IPSec 터널 구성 - Cisco VPN 3000 Concentrator를 Checkpoint 4.1 방화벽으로 구성

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
네트워크 다이어그램
표기 규칙
VPN 3000 Concentrator 구성
Checkpoint 4.1 방화벽 구성
다음을 확인합니다.
문제 해결
네트워크 요약
VPN 3000 Concentrator 디버그
검사점 4.1 방화벽 디버그
디버그 출력 샘플
관련 정보

소개

이 문서에서는 두 개의 프라이빗 네트워크에 연결하기 위해 사전 공유 키를 사용하여 IPsec 터널을 구성하는 방법을 설명합니다.

- Cisco VPN 3000 Concentrator(192.168.1.x) 내부의 사설 네트워크.
- Checkpoint 4.1 방화벽(10.32.50.x)에 있는 사설 네트워크.

이 컨피그레이션이 시작되기 전에 VPN Concentrator 내부 및 Checkpoint 내에서 인터넷(이 문서에서 172.18.124.x 네트워크로 표시됨)으로 이동하는 트래픽이 이동하는 것으로 가정합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

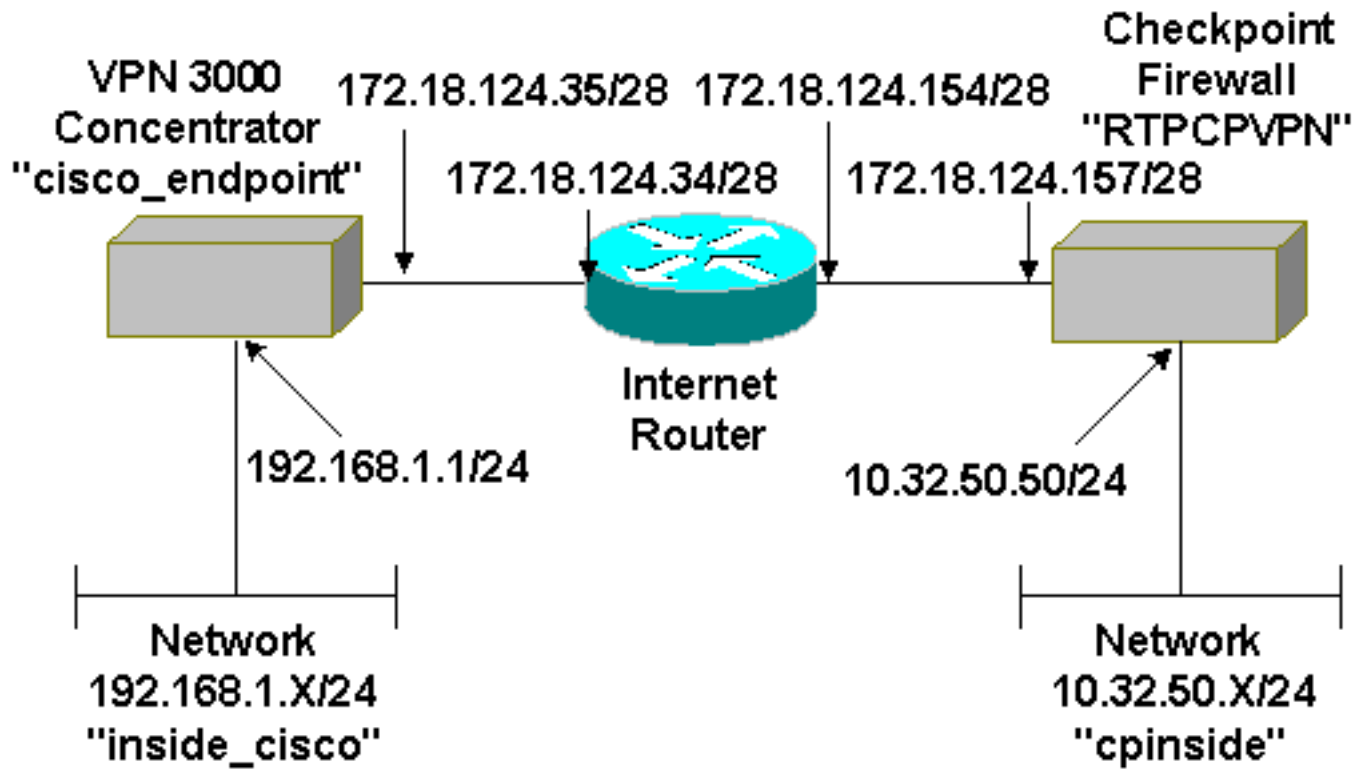
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VPN 3000 Concentrator
- VPN 3000 Concentrator 소프트웨어 릴리스 2.5.2.F
- 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.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



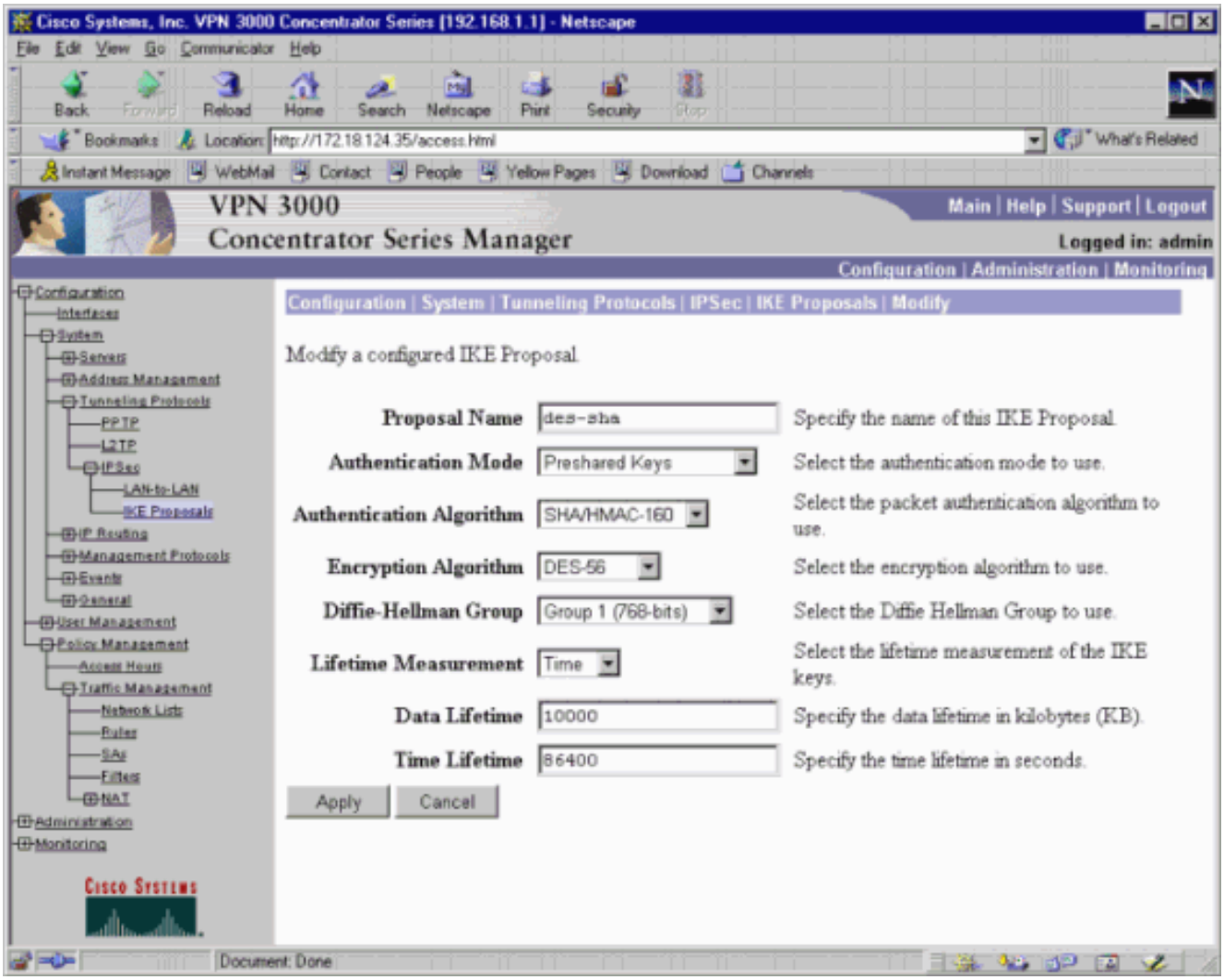
표기 규칙

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

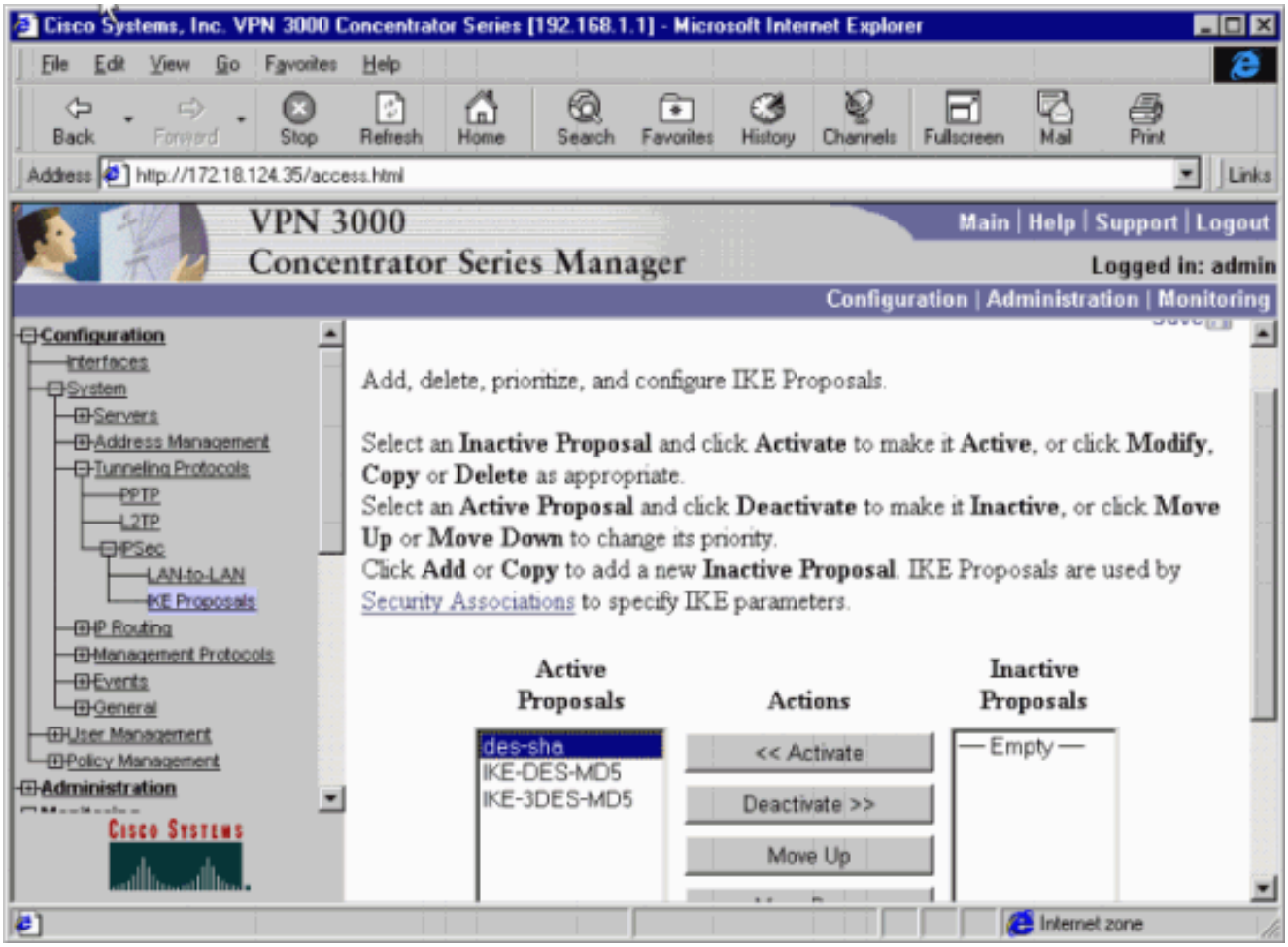
VPN 3000 Concentrator 구성

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

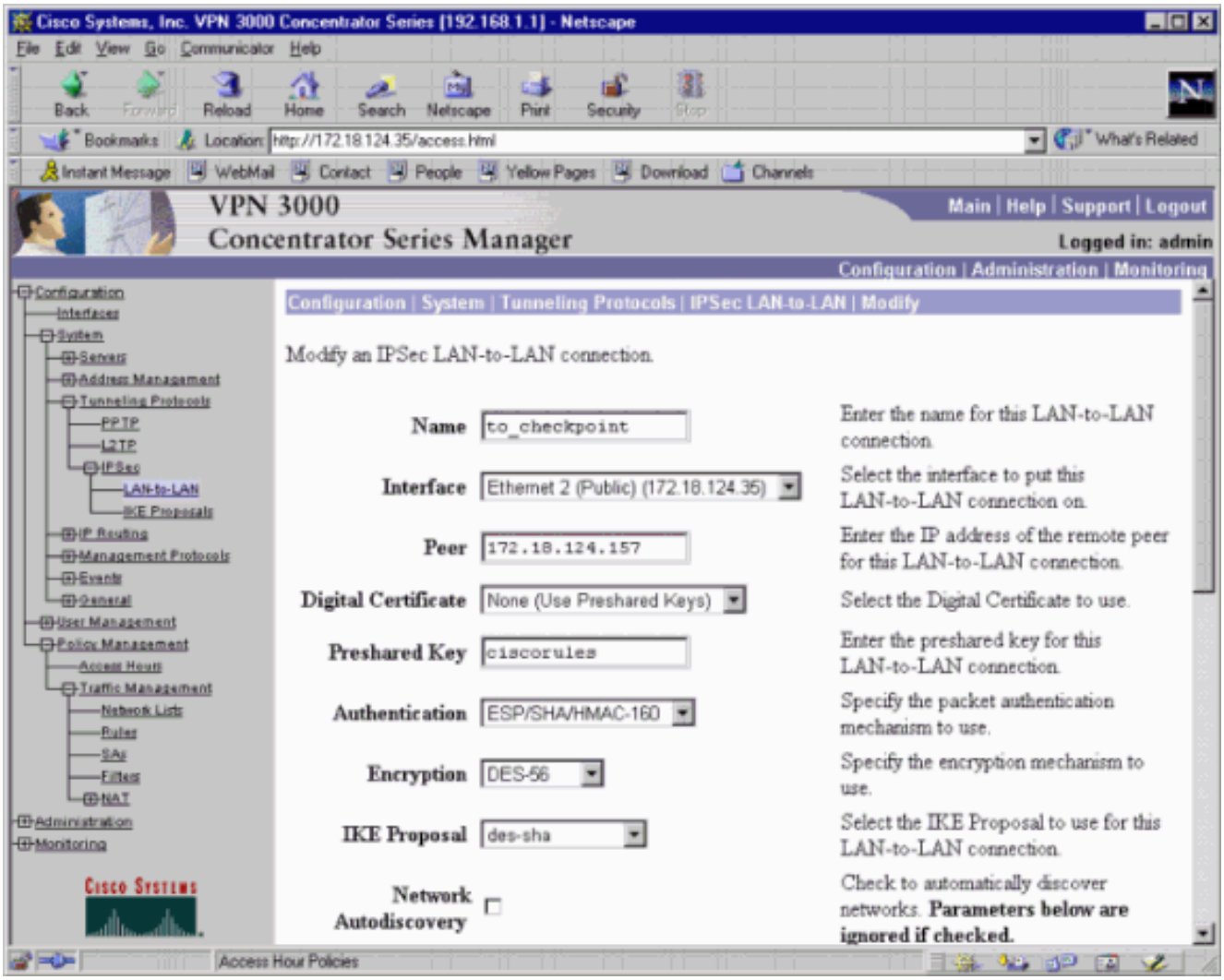
1. Configuration(**구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > IKE Proposals(IKE 제안) > Modify(수정)를** 선택하여 SHA(Secure Hash Algorithance) 해싱, DES(Data Encryption Standard) 및 Diffie-Hellman Group 1이라는 IKE 제안서를 생성합니다. 시간 수명을 기본 86400초로 유지합니다.**참고:** VPN Concentrator IKE 수명의 유효한 범위는 60-2147483647초입니다
   .

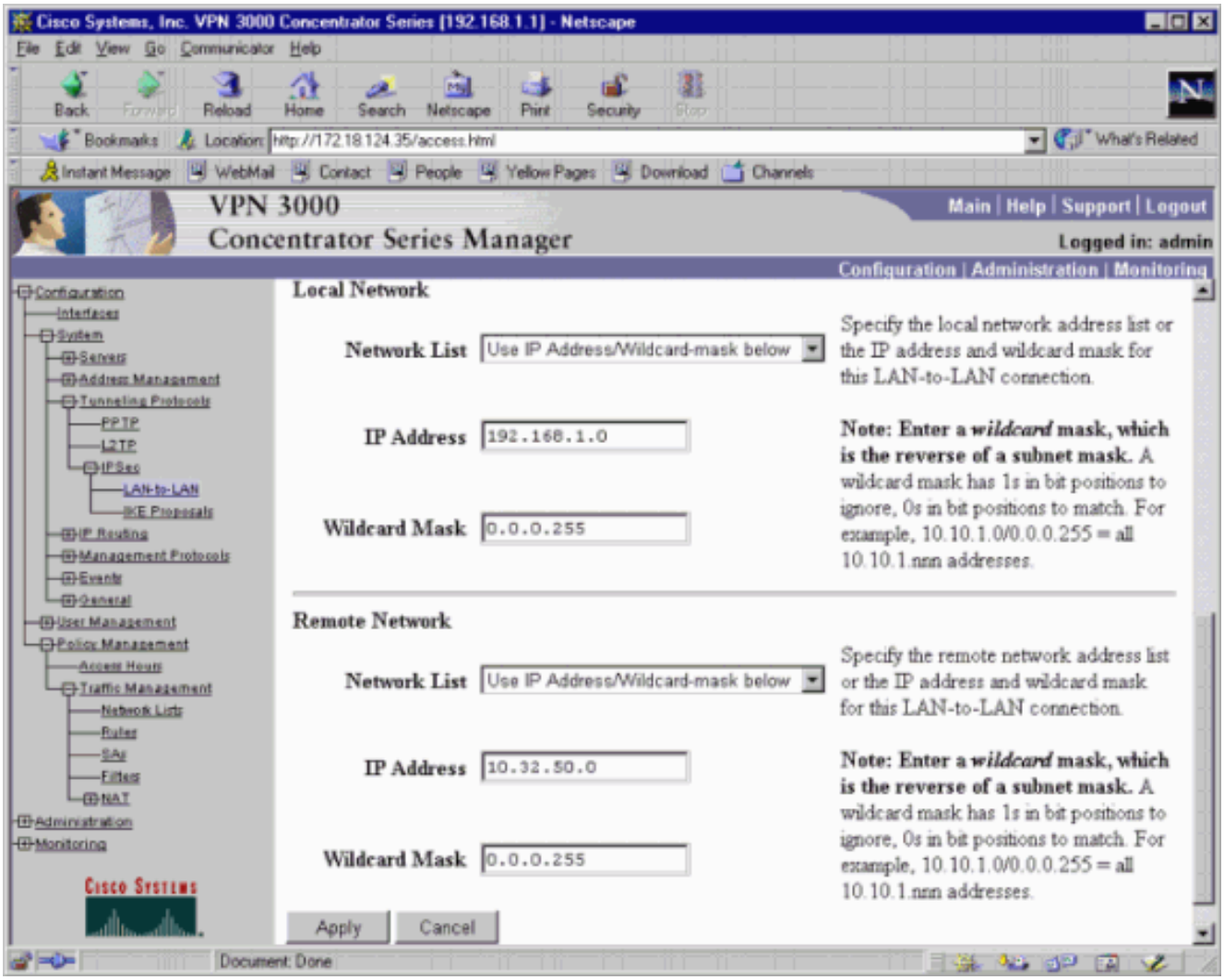


2. Configuration **> System > Tunneling Protocols > IPSec > IKE Proposals를 선택합니다**. "des-sha"를 선택하고 Activate(**활성화)**를 클릭하여 IKE 제안을 활성화합니다
.



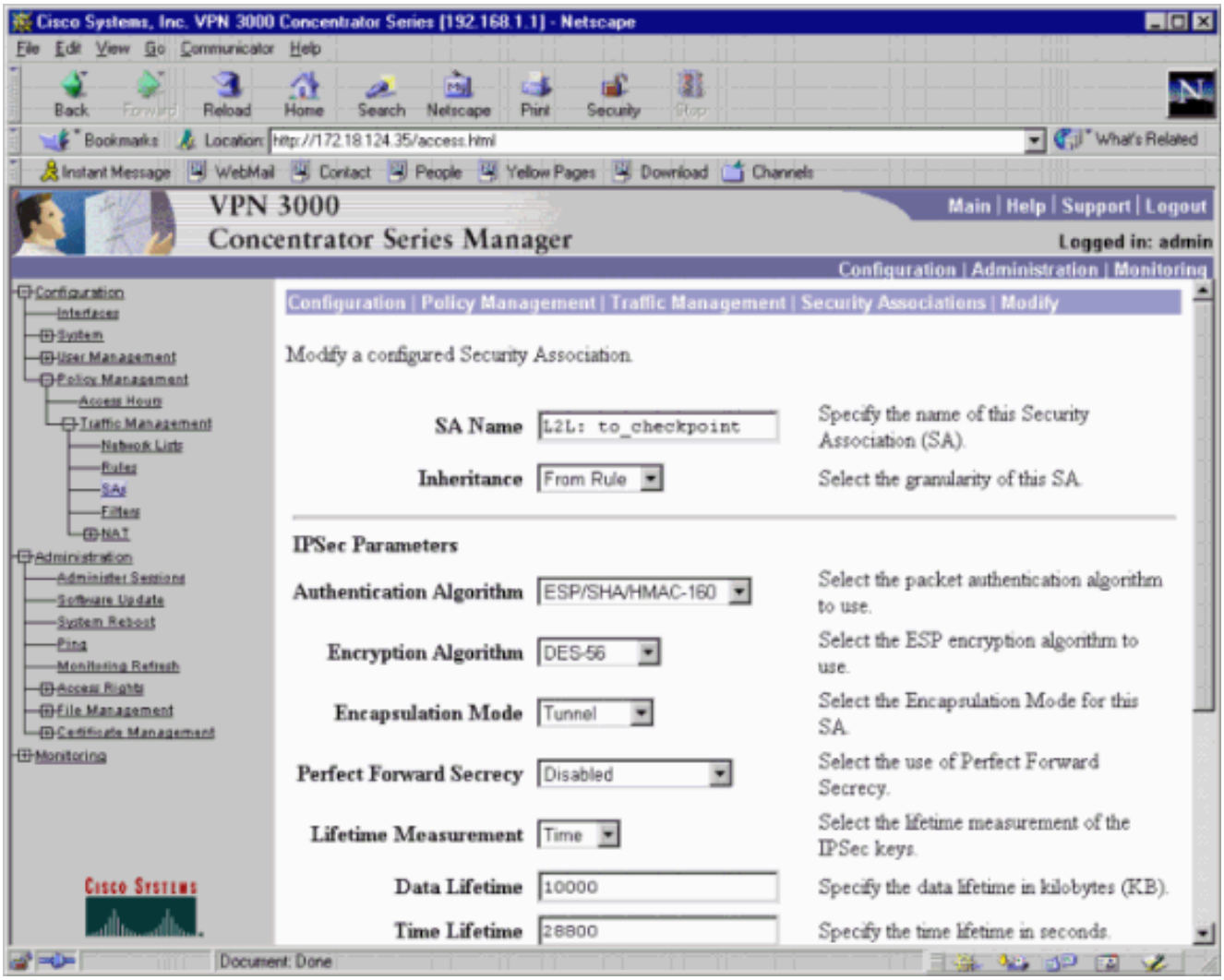
3. Configuration **> System > Tunneling Protocols > IPSec LAN-to-LAN > Add를 선택합니다** .Checkpoint 주소를 피어로 사용하여 "to_checkpoint"라는 IPsec 터널을 설정합니다. 사전 공유 키의 경우 실제 키를 입력합니다. Authentication(인증)에서 ESP/SHA/HMAC-160을 선택하고 Encryption(암호화)에 DES-56을 선택합니다. IKE 제안서("이 예에서는 "des-sha")와 로컬 및 원격 네트워크를 입력합니다
.

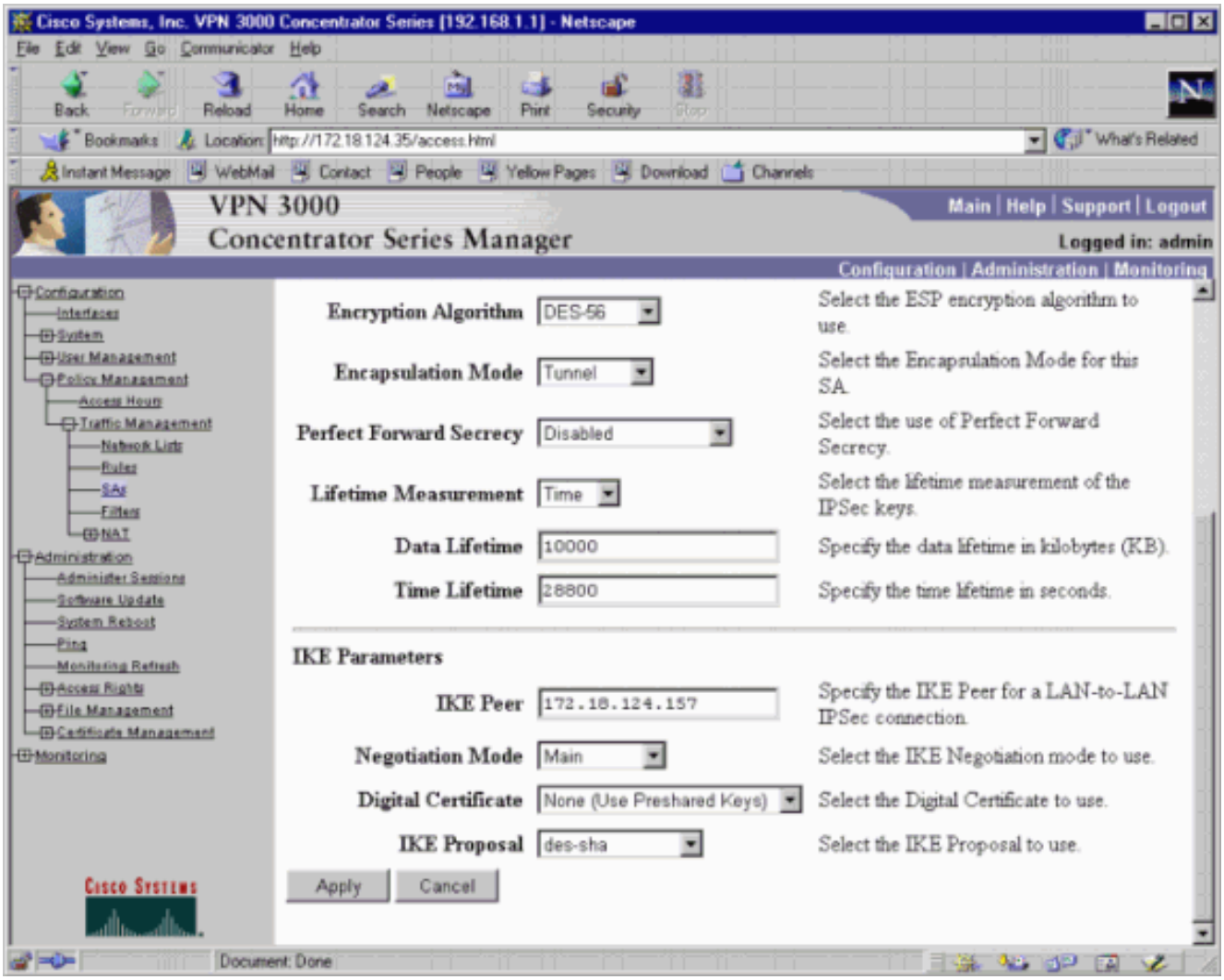

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies



4. Configuration **> Policy Management > Traffic Management > Security Associations > Modify를 선택합니다**. Perfect Forward Secrecy가 Disabled(**완전 순방향** 보안)인지 확인하고 IPsec 시간 수명을 기본 **28800**초로 둡니다.**참고:** VPN Concentrator IPsec 수명의 유효한 범위는 60-2147483647초입니다

.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Cisco Systems
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name L2L: to_checkpoint Specify the name of this Security Association (SA).
Inheritance From Rule Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm ESP/SHA/HMAC-160 Select the packet authentication algorithm to use.
Encryption Algorithm DES-56 Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000 Specify the data lifetime in kilobytes (KB).
Time Lifetime 28800 Specify the time lifetime in seconds.
Document: Done

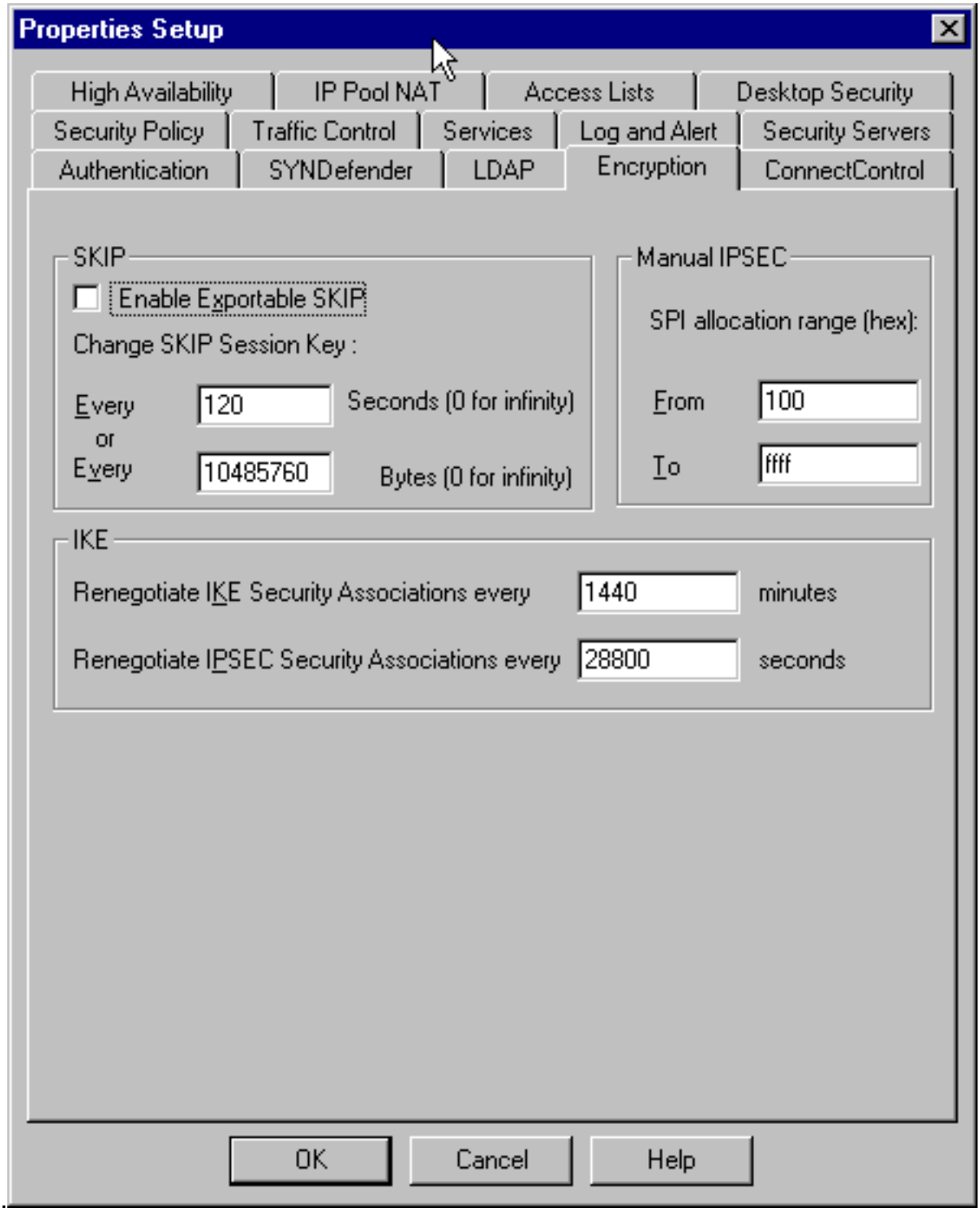


5. 컨피그레이션을 저장합니다.

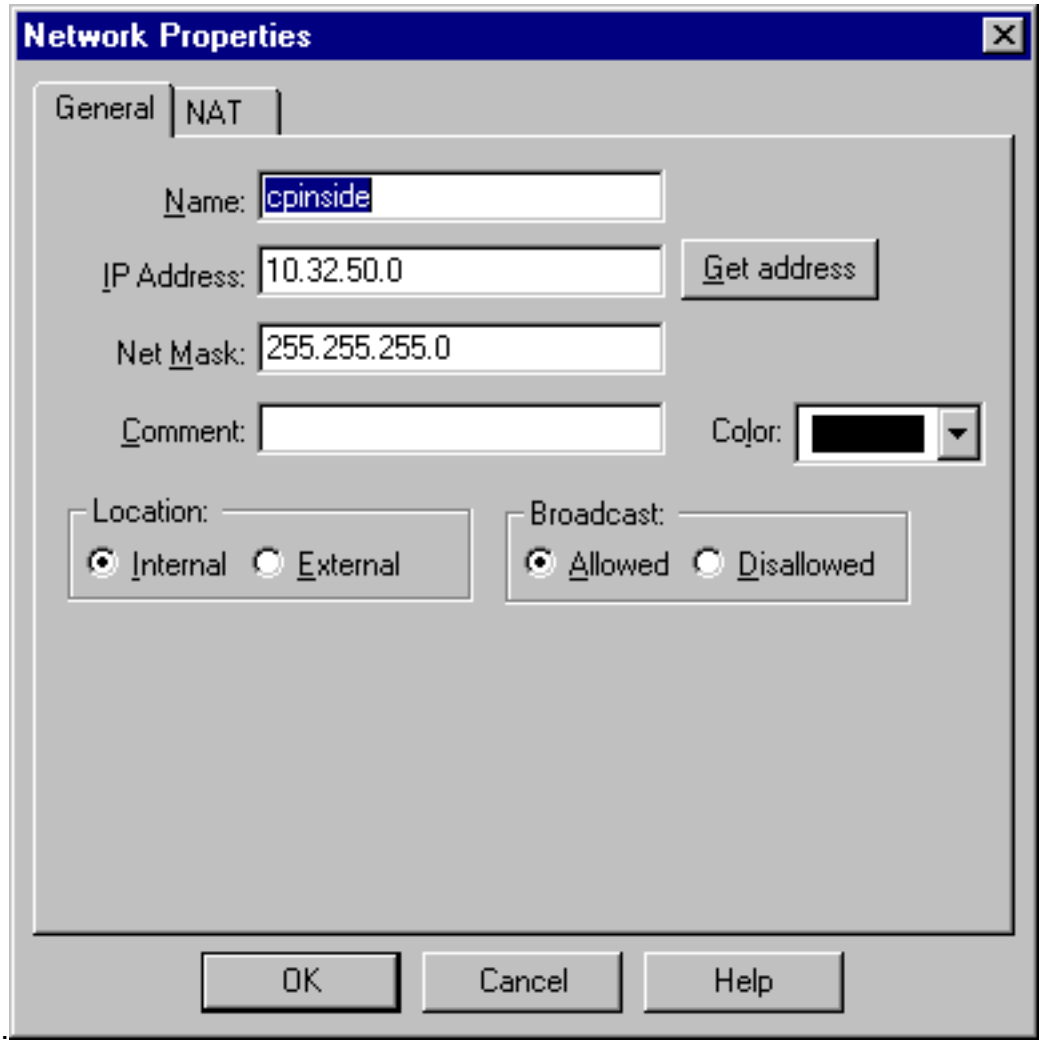
Checkpoint 4.1 방화벽 구성

Checkpoint 4.1 방화벽을 구성하려면 다음 단계를 완료하십시오.

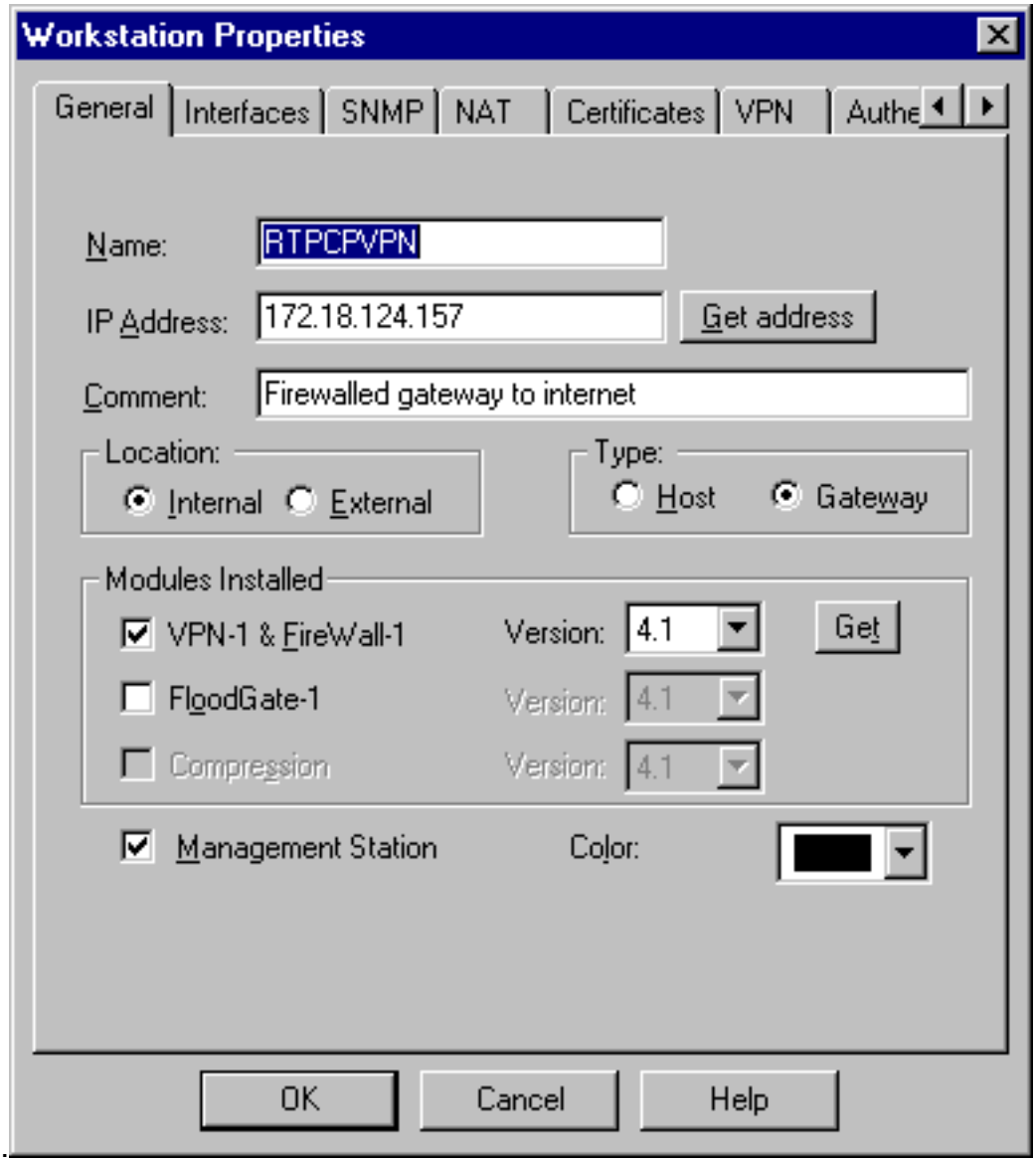
1. IKE 및 IPsec 기본 수명은 벤더 간에 다르기 때문에 Properties(**속성**) > Encryption(암호화)을 선택하여 Checkpoint lifetime을 설정하여 VPN Concentrator 기본값을 확인합니다.VPN Concentrator 기본 IKE 수명은 86400초(1440분)입니다.VPN Concentrator 기본 IPsec 수명은 28,800초입니다



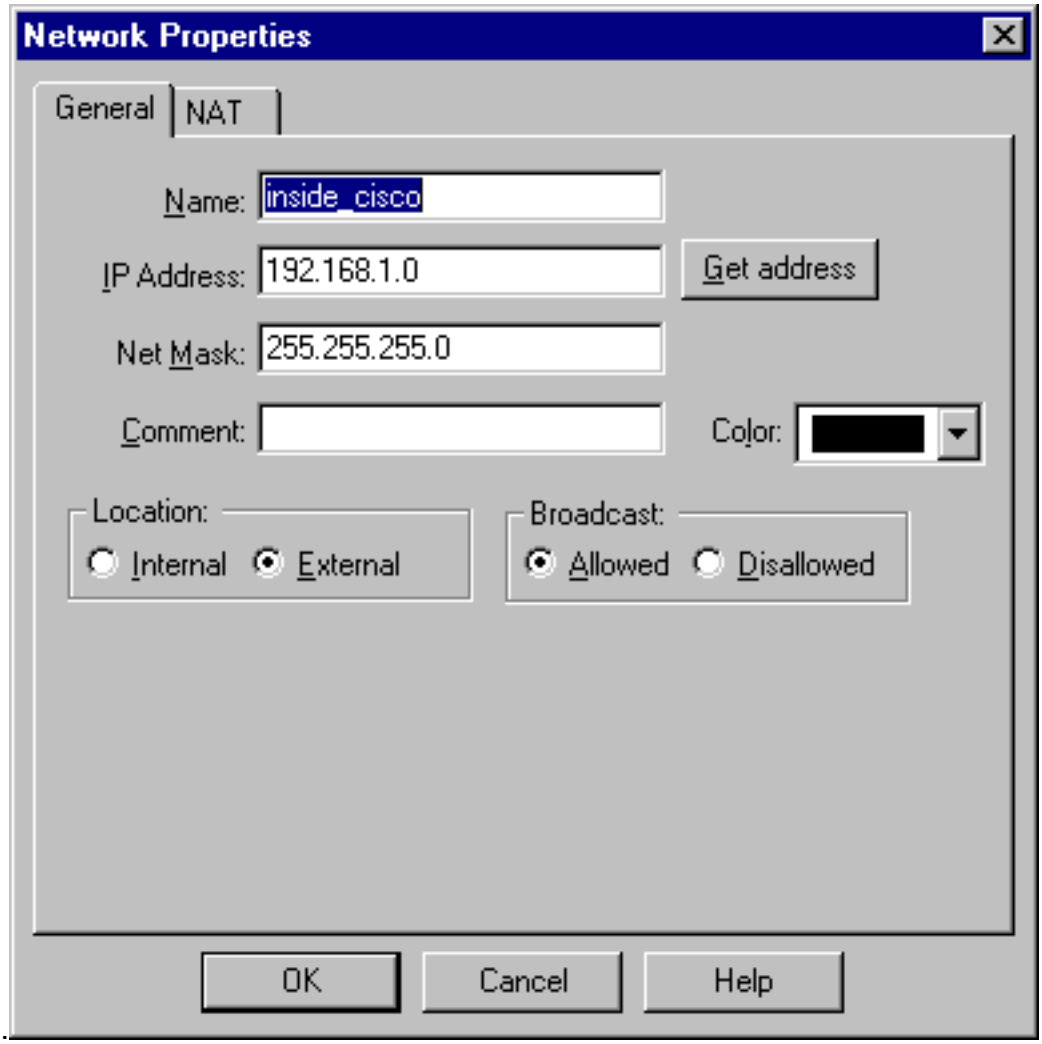
2. Manage(**관리) > Network objects(네트워크 개체) > New(또는 Edit) > Network(네트워크)**를 선택하여 체크포인트 뒤에 있는 내부("cpinside") 네트워크에 대한 개체를 구성합니다. 이는 VPN Concentrator의 "원격 네트워크"와 일치해야 합니다



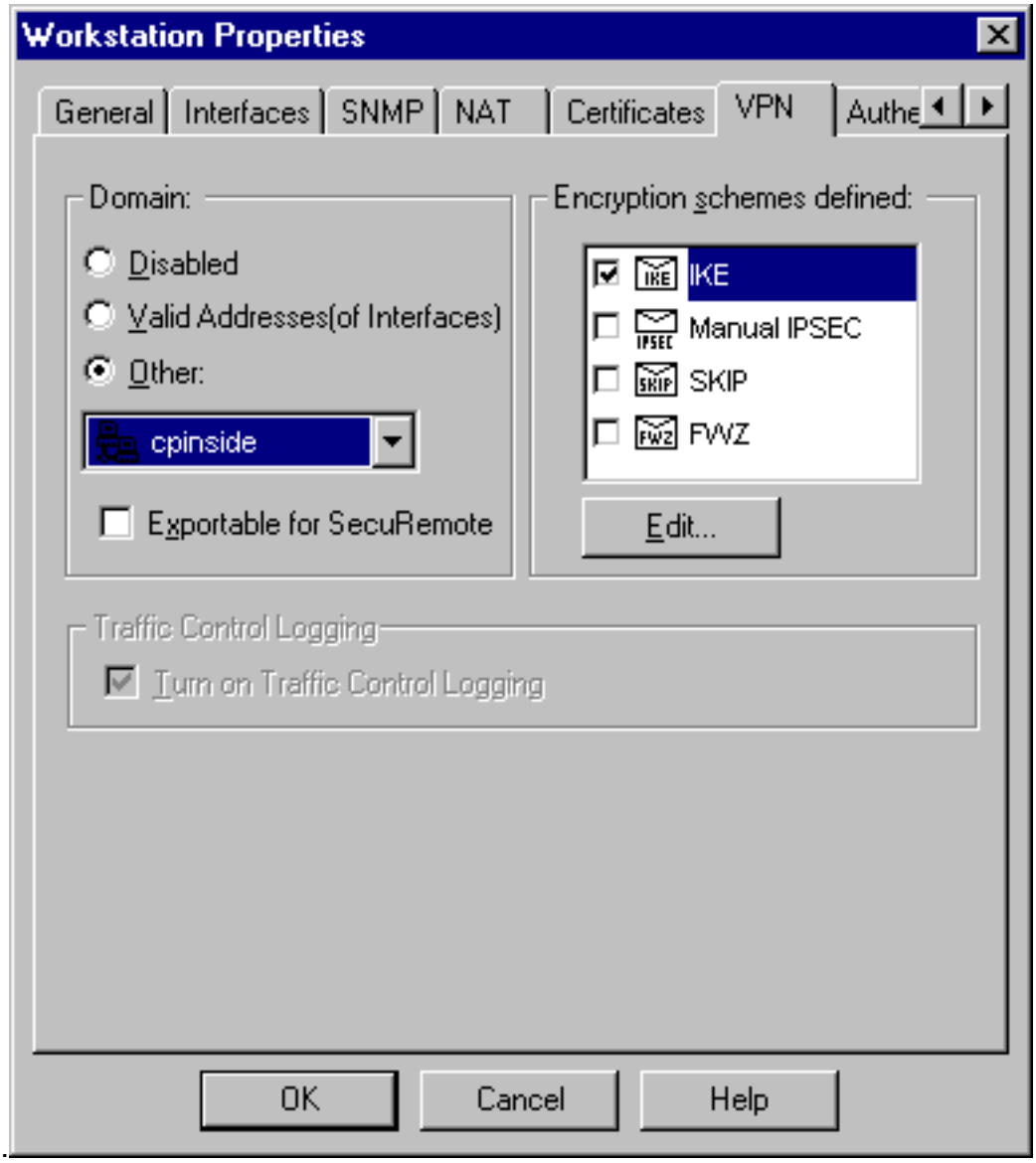
3. Manage(**관리) > Network objects(네트워크 개체) > Edit(편집)**를 선택하여 VPN Concentrator가 Peer(피어) 매개변수에 가지고 있는 게이트웨이("RTPCPVPN" Checkpoint) 엔드포인트의 개체를 편집합니다.위치(Location)에서 내부(Internal)를 **선택합니다**. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다. Modules Installed(설치된 모듈)에서 **VPN-1 및 FireWall-1을** 선택하고 **Management Station**을 **확인합니다**



4. Manage(**관리) > Network objects(네트워크 개체) > New(또는 Edit) > Network(네트워크)를 선택하여** VPN Concentrator 뒤에 있는 외부("inside_cisco") 네트워크에 대한 개체를 구성합니다. 이는 VPN Concentrator의 "로컬" 네트워크와 일치해야 합니다

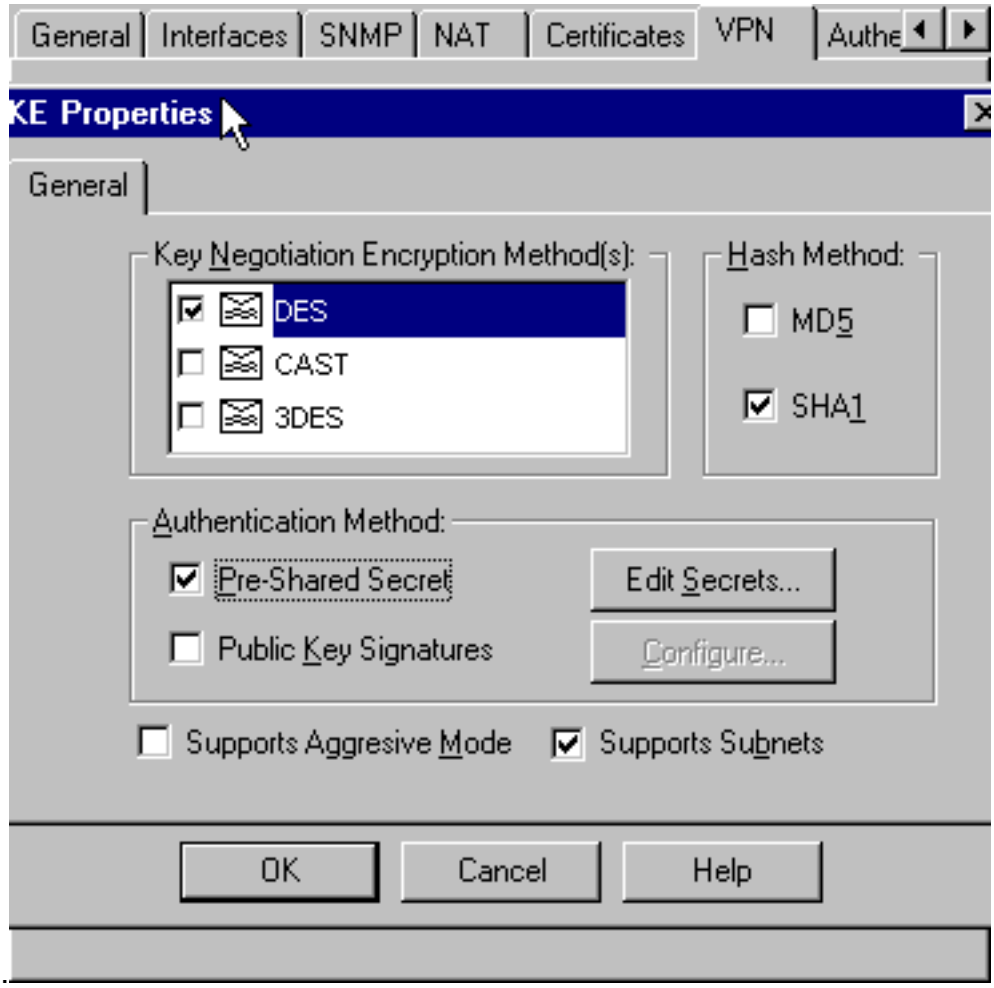


5. Manage(**관리) > Network objects(네트워크 개체) > New(새로 만들기) > Workstation(워크스테이션)을 선택하여** 외부("cisco_endpoint") VPN Concentrator 게이트웨이에 대한 개체를 추가합니다. VPN Concentrator "Public" 인터페이스입니다.위치에서 **외부**를 선택합니다. Type(유형)에서 **Gateway(게이트웨이)를** 선택합니다.**참고:** VPN-1/FireWall-1 확인란을 선택하지 마십시오.
6. Manage(**관리) > Network 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**

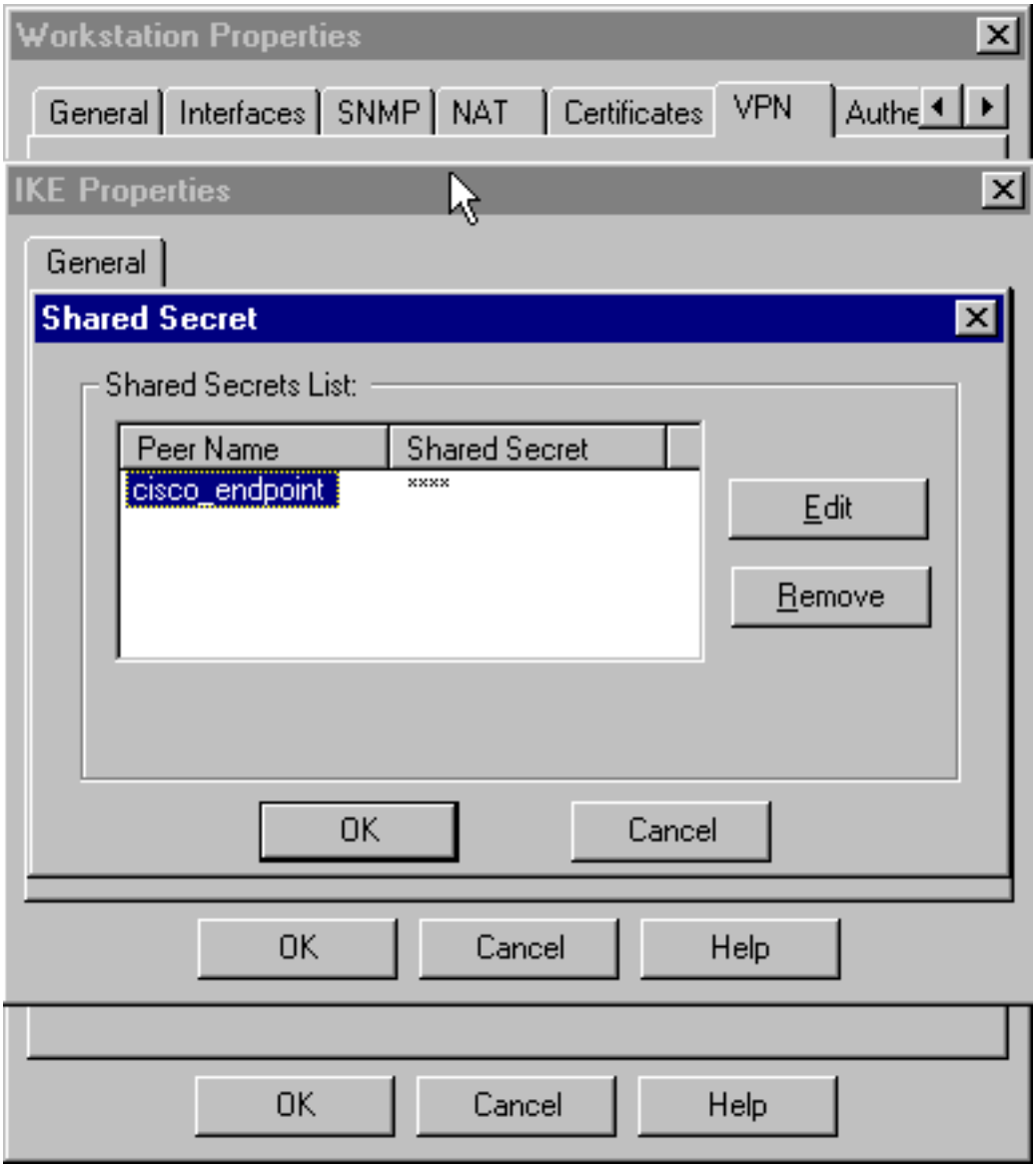


니다.

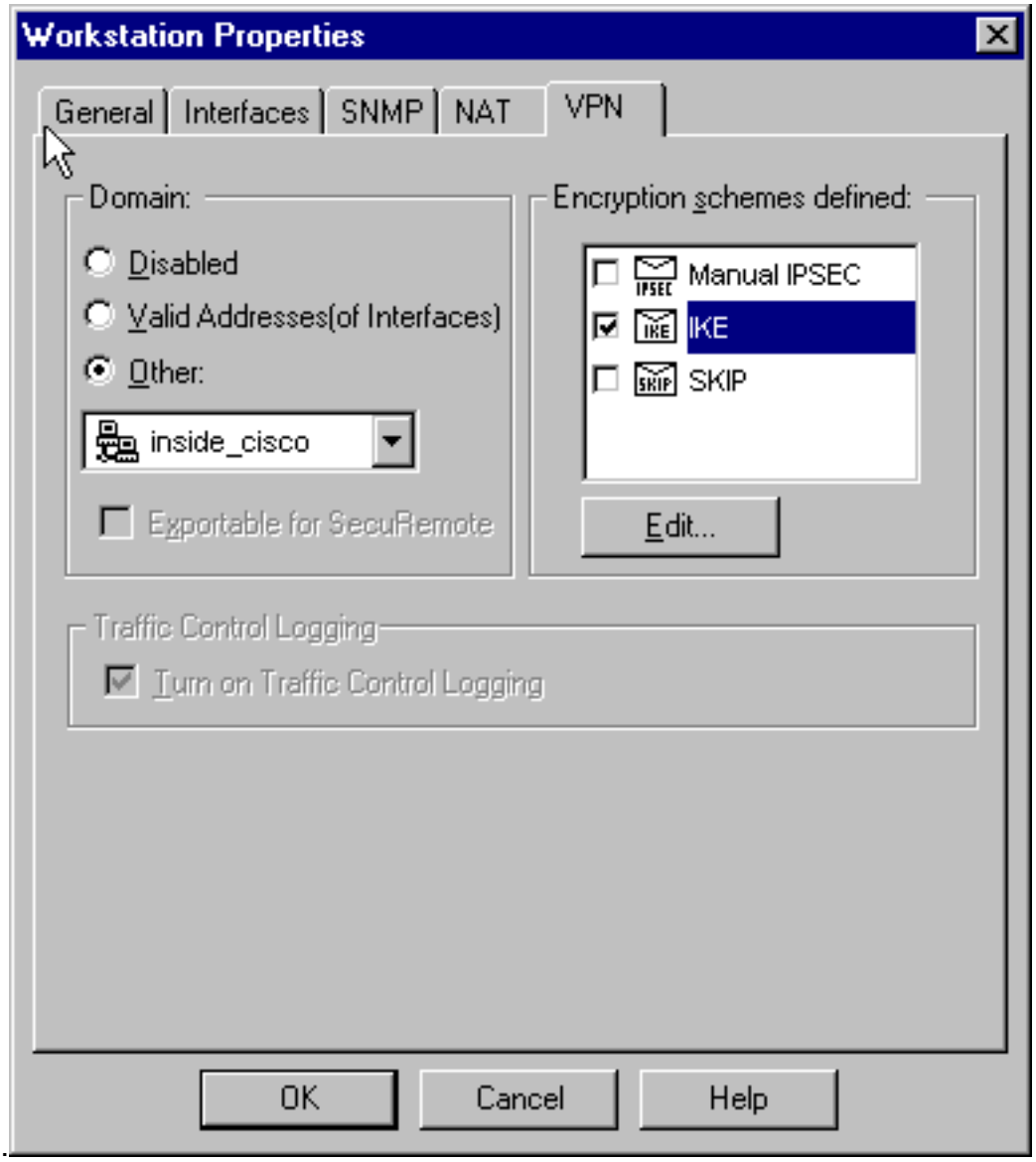
7. VPN Concentrator의 **DES-56** 및 **Encryption Algorithm**에 동의하도록 DES 암호화의 IKE 속성을 변경합니다.
8. VPN Concentrator에서 **SHA/HMAC-160** 알고리즘에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.Aggressive **Mode를 선택 취소합니다**.Supports Subnets(**서브넷 지원)를** 선택합니다.Authentication **Method(인증 방법)** 아래에서 Pre-Shared Secret(사전 공유 암호)을 선택합니다. 이는 VPN Concentrator Authentication Mode, Preshared Keys와 동일합니다



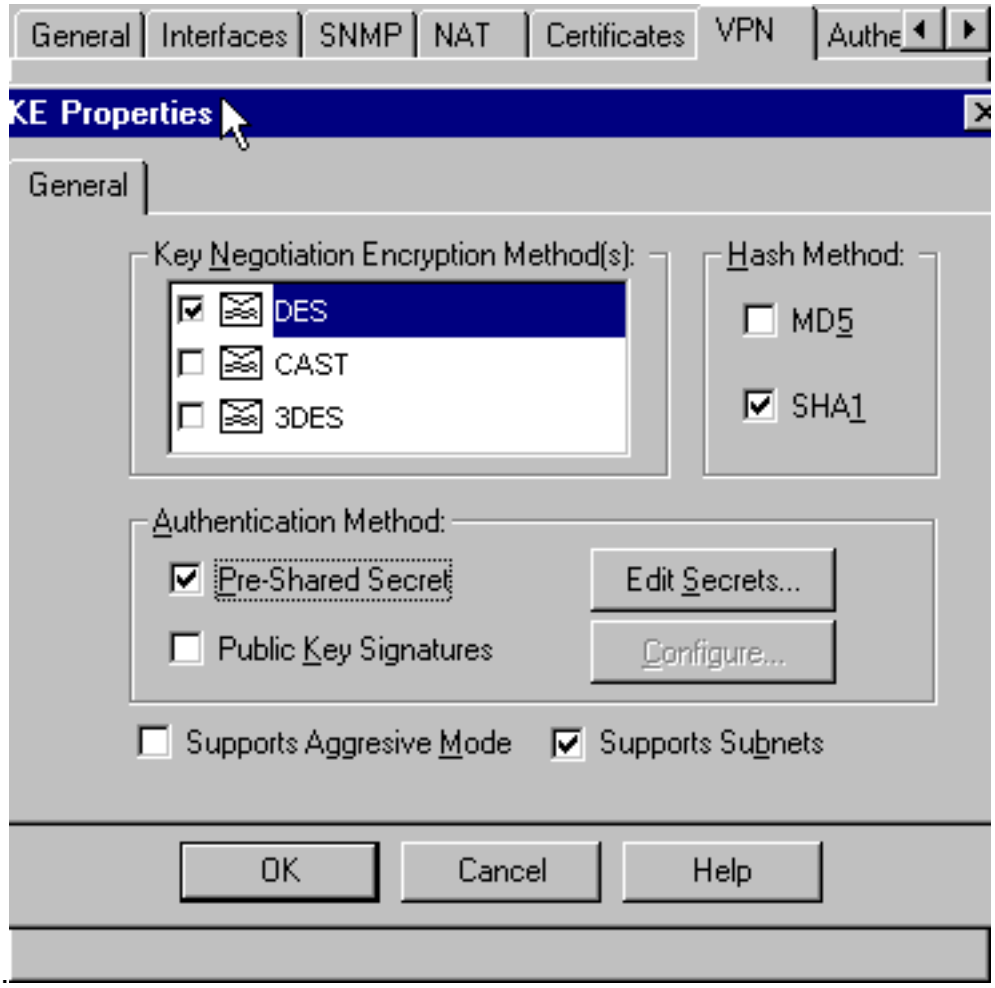
9. 실제 VPN Concentrator Preshared **Key**에 동의하도록 사전 공유 키를 설정하려면 Edit **Secrets를 클릭합니다.isakmp 키 주소 주소 넷마스크 넷마스크**



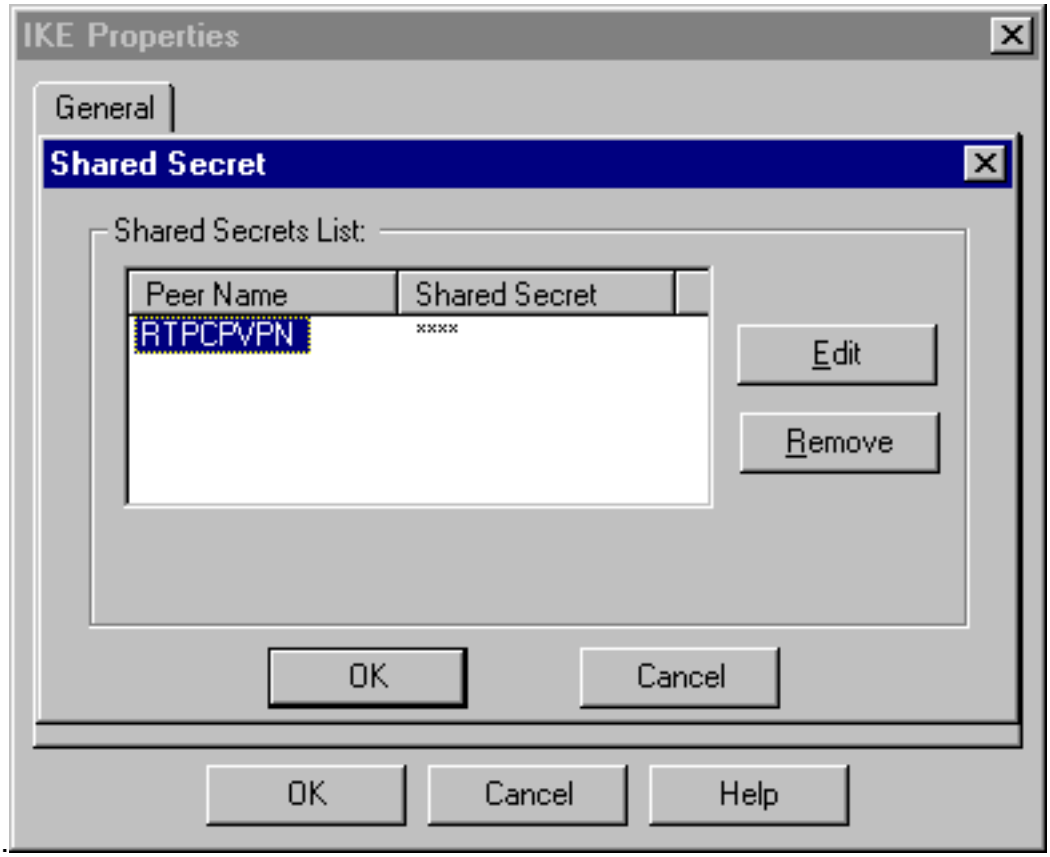
10. Manage(**관리) > Network objects(네트워크 개체) > Edit(편집)를 선택하여** "cisco_endpoint" VPN 탭을 편집합니다. Domain(도메인)에서 **Other(기타)**를 선택한 다음 Cisco 네트워크의 내부("inside_cisco"라고 함)를 선택합니다. Encryption schemes defined(정의된 암호화 체계)에서 **IKE**를 선택한 다음 Edit(수정)를 **클릭합니다**



11. VPN Concentrator의 DES-**56, Encryption Algorithm**과 일치하도록 IKE 속성 DES 암호화를 변경합니다.
12. VPN Concentrator에서 **SHA/HMAC-160** 알고리즘에 동의하려면 IKE 속성을 SHA1 해싱으로 변경합니다.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. 이는 사전 공유 키의 VPN Concentrator Authentication Mode(VPN 집중기 인증 모드)와 동일합니다



13. 실제 VPN Concentrator Preshared Key에 동의하도록 사전 공유 키를 설정하려면 Edit Secrets를 클릭합니다

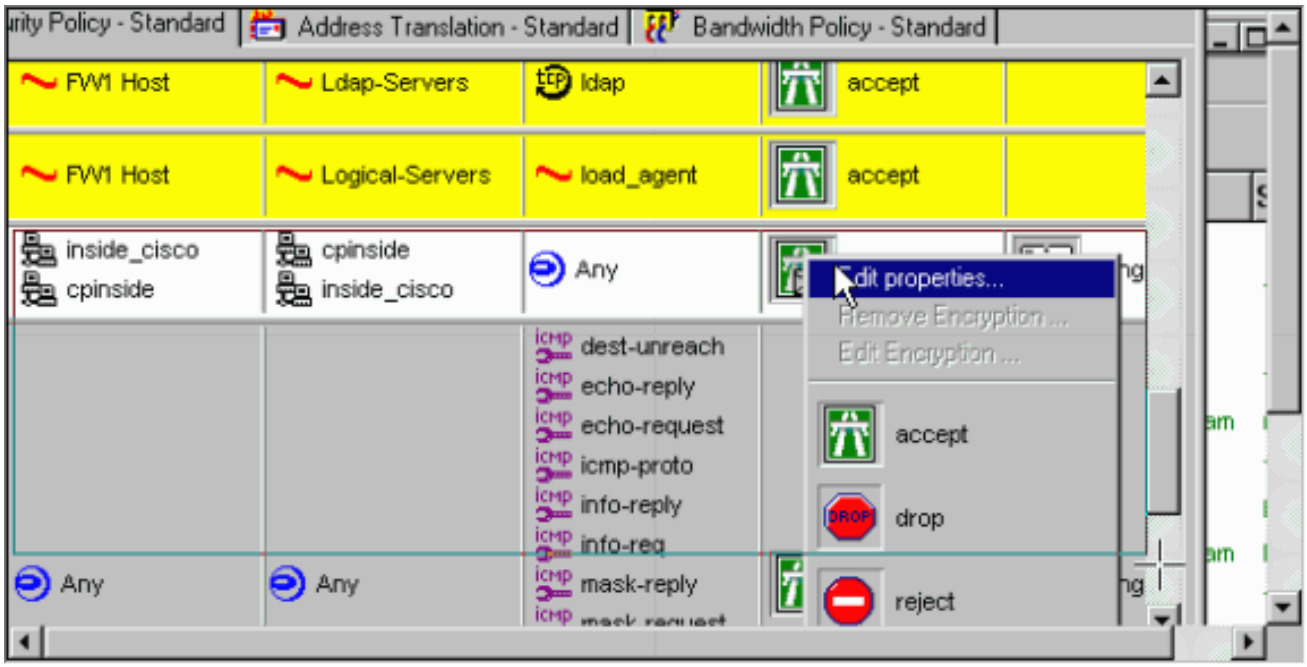


14. Policy Editor(정책 편집기) 창에서 Source(소스)와 Destination(대상)을 모두 "inside_cisco" 및 "cpinside"(양방향)로 포함하는 규칙을 삽입합니다. Service=Any, Action=Encrypt 및 Track=Long을 설정합니다

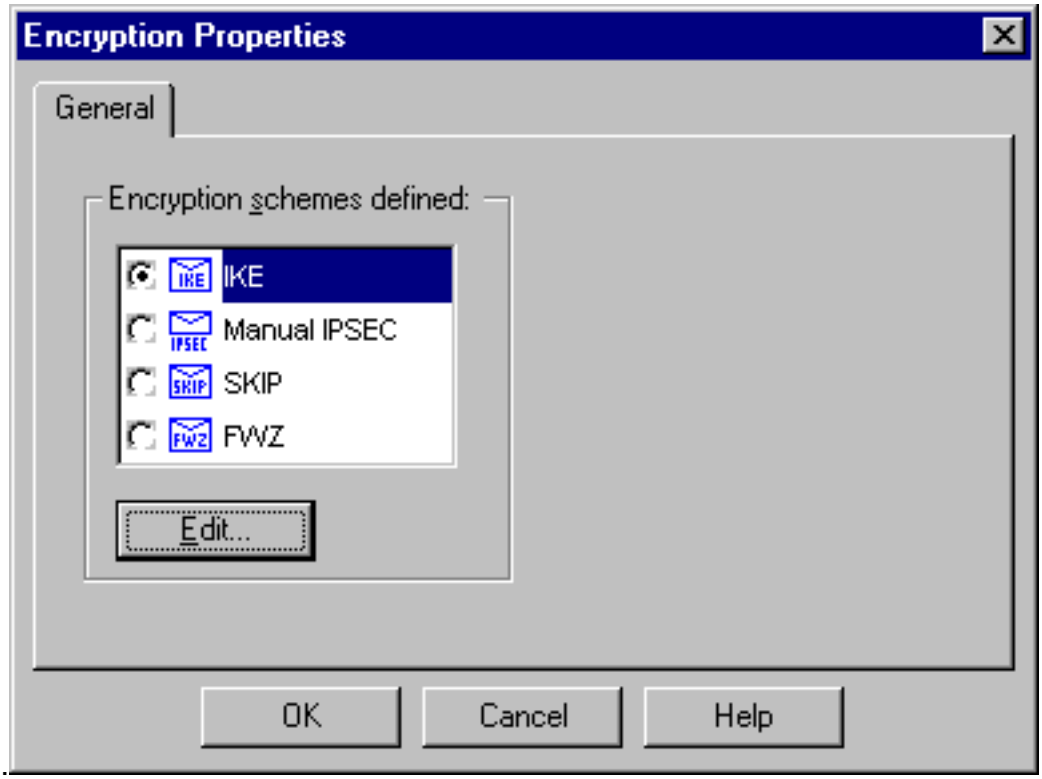
.

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

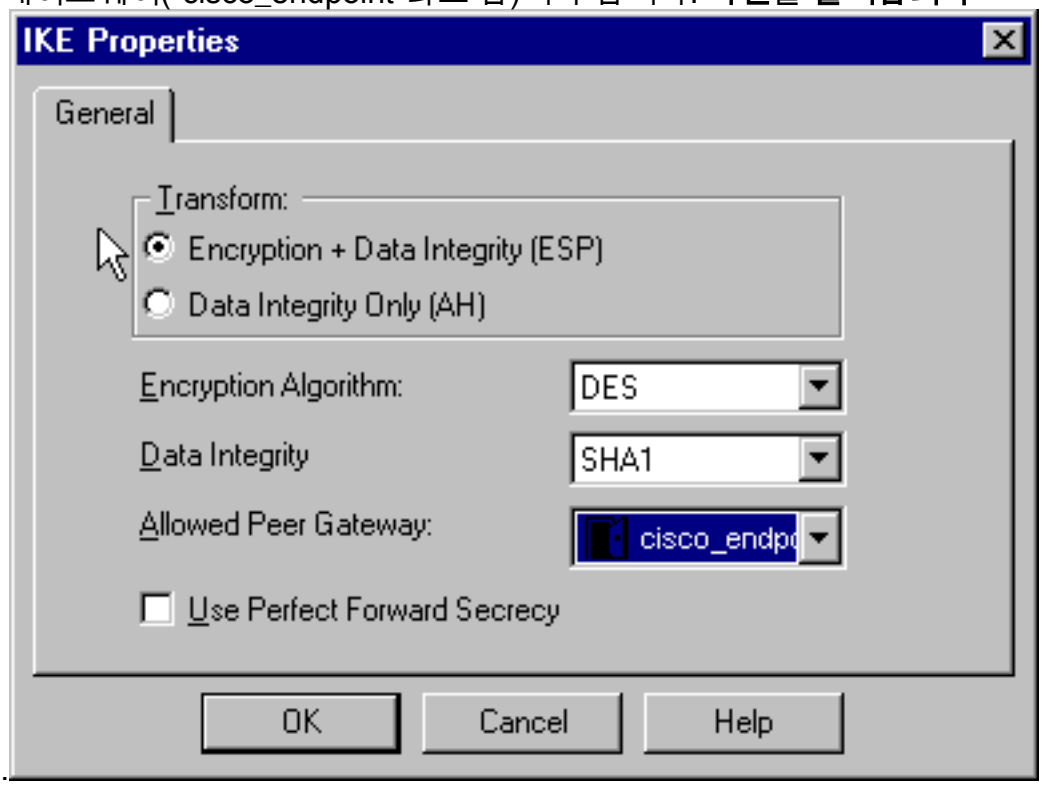
.



16. IKE를 선택한 다음 Edit를 **클릭합니다**



17. IKE Properties(IKE 속성) 창에서 이러한 속성을 VPN Concentrator IPsec 변환과 일치하도록 변경합니다.Transform(변형)에서 **Encryption + Data Integrity (ESP)를** 선택합니다. 암호화 알고리즘은 **DES**, 데이터 무결성은 SHA1이어야 하며, 허용된 피어 게이트웨이는 외부 Cisco 게이트웨이("cisco_endpoint"라고 함)여야 합니다. **확인을 클릭합니다**



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

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

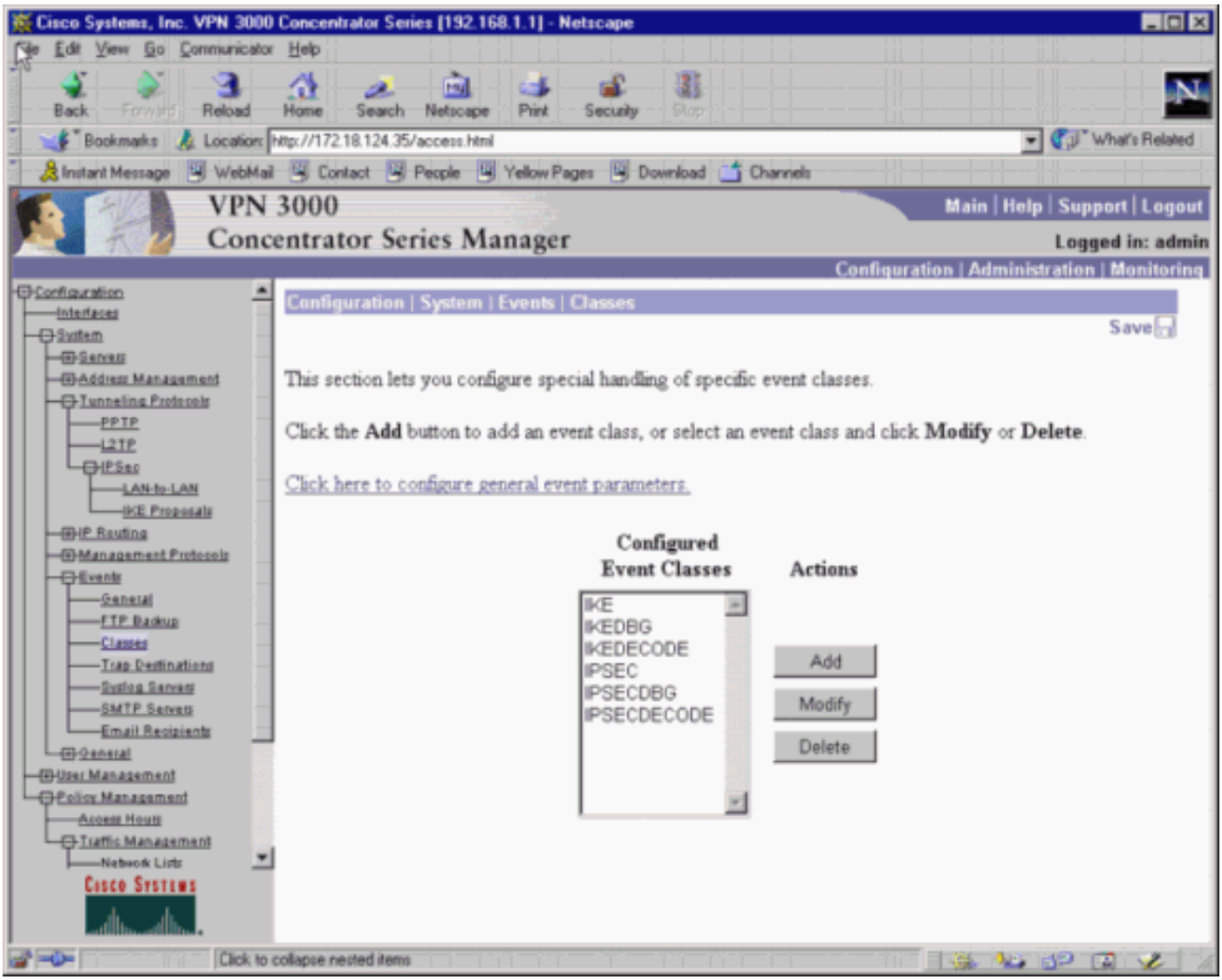
이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

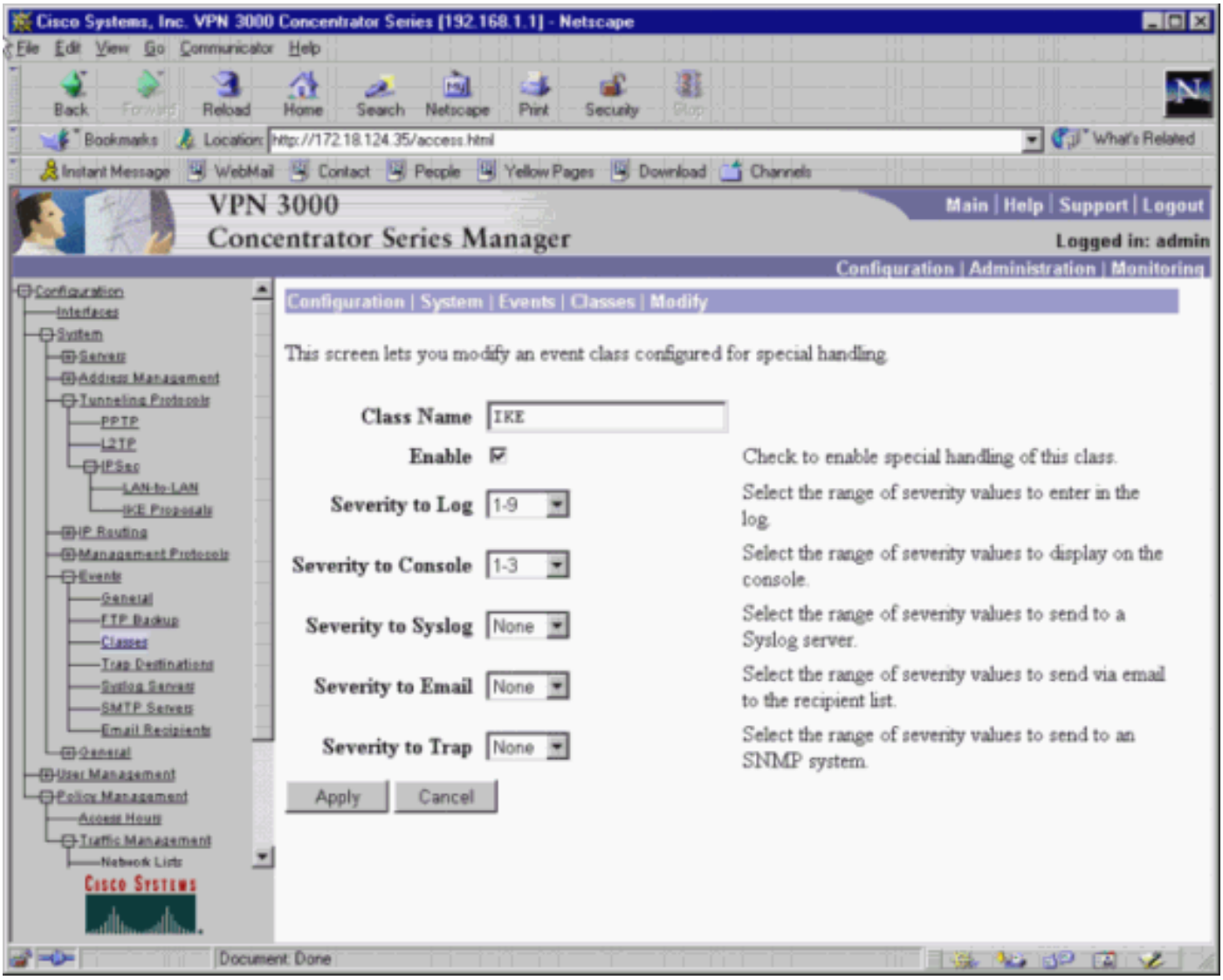
네트워크 요약

Checkpoint의 암호화 도메인에 인접한 여러 내부 네트워크가 구성된 경우, 해당 디바이스는 흥미로운 트래픽과 관련하여 이를 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 10.0.0.0 /23으로 요약될 수 있습니다.

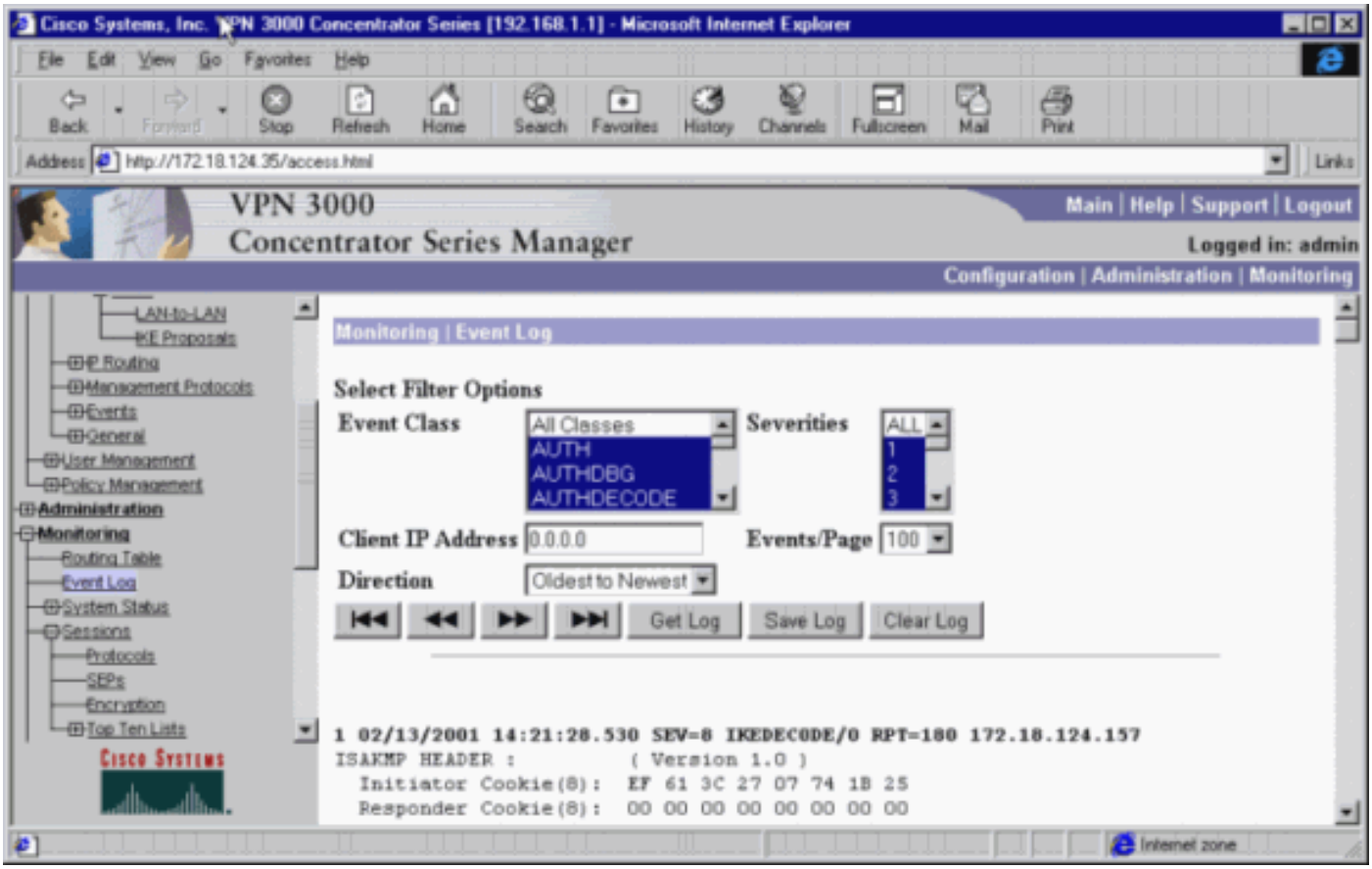
VPN 3000 Concentrator 디버그

가능한 VPN Concentrator 디버깅에는 IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE가 포함됩니다. 이는 Configuration(컨피그레이션) **> System(시스템) > Events(이벤트) > Classes(클래스)에서 설정됩니다**.

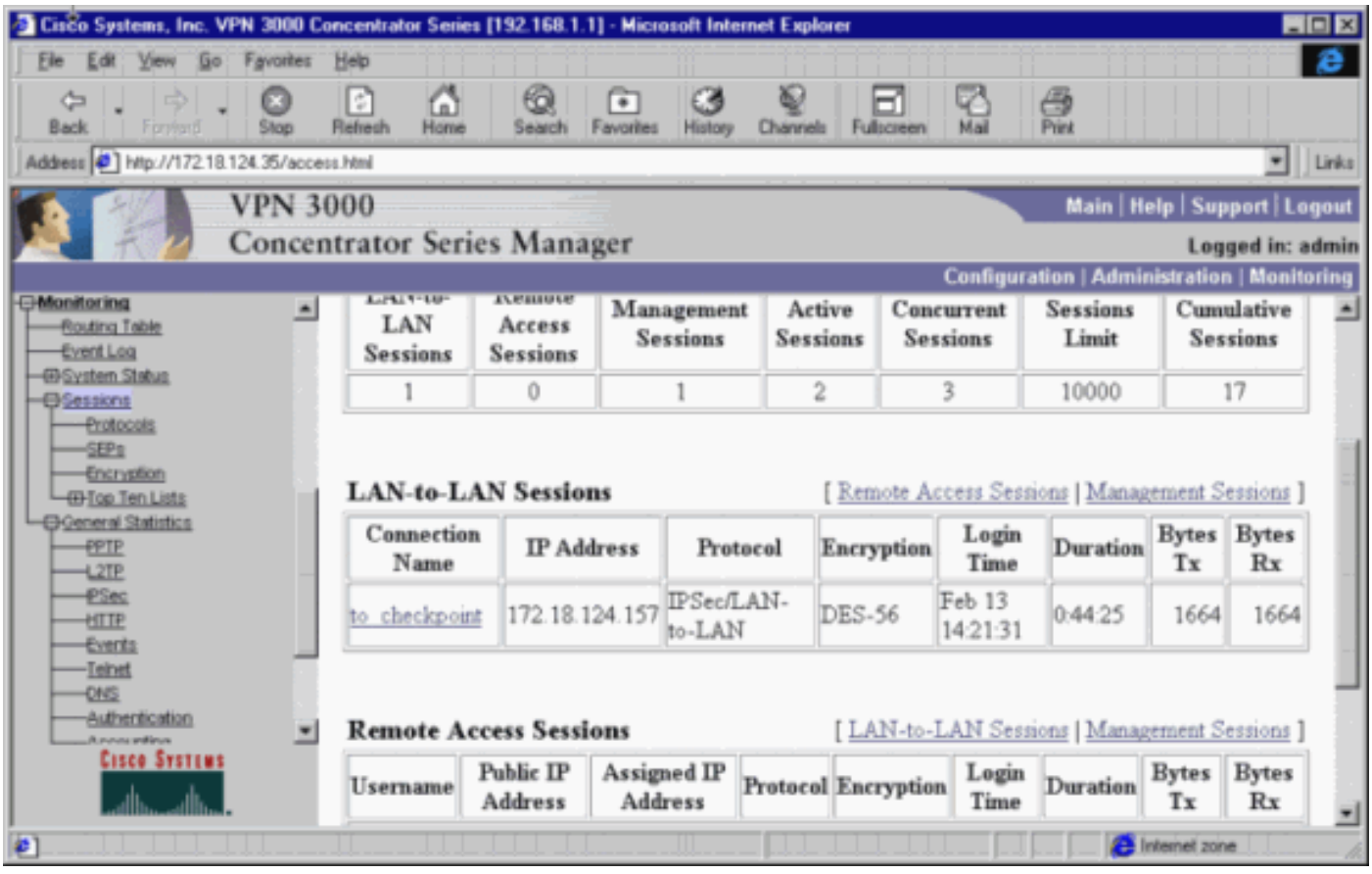




Monitoring(모니터링) **> Event log(이벤트 로그) > Get Log(로그 가져오기)**에서 디버깅을 볼 수 있습니다.



Monitoring **> Sessions를 선택하여** LAN-to-LAN 터널 트래픽을 모니터링합니다.



Administration **> Administer Sessions > LAN-to-LAN sessions > Actions - Logout을 선택하여** 터널을 지웁니다.

검사점 4.1 방화벽 디버그

참고: Microsoft Windows NT 설치입니다. 정책 편집기 창에서 추적이 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
```

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
```

예를 프롬프트에서 중단될 수 있습니다.

디버그 출력 샘플

Cisco VPN 3000 Concentrator

```
1 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=180 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       164

7 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=406 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164

9 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=407 172.18.124.157
processing SA payload

10 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=181 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       92

13 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=182 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       2
  Length        :       80
```

```
16 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=183 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

18 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=184 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 2 (2)
  Life Time     :       86400 seconds

23 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=185 172.18.124.157
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       36

25 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=186 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 1 (1)
  Life Time     :       86400 seconds

30 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=408 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

35 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=409 172.18.124.157
  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

38 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=410 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

41 02/13/2001 14:21:28.530 SEV=7 IKEDBG/0 RPT=411 172.18.124.157
Oakley proposal is acceptable

42 02/13/2001 14:21:28.530 SEV=9 IKEDBG/1 RPT=107 172.18.124.157
processing vid payload

43 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=412 172.18.124.157
processing IKE SA

44 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=413 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
```

```
    Cfg'd: Oakley Group 1

49 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=414 172.18.124.157
  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

52 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=415 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

55 02/13/2001 14:21:28.530 SEV=7 IKEDBG/28 RPT=3 172.18.124.157
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

56 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=416 172.18.124.157
constructing ISA_SA for isakmp

57 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=417 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

58 02/13/2001 14:21:28.630 SEV=8 IKEDECODE/0 RPT=187 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

64 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=418 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

66 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=419 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

68 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=420 172.18.124.157
processing ke payload

69 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=421 172.18.124.157
processing ISA_KE

70 02/13/2001 14:21:28.630 SEV=9 IKEDBG/1 RPT=108 172.18.124.157
processing nonce payload

71 02/13/2001 14:21:28.650 SEV=9 IKEDBG/0 RPT=422 172.18.124.157
constructing ke payload

72 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=109 172.18.124.157
constructing nonce payload

73 02/13/2001 14:21:28.650 SEV=9 IKEDBG/38 RPT=7 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

75 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=110 172.18.124.157
constructing vid payload
```

```
76 02/13/2001 14:21:28.650 SEV=9 IKE/0 RPT=26 172.18.124.157
Generating keys for Responder...

77 02/13/2001 14:21:28.650 SEV=8 IKEDBG/0 RPT=423 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

78 02/13/2001 14:21:28.770 SEV=8 IKEDECODE/0 RPT=188 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

84 02/13/2001 14:21:28.770 SEV=8 IKEDBG/0 RPT=424 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

86 02/13/2001 14:21:28.770 SEV=9 IKEDBG/1 RPT=111 172.18.124.157
Processing ID

87 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=425 172.18.124.157
processing hash

88 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=426 172.18.124.157
computing hash

89 02/13/2001 14:21:28.770 SEV=9 IKEDBG/23 RPT=7 172.18.124.157
Starting group lookup for peer 172.18.124.157

90 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=427 172.18.124.157
Found Phase 1 Group (172.18.124.157)

91 02/13/2001 14:21:28.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.157
Authentication configured for Internal

92 02/13/2001 14:21:28.870 SEV=9 IKEDBG/1 RPT=112 172.18.124.157
constructing ID

93 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=428
construct hash payload

94 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=429 172.18.124.157
computing hash


95 02/13/2001 14:21:28.870 SEV=8 IKEDBG/0 RPT=430 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5)  ... total length : 64

96 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=431 172.18.124.157
Starting phase 1 rekey timer

97 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=189 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
```

```
  Message ID    :       7755aa11
  Length        :       164

104 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=432 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 160

107 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=433 172.18.124.157
processing hash

108 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=434 172.18.124.157
processing SA payload

109 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=190 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       52

112 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=191 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E3
  Length        :       40

116 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=192 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       28

118 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=193 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  HMAC Algorithm:       SHA (2)
  Encapsulation :       Tunnel (1)

121 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=113 172.18.124.157
processing nonce payload

122 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=114 172.18.124.157
Processing ID

123 02/13/2001 14:21:29.030 SEV=5 IKE/35 RPT=14 172.18.124.157
Received remote IP Proxy Subnet data in ID Payload:
 Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0

125 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=115 172.18.124.157
Processing ID

126 02/13/2001 14:21:29.030 SEV=5 IKE/34 RPT=14 172.18.124.157
Received local IP Proxy Subnet data in ID Payload:
 Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

128 02/13/2001 14:21:29.030 SEV=5 IKE/66 RPT=4 172.18.124.157
IKE Remote Peer configured for SA: L2L: to_checkpoint

129 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=435 172.18.124.157
processing IPSEC SA

130 02/13/2001 14:21:29.030 SEV=7 IKEDBG/27 RPT=1 172.18.124.157
```

```
IPSec SA Proposal # 1, Transform # 1 acceptable

131 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=436 172.18.124.157
IKE: requesting SPI!

132 02/13/2001 14:21:29.030 SEV=8 IKEDBG/6 RPT=6
IKE got SPI from key engine: SPI = 0x4d6e483f

133 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=437 172.18.124.157
oakley constucting quick mode

134 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=438 172.18.124.157
constructing blank hash

135 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=439 172.18.124.157
constructing ISA_SA for ipsec

136 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=116 172.18.124.157
constructing ipsec nonce payload

137 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=117 172.18.124.157
constructing proxy ID

138 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=440 172.18.124.157
Transmitting Proxy Id:
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0

141 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=441 172.18.124.157
constructing qm hash

142 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=442 172.18.124.157
SENDING Message (msgid=7755aa11) with payloads :
HDR + HASH (8)  ... total length : 156

144 02/13/2001 14:21:29.270 SEV=8 IKEDECODE/0 RPT=194 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

151 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=443 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 52

153 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=444 172.18.124.157
processing hash

154 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=445 172.18.124.157
loading all IPSEC SAs

155 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=118 172.18.124.157
Generating Quick Mode Key!

156 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=119 172.18.124.157
Generating Quick Mode Key!

157 02/13/2001 14:21:29.270 SEV=7 IKEDBG/0 RPT=446 172.18.124.157
Loading subnet:
  Dst: 192.168.1.0  mask: 255.255.255.0
```

```
  Src: 10.32.50.0  mask: 255.255.255.0

159 02/13/2001 14:21:29.270 SEV=4 IKE/49 RPT=6 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3

161 02/13/2001 14:21:29.270 SEV=8 IKEDBG/7 RPT=6
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe3

162 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=447
pitcher: rcv KEY_UPDATE, spi 0x4d6e483f

163 02/13/2001 14:21:29.670 SEV=8 IKEDECODE/0 RPT=195 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

170 02/13/2001 14:21:29.670 SEV=6 IKE/0 RPT=27 172.18.124.157
Duplicate Phase 2 packet detected!

171 02/13/2001 14:21:29.760 SEV=8 IKEDECODE/0 RPT=196 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

178 02/13/2001 14:21:29.760 SEV=6 IKE/0 RPT=28 172.18.124.157
Duplicate Phase 2 packet detected!

179 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=448
pitcher: recv KEY_SA_ACTIVE spi 0x4d6e483f

180 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=449
KEY_SA_ACTIVE old rekey centry found with new spi 0x4d6e483f

181 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=5 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

182 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=450 172.18.124.157
IKE SA MM:f2ea8e68 rcv'd Terminate: state MM_ACTIVE_REKEY
flags 0x000000e6, refcnt 1, tuncnt 0

184 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=451 172.18.124.157
IKE SA MM:f2ea8e68 terminating:
flags 0x000000a6, refcnt 0, tuncnt 0

185 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=452
sending delete message

186 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=453 172.18.124.157
constructing blank hash

187 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=454
constructing delete payload
```

```
188 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=455 172.18.124.157
constructing qm hash

189 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=456 172.18.124.157
SENDING Message (msgid=87b7c1a4) with payloads :
HDR + HASH (8)  ... total length : 80

191 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=457 172.18.124.157
IKE SA MM:241840a1 rcv'd Terminate: state MM_REKEY_DONE
flags 0x00000082, refcnt 1, tuncnt 1

193 02/13/2001 14:21:29.880 SEV=6 IKE/0 RPT=29 172.18.124.157
Removing peer from peer table failed, no match!

194 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=458
sending delete message

195 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=459 172.18.124.157
constructing blank hash

196 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=460
constructing ipsec delete payload

197 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=461 172.18.124.157
constructing qm hash

198 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=462 172.18.124.157
SENDING Message (msgid=63f2abb8) with payloads :
HDR + HASH (8)  ... total length : 68

200 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=6 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

201 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=463 172.18.124.157
IKE SA MM:241840a1 terminating:
flags 0x00000082, refcnt 0, tuncnt 0

202 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=464
sending delete message

203 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=465 172.18.124.157
constructing blank hash

204 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=466
constructing delete payload

205 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=467 172.18.124.157
constructing qm hash

206 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=468 172.18.124.157
SENDING Message (msgid=d6a00071) with payloads :
HDR + HASH (8)  ... total length : 80

208 02/13/2001 14:21:29.880 SEV=4 AUTH/22 RPT=13
User 172.18.124.157 disconnected

209 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=469
pitcher: received key delete msg, spi 0x2962069b

210 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=470
pitcher: received key delete msg, spi 0xda163fe2

211 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=471
pitcher: received key delete msg, spi 0x4d6e483f
```

```
212 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=472
pitcher: received key delete msg, spi 0xda163fe3

213 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=473
pitcher: received a key acquire message!

214 02/13/2001 14:21:29.890 SEV=4 IKE/41 RPT=6 172.18.124.157
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157
local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0,
SA (L2L: to_checkpoint)

217 02/13/2001 14:21:29.890 SEV=9 IKEDBG/0 RPT=474 172.18.124.157
constructing ISA_SA for isakmp

218 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=475 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

219 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=197 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       84

225 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=476 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

227 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=477 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

229 02/13/2001 14:21:30.430 SEV=9 IKEDBG/0 RPT=478 172.18.124.157
processing SA payload

230 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=198 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       56

233 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=199 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       1
  Length        :       44

236 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=200 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

238 02/13/2001 14:21:30.440 SEV=8 IKEDECODE/0 RPT=201 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
```

```
  Auth Method   :       Preshared Key (1)
  Life Time     :       86400 seconds

243 02/13/2001 14:21:30.440 SEV=7 IKEDBG/0 RPT=479 172.18.124.157
Oakley proposal is acceptable

244 02/13/2001 14:21:30.440 SEV=9 IKEDBG/0 RPT=480 172.18.124.157
constructing ke payload

245 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=120 172.18.124.157
constructing nonce payload

246 02/13/2001 14:21:30.440 SEV=9 IKEDBG/38 RPT=8 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

248 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=121 172.18.124.157
constructing vid payload

249 02/13/2001 14:21:30.440 SEV=8 IKEDBG/0 RPT=481 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

250 02/13/2001 14:21:30.540 SEV=8 IKEDECODE/0 RPT=202 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

256 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=482 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

258 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=483 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

260 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=484 172.18.124.157
processing ke payload

261 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=485 172.18.124.157
processing ISA_KE

262 02/13/2001 14:21:30.540 SEV=9 IKEDBG/1 RPT=122 172.18.124.157
processing nonce payload

263 02/13/2001 14:21:30.560 SEV=9 IKE/0 RPT=30 172.18.124.157
Generating keys for Initiator...

264 02/13/2001 14:21:30.570 SEV=9 IKEDBG/1 RPT=123 172.18.124.157
constructing ID

265 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=486
construct hash payload

266 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=487 172.18.124.157
computing hash

267 02/13/2001 14:21:30.570 SEV=8 IKEDBG/0 RPT=488 172.18.124.157
SENDING Message (msgid=0) with payloads :
```

```
HDR + ID (5)  ... total length : 64

268 02/13/2001 14:21:30.740 SEV=8 IKEDECODE/0 RPT=203 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

274 02/13/2001 14:21:30.740 SEV=8 IKEDBG/0 RPT=489 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

276 02/13/2001 14:21:30.740 SEV=9 IKEDBG/1 RPT=124 172.18.124.157
Processing ID

277 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=490 172.18.124.157
processing hash

278 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=491 172.18.124.157
computing hash

279 02/13/2001 14:21:30.740 SEV=9 IKEDBG/23 RPT=8 172.18.124.157
Starting group lookup for peer 172.18.124.157

280 02/13/2001 14:21:30.830 SEV=8 IKEDECODE/0 RPT=204 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

286 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=31 172.18.124.157
Duplicate Phase 1 packet detected!

287 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=32
MM received unexpected event EV_RESEND_MSG in state MM_I_DONE

288 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=492 172.18.124.157
Found Phase 1 Group (172.18.124.157)

289 02/13/2001 14:21:30.840 SEV=7 IKEDBG/14 RPT=8 172.18.124.157
Authentication configured for Internal

290 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=493 172.18.124.157
Oakley begin quick mode

291 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=494 172.18.124.157
Starting phase 1 rekey timer

292 02/13/2001 14:21:30.840 SEV=4 AUTH/21 RPT=15
User 172.18.124.157 connected

293 02/13/2001 14:21:30.840 SEV=8 IKEDBG/6 RPT=7
IKE got SPI from key engine: SPI = 0x08201539

294 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=495 172.18.124.157
oakley constucting quick mode
```

```
295 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=496 172.18.124.157
constructing blank hash

296 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=497 172.18.124.157
constructing ISA_SA for ipsec

297 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=125 172.18.124.157
constructing ipsec nonce payload

298 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=126 172.18.124.157
constructing proxy ID

299 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=498 172.18.124.157
Transmitting Proxy Id:
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0

302 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=499 172.18.124.157
constructing qm hash

303 02/13/2001 14:21:30.840 SEV=8 IKEDBG/0 RPT=500 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 184

305 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=205 172.18.124.157
ISAKMP HEADER :          ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       23bc1709
  Length        :       164

312 02/13/2001 14:21:31.000 SEV=8 IKEDBG/0 RPT=501 172.18.124.157
RECEIVED Message (msgid=23bc1709) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 156

315 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=502 172.18.124.157
processing hash

316 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=503 172.18.124.157
processing SA payload

317 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=206 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       48

320 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=207 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E4
  Length        :       36

324 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=208 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
```

```
  Length        :       24

326 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=209 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  Encapsulation :       Tunnel (1)
  HMAC Algorithm:       SHA (2)

329 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=127 172.18.124.157
processing nonce payload

330 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=128 172.18.124.157
Processing ID

331 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=129 172.18.124.157
Processing ID

332 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=504 172.18.124.157
loading all IPSEC SAs

333 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=130 172.18.124.157
Generating Quick Mode Key!

334 02/13/2001 14:21:31.010 SEV=9 IKEDBG/1 RPT=131 172.18.124.157
Generating Quick Mode Key!

335 02/13/2001 14:21:31.010 SEV=7 IKEDBG/0 RPT=505 172.18.124.157
Loading subnet:
  Dst: 10.32.50.0  mask: 255.255.255.0
  Src: 192.168.1.0  mask: 255.255.255.0

337 02/13/2001 14:21:31.010 SEV=4 IKE/49 RPT=7 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4

339 02/13/2001 14:21:31.010 SEV=9 IKEDBG/0 RPT=506 172.18.124.157
oakley constructing final quick mode

340 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=507 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 76

342 02/13/2001 14:21:31.010 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe4

343 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=508
pitcher: rcv KEY_UPDATE, spi 0x8201539

344 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=509
pitcher: recv KEY_SA_ACTIVE spi 0x8201539

345 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=510
KEY_SA_ACTIVE no old rekey centry found with new spi 0x8201539, mess_id 0x0
```

관련 정보

- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems