정되었으므로 거부된 트래픽은 로그 뷰어에 빨간색으로 표시되어야 합니다. 자세한 디버그 정보는 다음을 사용하여 확인할 수 있습니다.

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

다른 창에서 다음을 수행합니다.

```
C:\WINNT\FW1\4.1\fwstart
```

**참고:** Microsoft Windows NT 설치입니다.

체크포인트에서 SA를 지우려면 다음 명령을 실행합니다.

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

**예**에 대답하시겠습니까? 프롬프트에서 중단될 수 있습니다.

## 디버그 출력 샘플

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
```

```
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
```

```
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0

     local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, media mtu 1500
     current outbound spi: 181C6E59

     inbound esp sas:
      spi: 0xA29984CA(2727969994)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--                 sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x181C6E59(404516441)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4607997/3447)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


cisco_endpoint#show crypto isakmp sa
    dst           src          state        conn-id   slot
172.18.124.157 172.18.124.35  QM_IDLE           1       0

cisco_endpoint#exit
```

# 관련 정보

- IPSec 협상/IKE 프로토콜
- IPsec 네트워크 보안 구성

- 인터넷 키 교환 보안 프로토콜 구성
- 기술 지원 및 문서 – Cisco Systems