Cisco VPN 3000 Concentrator와 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 VPN 3000 Concentrator 내의 192.168.10.x 프라이빗 네트워크와 NG(Checkpoint Next Generation) 방화벽 내의 10.32.x.x 프라이빗 네트워크입니다.

사전 요구 사항

요구 사항

- VPN Concentrator 내부 및 Checkpoint NG에서 인터넷(172.18.124.x 네트워크로 표시)으로의 트래픽은 이 컨피그레이션을 시작하기 전에 흐름되어야 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 변환을 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 컨피그레이션은 다음 소프트웨어 및 하드웨어 버전에서 개발 및 테스트되었습니다.

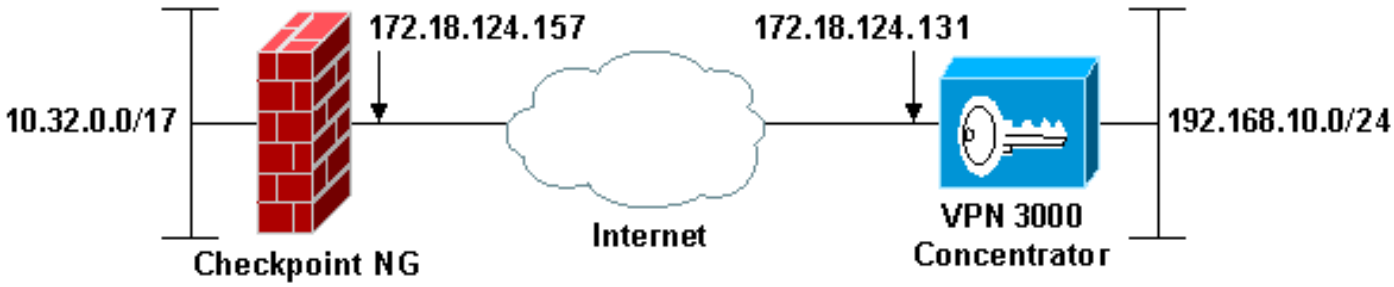
- VPN 3000 Series Concentrator 3.5.2
- 체크포인트 NG 방화벽

표기 규칙

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



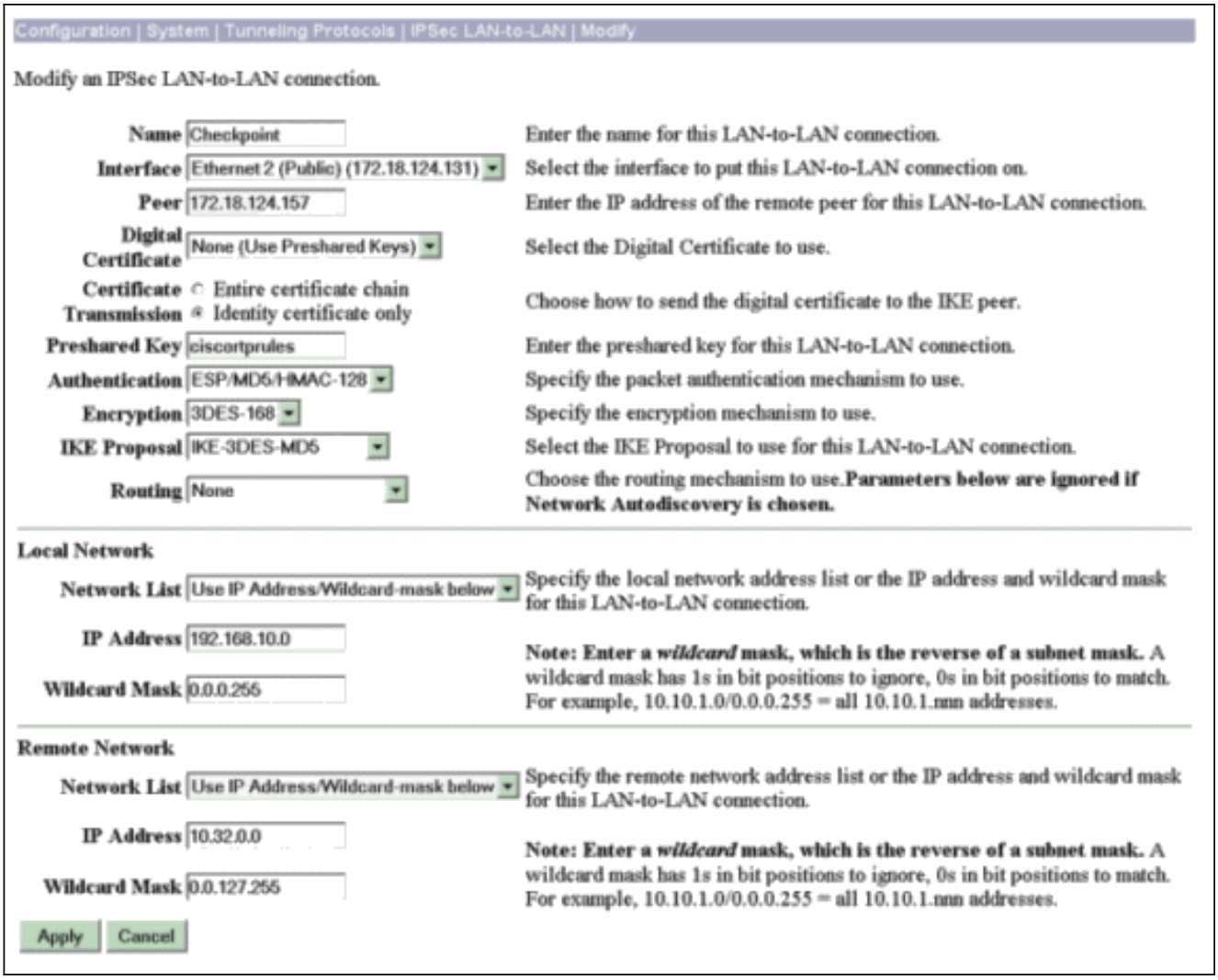
참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환경에서 사용된 RFC 1918 주소입니다.

구성

VPN 3000 Concentrator 구성

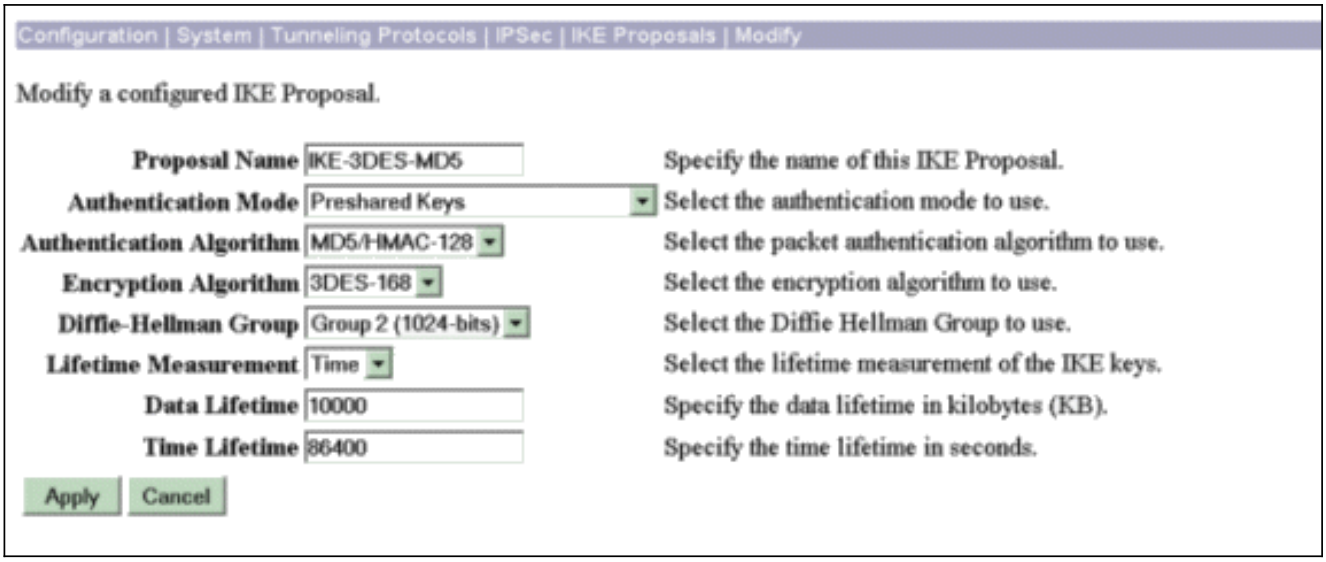
VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

1. LAN-to-**LAN** 세션을 구성하려면 Configuration**(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec LAN-to-LAN**으로 이동합니다. 인증 및 IKE 알고리즘, 사전 공유 키, 피어 IP 주소, 로컬 및 원격 네트워크 매개변수에 대한 옵션을 설정합니다. Apply를 **클릭합니다**.이 컨피그레이션에서는 인증이 ESP-MD5-HMAC로 설정되었고 암호화가 3DES로 설정되었습니다
.



2. Configuration(컨피그레이션) **> System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > IKE Proposals(IKE 제안)로 이동하여** 필요한 매개변수를 설정합니다.IKE 제안서 IKE-3DES-MD5를 선택하고 제안서에 대해 선택한 매개변수를 확인합니다. LAN-to-LAN 세션을 구성하려면 Apply를 클릭합니다.이 컨피그레이션의 매개변수는 다음과 같습니다

.

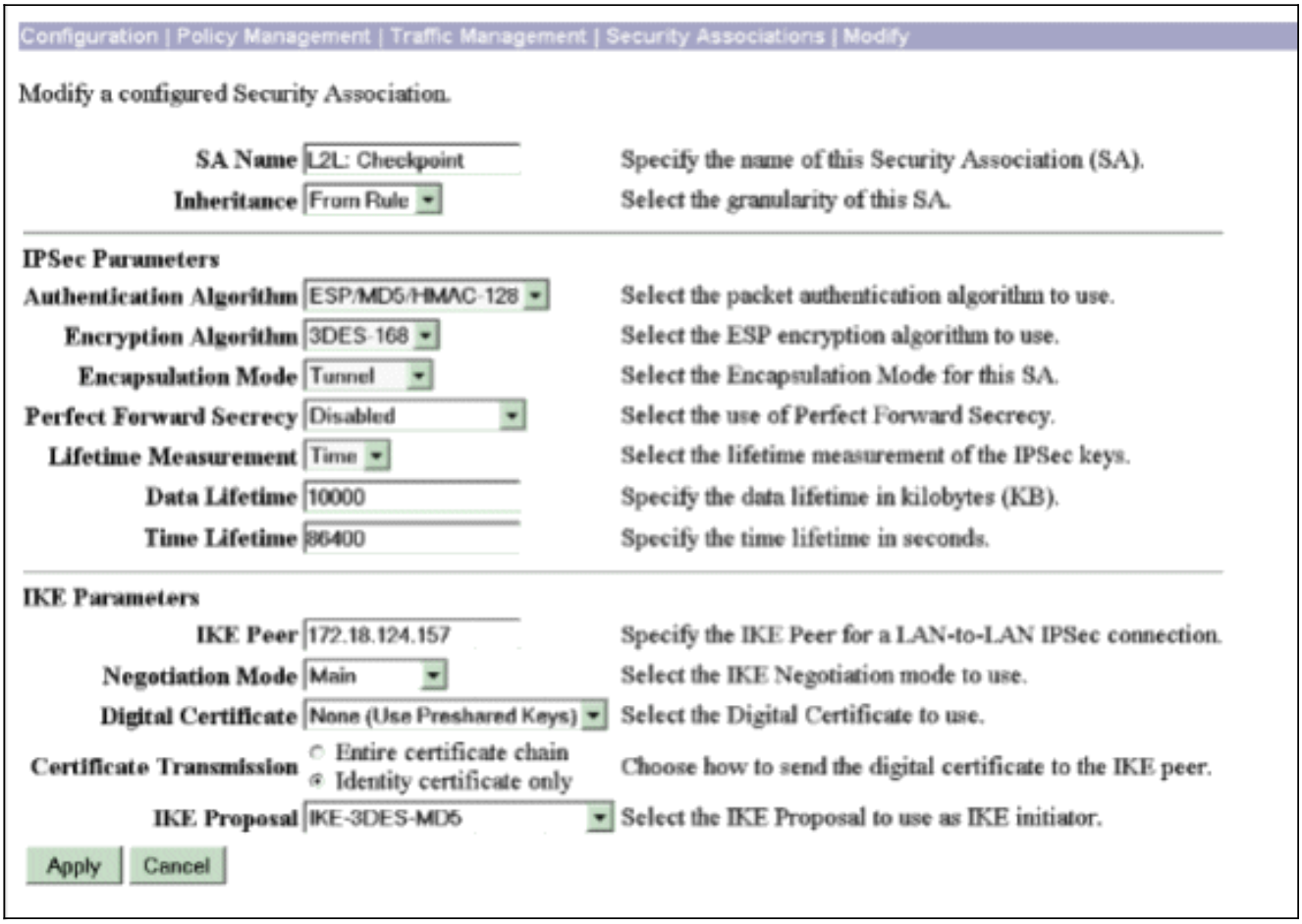


3. Configuration(**컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결)**로 이동하여 세션에 대해 생성된 IPSec SA를 선택하고 LAN-to-LAN 세션에 대해 선택한 IPSec SA 매개변수를 확인합니다.이 컨피그레이션에서는 LAN-to-LAN 세션 이름이 "Checkpoint"이므로 IPSec SA가 "L2L: 체크포인트

."

다음은 이 SA의 매개변수입니다

.

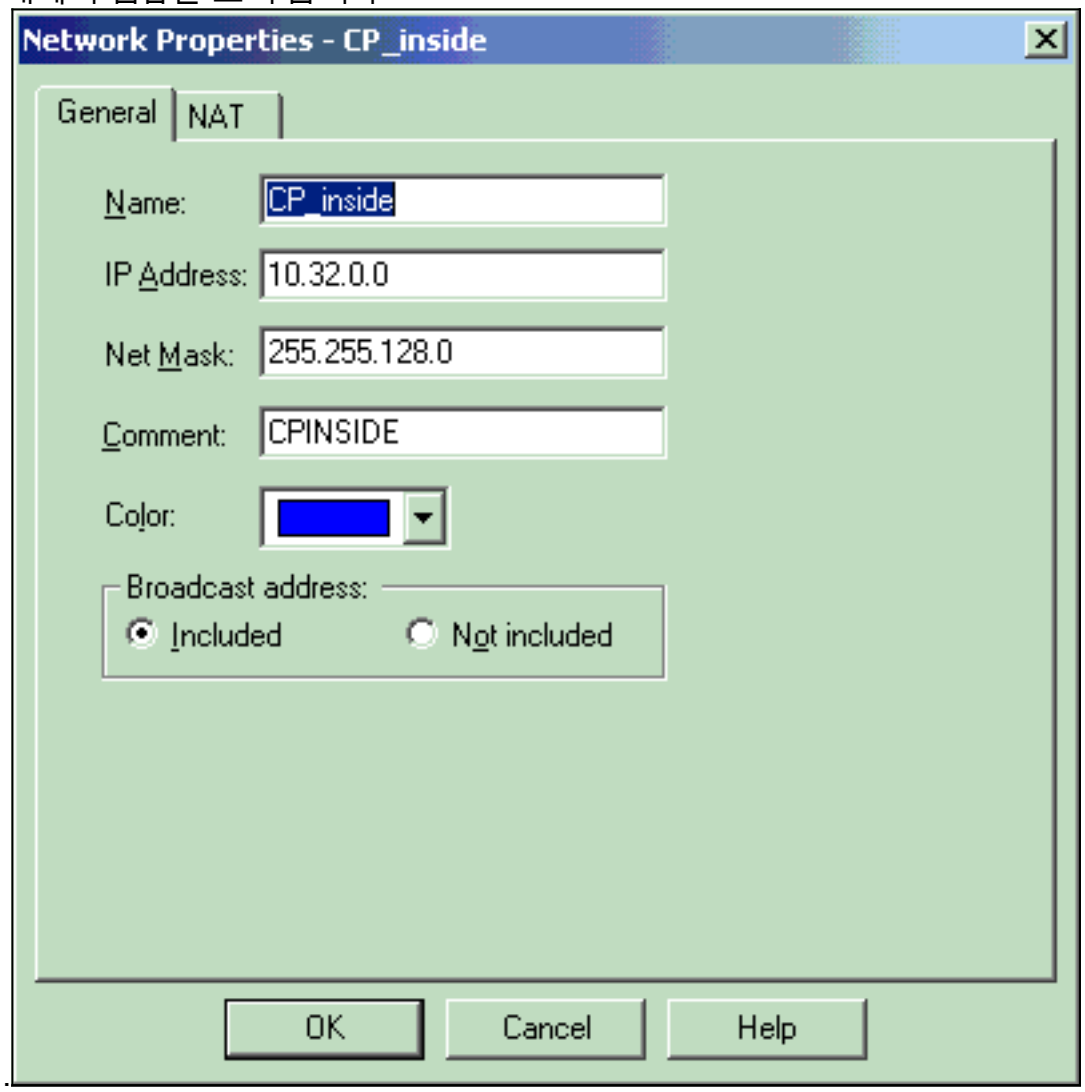


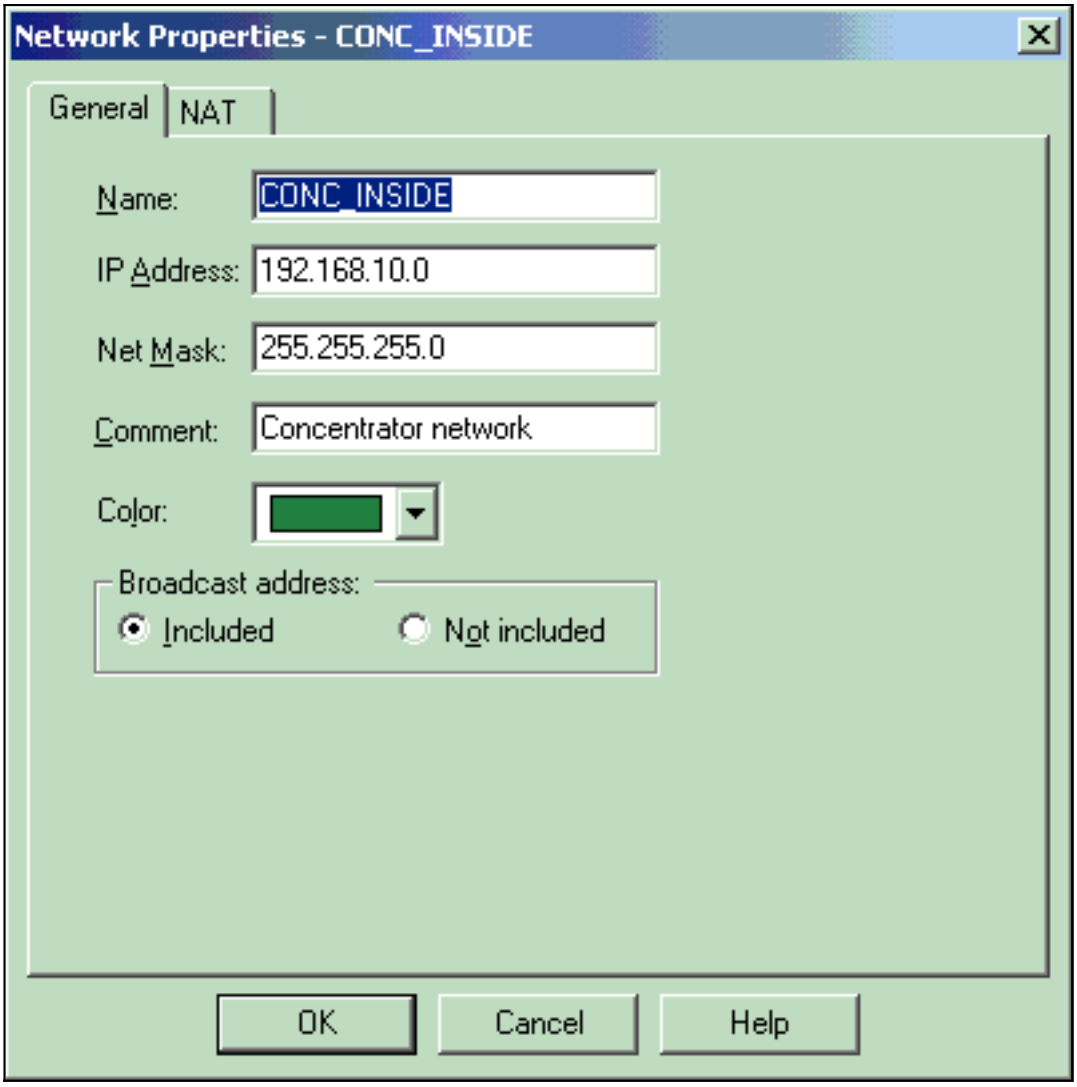
체크포인트 NG 구성

설정할 VPN 컨피그레이션과 관련된 정책을 구성하기 위해 네트워크 객체 및 규칙이 체크포인트 NG에 정의됩니다. 그런 다음 이 정책을 Checkpoint NG 정책 편집기와 함께 설치하여 컨피그레이션의 Checkpoint NG 측면을 완료합니다.

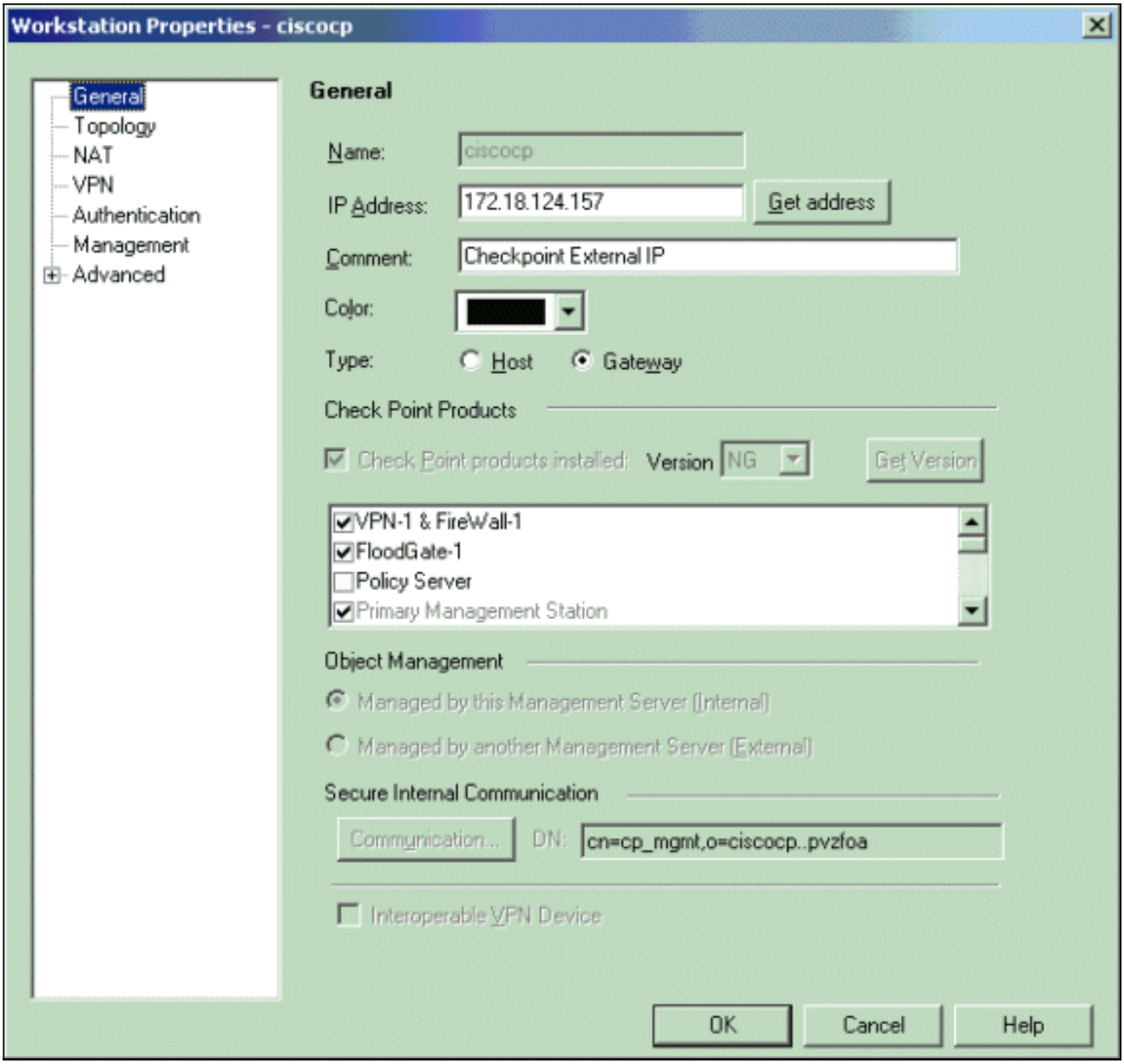
1. Checkpoint NG 네트워크와 관심 있는 트래픽을 암호화하는 VPN Concentrator 네트워크를 위한 두 개의 네트워크 개체를 만듭니다.객체를 생성하려면 **Manage(관리) > Network Objects(네트워크 객체)를** 선택한 다음 New(새로 만들기) **> Network(네트워크)를** 선택합니다. 적절한 네트워크 정보를 입력한 다음 OK를 클릭합니다.다음 예에서는 CP_inside(Checkpoint NG의 내부 네트워크) 및 CONC_INSIDE(VPN Concentrator의 내부 네트워크)라는 네트워크

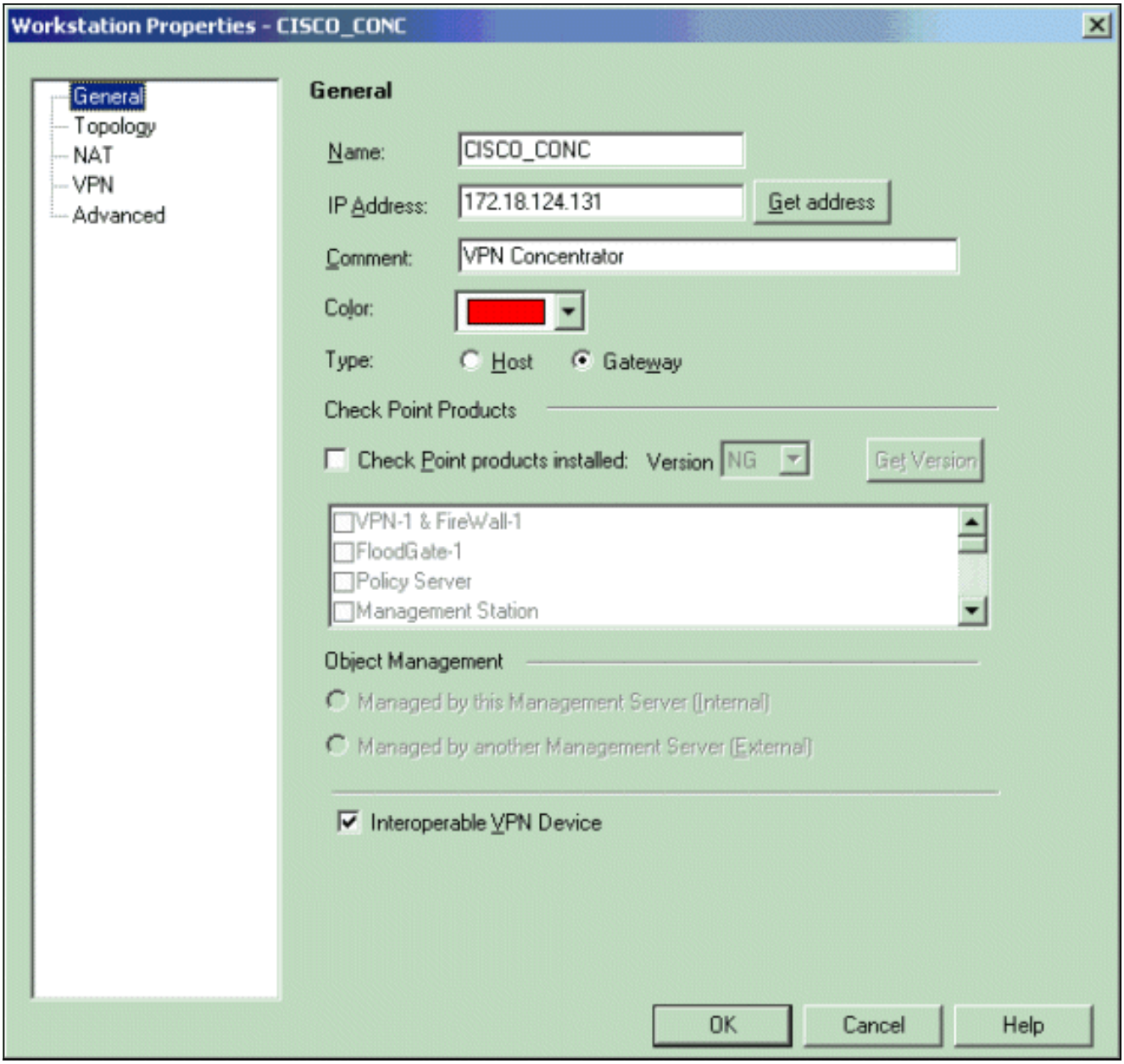
개체의 집합을 보여 줍니다





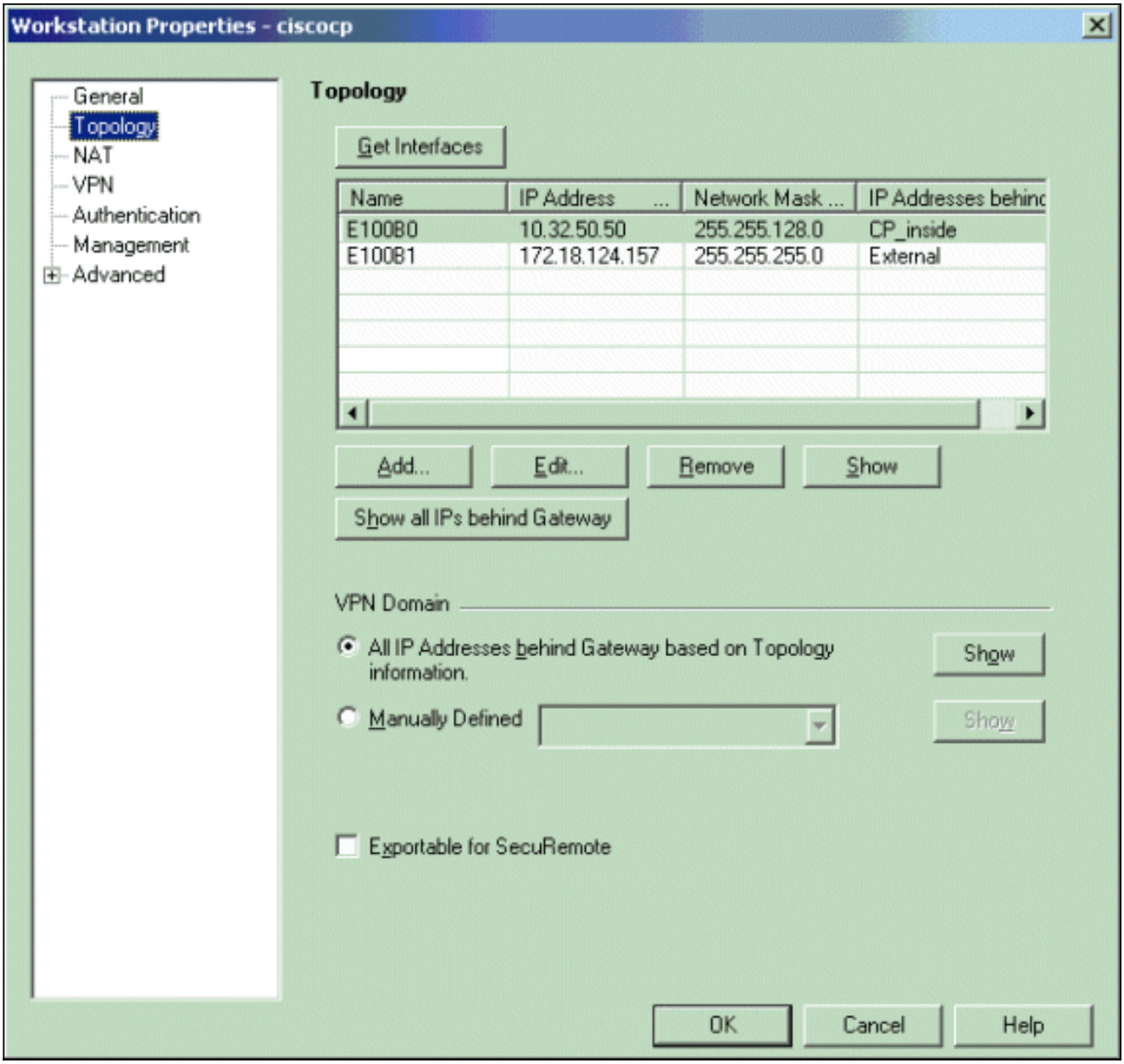
2. Manage(**관리**) > **Network Objects(네트워크 개체**)로 이동하고 **New(새로 만들기) > Workstation(워크스테이션)을** 선택하여 VPN 디바이스, Checkpoint NG 및 VPN Concentrator에 대한 워크스테이션 개체를 생성합니다.**참고:** 초기 체크포인트 NG 설정 중에 생성된 체크포인트 NG 워크스테이션 객체를 사용할 수 있습니다. 워크스테이션을 Gateway(게이트웨이) 및 Interoperable VPN Device(상호 운용 가능한 VPN 디바이스)로 설정하는 옵션을 선택하고 **OK(확인)**를 클릭합니다.다음 예에서는 ciscocp(Checkpoint NG) 및 CISCO_CONC(VPN 3000 Concentrator)라는 개체 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

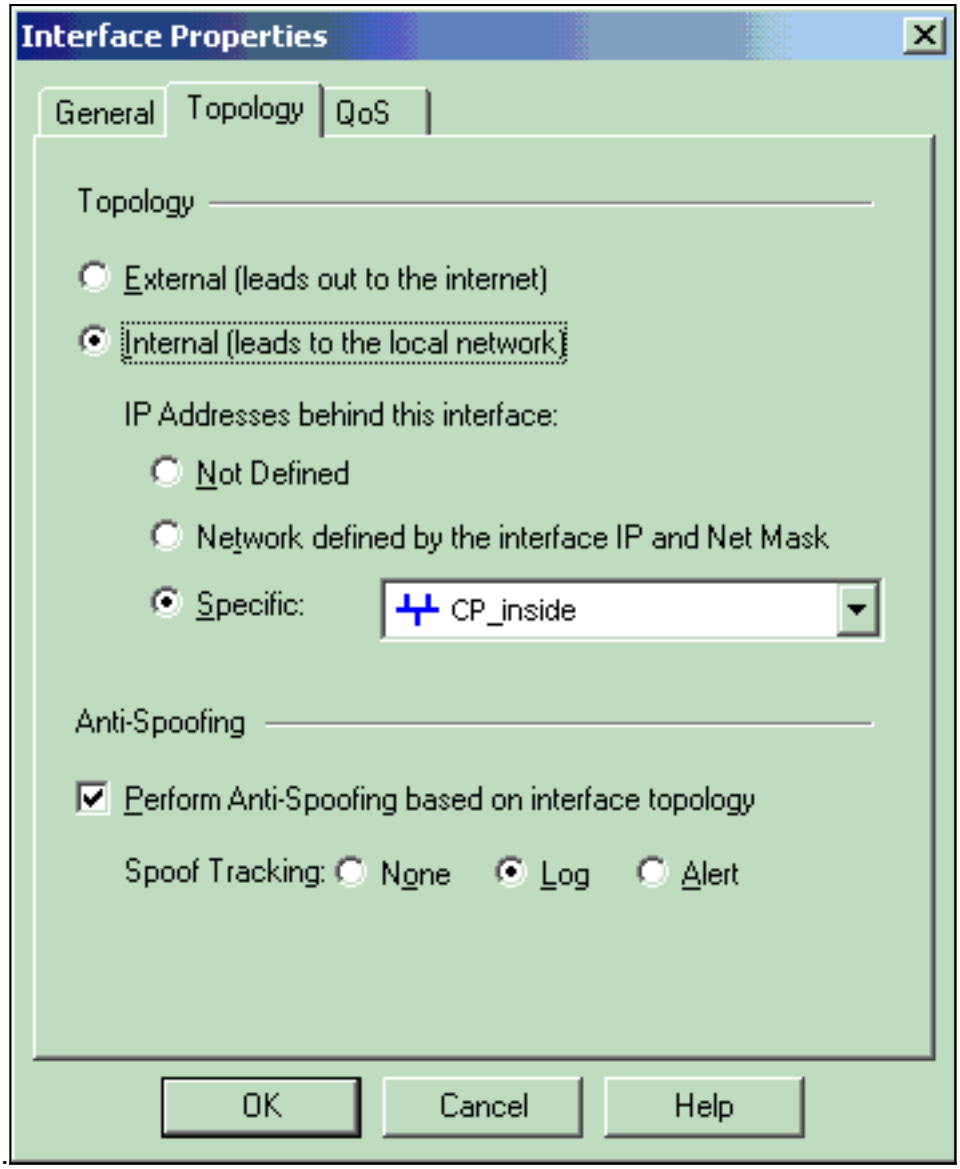


3. Manage(**관리**) > **Network Objects(네트워크 개체) > Edit(편집)로 이동하여 Checkpoint** NG 워크스테이션의 Workstation Properties(워크스테이션 속성) 창을 엽니다(이 예에서는 ciscocp). 창 왼쪽에 있는 선택 사항에서 Topology(토폴로지)를 선택한 다음 암호화할 네트워크를 선택합니다. 인터페이스 속성**을** 설정하려면 Edit를 클릭합니다.이 예에서 CP_inside는 체크포인트 NG의 내부 네트워크입니다

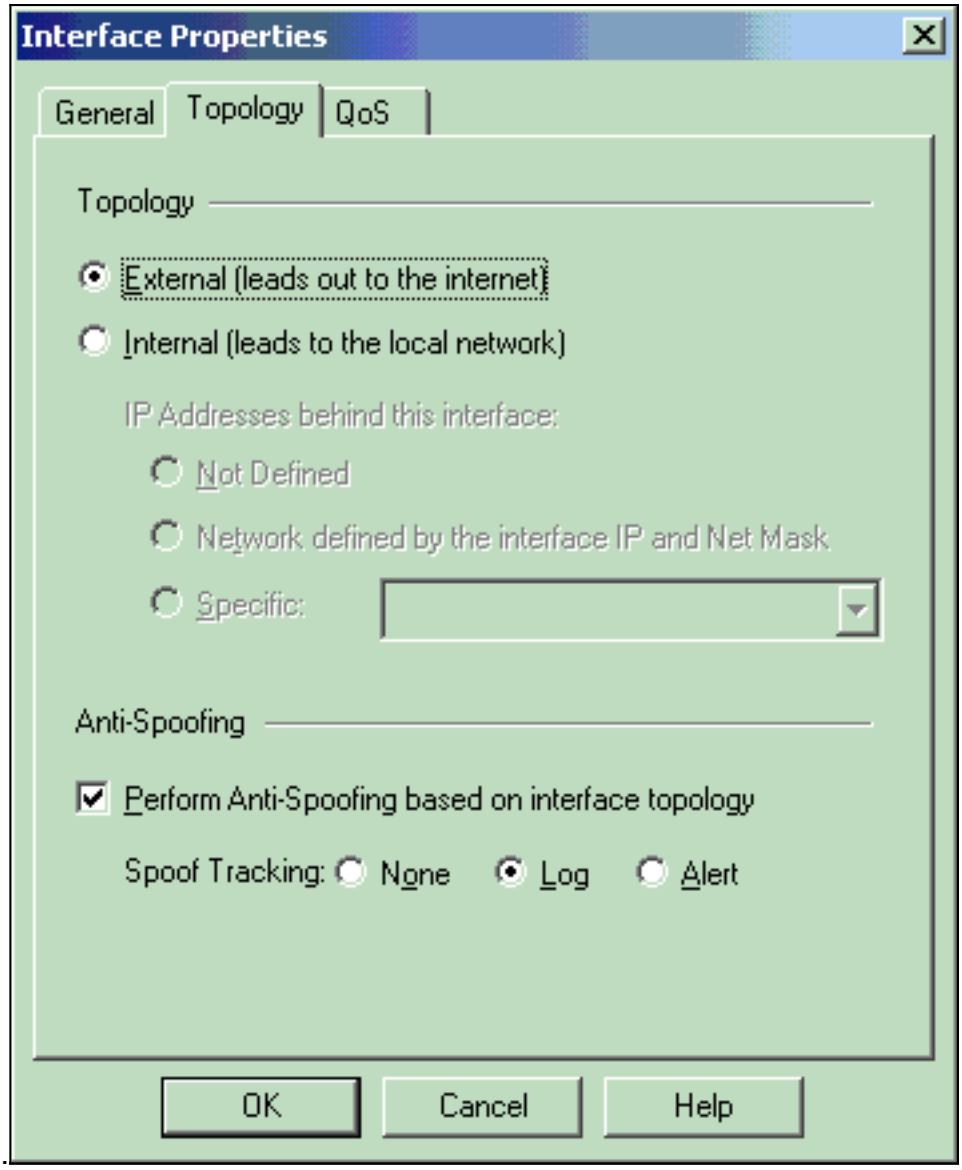
.



4. Interface Properties(인터페이스 속성) 창에서 워크스테이션을 internal(내부)로 지정하는 옵션을 선택한 다음 적절한 IP 주소를 지정합니다. **확인**을 **클릭합니다**.표시된 토폴로지 선택 항목은 워크스테이션을 internal로 지정하고 CP_inside 인터페이스 뒤에 IP 주소를 지정합니다



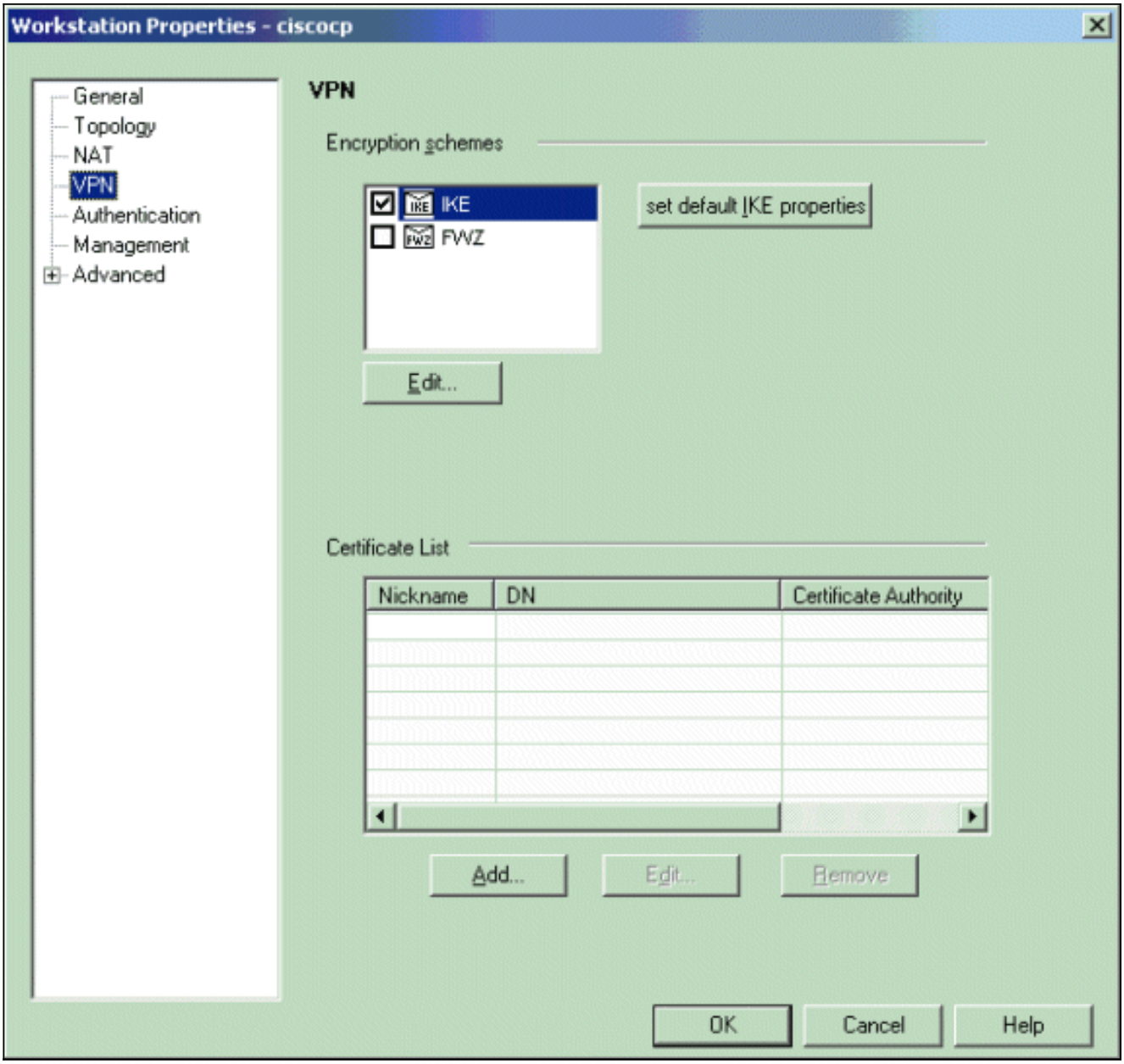
5. Workstation Properties(워크스테이션 속성) 창의 Checkpoint NG에서 인터넷으로 연결되는 외부 인터페이스를 선택한 다음 Edit(**편집**)를 클릭하여 인터페이스 속성을 설정합니다. 토폴로지를 외부로 지정하려면 옵션을 선택한 다음 **확인**을 클릭합니다



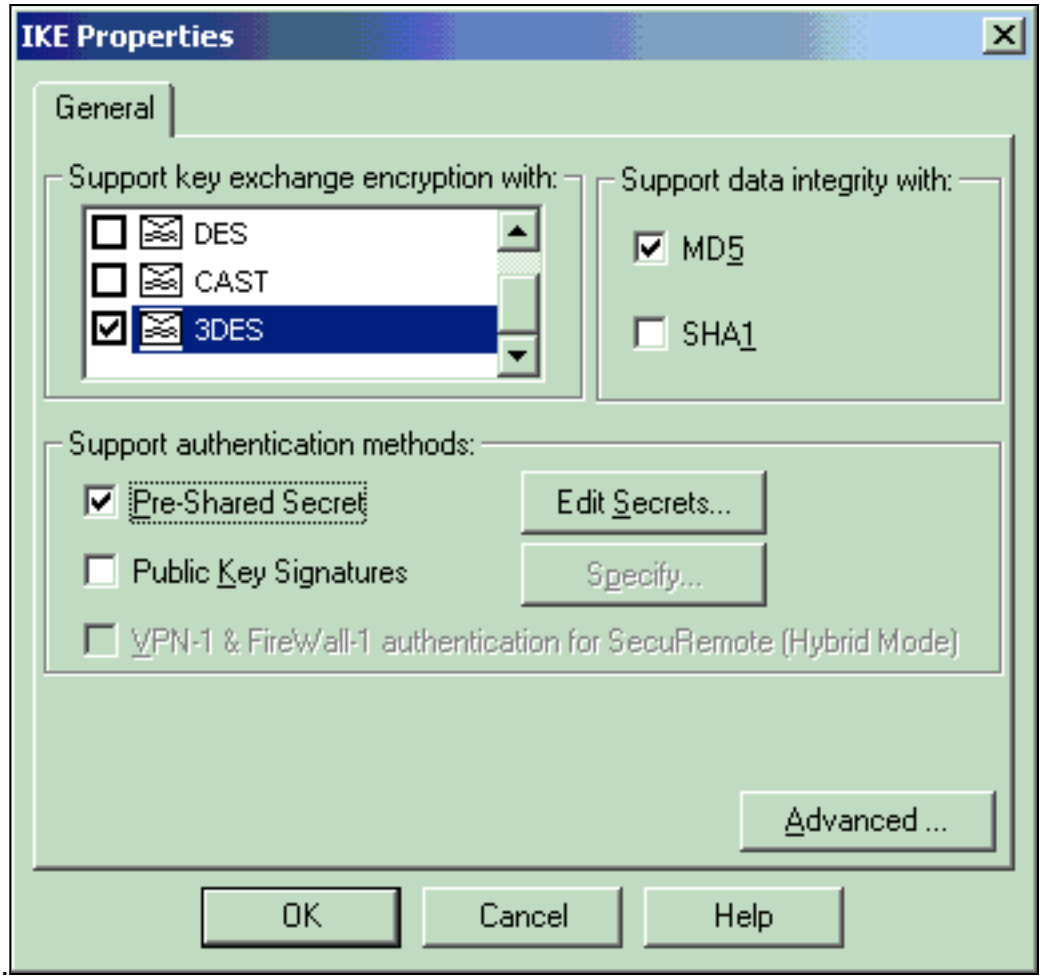
.

6. Checkpoint NG의 Workstation Properties(워크스테이션 속성) 창에서 창 왼쪽에 있는 선택 사항 중에서 **VPN**을 선택한 다음 암호화 및 인증 알고리즘에 대한 IKE 매개변수를 선택합니다. IKE 속성을 구성하려면 Edit를 클릭합니다

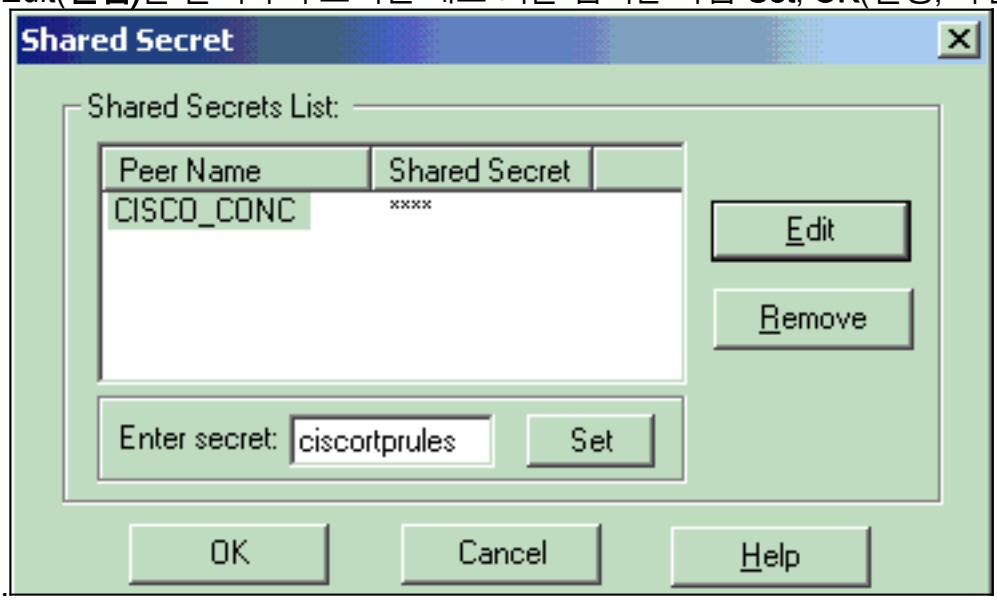
.



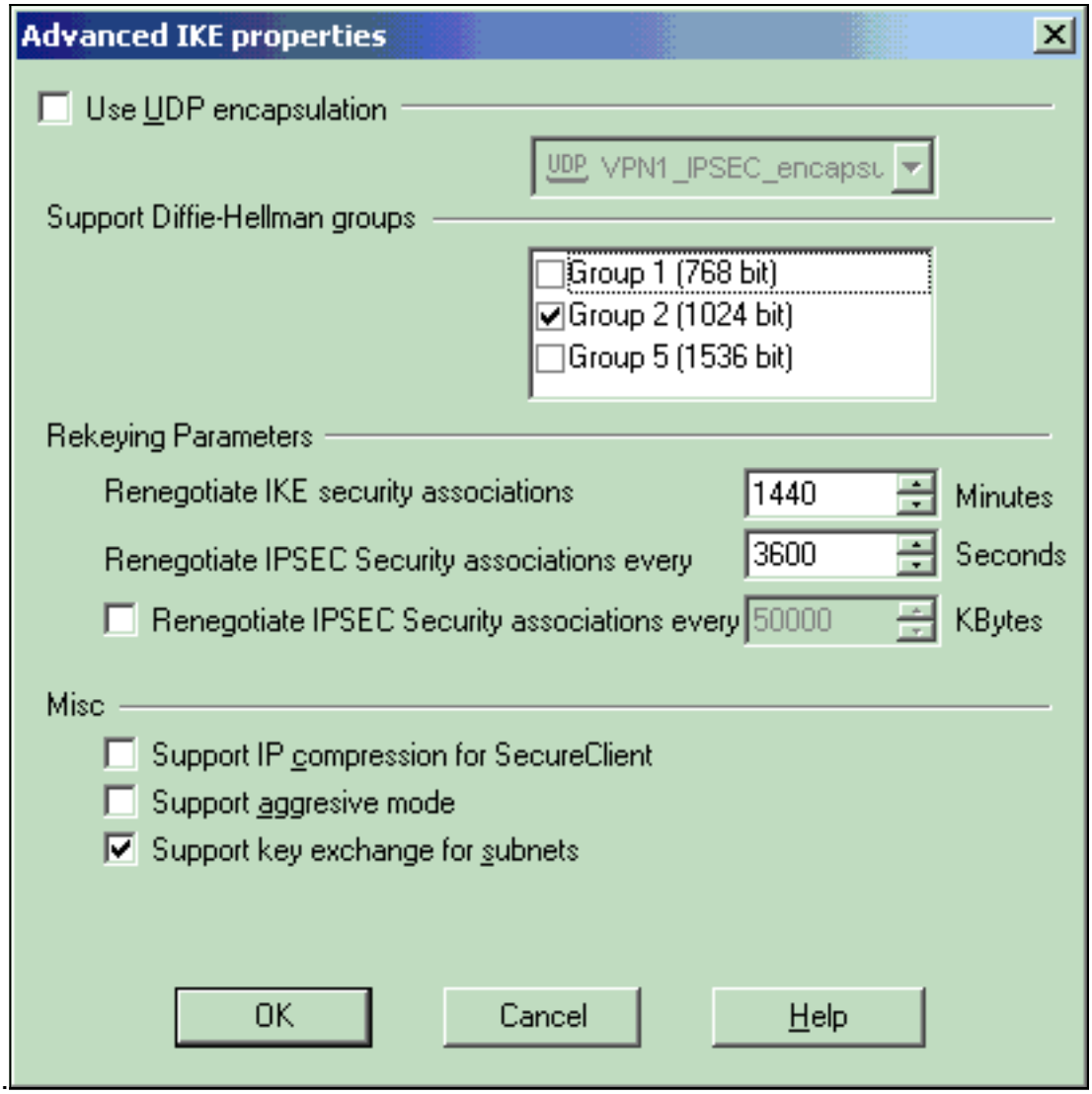
7. VPN Concentrator의 속성과 일치하도록 IKE 속성을 설정합니다.이 예에서 **3DES**의 암호화 옵션 및 **MD5**의 해싱 옵션을 선택합니다



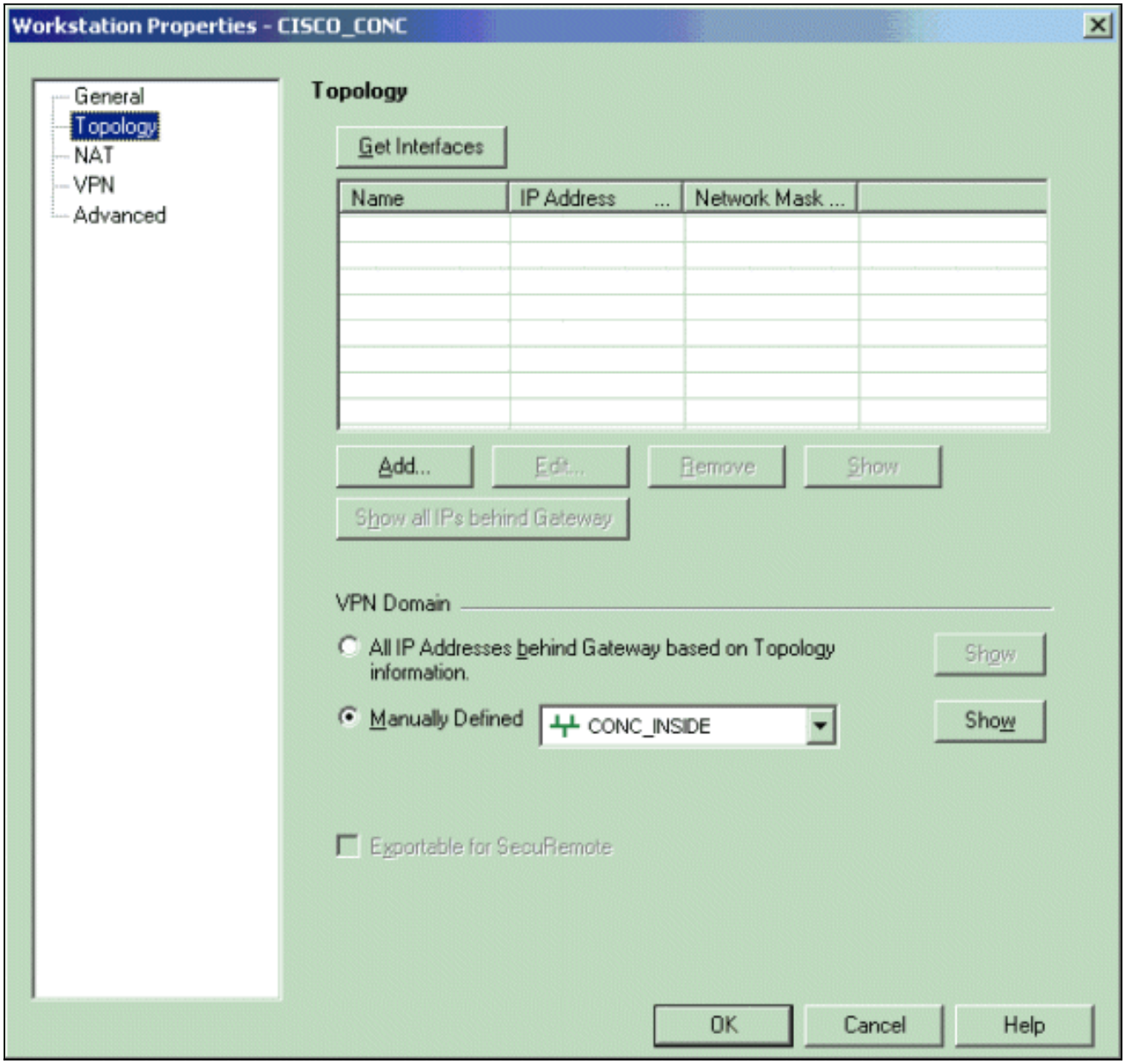
8. **Pre-Shared Secrets(사전 공유 암호)**에 대한 인증 옵션을 선택한 다음 **Edit Secrets(**보안 수정**)**를 클릭하여 VPN Concentrator의 사전 공유 키와 호환되도록 사전 공유 키를 설정합니다. Edit(**편집)**를 클릭하여 표시된 대로 키를 입력한 다음 **Set**, **OK**(설정, 확인)를 **클릭합니다**



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**, **OK**를 클릭합니다

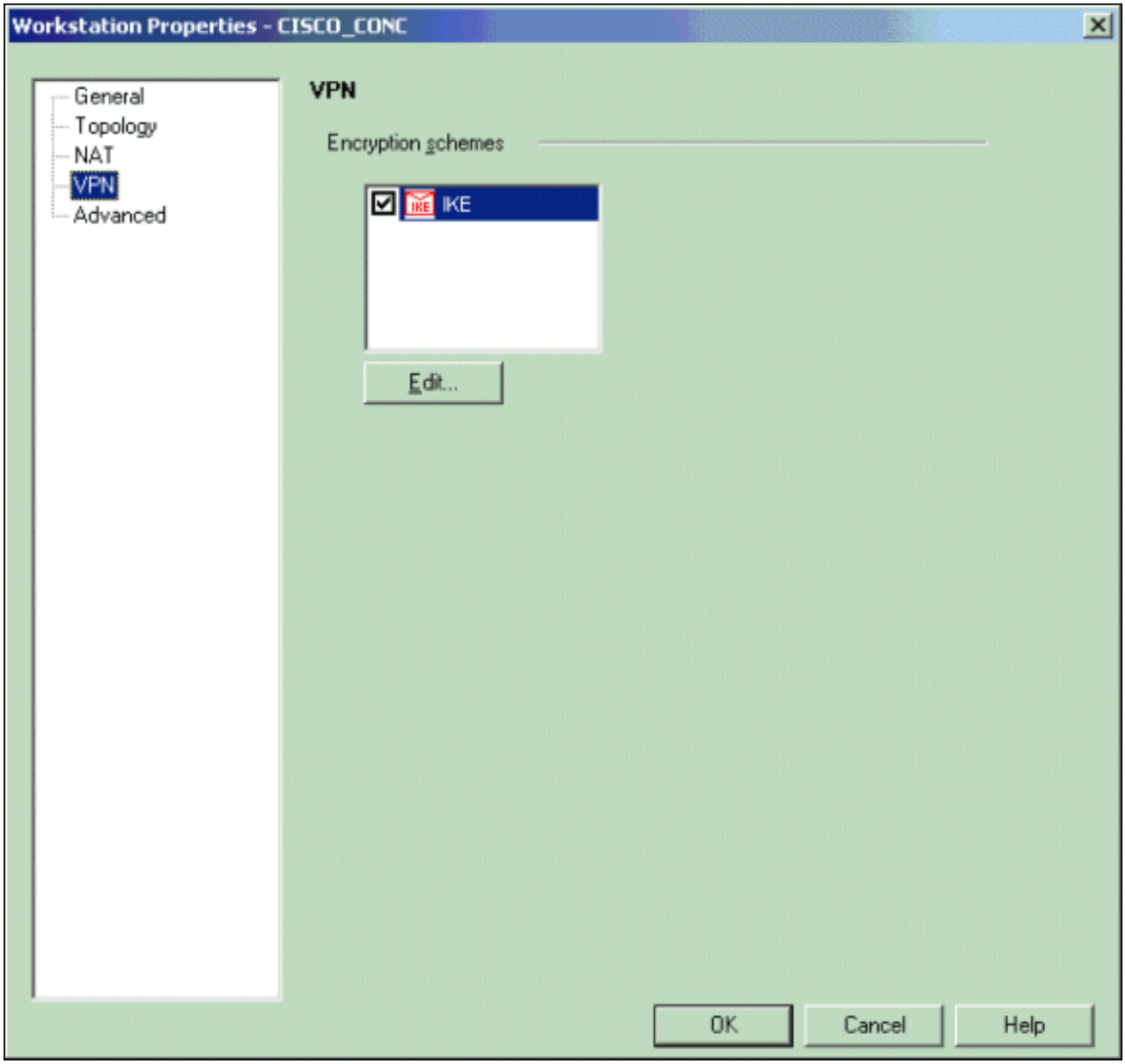


10. Manage(**관리) > Network Objects(네트워크 개체) > Edit(편집)**로 이동하여 VPN Concentrator의 Workstation Properties(워크스테이션 속성) 창을 엽니다. VPN 도메인을 수동으로 정의하려면 창 왼쪽의 선택 항목에서 Topology를 선택합니다.이 예에서는 CONC_INSIDE(VPN Concentrator의 내부 네트워크)가 VPN 도메인으로 정의됩니다
.

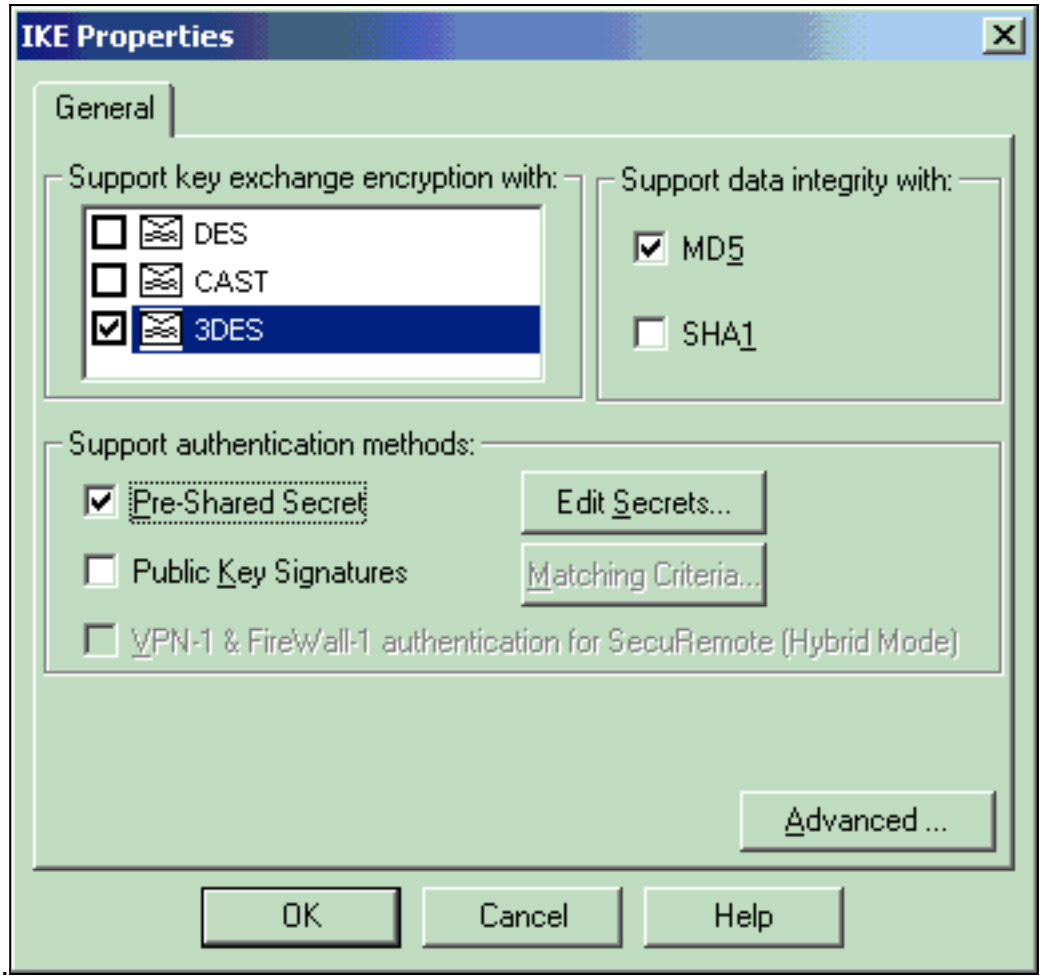


11. 창 왼쪽에 있는 선택 사항에서 VPN을 선택한 다음 **IKE**를 암호화 체계로 선택합니다. IKE 속성을 구성하려면 Edit를 클릭합니다

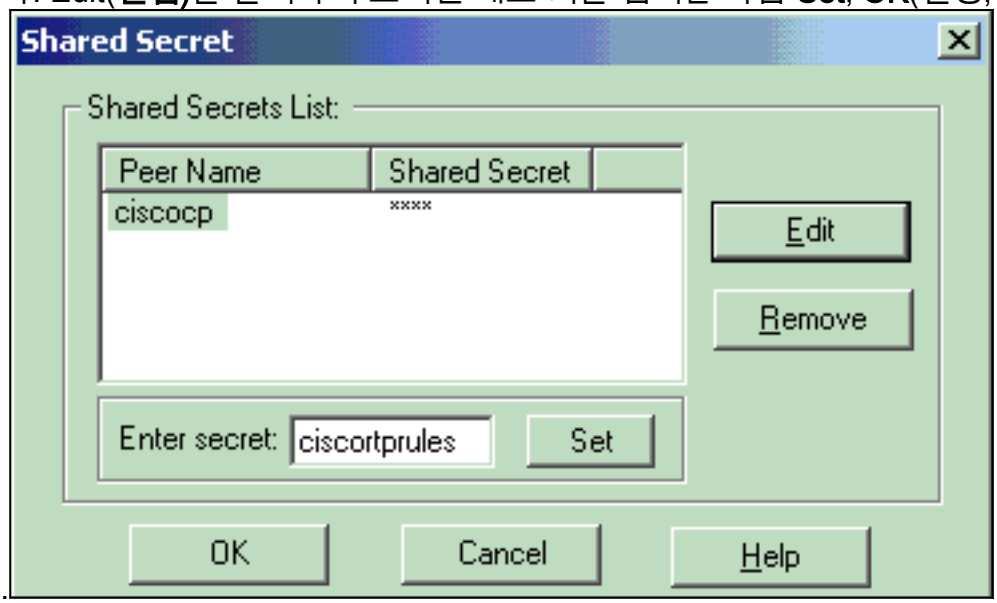
.



12. VPN Concentrator의 현재 컨피그레이션을 반영하도록 IKE 속성을 설정합니다.이 예에서는 **3DES**의 암호화 옵션 및 **MD5**의 해싱 옵션을 **설정합니다**

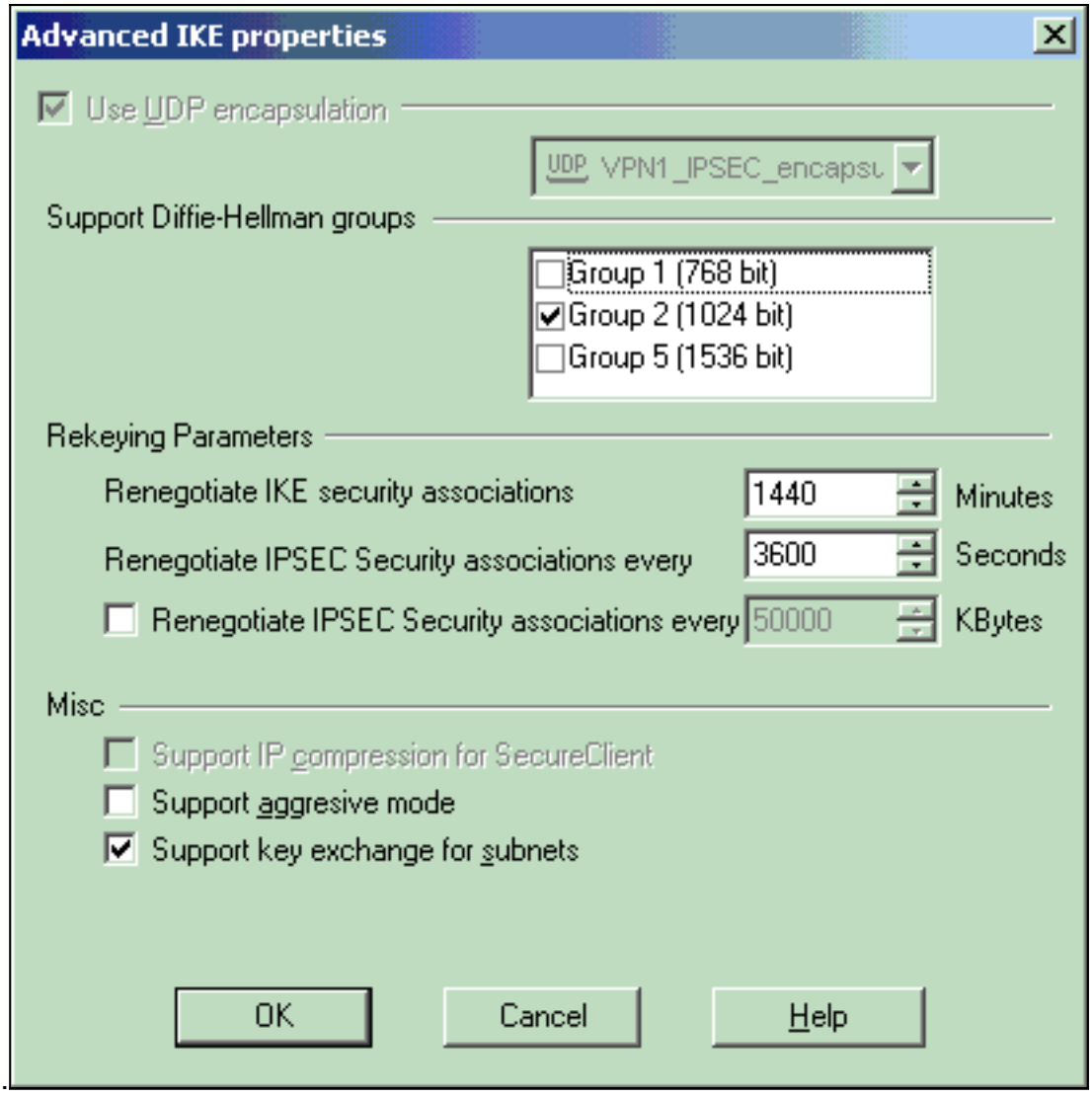


13. **사전 공유 암호**에 대한 인증 옵션**을** 선택한 다음 **Edit Secrets를** 클릭하여 사전 공유 키를 설정합니다. Edit(**편집)**를 클릭하여 표시된 대로 키를 입력한 다음 **Set**, **OK**(설정, 확인)를 **클릭**



합니다.

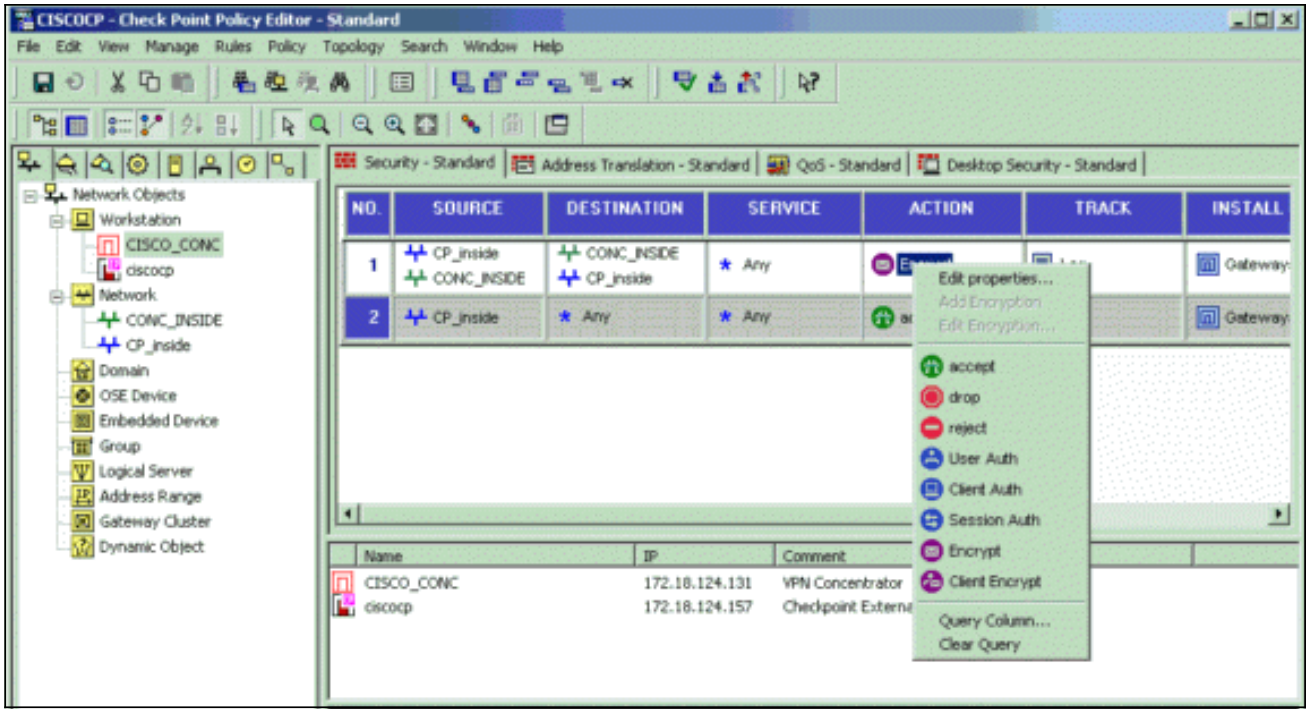
14. IKE 속성 창에서 **Advanced...를** 클릭하고 다음 설정을 변경합니다.IKE 속성에 적합한 Diffie-Hellman 그룹을 선택합니다.**Support aggressive 모드**에 대한 옵션**을 선택 취소합니다**.서브넷에 **대한 Support key exchange(키 교환 지원) 옵션을 선택합니다**.완료되면 **OK**, **OK**를 클릭



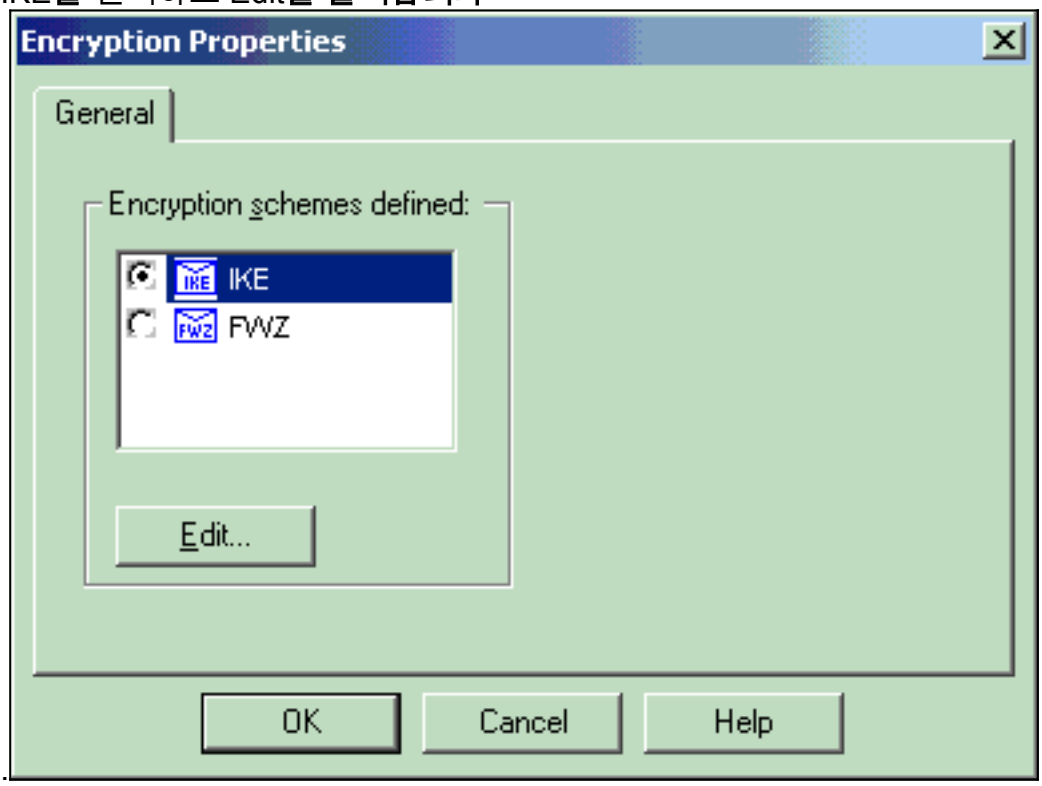
합니다.

15. 정책에 대한 암호화 규칙을 구성하려면 **Rules > Add Rules > Top**을 선택합니다. Policy Editor(정책 편집기) 창에서 소스가 CP_inside(Checkpoint NG의 내부 네트워크)이고 대상이 CONC_INSIDE(VPN Concentrator의 내부 네트워크)인 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

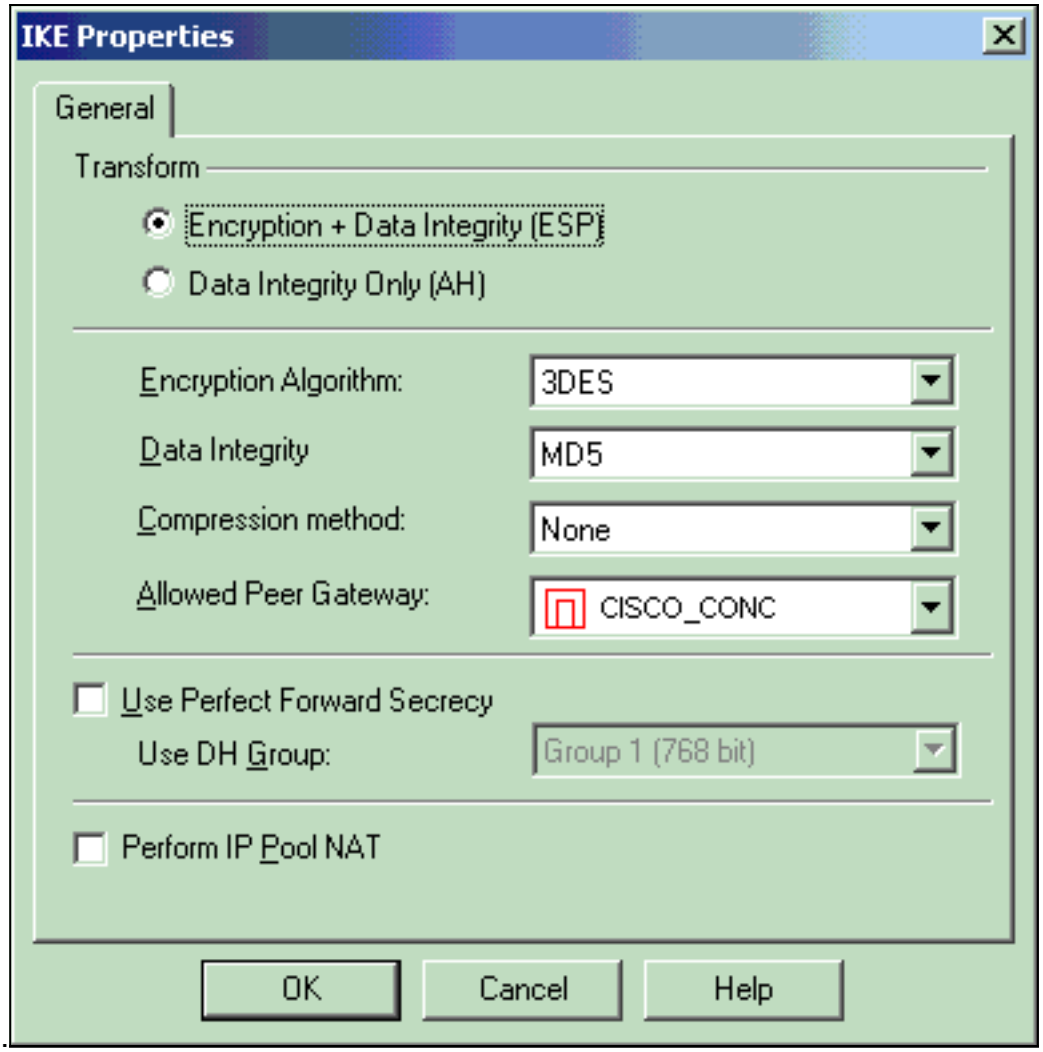
.



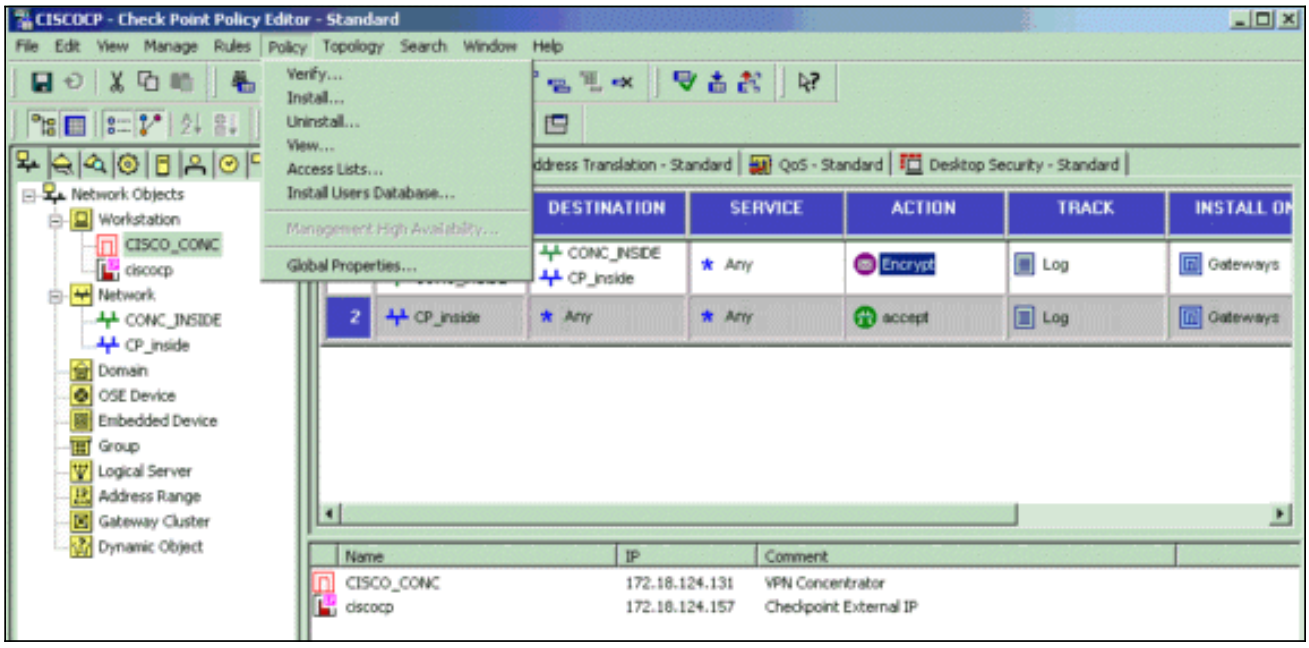
16. IKE를 선택하고 Edit를 **클릭합니다**



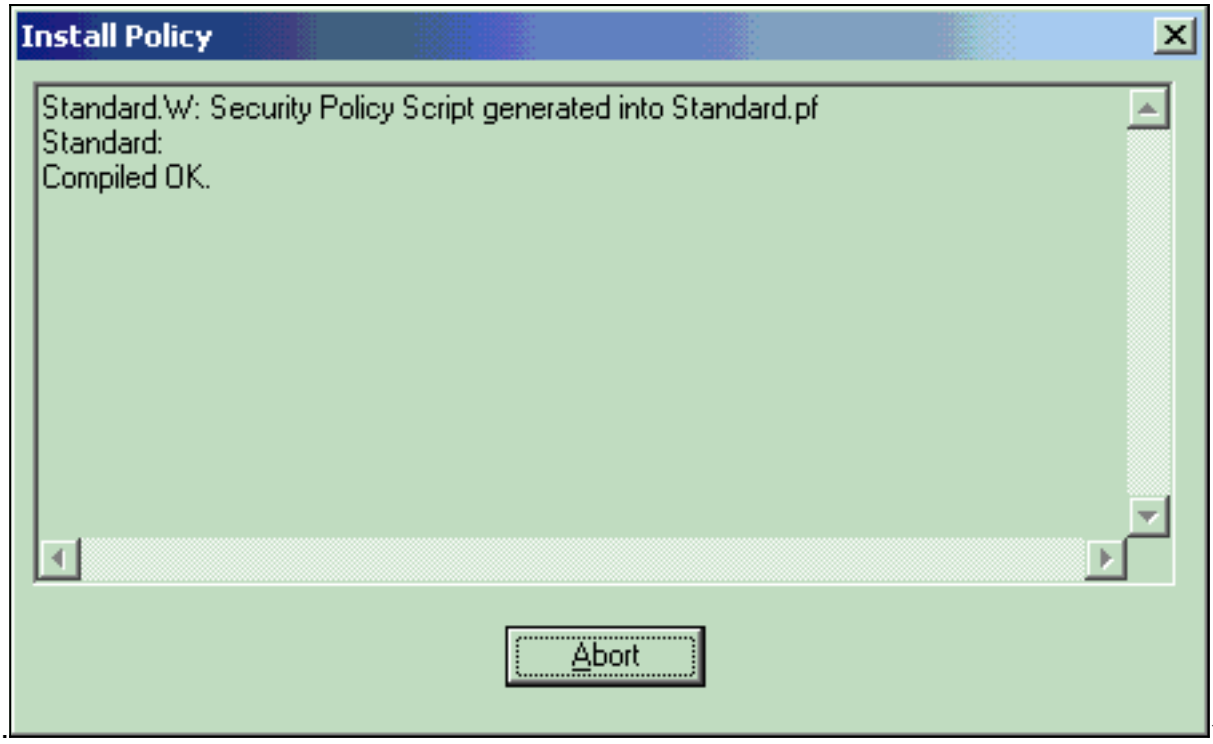
17. IKE Properties(IKE 속성) 창에서 VPN Concentrator 변환에 동의하도록 속성을 변경합니다 .Transform(변형) 옵션을 **Encryption + Data Integrity(ESP)로 설정합니다**.Encryption Algorithm(암호화 알고리즘)을 **3DES**로 **설정합니다**.데이터 무결성을 **MD5**로 **설정합니다** .VPN Concentrator(CISCO_CONC)와 일치하도록 Allowed Peer Gateway(허용된 피어 게이트웨이)를 설정합니다.완료되면 **확인**을 클릭합니다



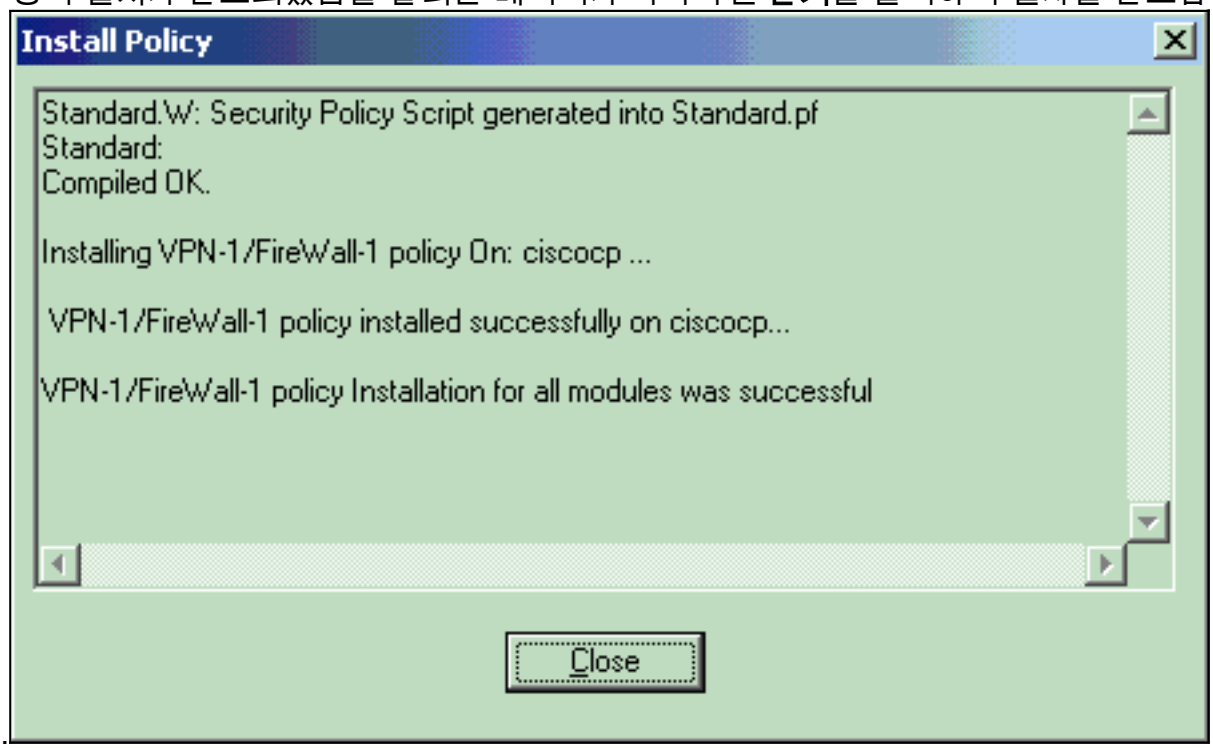
18. Checkpoint NG가 구성된 후 정책을 저장하고 Policy(**정책) > Install(설치**)을 선택하여 활성화합니다



정책이 컴파일될 때 설치 창에 진행 정보가 표시됩니다



.설치 창에 정책 설치가 완료되었음을 알리는 메시지가 나타나면 **닫기**를 클릭하여 절차를 완료합니다.

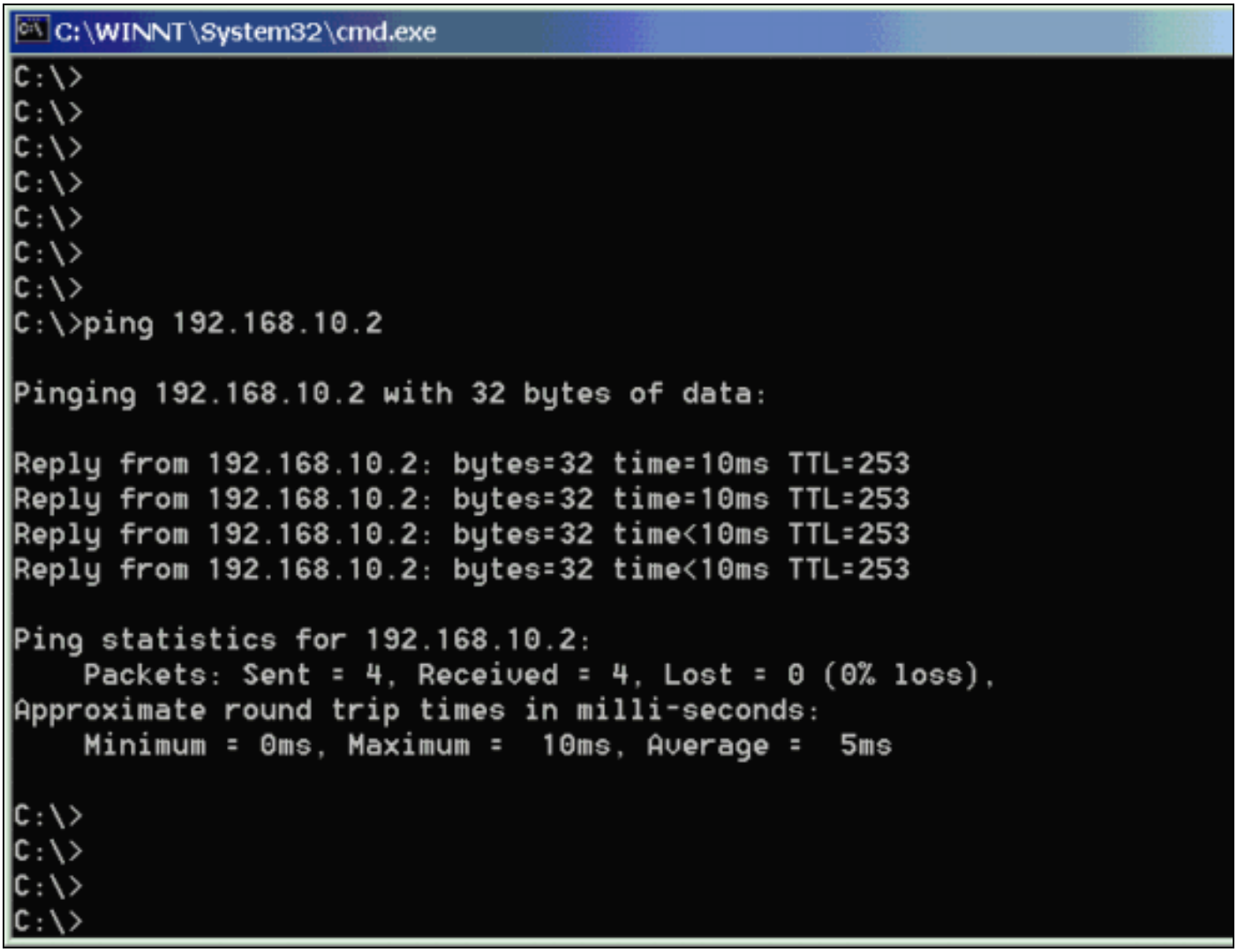


다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

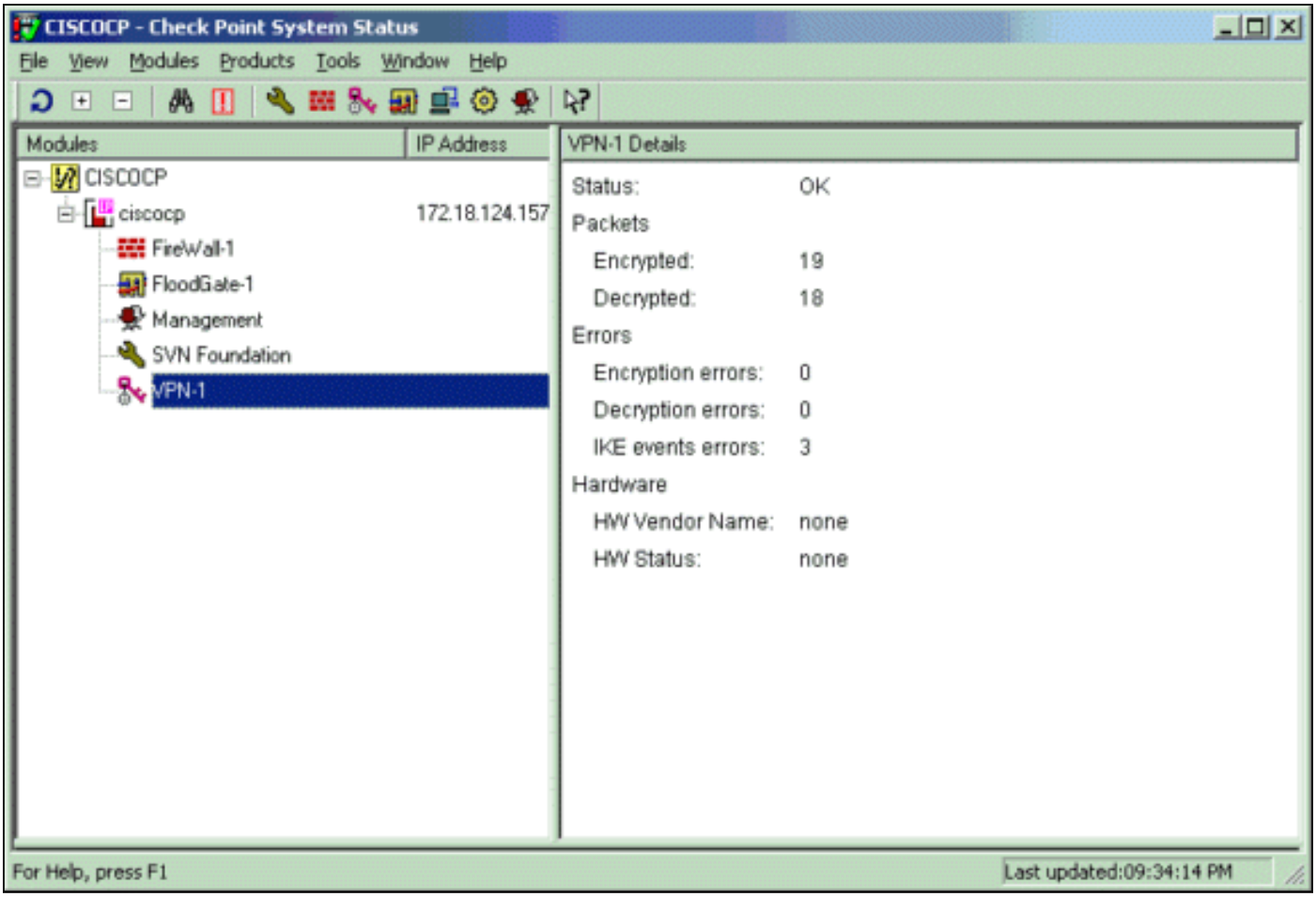
네트워크 통신 확인

두 프라이빗 네트워크 간의 통신을 테스트하려면 사설 네트워크 중 하나에서 다른 프라이빗 네트워크로 ping을 시작할 수 있습니다. 이 컨피그레이션에서는 Checkpoint NG 측(10.32.50.51)에서 VPN Concentrator 네트워크(192.168.10.2)으로 ping이 전송되었습니다.



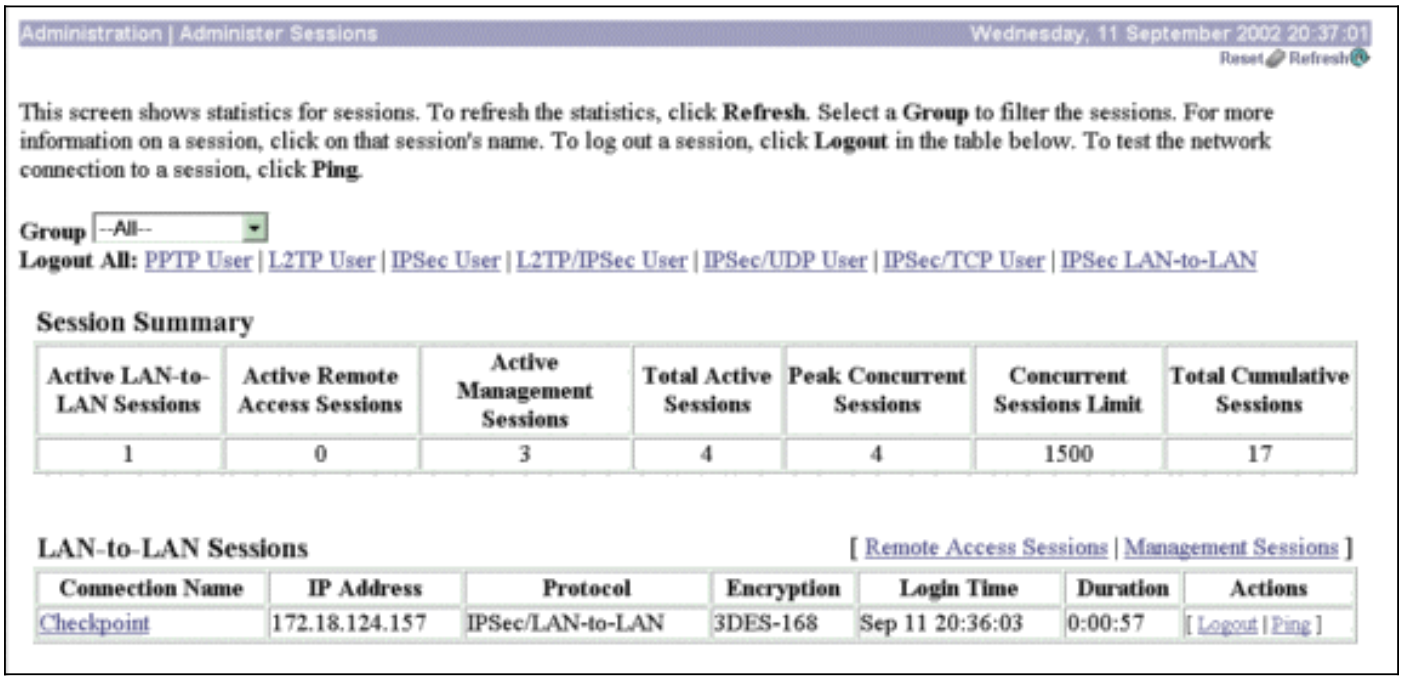
체크포인트 NG에서 터널 상태 보기

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



VPN Concentrator에서 터널 상태 보기

VPN Concentrator에서 터널 상태를 확인하려면 Administration(관리) **> Administer Sessions(세션 관리)로 이동합니다**.



LAN-to-LAN Sessions(LAN-to-LAN 세션) 아래에서 생성된 SA에 대한 세부 정보와 전송/수신된 패킷 수를 볼 체크포인트의 연결 이름을 선택합니다.

Administration | Administer Sessions | Detail Wednesday, 11 September 2002 20:37:59

Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	**IKE Negotiation Mode**	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	**Remote Address**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

문제 해결

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

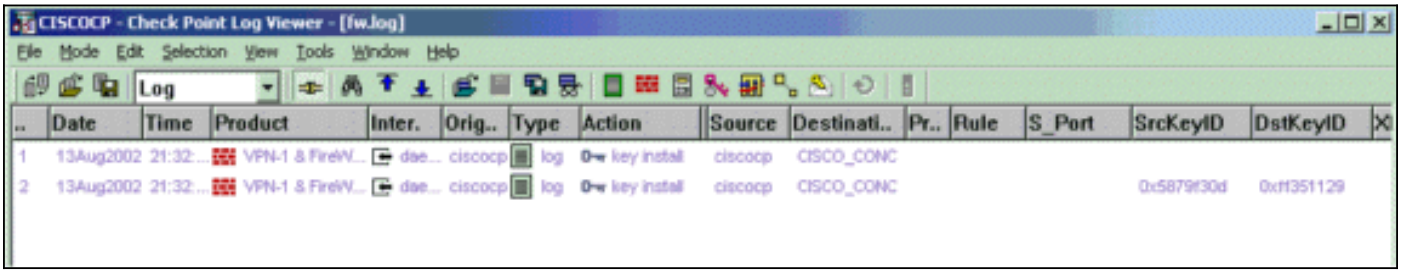
참고: 트래픽은 VPN Concentrator 공용 IP 주소(외부 인터페이스)를 사용하여 IPSec 터널을 통해 PAT되지 않아야 합니다. 그렇지 않으면 터널이 실패합니다. 따라서 PATing에 사용되는 IP 주소는 외부 인터페이스에 구성된 주소 이외의 주소여야 합니다.

네트워크 요약

Checkpoint의 암호화 도메인에 여러 개의 인접 네트워크가 구성된 경우, 해당 디바이스는 관심 있는 트래픽과 관련된 네트워크를 자동으로 요약할 수 있습니다. VPN Concentrator가 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 이러한 네트워크는 10.0.0.0 /23으로 요약할 수 있습니다.

검사점 NG용 디버그

로그를 보려면 **창 > 로그 뷰어**를 선택합니다.



VPN Concentrator용 디버그

VPN Concentrator에서 디버그를 활성화하려면 Configuration(컨피그레이션) **> System(시스템) >**

Events(이벤트) > Classes(클래스)로 이동합니다. 심각도에 대해 AUTH, AUTHDBG, IKE, IKEDBG, IPSEC 및 IPSECDBG를 활성화하여 1 - 13으로 기록합니다. 디버그를 보려면 **모니터링 > 필터링 가능한 이벤트 로그를** 선택합니다.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157
constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184
```

```
31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157
processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157
processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157
processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157
constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157
constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157
constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157
constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157
Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157
constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157
Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157
Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157
Group [172.18.124.157]
Processing ID

51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157
Group [172.18.124.157]
processing hash

52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157
Group [172.18.124.157]
computing hash

53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157
Group [172.18.124.157]
```

```
Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10
AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10
Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10
AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10
AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10
AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10
Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10
AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10
Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10
AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10
AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10
Reply timer started: handle = 4B0018, timestamp = 1163319,
timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10
AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19
IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19
IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10
xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20
IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10
IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10
AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20
IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10
IntDB_Rcv(51a6b48)

74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10
```

```
AUTH_DeleteTimer(51a6b48, 0, 0)

75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10
Reply timer stopped: handle = 4B0018, timestamp = 1163329

76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10
AUTH_Callback(51a6b48, 0, 0)

77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157
Authentication successful: handle = 9, server = Internal,
group = 172.18.124.157

78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157
Group [172.18.124.157]
Found Phase 1 Group (172.18.124.157)

79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10
AUTH_GetAttrTable(9, 748420)

80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157
Group [172.18.124.157]
Authentication configured for Internal

81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: IP Compression = disabled

82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10
AUTH_Close(9)

84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157
Group [172.18.124.157]
constructing ID

85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527
Group [172.18.124.157]
construct hash payload

86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157
Group [172.18.124.157]
computing hash

87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157
Group [172.18.124.157]
constructing dpd vid payload

88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 80

90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157
Group [172.18.124.157]
PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157
Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157
Keep-alives configured on but peer does not
support keep-alives (type = None)
```

```
93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157
Group [172.18.124.157]
Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16
User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10
AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10
AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10
Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157
Group [172.18.124.157]
processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157
Group [172.18.124.157]
processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157
Group [172.18.124.157]
processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157
Group [172.18.124.157]
Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157
Group [172.18.124.157]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157
Group [172.18.124.157]
Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534
QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157
Group [172.18.124.157]
IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157
Group [172.18.124.157]
```

```
processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157
Group [172.18.124.157]
IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157
Group [172.18.124.157]
IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0,
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139
Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10
Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10
IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157
Group [172.18.124.157]
oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157
Group [172.18.124.157]
constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157
Group [172.18.124.157]
constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157
Group [172.18.124.157]
constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157
Group [172.18.124.157]
constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157
Group [172.18.124.157]
Transmitting Proxy Id:
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157
Group [172.18.124.157]
constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157
SENDING Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157
```

```
Group [172.18.124.157]
processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157
Group [172.18.124.157]
loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157
Group [172.18.124.157]
Loading subnet:
Dst: 192.168.10.0 mask: 255.255.255.0
Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157
Group [172.18.124.157]
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40
IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,
spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140
Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141
key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142
No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143
KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144
KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145
KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,
dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146
KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!

165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
```

```
Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

관련 정보

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support - Cisco Systems