IPSec 터널 구성 - Cisco Secure PIX Firewall to Checkpoint 4.1 Firewall

목차

소개

이 샘플 컨피그레이션에서는 미리 공유된 키를 사용하여 IPSec 터널을 형성하여 두 개의 프라이빗 네트워크에 연결하는 방법을 보여 줍니다. 이 예에서는 연결된 네트워크가 Cisco PIX(Secure Pix Firewall) 내부의 192.168.1.X 프라이빗 네트워크와 체크포인트 내의 10.32.50.X 프라이빗 네트워크입니다. 이 컨피그레이션을 시작하기 전에 PIX 내부 및 Checkpoint 4.1 방화벽 내부에서 인터넷(172.18.124.X 네트워크로 표시)으로 이동하는 트래픽이 플로우된다고 가정합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 소프트웨어 버전 5.3.1

- Checkpoint 4.1 방화벽

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 규칙을 참조하십시오.

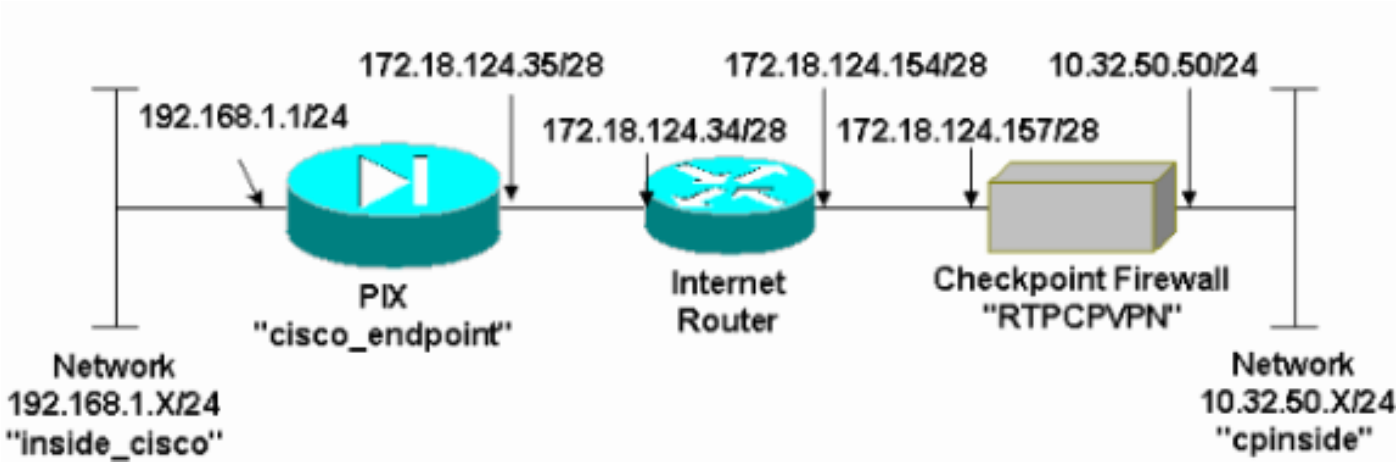
구성

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.

네트워크 다이어그램

이 문서에서는 다음 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 이 섹션에 표시된 구성을 사용합니다.

PIX 컨피그레이션

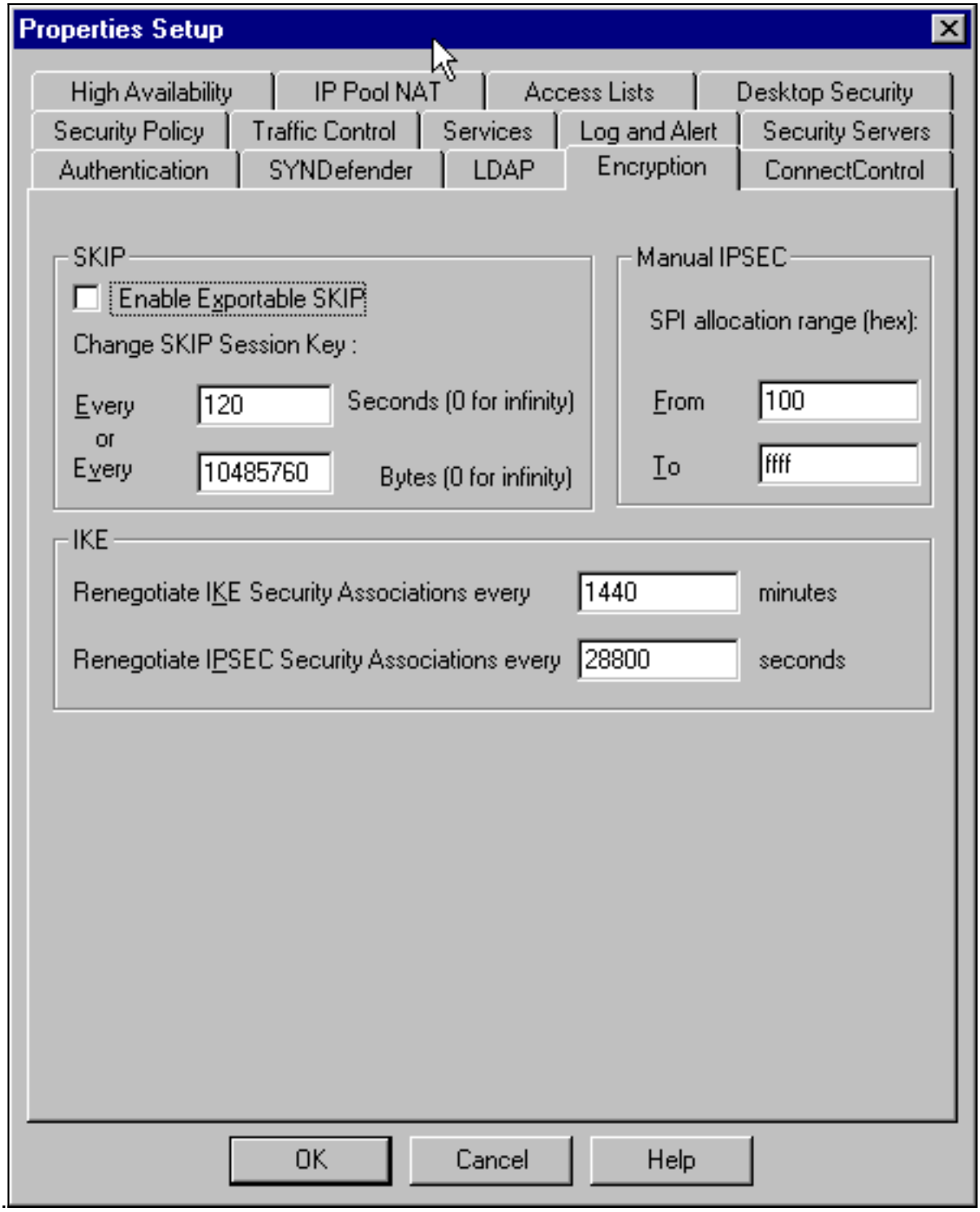
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
```

```
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
```

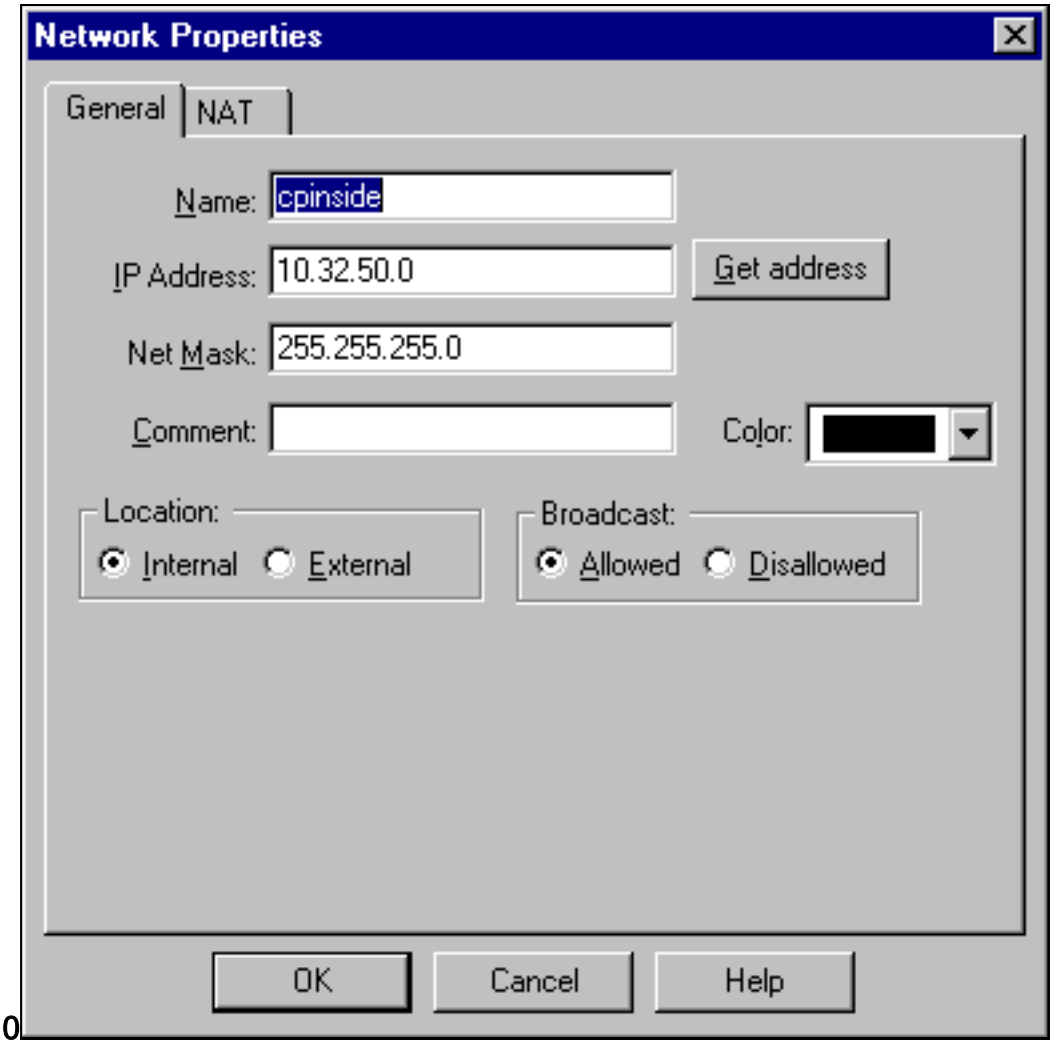
```
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

체크포인트 방화벽

1. IKE 및 IPSec 기본 수명은 벤더 간에 다르므로 Properties(**속성**) > **Encryption(암호화**)을 선택하여 Checkpoint lifetime을 PIX 기본값에 맞게 설정합니다.PIX 기본 IKE 수명은 86400초(=1440분)이며, 이 명령으로 수정할 수 있습니다. **isakmp 정책 # 수명 86400**PIX IKE 수명은 60~86400초 사이로 구성할 수 있습니다.PIX 기본 IPSec 수명은 28800초이며, 이 명령을 통해 수정할 수 있습니다. **crypto ipsec 보안 연결 수명 초 #**120~86400초 사이의 PIX IPSec 수명을 구성할 수 있습니다

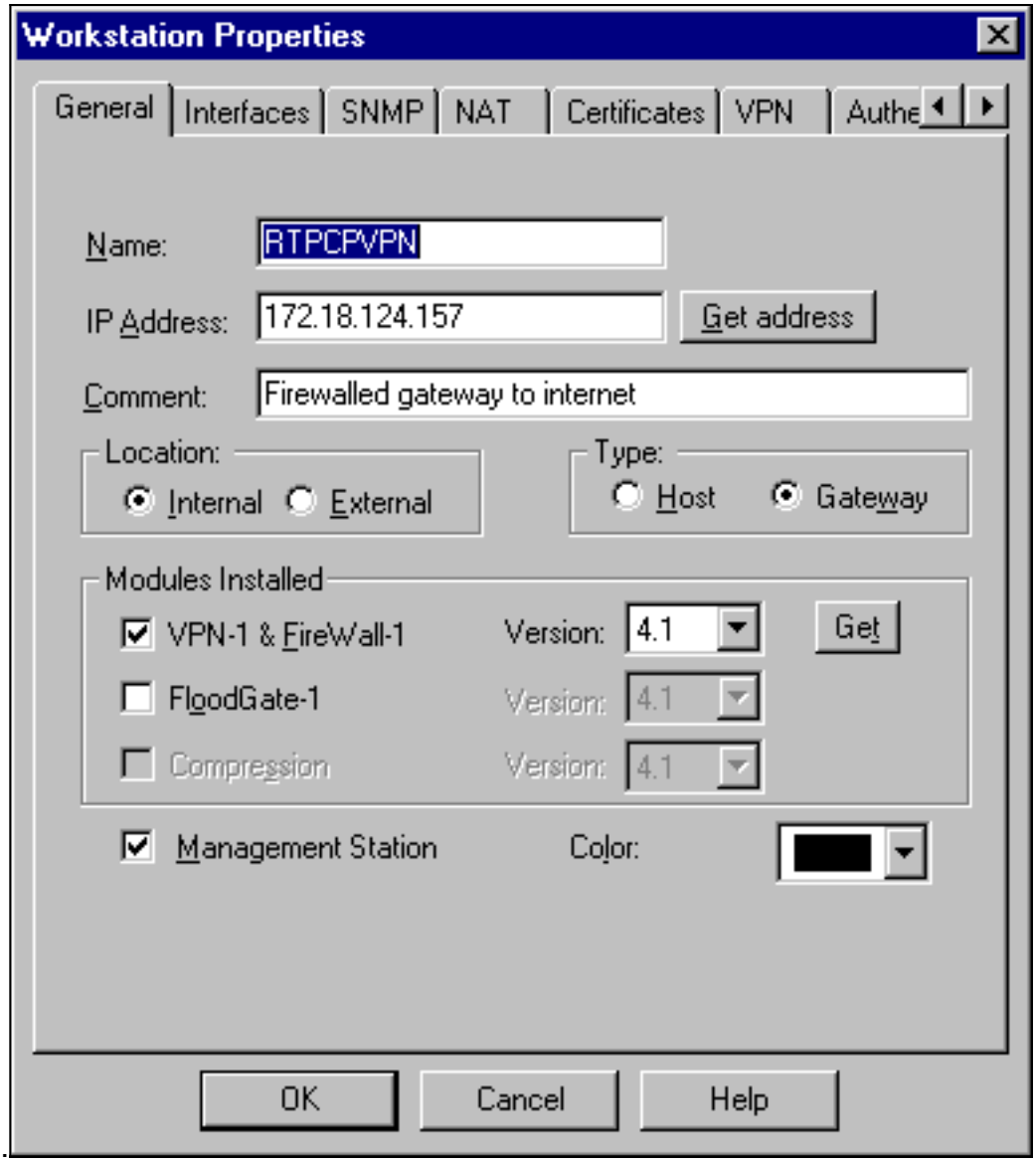


2. Manage(**관리**) > **Network objects(네트워크 개체)** > New(**또는 Edit) > Network(네트워크)**를 선택하여 체크포인트 뒤에 있는 내부("cpinside") 네트워크에 대한 개체를 구성합니다.이는 다음 PIX 명령에서 대상(두 번째) 네트워크와 일치해야 합니다. **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**

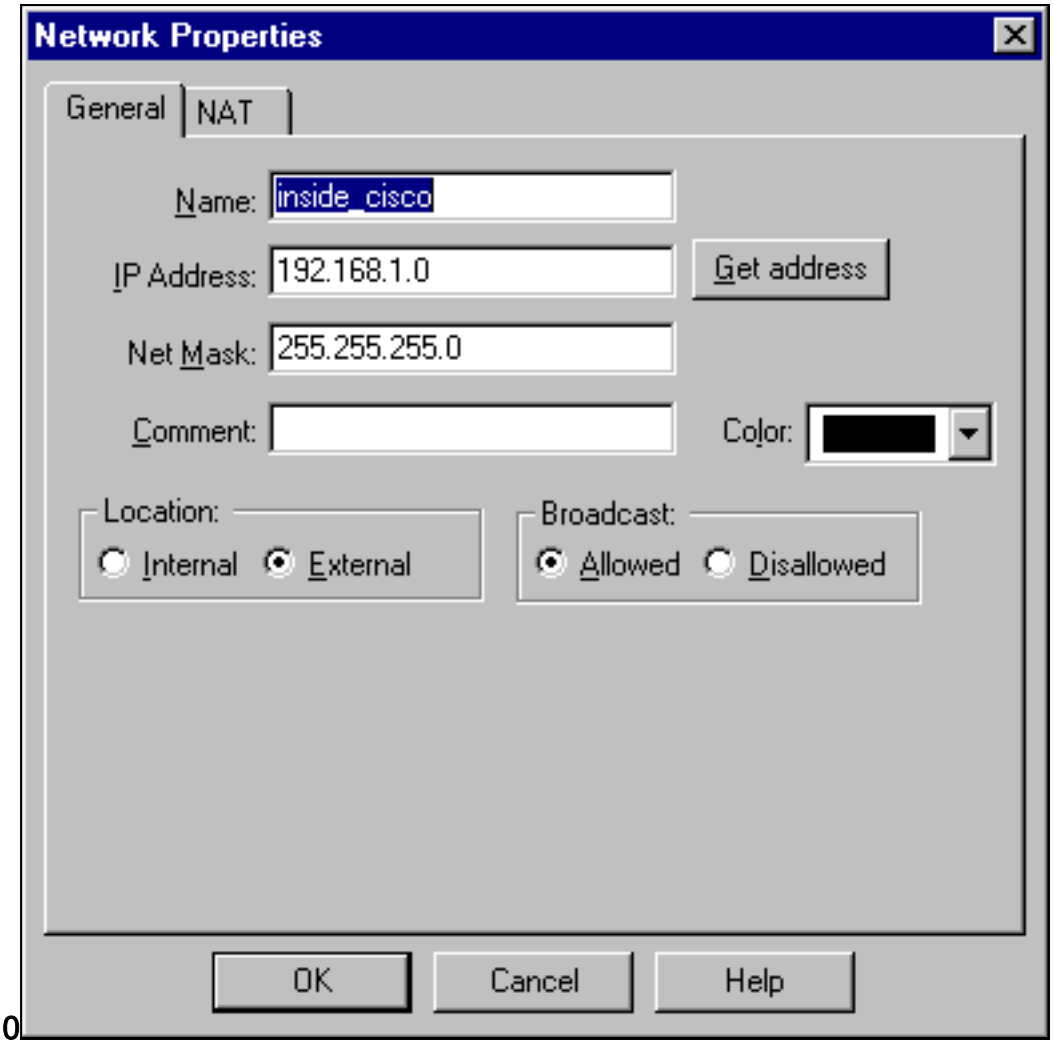


255.255.255.0

3. Manage(**관리**) > **Network objects(네트워크 개체) > Edit(편집)를** 선택하여 PIX가 이 명령에서 가리키는 게이트웨이("RTPCPVPN" Checkpoint) 엔드포인트의 개체를 편집합니다. **암호화 맵 이름 # set peer ip_address**위치(Location)에서 내부(Internal)를 **선택합니다**. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다. Modules Installed(모듈 설치됨)에서 **VPN-1 및 FireWall-1** 확인란을 선택하고 **Management Station(관리 스테이션)** 확인란을 선택합니다

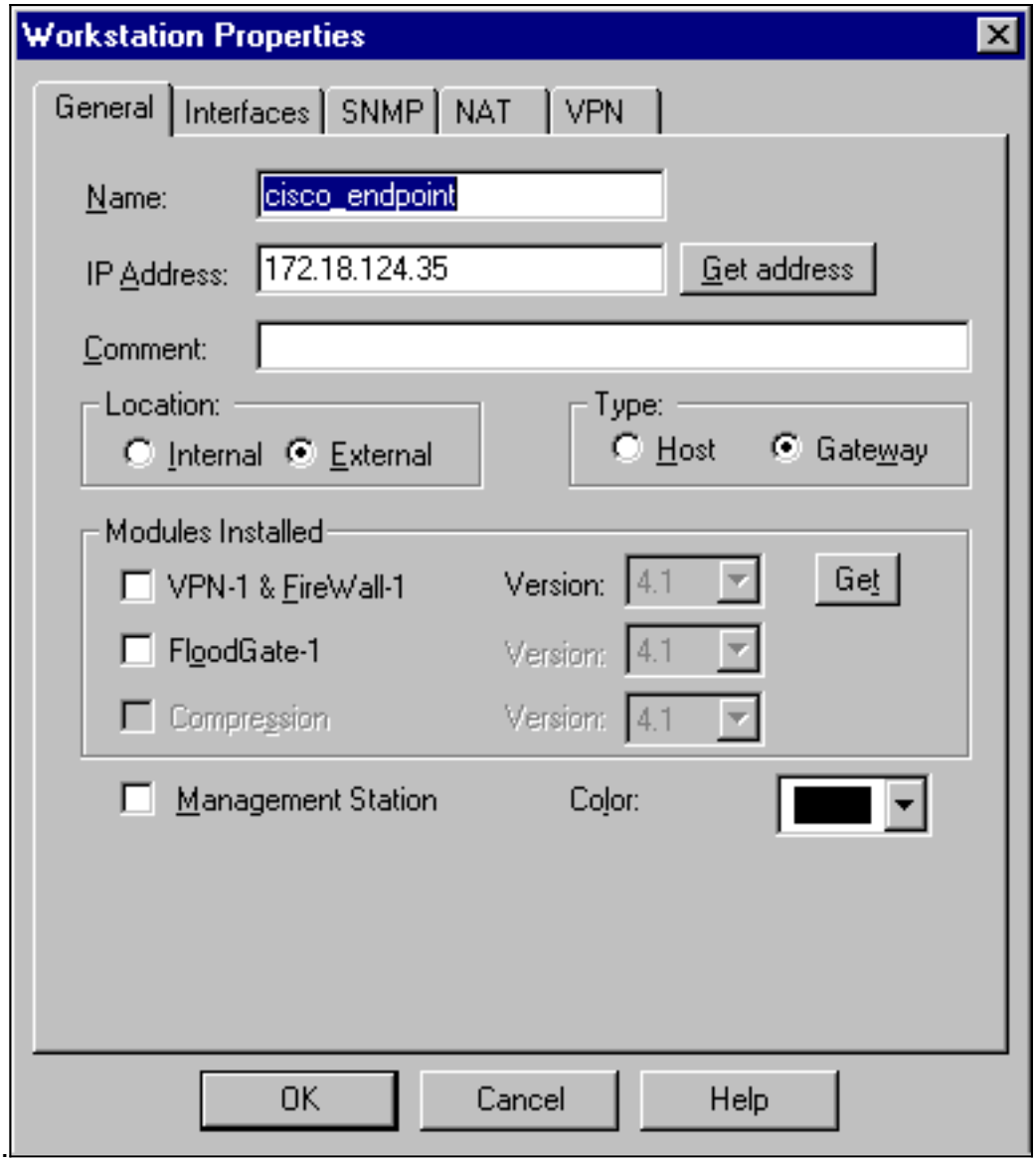


4. Manage(**관리**) > **Network objects(네트워크 개체)** > New(새로 만들기) > **Network(네트워크)**를 선택하여 PIX 뒤에 있는 외부("inside_cisco") 네트워크에 대한 개체를 구성합니다.이는 다음 PIX 명령의 소스(첫 번째) 네트워크와 일치해야 합니다. **access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**



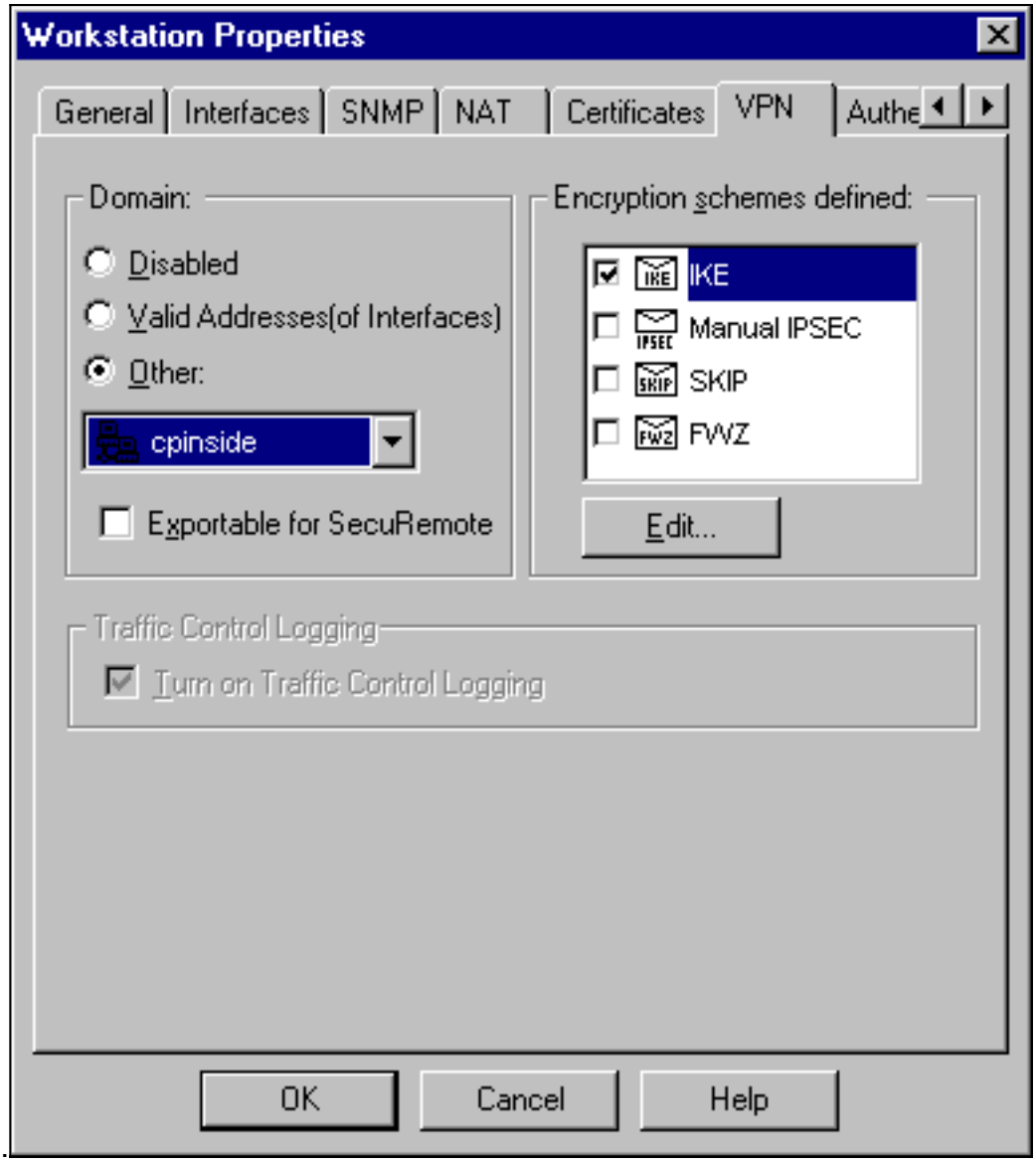
255.255.255.0

5. Manage(**관리**) > **Network objects(네트워크 개체)** > New(새로 만들기) > **Workstation**을 선택하여 외부("cisco_endpoint") PIX 게이트웨이에 대한 개체를 추가합니다. 이 명령이 적용되는 PIX 인터페이스입니다. **암호화 맵** ***이름*** **인터페이스 외부**위치에서 **외부**를 선택합니다. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다.**참고:** VPN-1/FireWall-1 확인란을 선택하지 마십



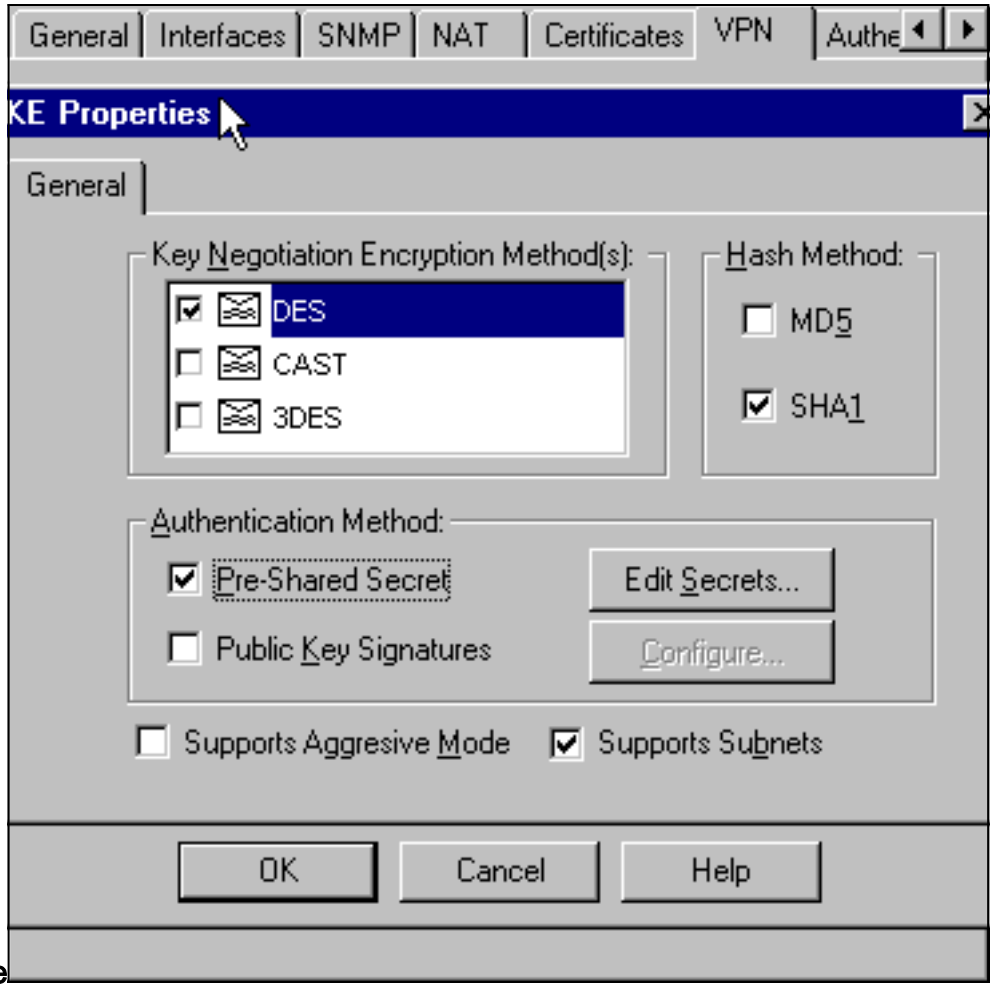
시오.

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**



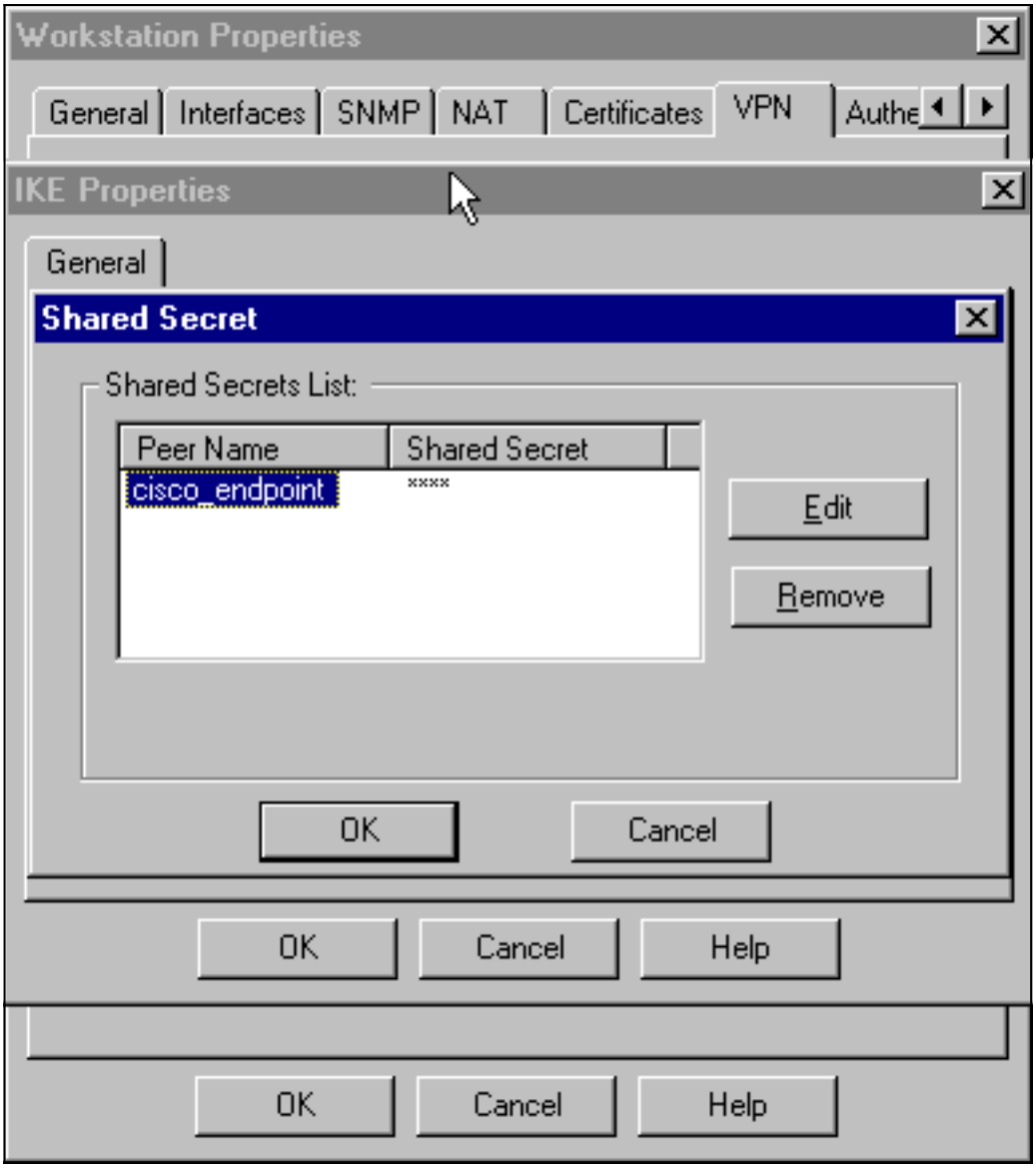
니다.

7. DES 암호화를 위한 IKE 속성을 이 명령에 동의하도록 변경합니다.**isakmp 정책 # 암호화 des**
8. 이 명령에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.**isakmp 정책 # 해시 sha**다음 설정을 변경합니다.Aggressive **Mode를 선택 취소합니다**.서브넷 **지원** 확인란**을** 선택합니다 .Authentication Method(인증 방법)에서 **Pre-Shared Secret(사전 공유 암호)** 확인란을 선택합니다. 이 명령은 다음과 같습니다.**isakmp 정책 # 인증 pre-**

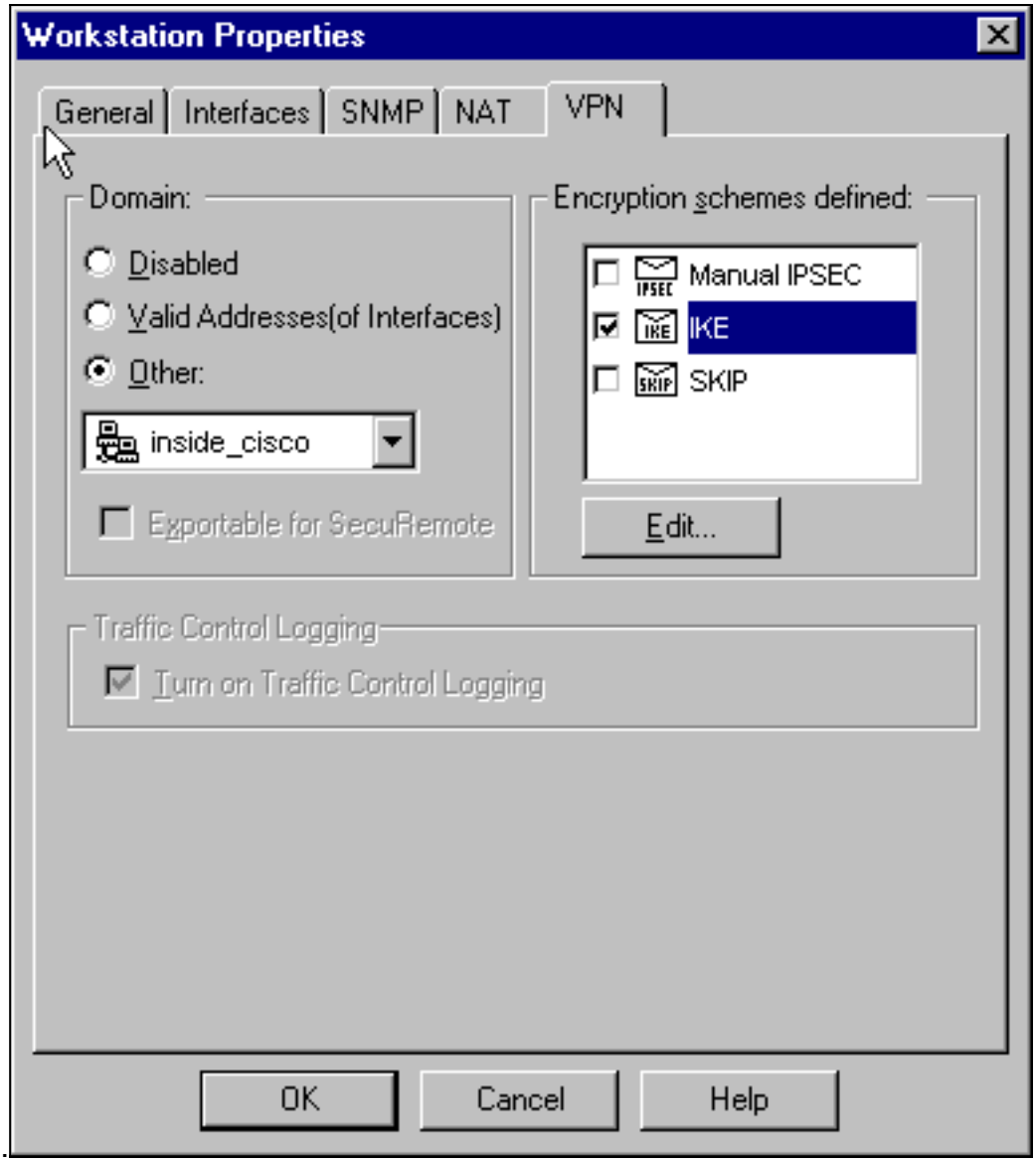


share

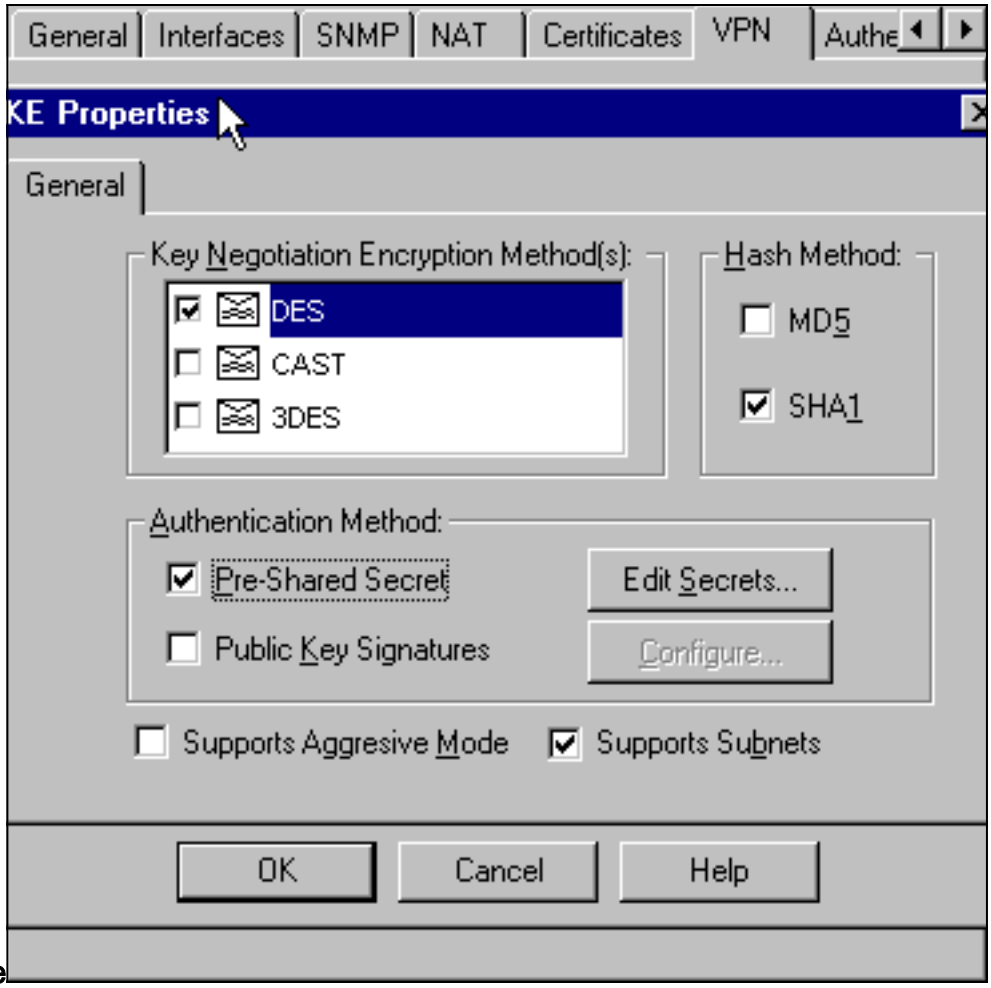
9. Edit **Secrets**(비밀 수정)를 클릭하여 PIX 명령에 동의하도록 사전 공유 키를 설정합니다 .**isakmp 키** ***키*** **주소 넷마스크** ***넷마스크***



10. "cisco_endpoint" VPN 탭을 편집하려면 **Manage > Network Objects > Edit**를 선택합니다. Domain(도메인)에서 **Other(기타)**를 선택한 다음 PIX 네트워크의 내부("inside_cisco"라고 함)를 선택합니다. Encryption schemes defined(정의된 암호화 체계)에서 **IKE**를 선택한 다음 Edit(수정)를 **클릭합니다**

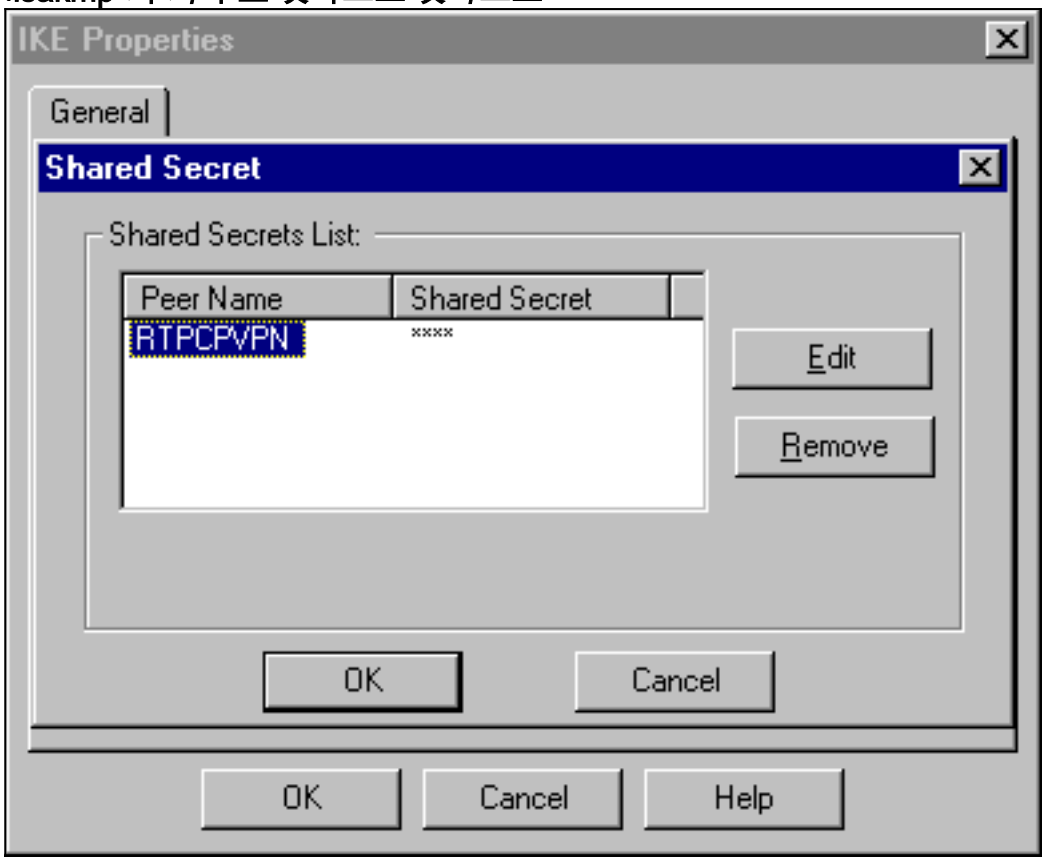


11. IKE 속성 DES 암호화를 이 명령에 동의하도록 변경합니다.**isakmp 정책 # 암호화 des**
12. 이 명령에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.**crypto isakmp policy # hash sha**다음 설정을 변경합니다.Aggressive **Mode를 선택 취소합니다**.서브넷 **지원** 확인란**을** 선택합니다.Authentication Method(인증 방법)에서 **Pre-Shared Secret(사전 공유 암호)** 확인란을 선택합니다. 이 작업은 다음 명령에 동의합니다.**isakmp 정책 # 인증 pre-**

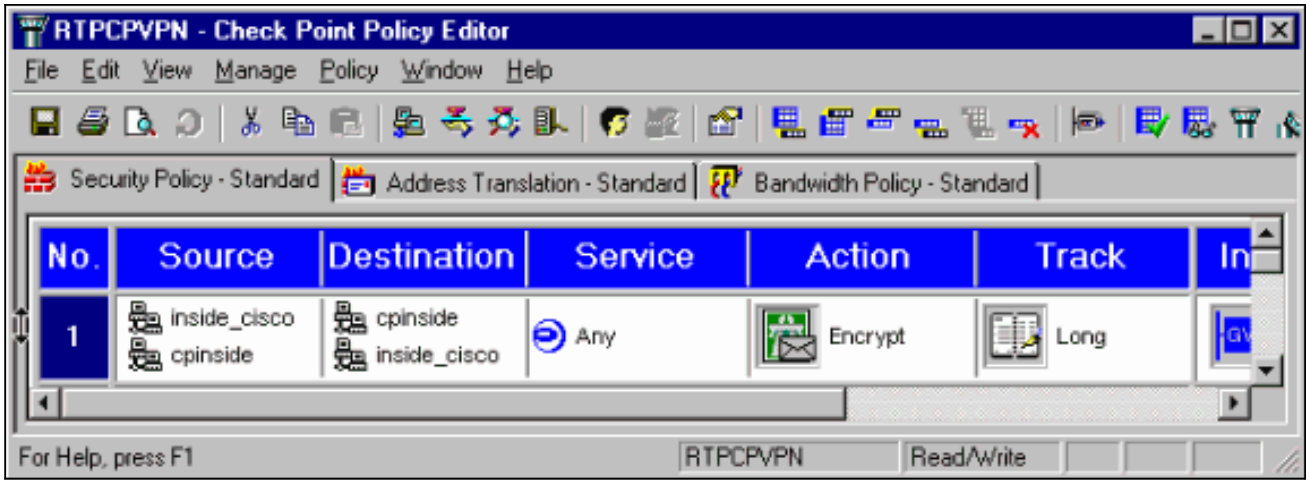


share

13. Edit **Secrets**(비밀 수정)를 클릭하여 이 PIX 명령에 동의하도록 사전 공유 키를 설정합니다 .**isakmp 키** *키* **주소 넷마스크** *넷마스크*

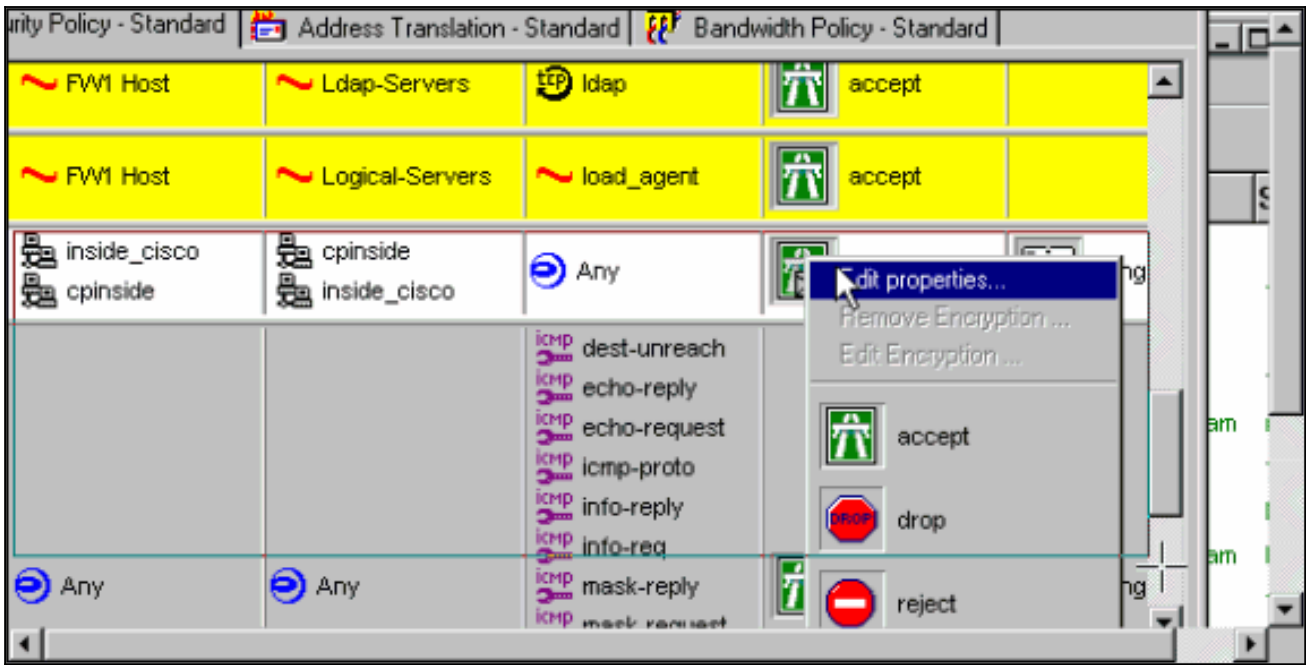


14. Policy Editor(정책 편집기) 창에서 Source(소스)와 Destination(대상)을 모두 "inside_cisco" 및 "cpinside"(양방향)로 포함하는 규칙을 삽입합니다. Set **Service=Any**, **Action=Encrypt** 및 **Track=Long**.

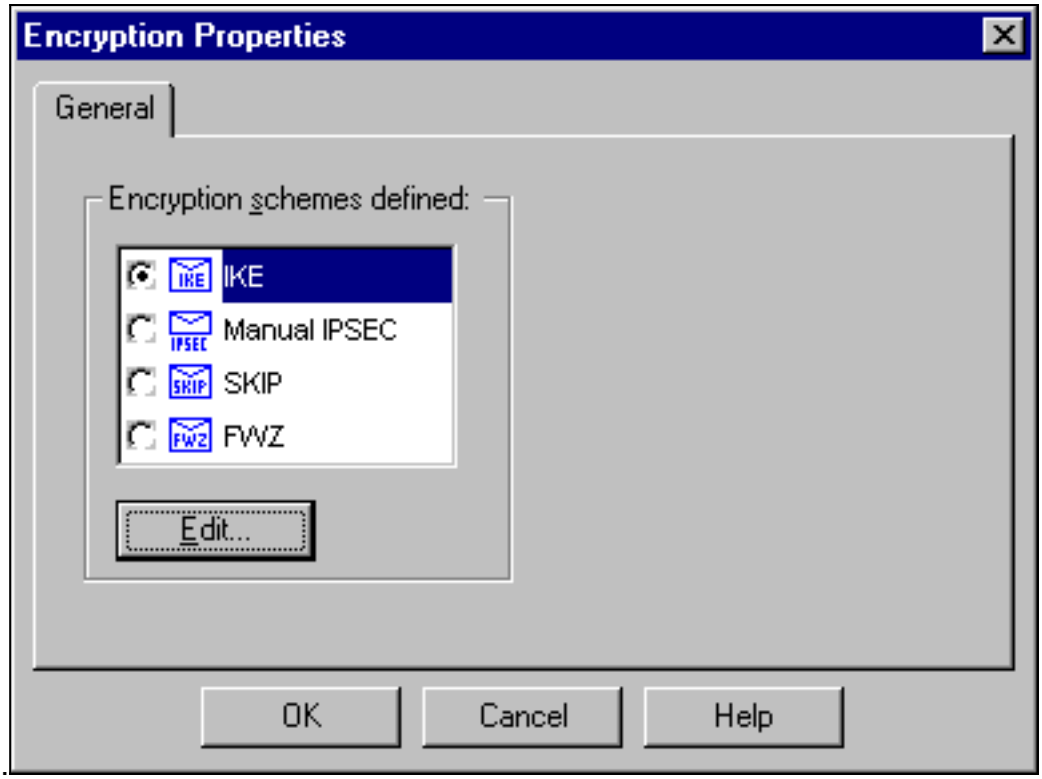


15. Action(작업) 제목 아래에서 녹색 **Encrypt(암호화)** 아이콘을 클릭하고 **Edit properties(속성 편집)를** 선택하여 암호화 정책을 구성합니다

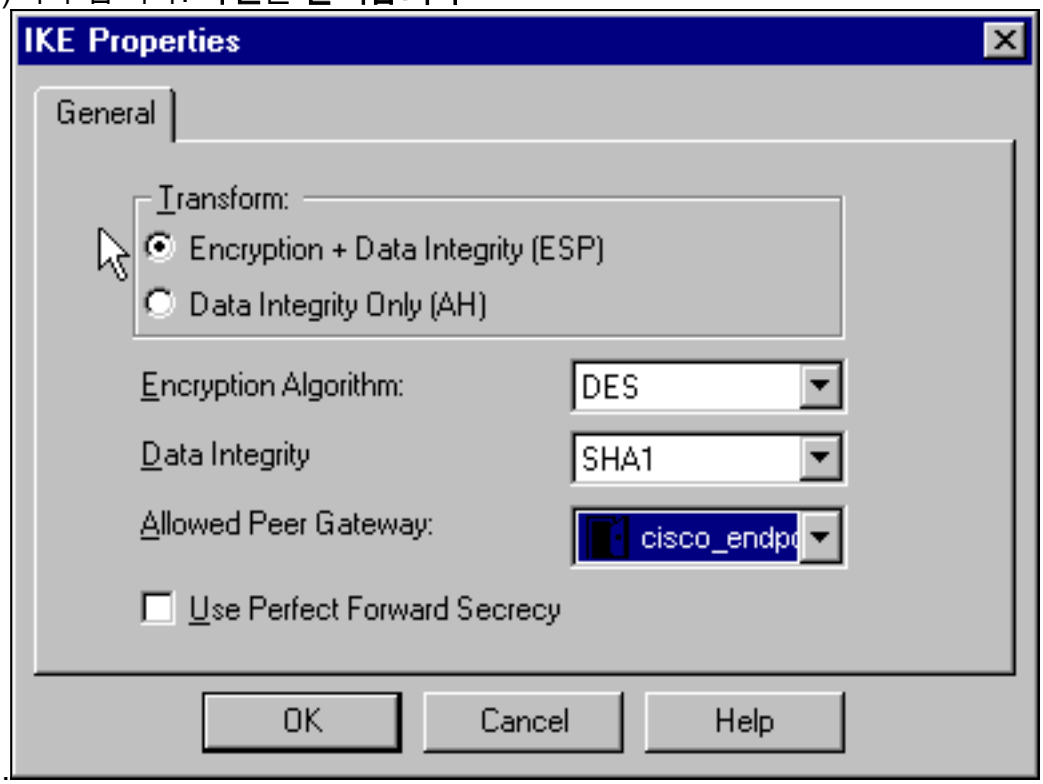
.



16. IKE**를** 선택한 다음 Edit를 **클릭합니다**



17. IKE Properties(IKE 속성) 화면에서 다음 속성을 변경하여 이 명령의 PIX IPSec 변환과 일치시킵니다.**crypto ipsec transform-set myset esp-des esp-sha-hmac**Transform(변형)에서 **Encryption + Data Integrity (ESP)**를 선택합니다. 암호화 알고리즘은 **DES**, 데이터 무결성은 **SHA1**이어야 하며, 허용된 피어 게이트웨이는 외부 PIX 게이트웨이("cisco_endpoint"라고 함)여야 합니다. **확인**을 **클릭합니다**



18. Checkpoint를 구성한 후 변경 사항을 적용하려면 Checkpoint 메뉴에서 Policy(**정책**) > **Install(설치**)을 선택합니다.

debug, show 및 clear 명령

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

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

debug 명령을 실행하기 전에 Debug Commands에 대한 중요 정보를 참조하십시오.

Cisco PIX 방화벽

- **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.
- **show crypto isakmp sa** - 피어에서 현재 IKE SA(Security Association)를 모두 봅니다.
- **show crypto ipsec sa** - 현재 보안 연결에서 사용하는 설정을 봅니다.
- **clear crypto isakmp sa** - (컨피그레이션 모드에서) 모든 활성 IKE 연결을 지웁니다.
- **clear crypto ipsec sa** - (컨피그레이션 모드에서) 모든 IPSec 보안 연결을 삭제합니다.

체크포인트:

14단계에 표시된 정책 편집기 창에서 추적 기능이 Long으로 설정되었으므로 거부된 트래픽은 로그 뷰어에 빨간색으로 표시됩니다. 다음을 입력하여 자세한 디버그 정보를 얻을 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.

다음 명령을 사용하여 체크포인트에서 SA를 지울 수 있습니다.

```
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
```

예에 답하십시오. 프롬프트에서 중단될 수 있습니다.

문제 해결

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

네트워크 요약

Checkpoint의 암호화 도메인에서 서로 인접한 여러 개의 내부 네트워크가 구성된 경우, 해당 디바

이스는 흥미로운 트래픽과 관련하여 이를 자동으로 요약할 수 있습니다. PIX의 암호화 ACL이 일치하도록 구성되지 않은 경우 터널이 실패할 수 있습니다. 예를 들어 10.0.0.0 /24 및 10.0.1.0 /24의 내부 네트워크가 터널에 포함되도록 구성된 경우 10.0.0.0 /23으로 요약할 수 있습니다.

PIX의 샘플 디버그 출력

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
cisco_endpoint# term mon
cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.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

ISAKMP (0): processing NONCE payload. message ID = 2112882468
```

```
ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
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= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR2303: 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= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
    Crypto map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #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 #send errors 0, #recv errors 0

     local crypto endpt.: 172.18.124.35,
```

```
     remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 0, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   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: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #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, ipsec overhead 56, media mtu 1500
     current outbound spi: ebc8c823

     inbound esp sas:
      spi: 0x9d71f29c(2641490588)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xebc8c823(3955804195)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 4, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

cisco_endpoint# sho cry is sa
        dst             src         state     pending    created
  172.18.124.157   172.18.124.35    QM_IDLE         0           2
```

관련 정보

- PIX 지원 페이지
- PIX 명령 참조
- RFC(Request for Comments)
- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- PIX 5.2: IPSec 구성
- PIX 5.3: IPSec 구성
- IPSec 지원 페이지
- Technical Support - Cisco Systems