Cisco Secure PIX Firewall과 Checkpoint NG 방화벽 간의 IPSec 터널 구성

목차

소개

이 문서에서는 두 프라이빗 네트워크 간에 통신하기 위해 사전 공유 키를 사용하여 IPsec 터널을 구성하는 방법을 보여 줍니다. 이 예에서 통신 네트워크는 Cisco Secure PIX Firewall 내의 192.168.10.x 프라이빗 네트워크와 CheckpointTM NG(Next Generation) 방화벽 내의 10.32.x.x 프라이빗 네트워크입니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- PIX 내부 및 CheckpointTM NG 내부에서 인터넷(172.18.124.x 네트워크로 표시)으로 이동하는 트래픽은 이 컨피그레이션을 시작하기 전에 플로우되어야 합니다.
- 사용자는 IPsec 협상에 익숙해야 합니다. 이 프로세스는 2개의 IKE(Internet Key Exchange) 단계를 포함하여 5단계로 나눌 수 있습니다.IPsec 터널은 흥미로운 트래픽에 의해 시작됩니다. 트래픽은 IPsec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.IKE 1단계에서 IPsec 피어는 설정된 IKE SA(Security Association) 정책을 협상합니다. 피어가 인증되면 ISAKMP(Internet

Security Association and Key Management Protocol)를 사용하여 보안 터널이 생성됩니다.IKE 2단계에서 IPsec 피어는 IPsec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다. 공유 정책의 협상은 IPsec 터널의 설정 방법을 결정합니다.IPsec 터널이 생성되고 IPsec 변형 집합에 구성된 IPsec 매개변수를 기반으로 IPsec 피어 간에 데이터가 전송됩니다.IPsec 터널은 IPsec SA가 삭제되거나 수명이 만료될 때 종료됩니다.

사용되는 구성 요소

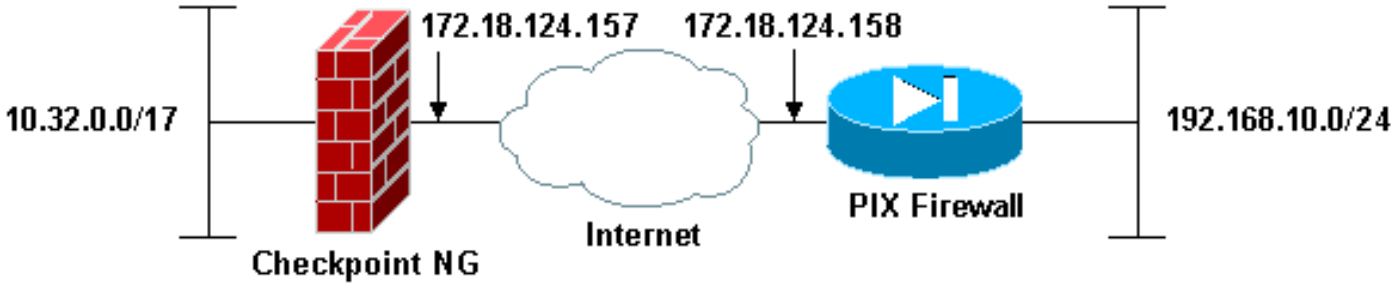
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 소프트웨어 버전 6.2.1
- CheckpointTM NG 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.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

PIX 구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 방법을 설명합니다.

PIX 컨피그레이션

```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
```

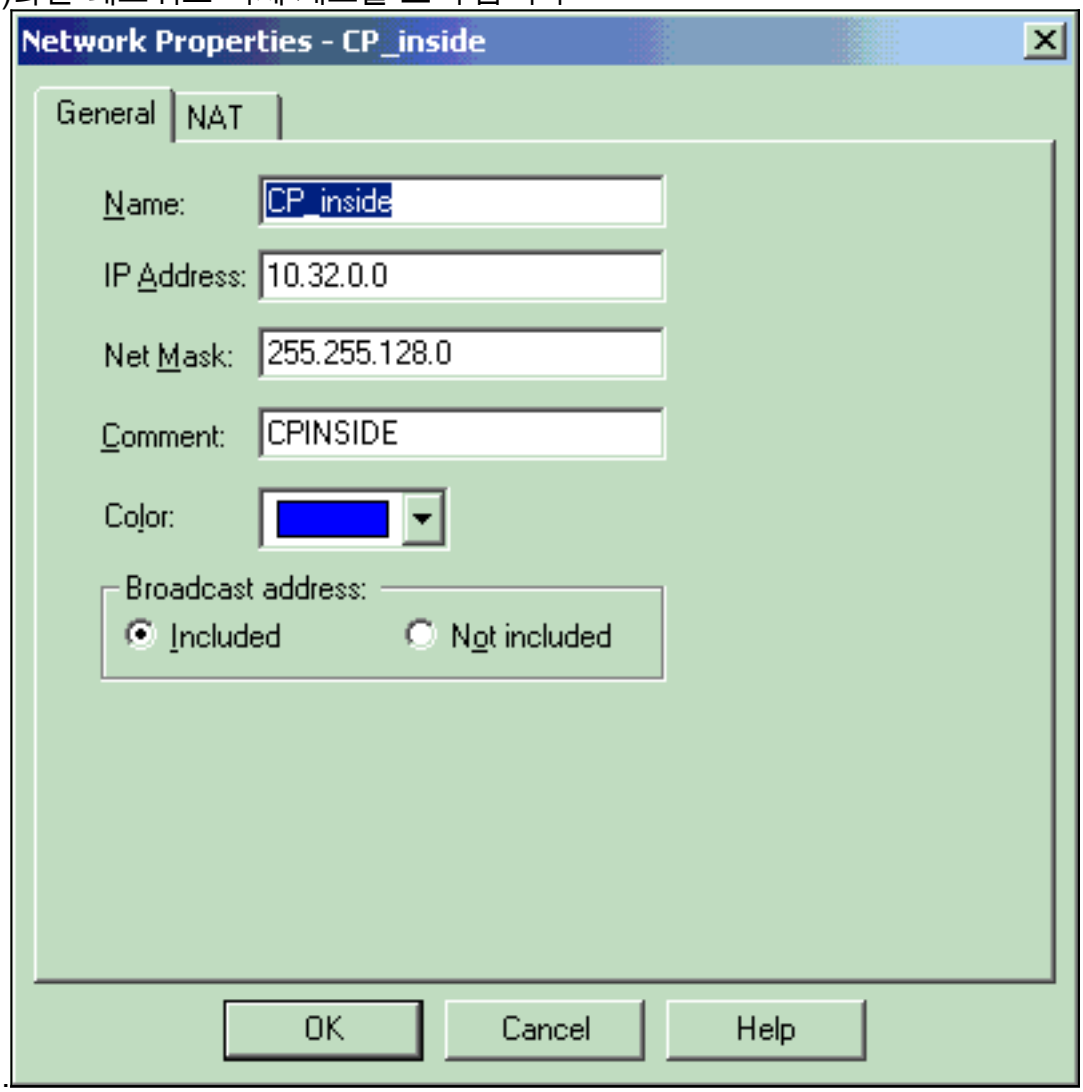
```
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Interesting traffic to be encrypted to the
Checkpoint™ NG. access-list 101 permit ip 192.168.10.0
255.255.255.0 10.32.0.0 255.255.128.0
!--- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint™ NG. access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.158 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not perform NAT on traffic to the Checkpoint™
NG. nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Permit all inbound IPsec authenticated cipher
sessions. sysopt connection permit-ipsec
no sysopt route dnat
!--- Defines IPsec encryption and authentication
algorithms. crypto ipsec transform-set rtptac esp-3des
esp-md5-hmac
!--- Defines crypto map. crypto map rtprules 10 ipsec-
isakmp
crypto map rtprules 10 match address 101
crypto map rtprules 10 set peer 172.18.124.157
crypto map rtprules 10 set transform-set rtptac
!--- Apply crypto map on the outside interface. crypto
map rtprules interface outside
isakmp enable outside
!--- Defines pre-shared secret used for IKE
authentication. isakmp key ******** address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
```

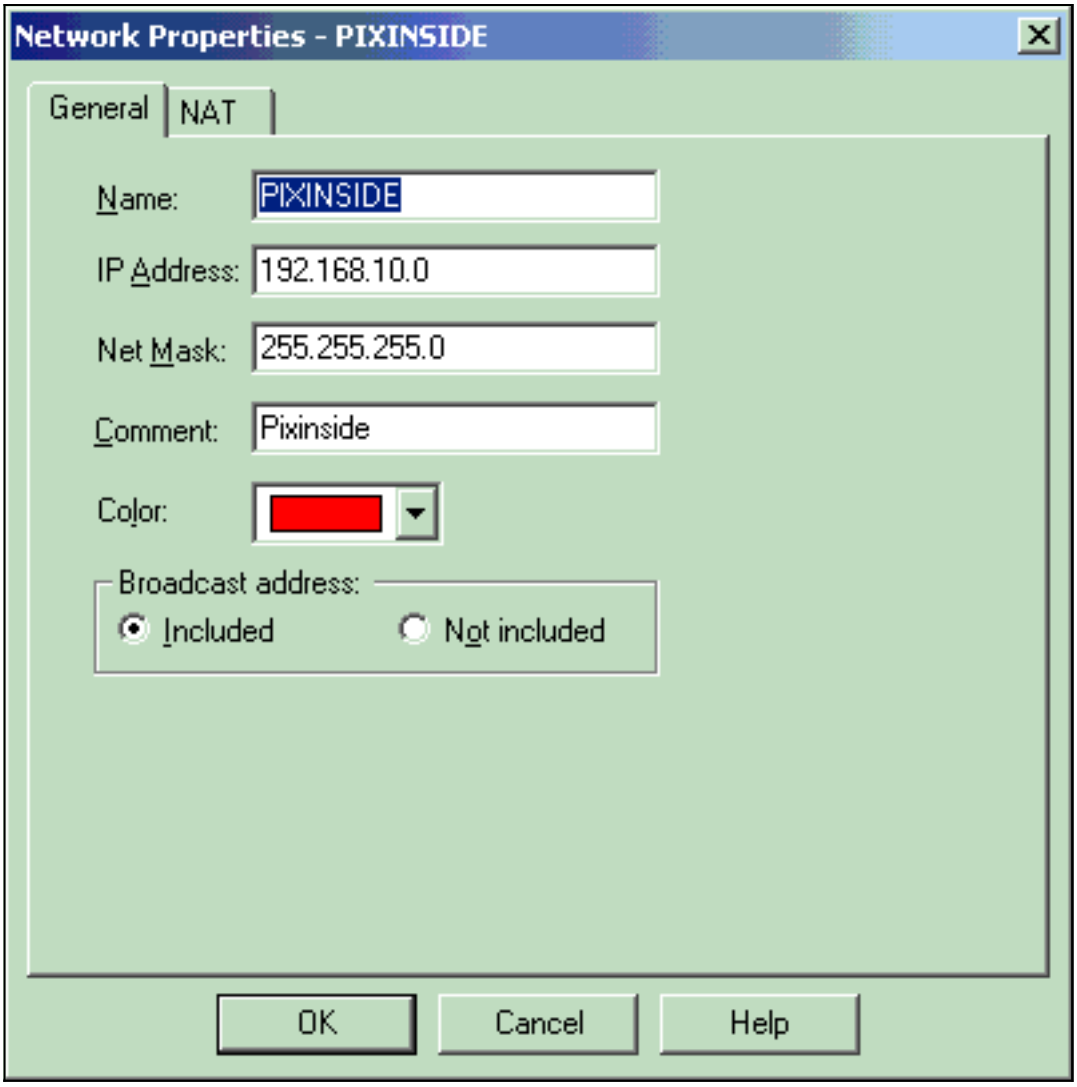
```
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end
```

체크포인트 NG 구성

네트워크 객체 및 규칙은 CheckpointTM NG에 정의되어 설정할 VPN 컨피그레이션과 관련된 정책을 구성합니다. 그런 다음 CheckpointTM NG 정책 편집기를 사용하여 컨피그레이션의 CheckpointTM NG 측을 완료합니다.

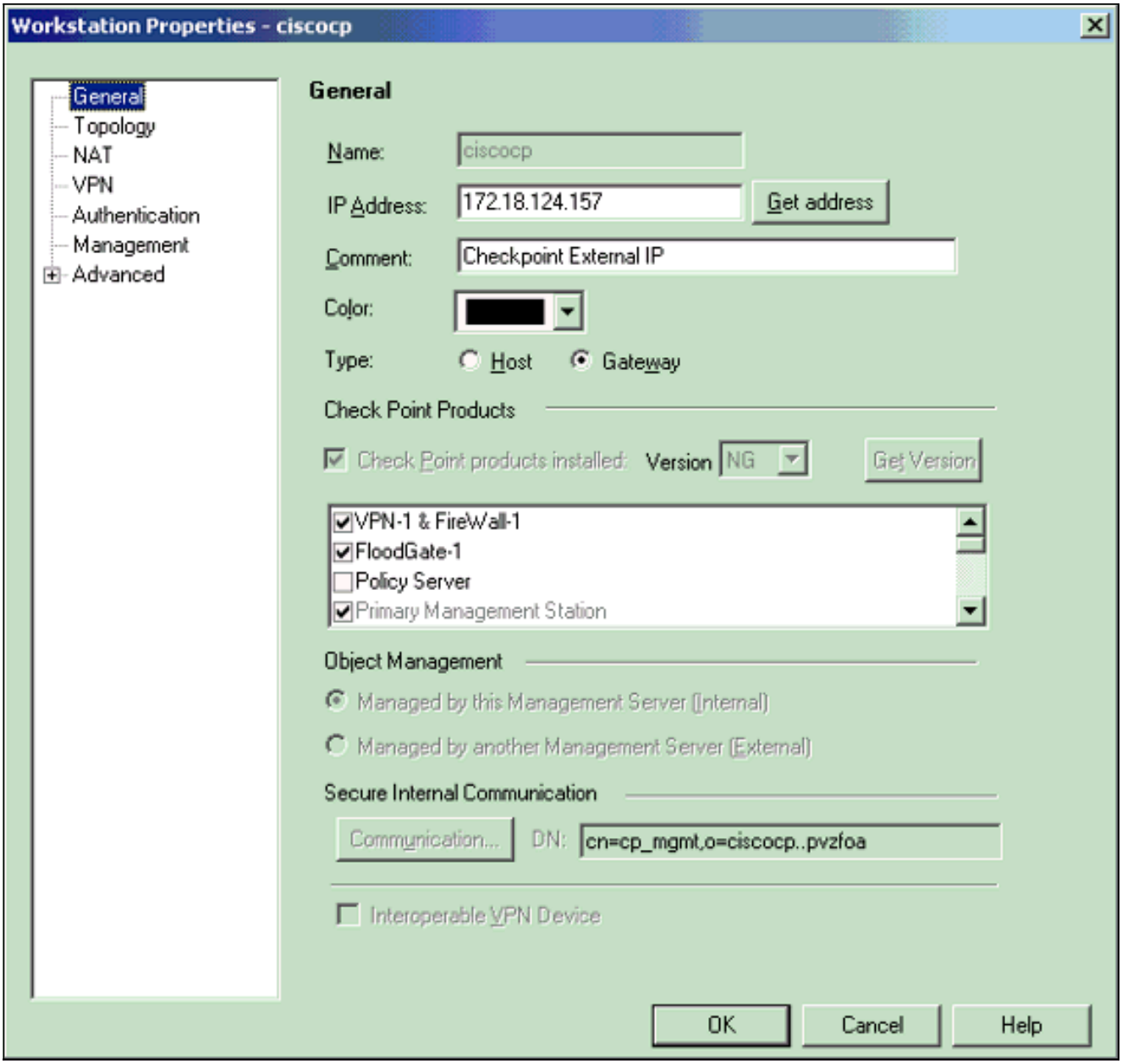
1. Checkpoint 네트워크 및 관심 있는 트래픽을 암호화하는 PIX Firewall 네트워크를 위한 두 개의 네트워크 객체를 생성합니다.이렇게 하려면 **관리 > 네트워크 객체**를 선택한 다음 **새로 만들기 > 네트워크**를 선택합니다. 적절한 네트워크 정보를 입력한 다음 **확인**을 클릭합니다.다음 예에서는 CP_Inside(CheckpointTM NG의 내부 네트워크) 및 PIXINSIDE(PIX의 내부 네트워크)라는 네트워크 객체 세트를 보여 줍니다

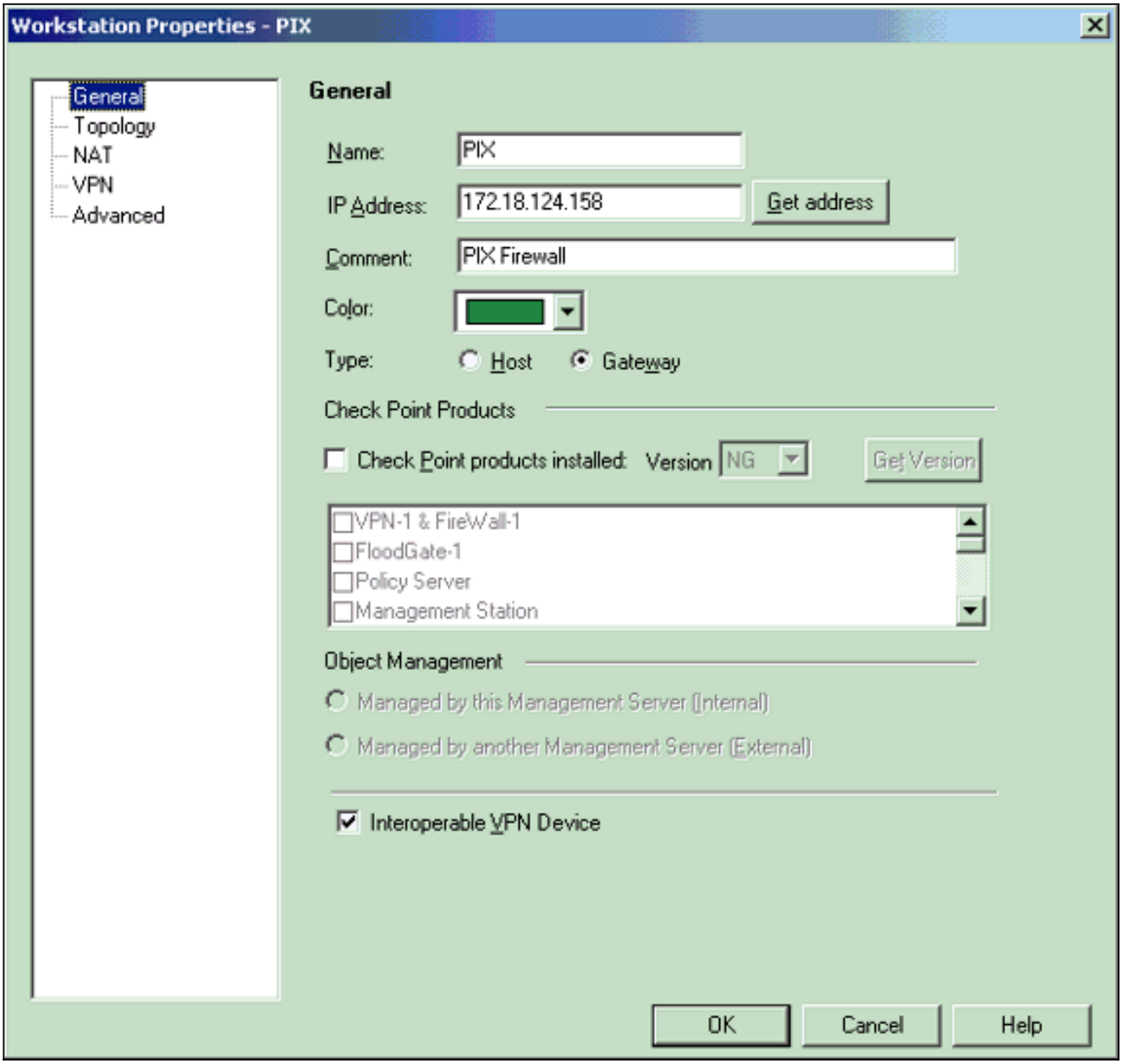




2. CheckpointTM NG 및 PIX용 워크스테이션 객체를 생성합니다. 이렇게 하려면 **관리 > 네트워크 개체 > 새로 만들기 > 워크스테이션**을 선택합니다.초기 CheckpointTM NG 설정 중에 생성된 CheckpointTM NG 워크스테이션 객체를 사용할 수 있습니다. 워크스테이션을 Gateway(게이트웨이) 및 Interoperable VPN Device(상호 운용 가능한 VPN 디바이스)로 설정하는 옵션을 선택한 다음 **OK(확인)**를 클릭합니다.다음 예에서는 ciscocp(CheckpointTM NG) 및 PIX(PIX Firewall)라는 객체의 집합을 보여 줍니다

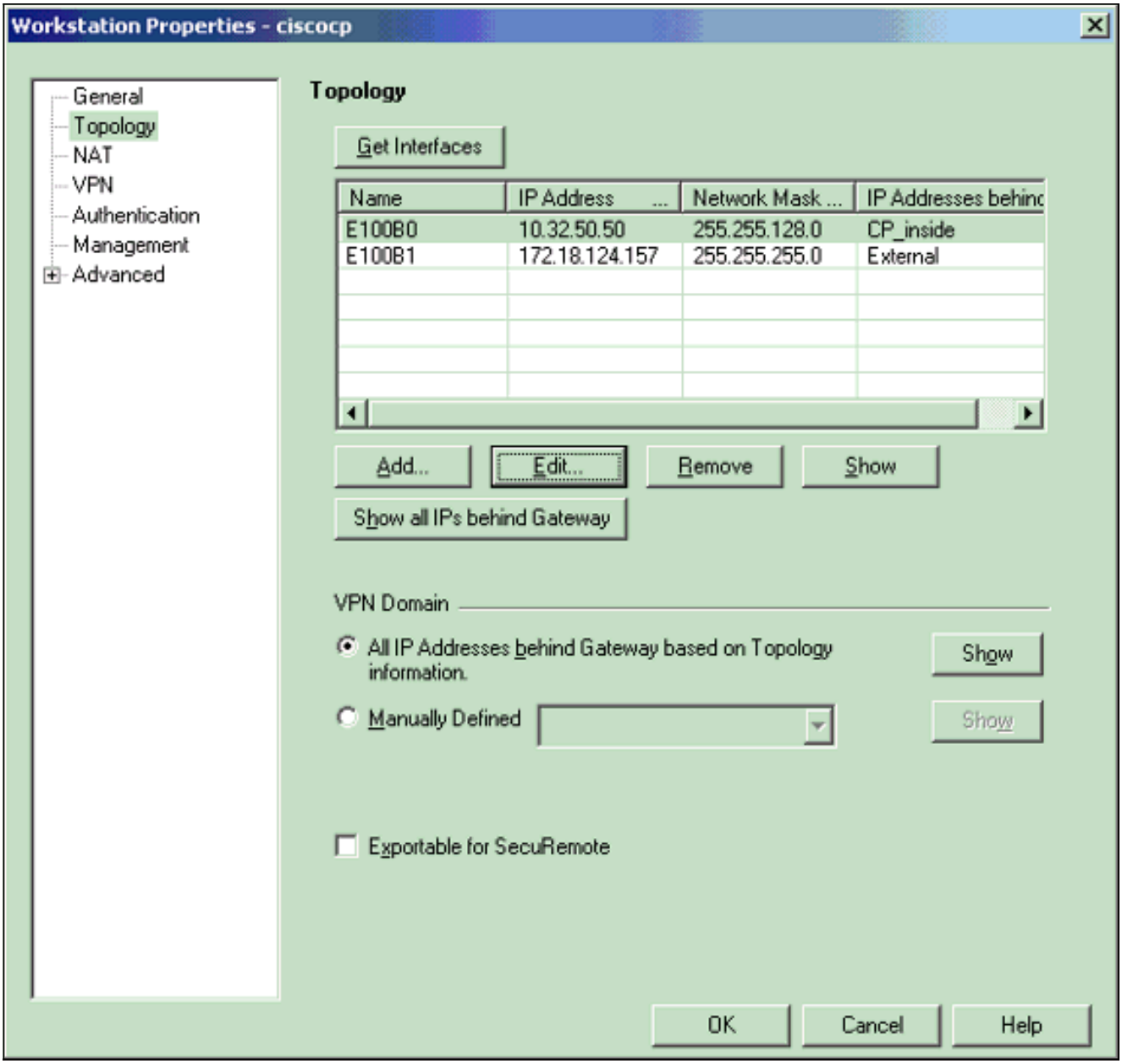
.


Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help

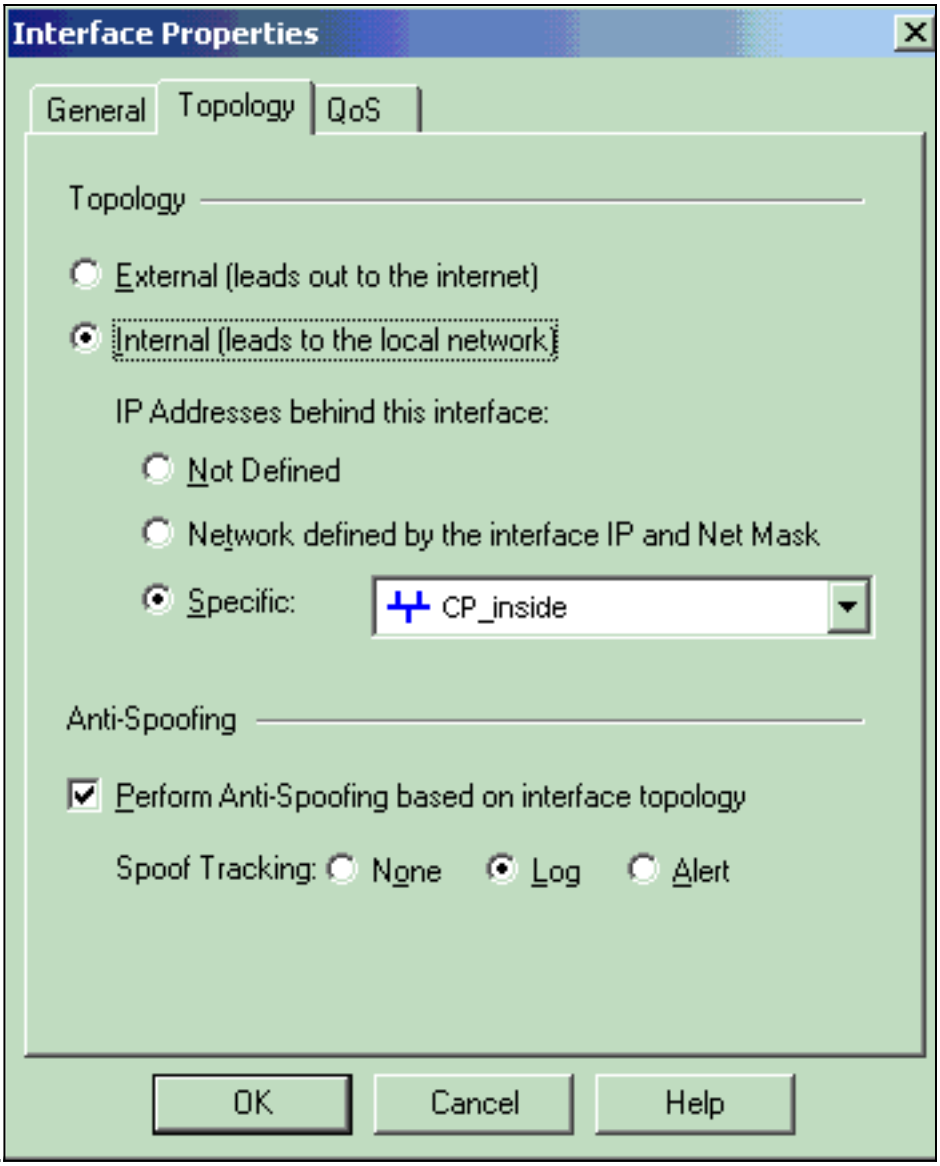


3. CheckpointTM NG 워크스테이션(이 예에서 ciscocp)에 대한 Workstation Properties(워크스테이션 속성) 창을 열려면 Manage(**관리**) > **Network objects**(**네트워크 개체**) > **Edit(편집**)를 선택합니다.창 왼쪽에 있는 선택 사항에서 Topology(토폴로지)를 선택한 다음 암호화할 네트워크를 선택합니다. Edit(**편집)**를 클릭하여 인터페이스 속성을 설정합니다

.

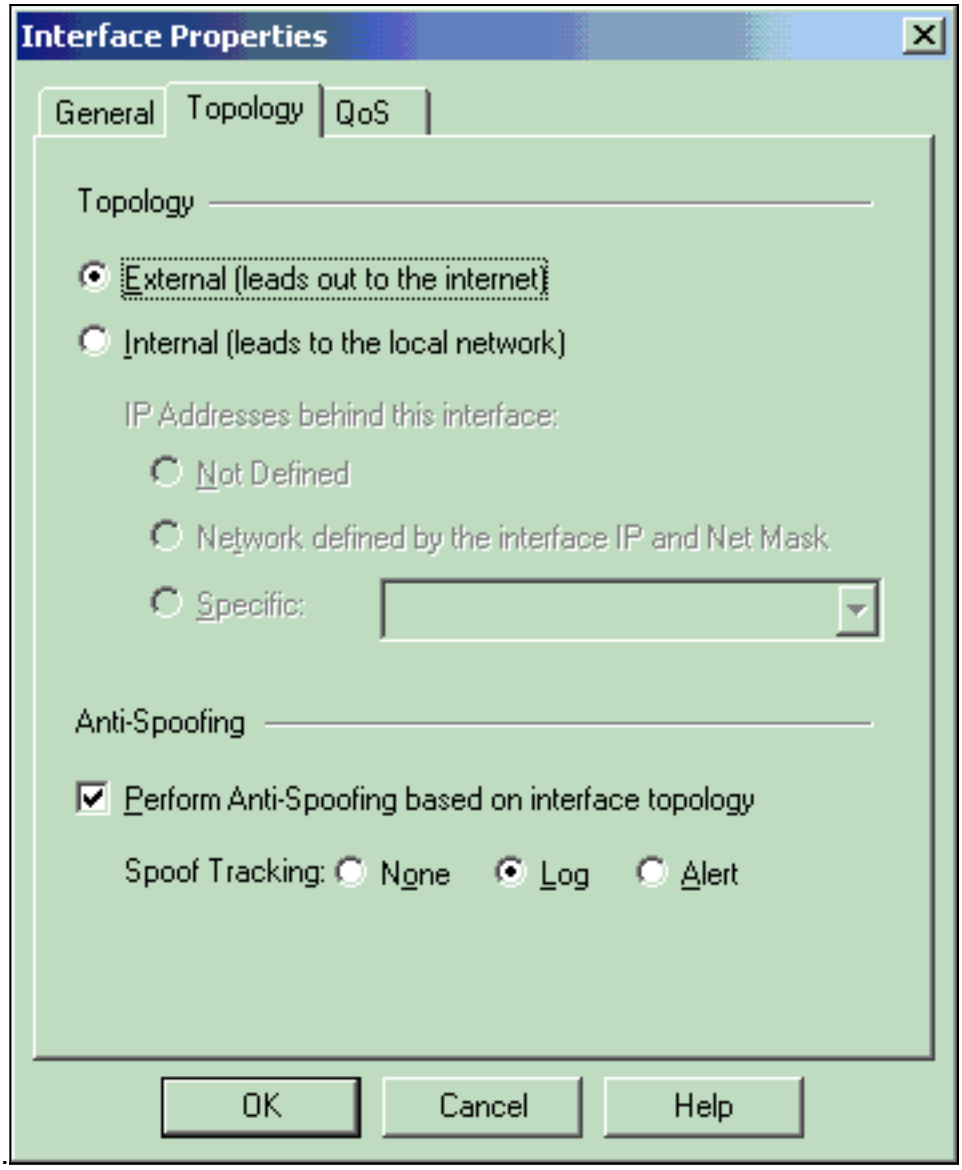


4. 워크스테이션을 internal로 지정하는 옵션을 선택한 다음 적절한 IP 주소를 지정합니다. **확인**을 **클릭합니다**.이 컨피그레이션에서는 CP_inside가 CheckpointTM NG의 내부 네트워크입니다. 여기에 표시된 토폴로지 선택은 워크스테이션을 internal로 지정하고 주소를 CP_inside로



지정합니다.

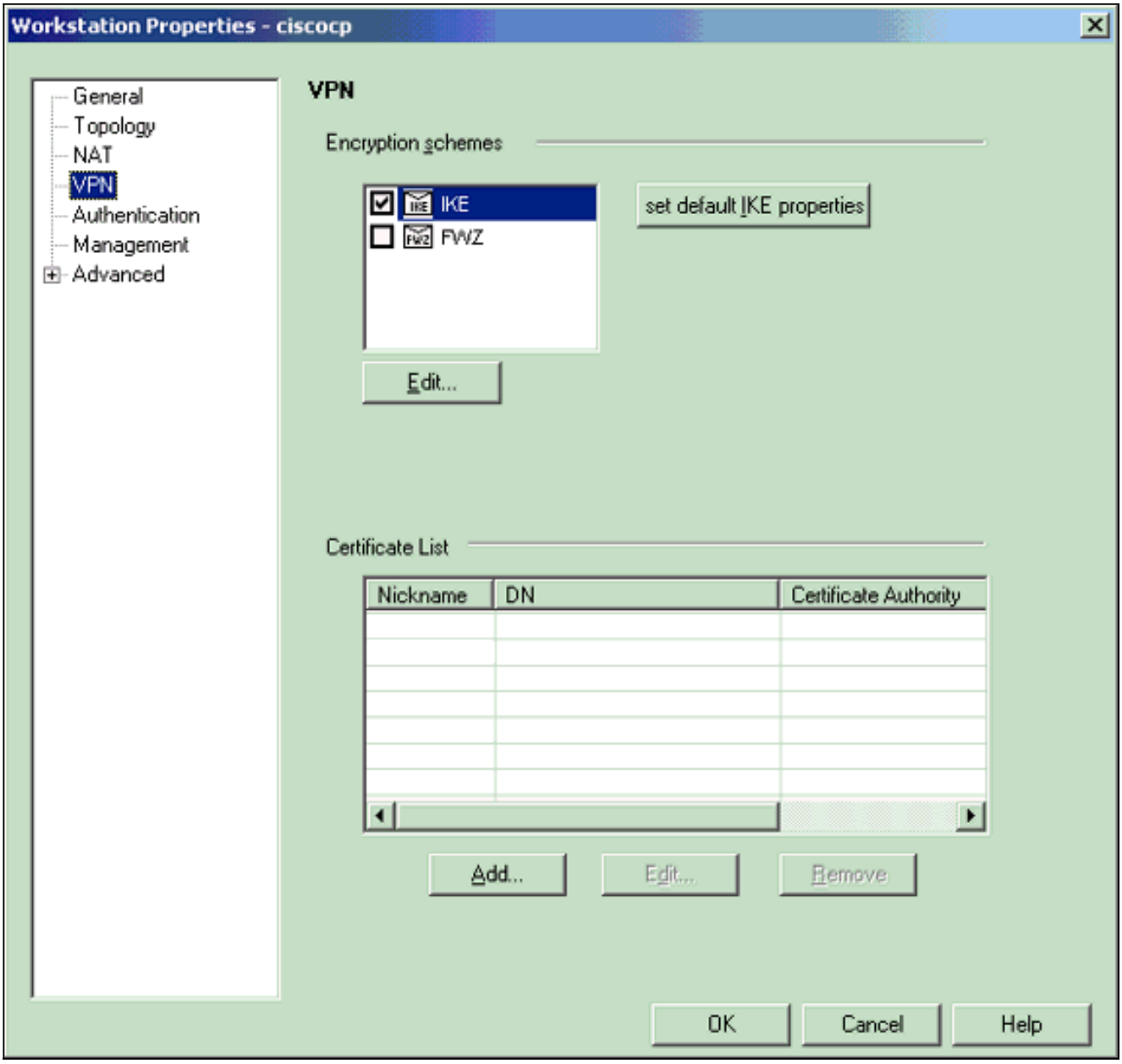
5. Workstation Properties(워크스테이션 속성) 창에서 인터넷으로 연결되는 CheckpointTM NG의 외부 인터페이스를 선택한 다음 Edit(**편집**)를 클릭하여 인터페이스 속성을 설정합니다. 토폴로지를 외부로 지정하려면 옵션을 선택한 다음 **확인**을 클릭합니다



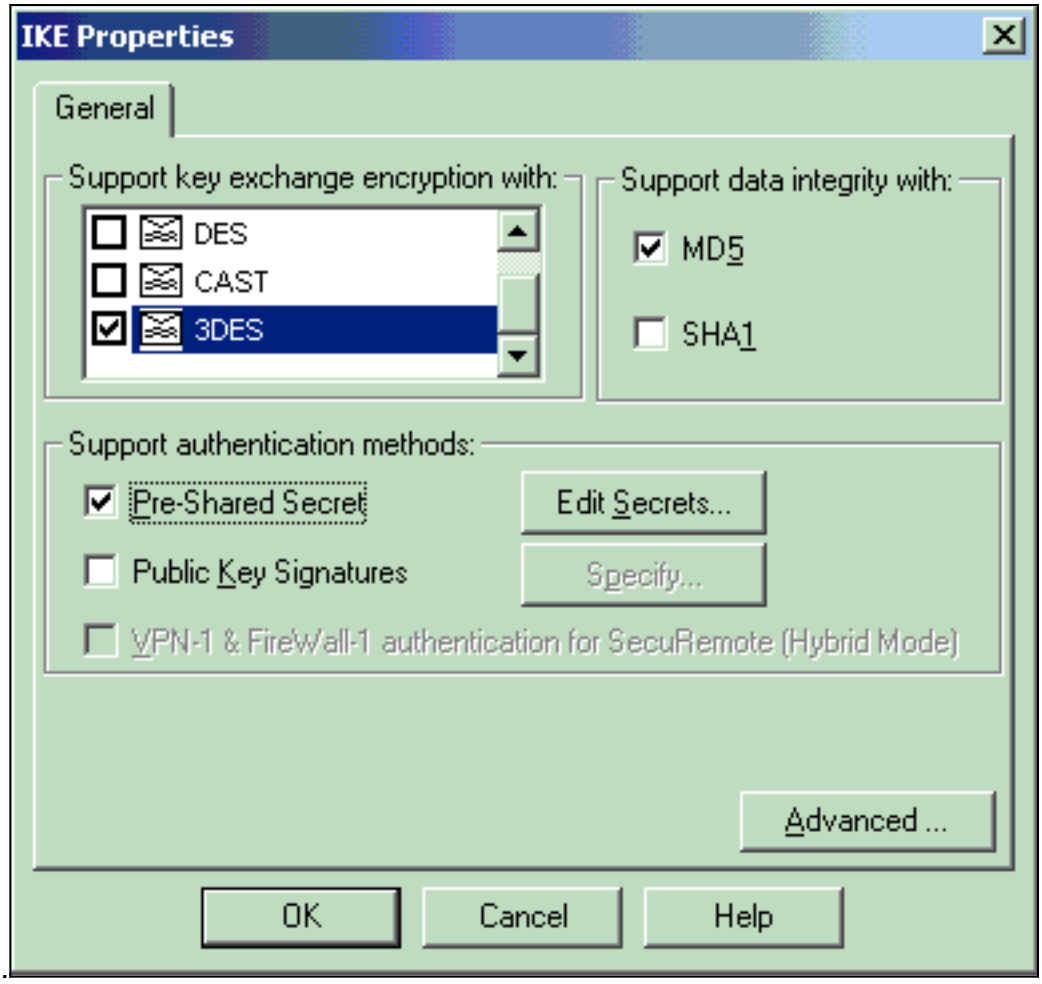
.

6. CheckpointTM NG의 Workstation Properties(워크스테이션 속성) 창의 왼쪽 선택 사항에서 VPN을 선택한 다음 암호화 및 인증 알고리즘에 대한 IKE 매개변수를 선택합니다. Edit(**수정**)를 클릭하여 IKE 속성을 구성합니다

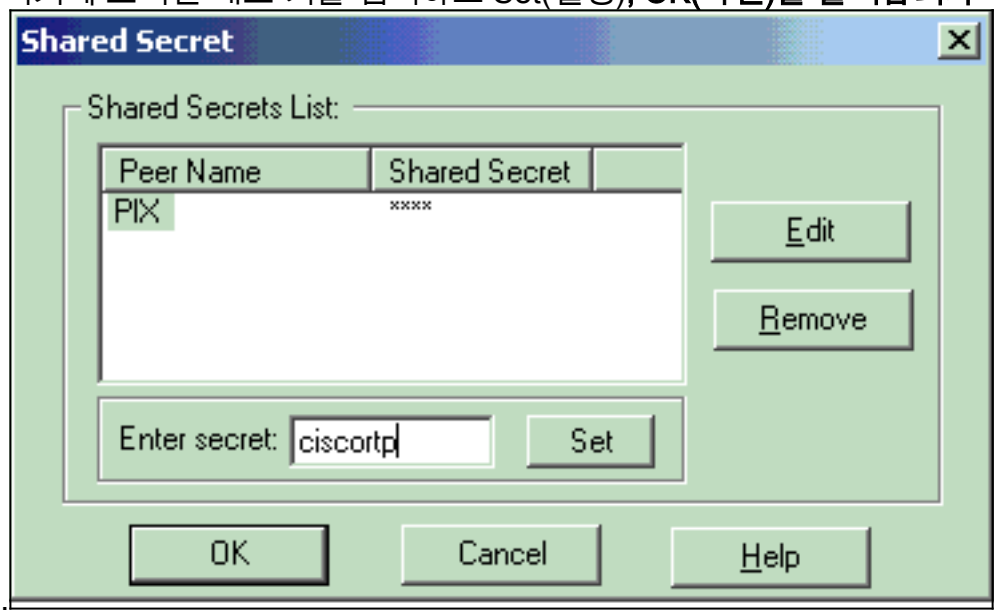
.



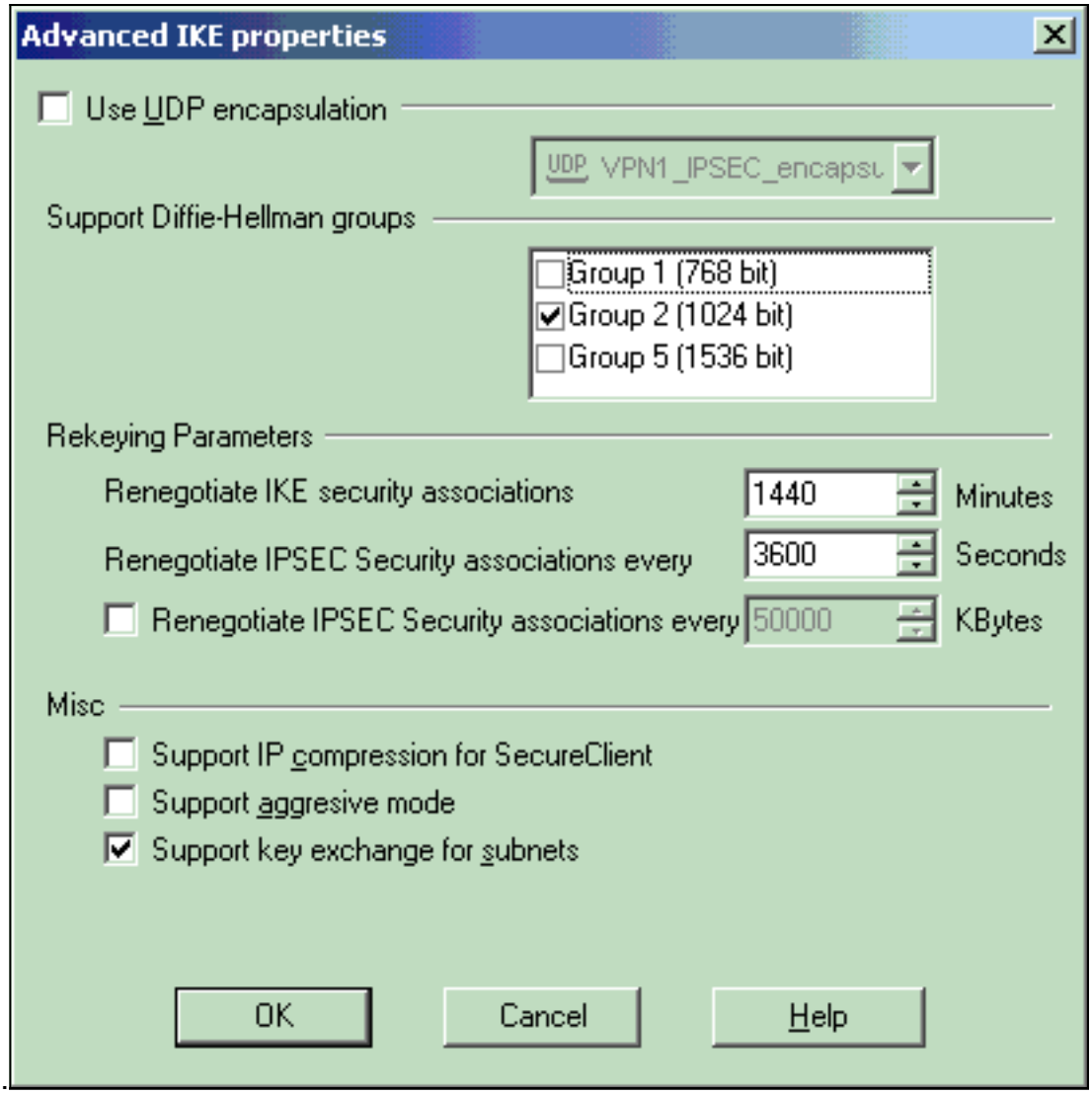
7. IKE 속성을 구성합니다.IKE 속성이 isakmp **policy # encryption 3des** 명령과 호환되도록 **3DES** 암호화 옵션**을** 선택합니다.IKE 속성이 crypto isakmp **policy # hash md5** 명령과 호환되도록 **MD5** 옵션**을 선택합니다**



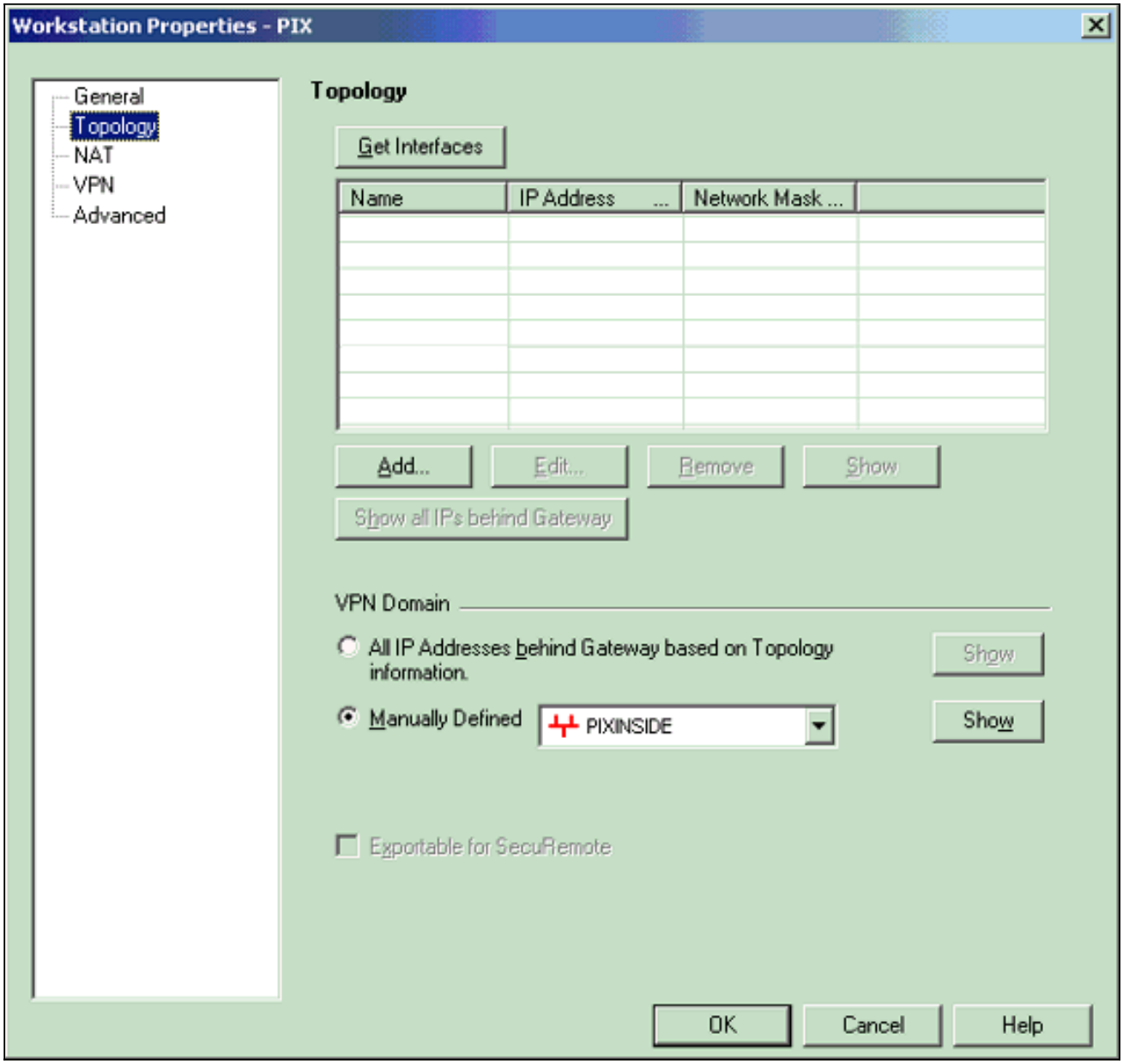
8. **사전 공유 암호**에 대한 인증 옵션을 선택한 다음 **Edit Secrets**를 클릭하여 사전 공유 키를 PIX 명령 isakmp key **address *netmask 넷마스크와 호환되도록* 설정합니다.** Edit(**편집**)를 클릭하여 여기에 표시된 대로 키를 입력하고 Set(설정), **OK(확인)를 클릭합니다**



9. IKE 속성 창에서 **Advanced...를** 클릭하고 다음 설정을 변경합니다.**Support aggressive 모드**에 대한 옵션**을 선택 취소합니다**.서브넷에 **대한 Support key exchange(키 교환 지원) 옵션을 선택합니다**.완료되면 **OK**(확인)를 클릭합니다

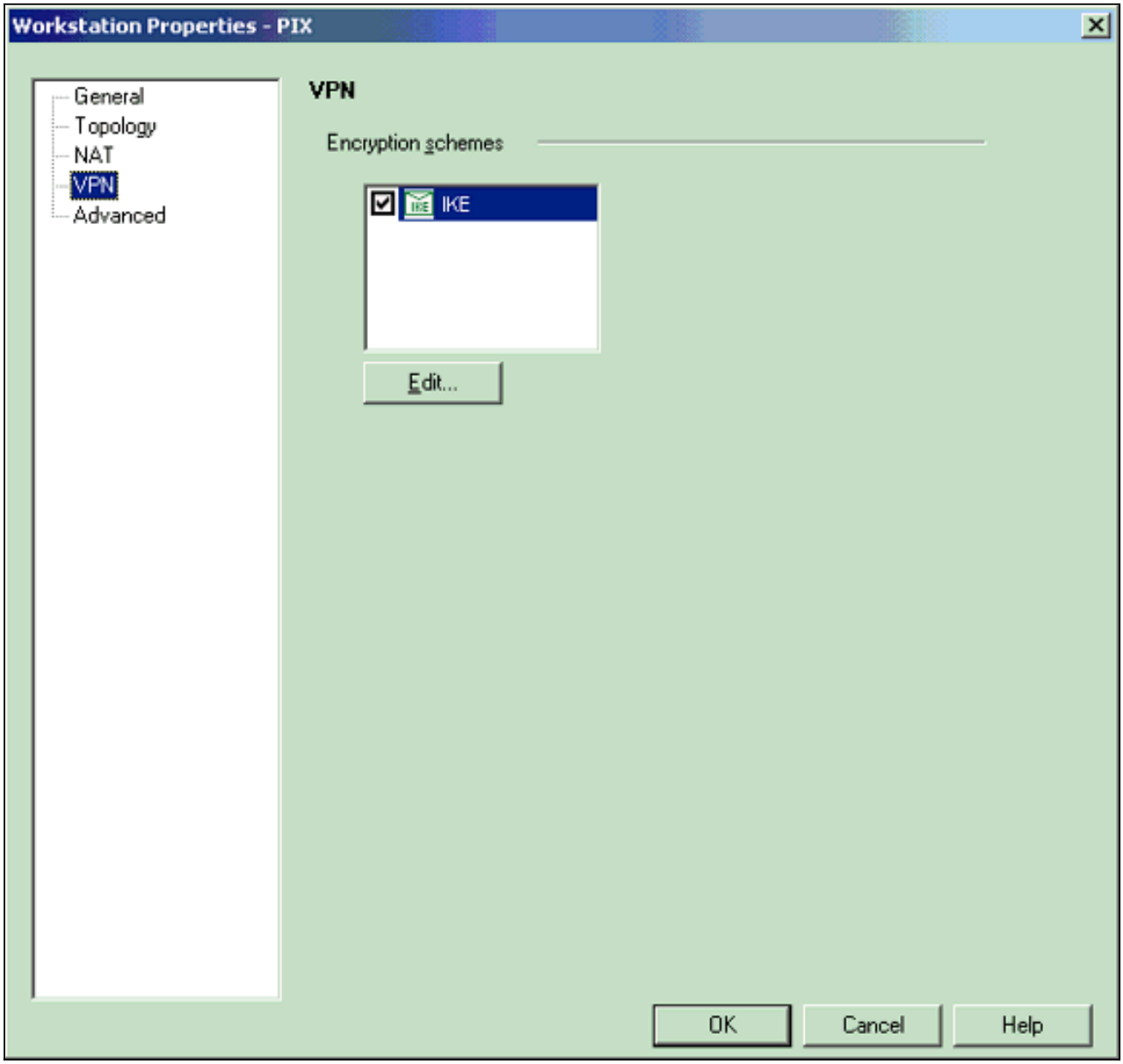


10. Manage(**관리**) > **Network objects(네트워크 개체)** > **Edit(편집)**를 선택하여 PIX의 Workstation Properties(워크스테이션 속성) 창을 엽니다. 창 왼쪽의 선택 사항 중에서 Topology를 선택하여 VPN 도메인을 수동으로 정의합니다.이 컨피그레이션에서는 PIXINSIDE(PIX의 내부 네트워크)가 VPN 도메인으로 정의됩니다
.

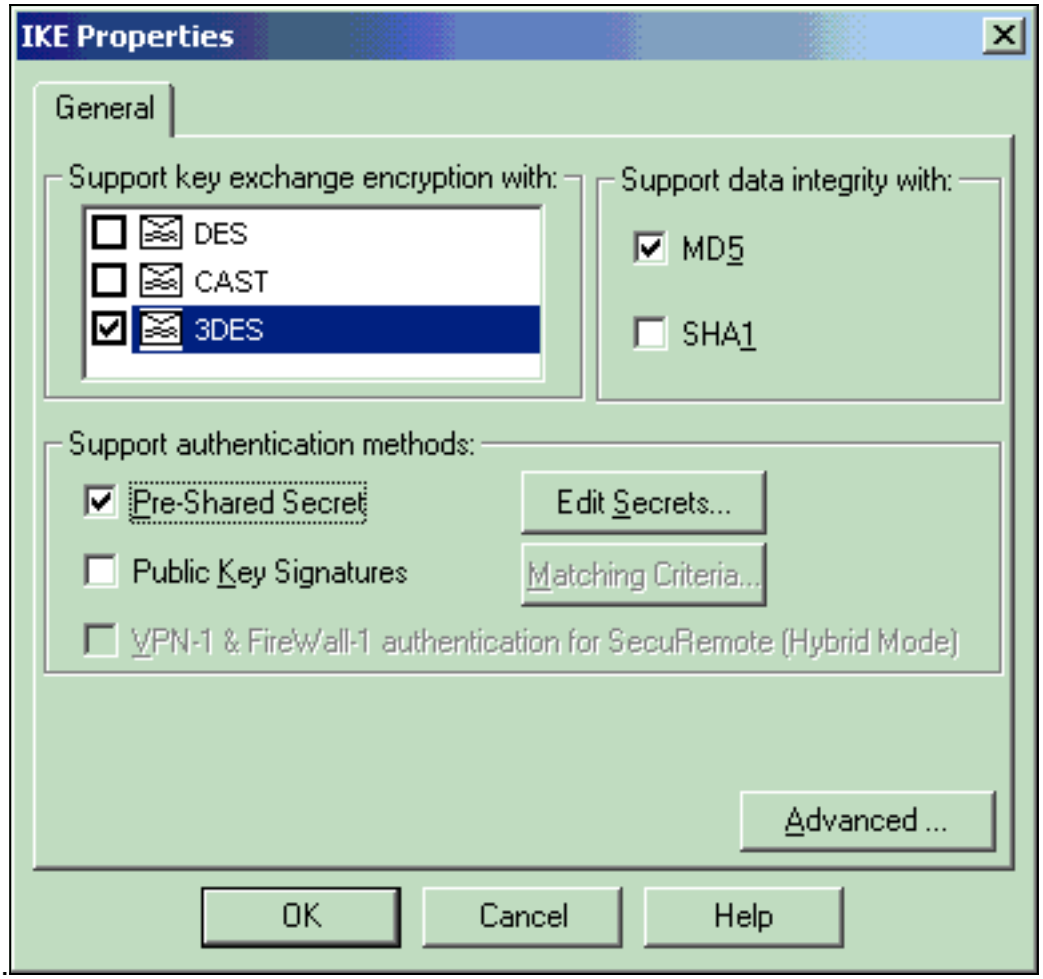


11. 창 왼쪽에 있는 선택 사항에서 VPN을 선택한 다음 암호화 구성표로 IKE를 선택합니다. Edit(**수정)**를 클릭하여 IKE 속성을 구성합니다

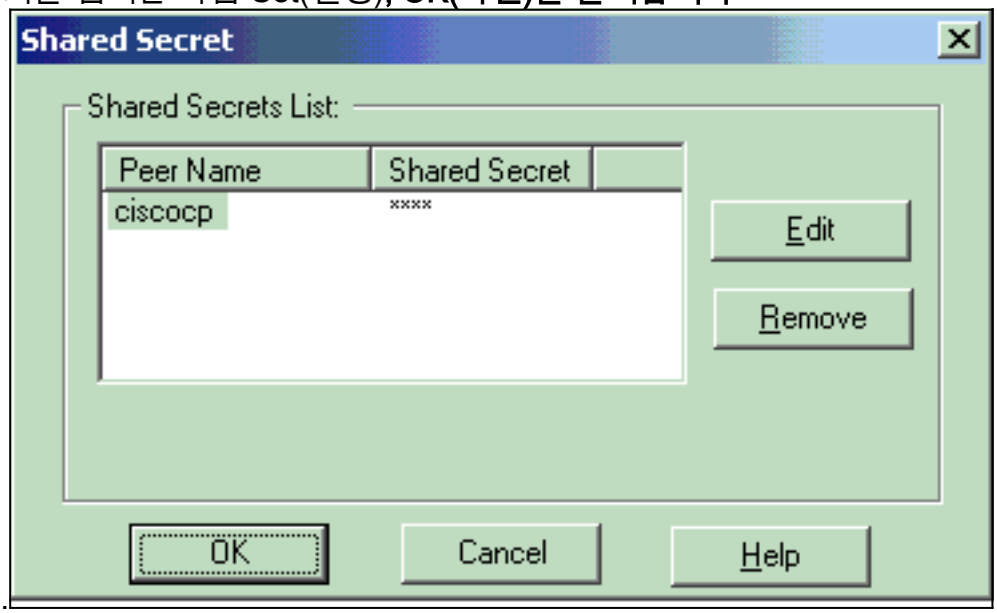
.



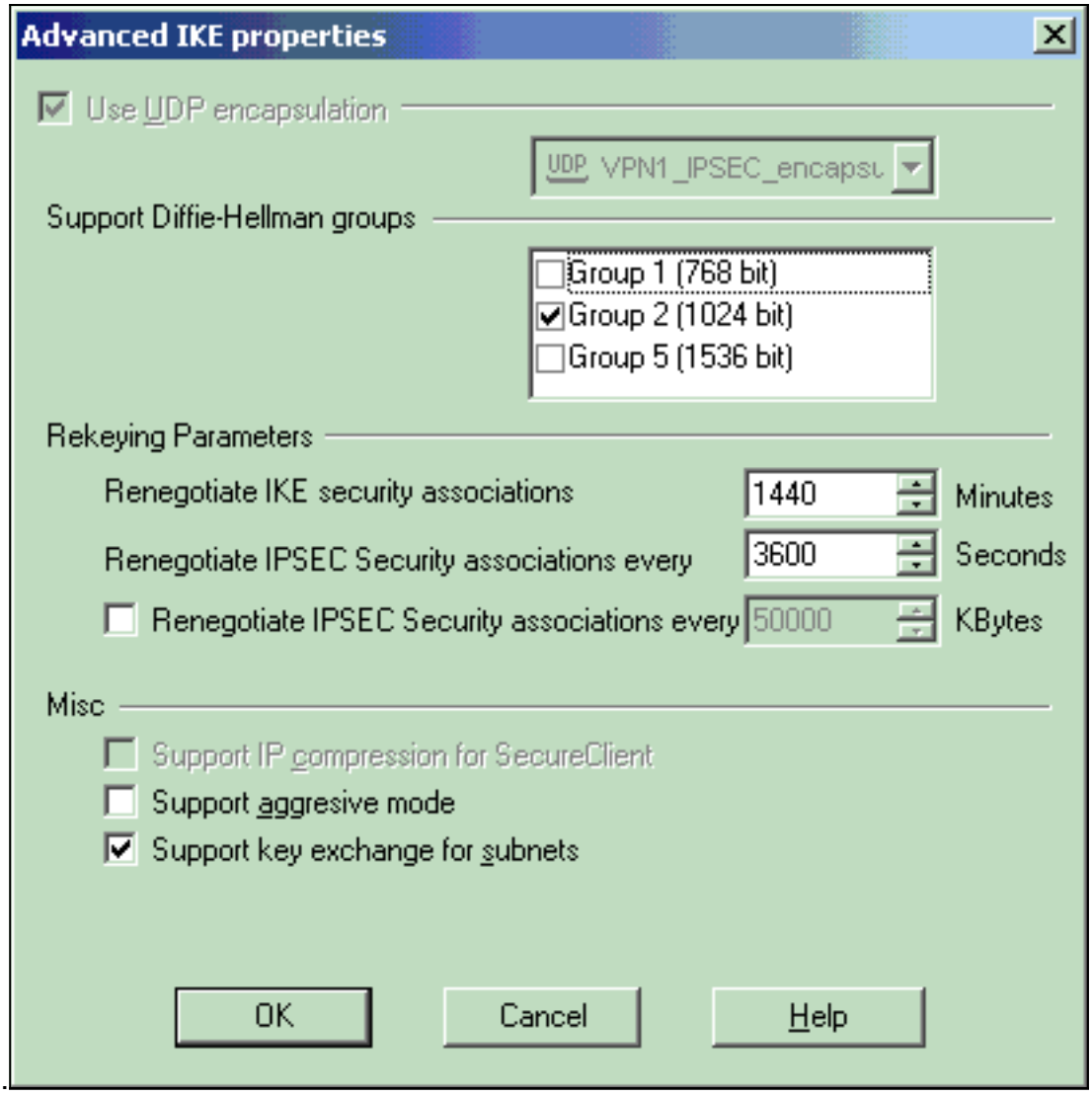
12. 다음과 같이 IKE 속성을 구성합니다.IKE 속성이 isakmp **policy # encryption 3des** 명령과 호환되도록 **3DES** 암호화 옵션을 선택합니다.IKE 속성이 crypto isakmp **policy # hash md5** 명령과 호환되도록 **MD5** 옵션을 선택합니다



13. **사전 공유 암호**에 대한 인증 옵션을 선택한 다음 **Edit Secrets**를 클릭하여 사전 공유 키를 PIX 명령 isakmp **키** *키* **주소** *넷마스크* **넷마스크와 호환되도록 설정합니다.** Edit(**편집**)를 클릭하여 키를 입력한 다음 Set(설정), **OK(확인)를 클릭합니다**



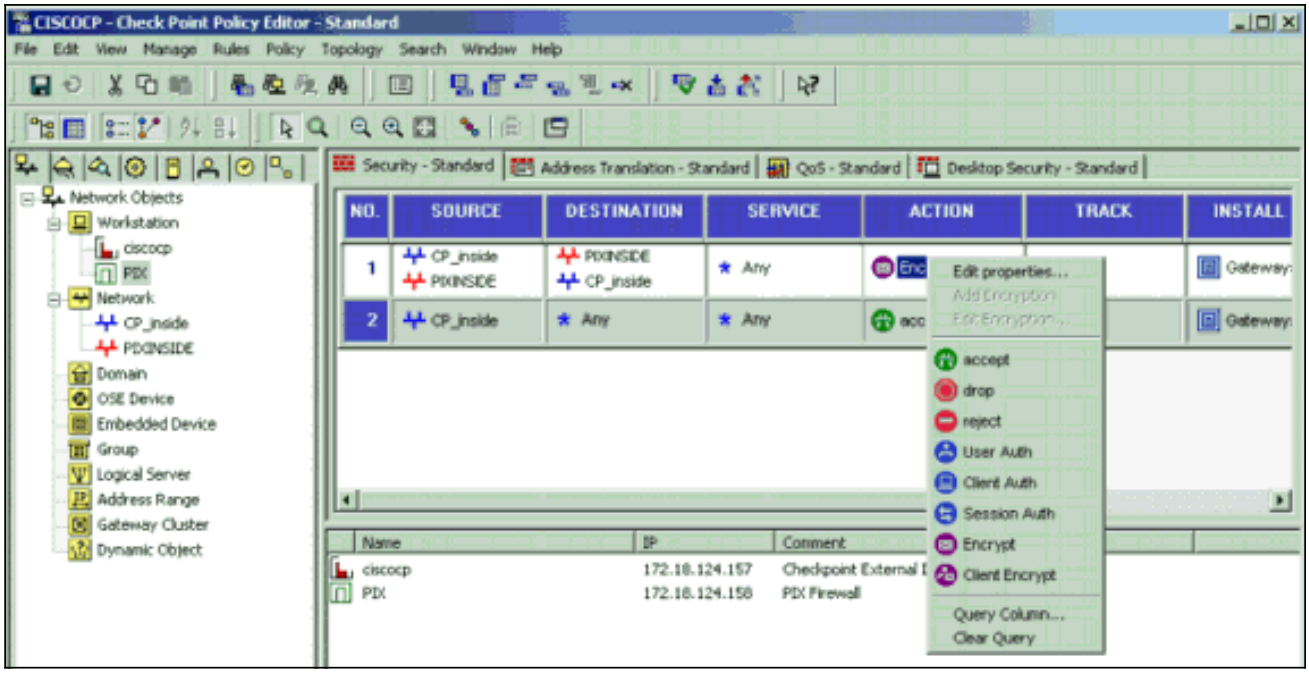
14. IKE 속성 창에서 **고급...을** 클릭하고 이러한 설정을 변경합니다.IKE 속성에 적합한 Diffie-Hellman 그룹을 선택합니다.**Support aggressive 모드**에 대한 옵션**을 선택 취소합니다**.서브넷에 **대한 Support key exchange(키 교환 지원) 옵션을 선택합니다**.완료되면 **OK(확인)**를 클



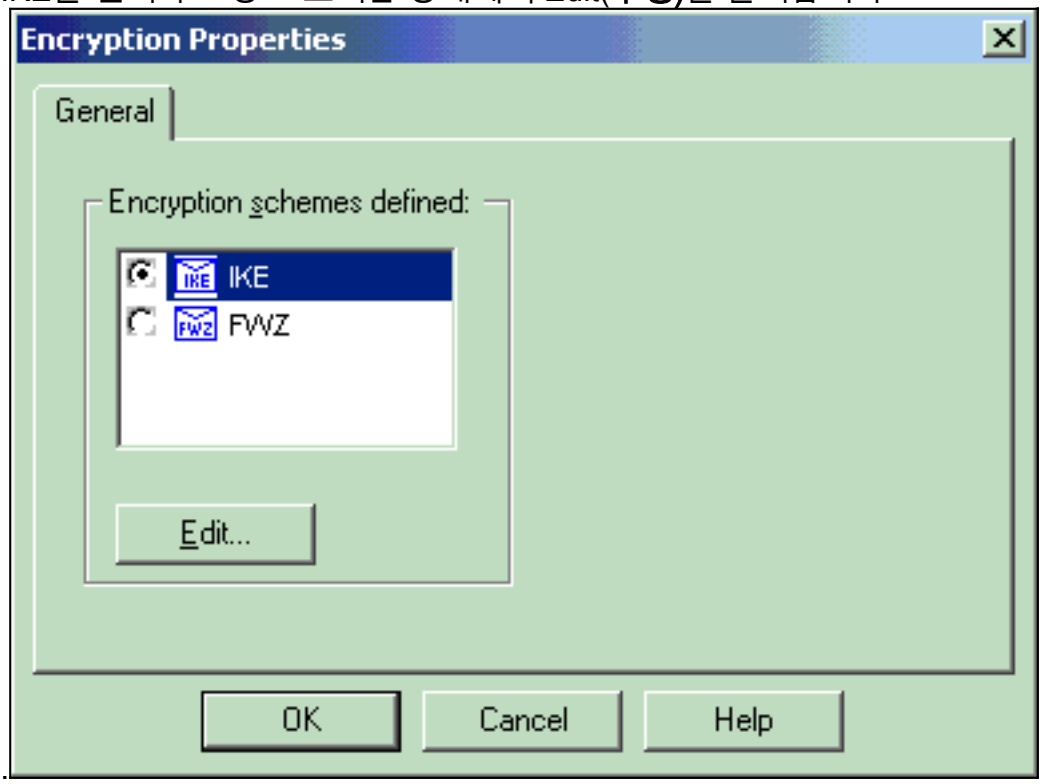
릭합니다.

15. Rules(**규칙**) > **Add Rules(규칙 추가)** > **Top**(상단)을 선택하여 정책에 대한 암호화 규칙을 구성합니다.Policy Editor(정책 편집기) 창에서 소스 및 대상 열 모두에서 CP_inside(Checkpoint ™ NG의 내부 네트워크) 및 PIXINSIDE(PIX의 내부 네트워크)의 소스가 포함된 규칙을 삽입합니다. **Service = Any, Action = Encrypt**, **Track = Log**에 대한 값**을 설정합니다**. 규칙의 Encrypt Action(암호화 작업) 섹션을 추가한 경우 Action(작업)을 마우스 오른쪽 버튼으로 **클릭하고 Edit Properties(속성 편집)를** 선택합니다

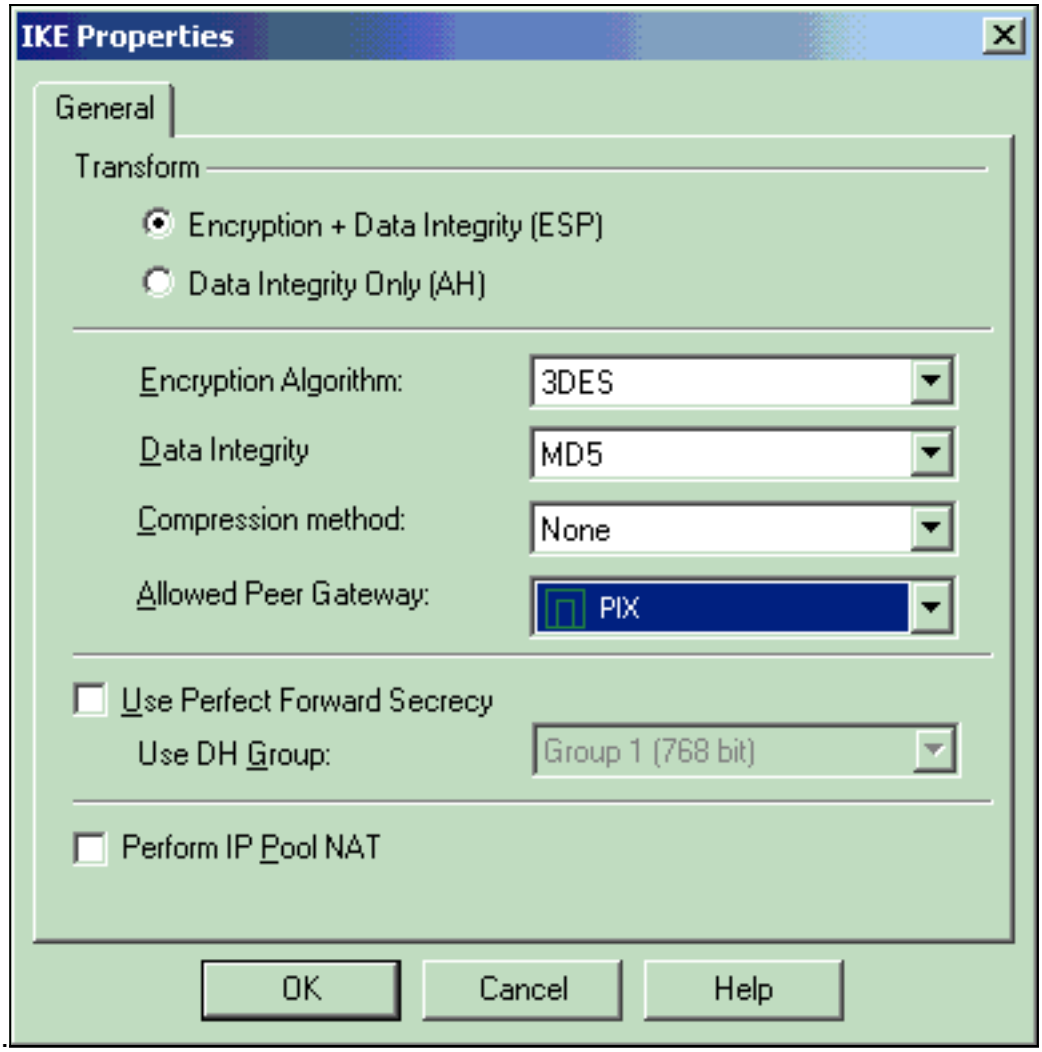
.



16. IKE를 선택하고 강조 표시한 상태에서 Edit(**수정**)를 클릭합니다



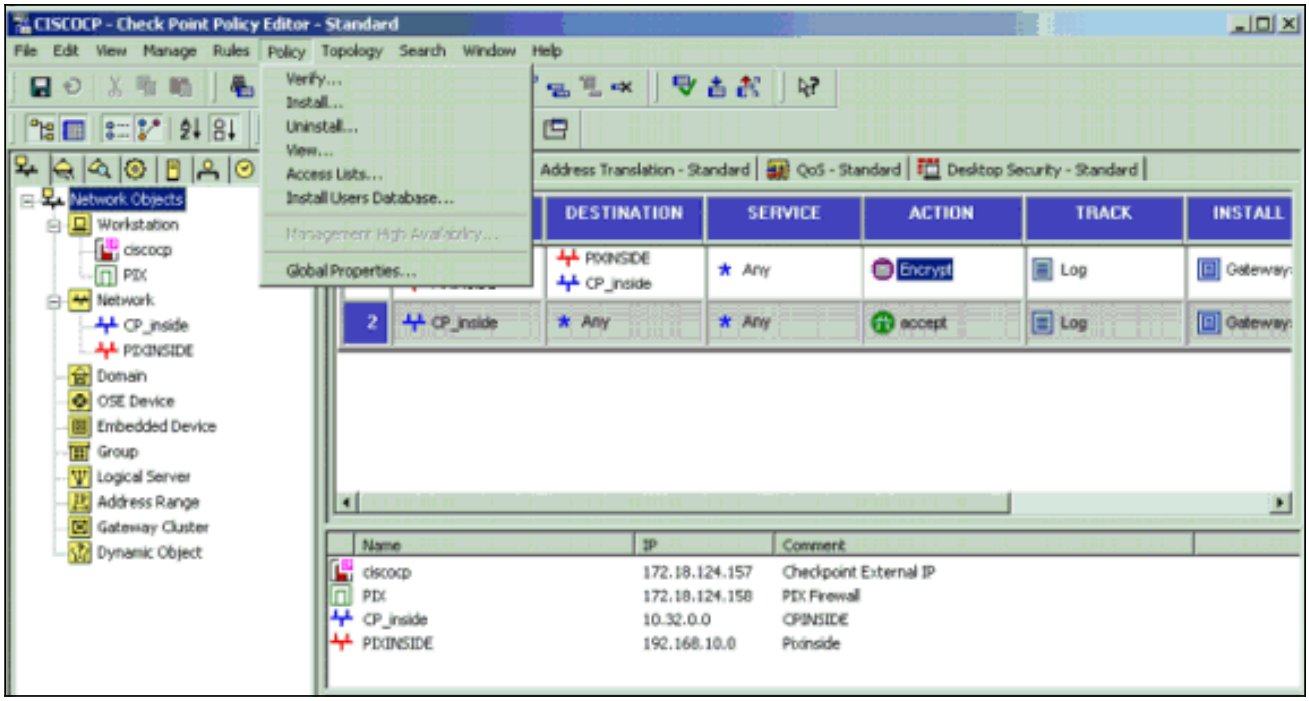
17. IKE Properties(IKE 속성) 창에서 crypto ipsec transform-set rtptac esp-**3des esp-md5-hmac** 명령의 PIX IPsec 변환**에** 동의하도록 속성을 변경합니다.Transform(변형) 옵션을 **Encryption + Data Integrity(ESP)로 설정하고 Encryption Algorithm(암호화 알고리즘)**을 **3DES**로 설정하고 Data Integrity(데이터 무결성)를 **MD5**로 설정하고 Allowed Peer Gateway(허용되는 피어 게이트웨이)를 외부 PIX 게이트웨이(PIX here)와 일치하도록 설정합니다. **확인**을 **클릭합니**



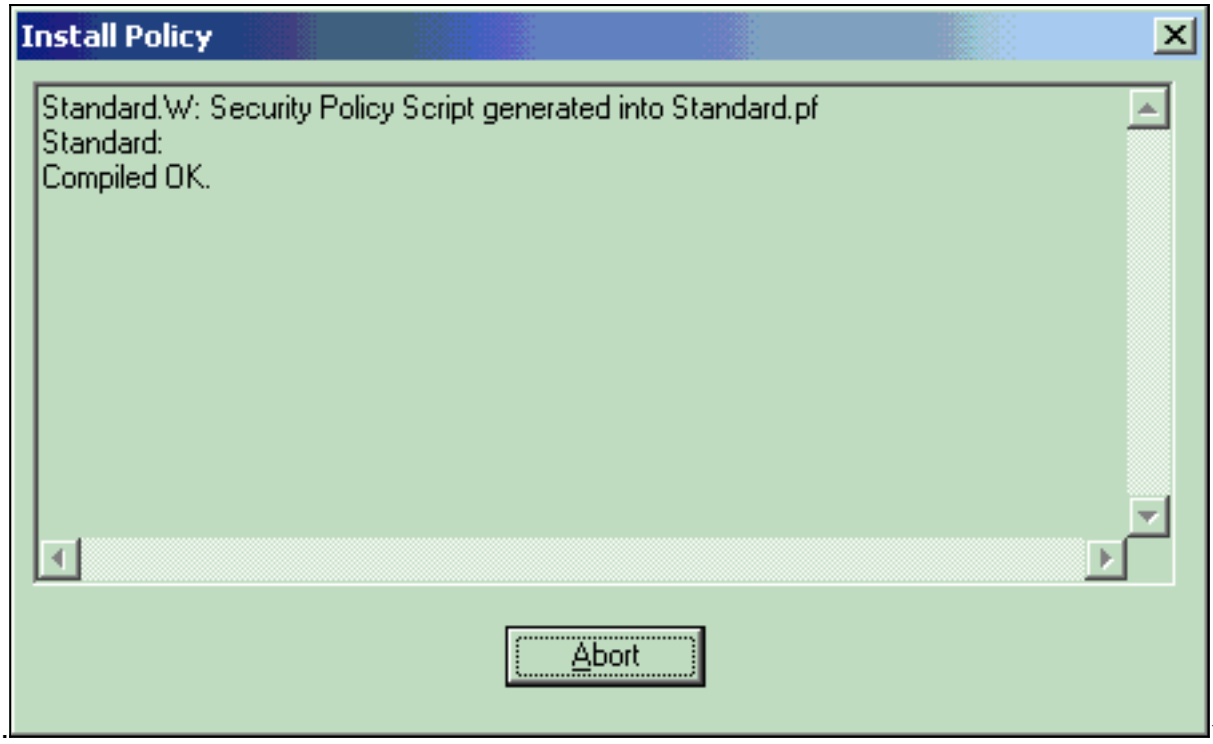
다.

18. CheckpointTM NG를 구성한 후 정책을 저장하고 **Policy > Install**을 선택하여 활성화합니다

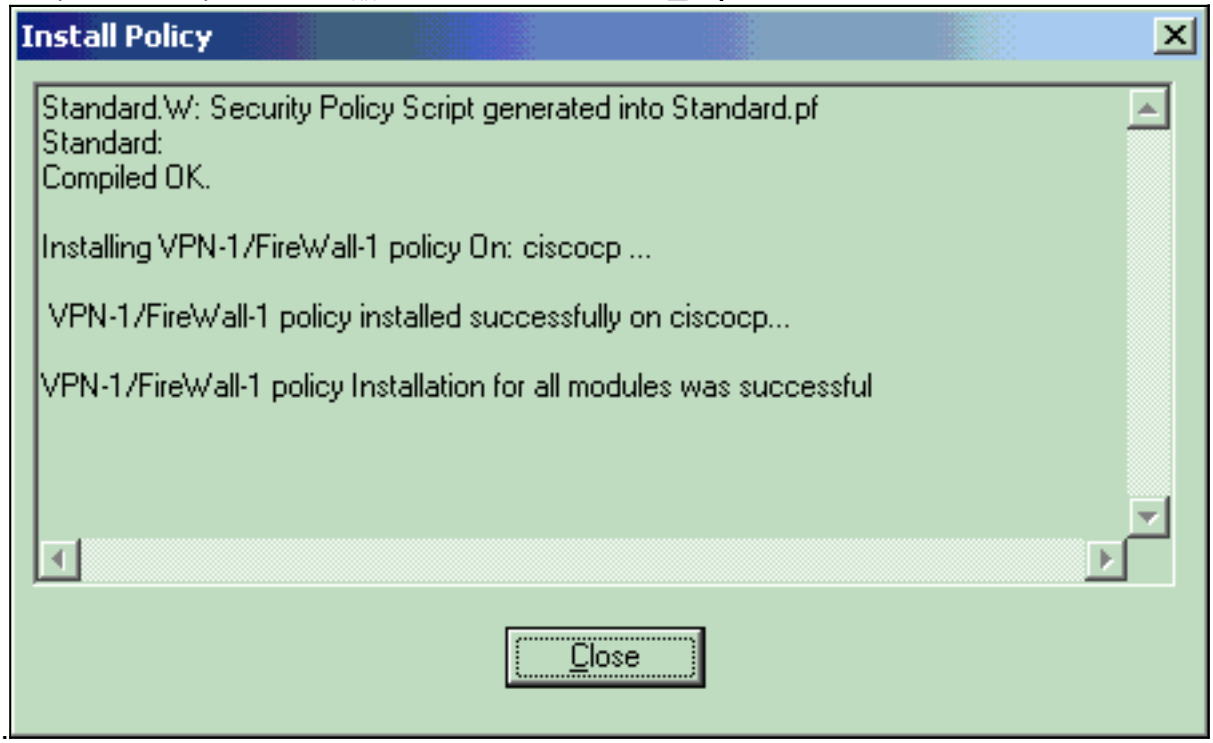
.



정책이 컴파일될 때 설치 창에 진행 정보가 표시됩니다



. 설치 창에 정책 설치가 완료되었음을 나타내는 경우 **닫기**를 클릭하여 절차를 완료합니다



.

다음을 확인합니다.

PIX 컨피그레이션 확인

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

프라이빗 네트워크 중 하나에서 다른 프라이빗 네트워크로 ping을 시작하여 두 프라이빗 네트워크 간의 통신을 테스트합니다. 이 컨피그레이션에서는 PIX 측(192.168.10.2)에서 CheckpointTM NG

내부 네트워크(10.32.50.51)으로 ping[이] 전송되었습니다.

- **show crypto isakmp sa** - 피어의 현재 모든 IKE SA를 표시합니다.

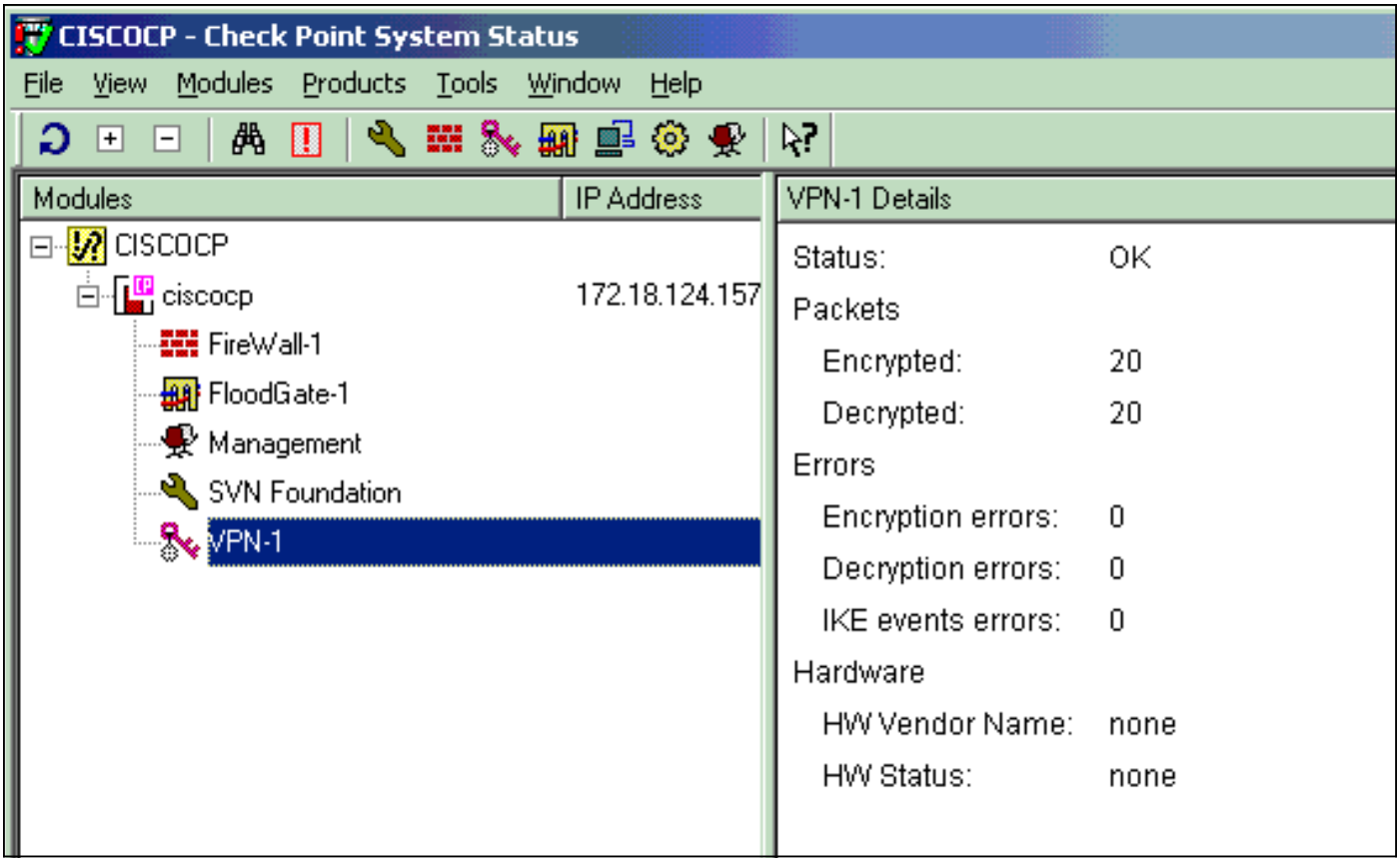
```
show crypto isakmp sa
Total    : 1
Embryonic : 0
             dst                     src                   state     pending   created
  172.18.124.157   172.18.124.158   QM_IDLE          0          1
```

- **show crypto ipsec sa** - 현재 SA에서 사용하는 설정을 표시합니다.

```
PIX501A#show cry ipsec sa

interface: outside
    Crypto map tag: rtprules, local addr. 172.18.124.158

   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #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.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 6b15a355

     inbound esp sas:
      spi: 0xced238c7(3469883591)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: rtprules
        sa timing: remaining key lifetime (k/sec): (4607998/27019)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
     inbound pcp sas:

     outbound esp sas:
      spi: 0x6b15a355(1796580181)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 4, crypto map: rtprules
        sa timing: remaining key lifetime (k/sec): (4607998/27019)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:

     outbound pcp sas:
```

체크포인트 NG에서 터널 상태 보기

Policy Editor(정책 편집기)로 이동하여 **Window(창)** > **System Status(시스템 상태)**를 선택하여 터널 상태를 확인합니다.



문제 해결

PIX 구성 문제 해결

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

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

PIX 방화벽에서 디버그를 활성화하려면 다음 명령을 사용합니다.

- **debug crypto engine** - 암호화 및 해독을 수행하는 암호화 엔진에 대한 디버그 메시지를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
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-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 and conn_id 4 and flags 4
lifetime of 28800 seconds
```

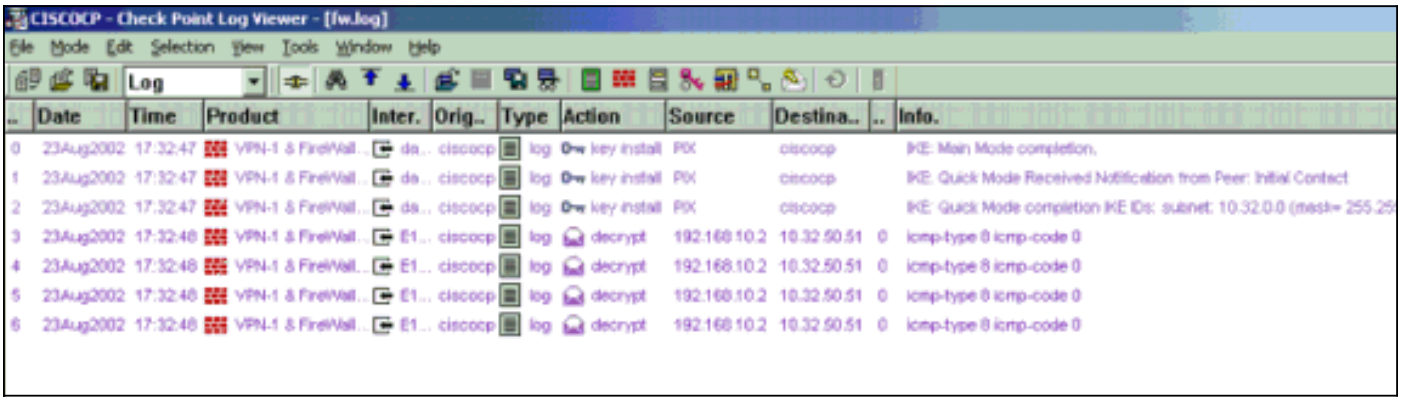
```
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

네트워크 요약

Checkpoint의 암호화 도메인에 인접한 여러 내부 네트워크가 구성된 경우, 해당 디바이스는 흥미로운 트래픽과 관련하여 이를 자동으로 요약할 수 있습니다. PIX의 암호화 ACL(Access Control List)이 일치하도록 구성되지 않으면 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 요약할 수 있습니다.

체크포인트 NG 로그 보기

로그를 보려면 **Window > Log Viewer**를 선택합니다.



관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems