Cisco 라우터에 Cisco VPN 3000 Concentrator 구성

목차

소개

이 샘플 컨피그레이션은 Cisco IOS® 소프트웨어를 실행하는 라우터 뒤에 있는 사설 네트워크를 Cisco VPN 3000 Concentrator 뒤에 있는 사설 네트워크에 연결하는 방법을 보여줍니다. 네트워크의 디바이스는 개인 주소를 통해 서로를 인식합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2611 라우터(Cisco IOS Software 릴리스 12.3.(1)a**참고:** Cisco 2600 Series 라우터가 VPN 기능을 지원하는 암호화 IPsec VPN IOS 이미지와 함께 설치되어 있는지 확인하십시오.

- Cisco VPN 3000 Concentrator 4.0.1 B

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

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

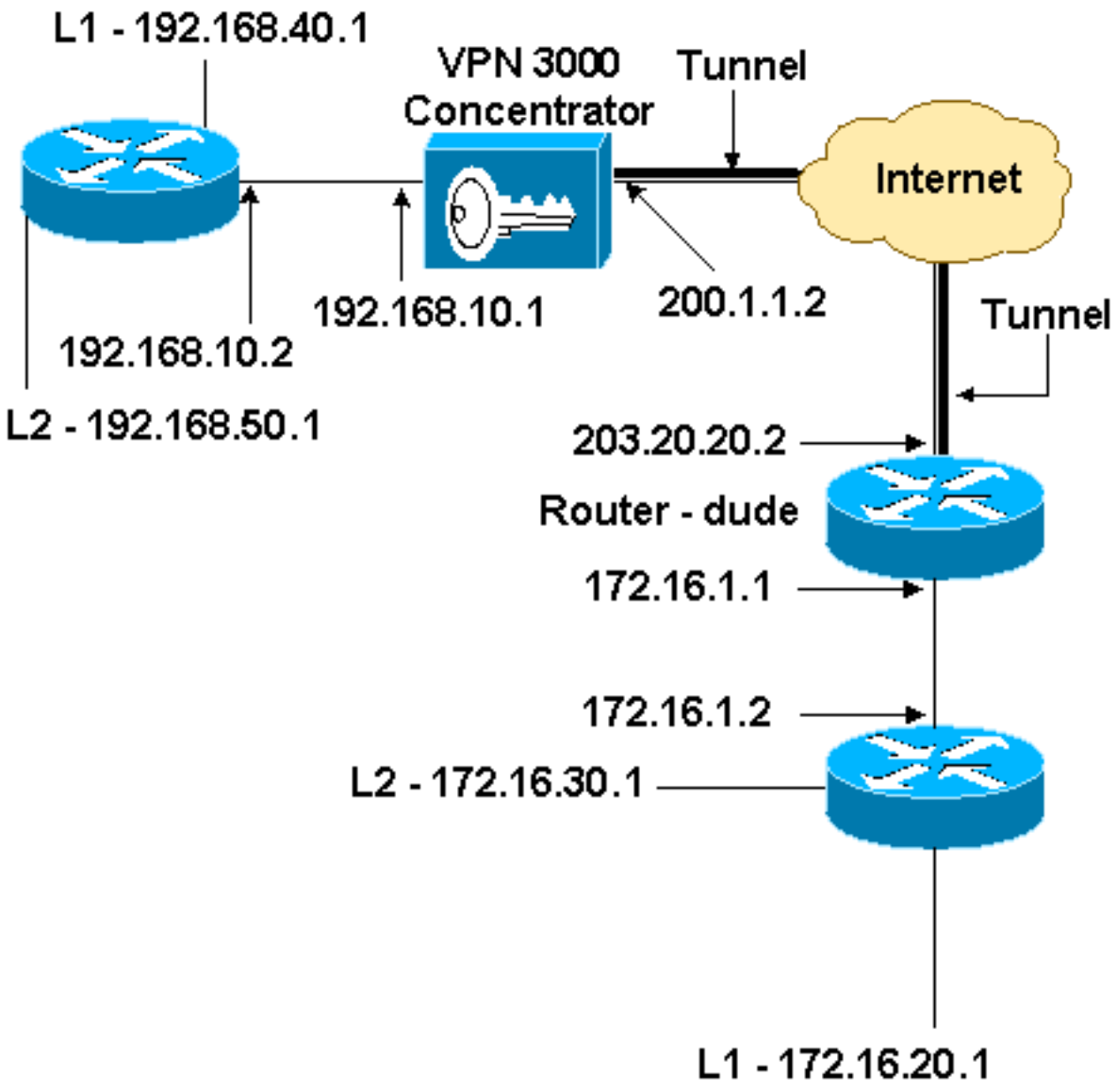
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이 구성을 사용합니다.

라우터 컨피그레이션

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
```

```
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN Concentrator 컨피그레이션

이 Lab 설정에서 VPN Concentrator는 먼저 콘솔 포트를 통해 액세스되고 최소 컨피그레이션이 추가되어 그래픽 사용자 인터페이스(GUI)를 통해 추가 컨피그레이션을 수행할 수 있습니다.

Administration(**관리**) > **System Reboot(시스템 재부팅)> Schedule reboot(재부팅 예약)** > Reboot with **Factory/Default Configuration(공장/기본 컨피그레이션으로 재부팅)을 선택하여** VPN Concentrator에 기존 컨피그레이션이 없는지 확인합니다.

VPN Concentrator가 빠른 구성에 나타나며 이러한 항목은 재부팅 후 구성됩니다.

- 시간/날짜
- Interfaces/Masks in **Configuration(컨피그레이션**의 인터페이스/마스크) > Interfaces(공용 =200.1.1.2/24, private=192.168.10.1/24)
- Configuration(컨피그레이션)의 **Default Gateway(기본 게이트웨이) > System(시스템) > IP 라우팅 > Default_Gateway**(200.1.1.1)

이때 VPN Concentrator는 내부 네트워크에서 HTML을 통해 액세스할 수 있습니다.

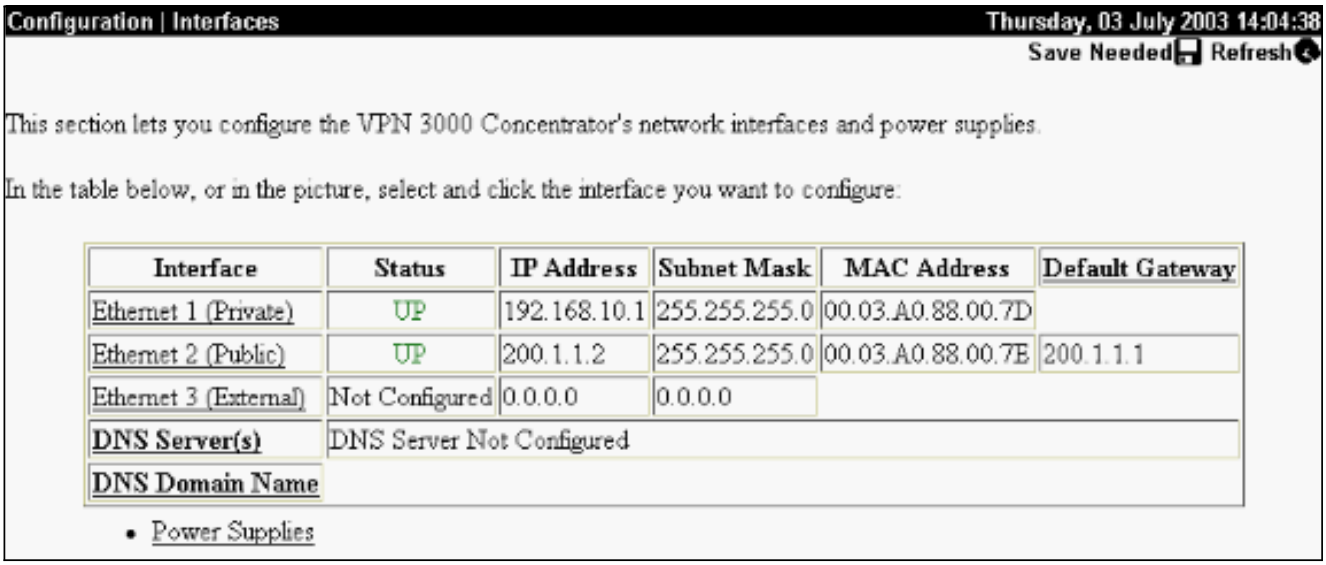
참고: VPN Concentrator는 외부에서 관리되므로 다음을 선택해야 합니다.

- **Configuration > Interfaces > 2-public > Select IP Filter > 1. Private(기본값)**.
- **Administration(관리) > Access Rights(액세스 권한)** > Access Control List(**액세스 제어 목록) >** Add Manager Workstation(**관리자 워크스테이션 추가)을 클릭하여** *외부* 관리자의 IP 주소를 추가합니다.

*외부*에서 VPN Concentrator를 관리하지 않는 한 이 작업은 필요하지 않습니다.

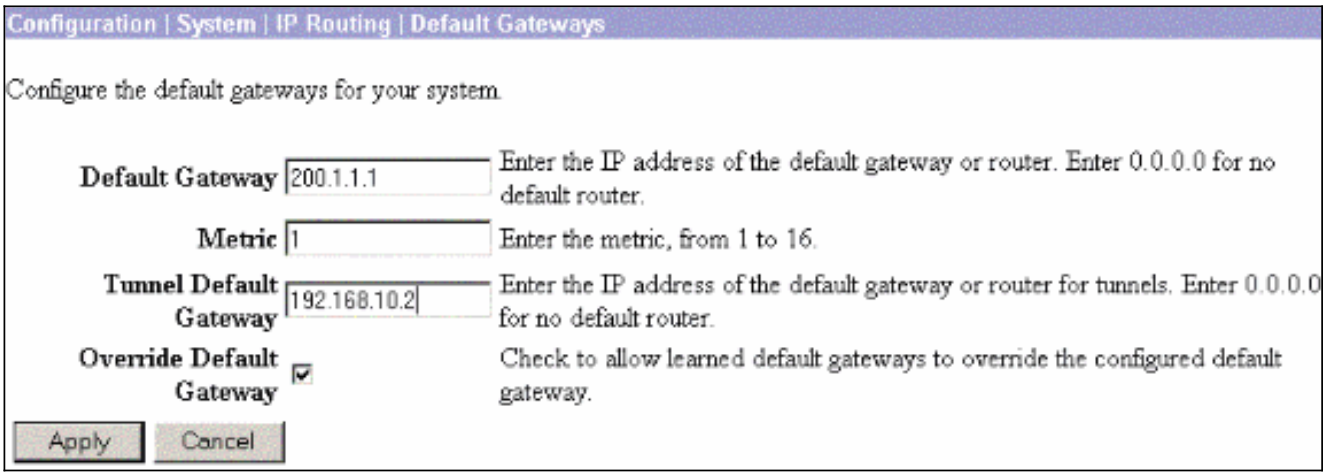
1. GUI를 표시한 후 인터페이스를 다시 확인하려면 Configuration > Interfaces를 선택합니다

.



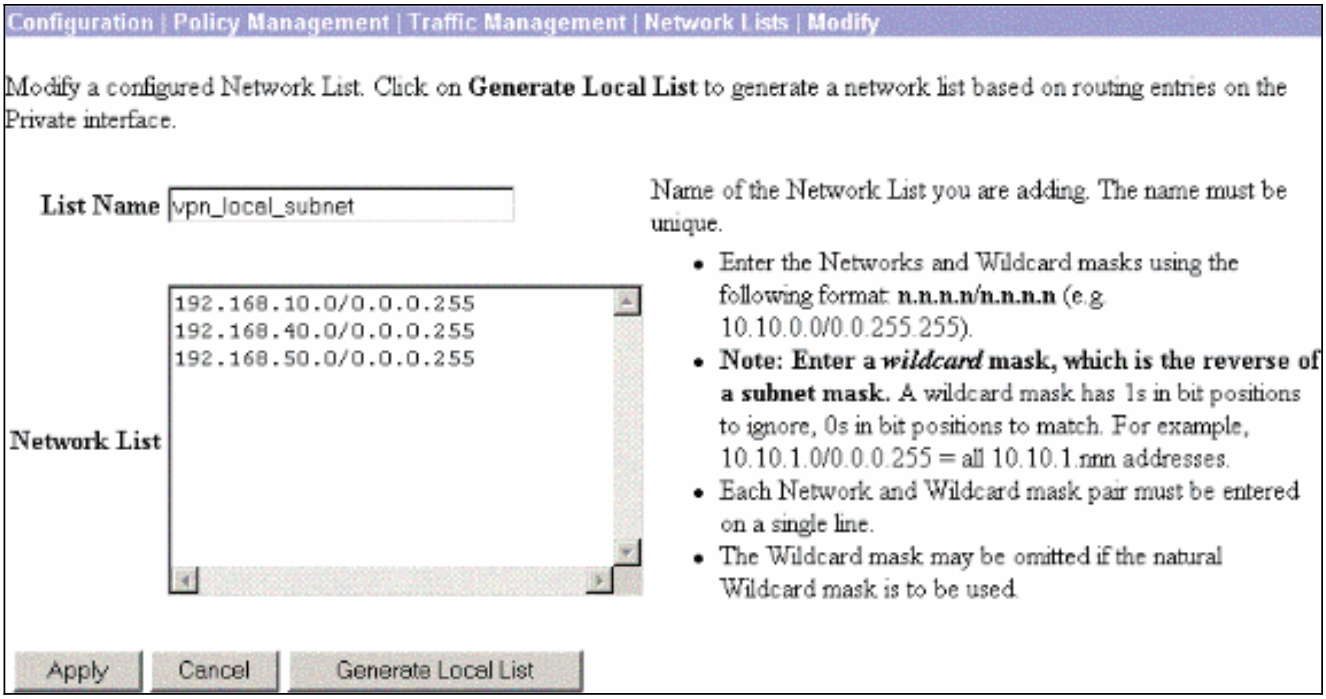
2. Configuration > System > IP Routing > Default Gateways를 선택하여 Default(Internet) Gateway 및 IPsec**용 Tunnel Default(내부) Gateway for IPsec을 프라이빗 네트워크의 다른 서브넷에 연결하도록 구성합니다**

.



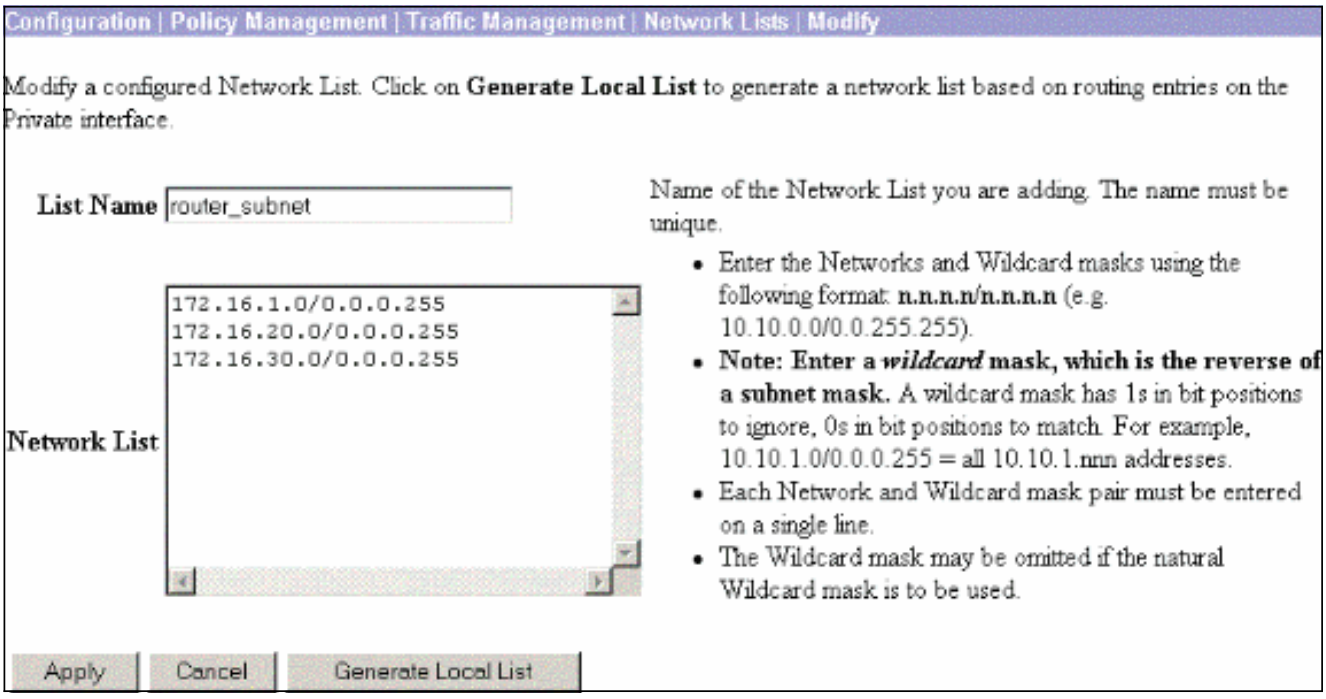
3. Configuration(**컨피그레이션**) > **Policy Management(정책 관리**) > **Network Lists(네트워크 목록**)를 선택하여 암호화할 트래픽을 정의하는 네트워크 목록을 생성합니다.다음은 로컬 네트워크입니다

.



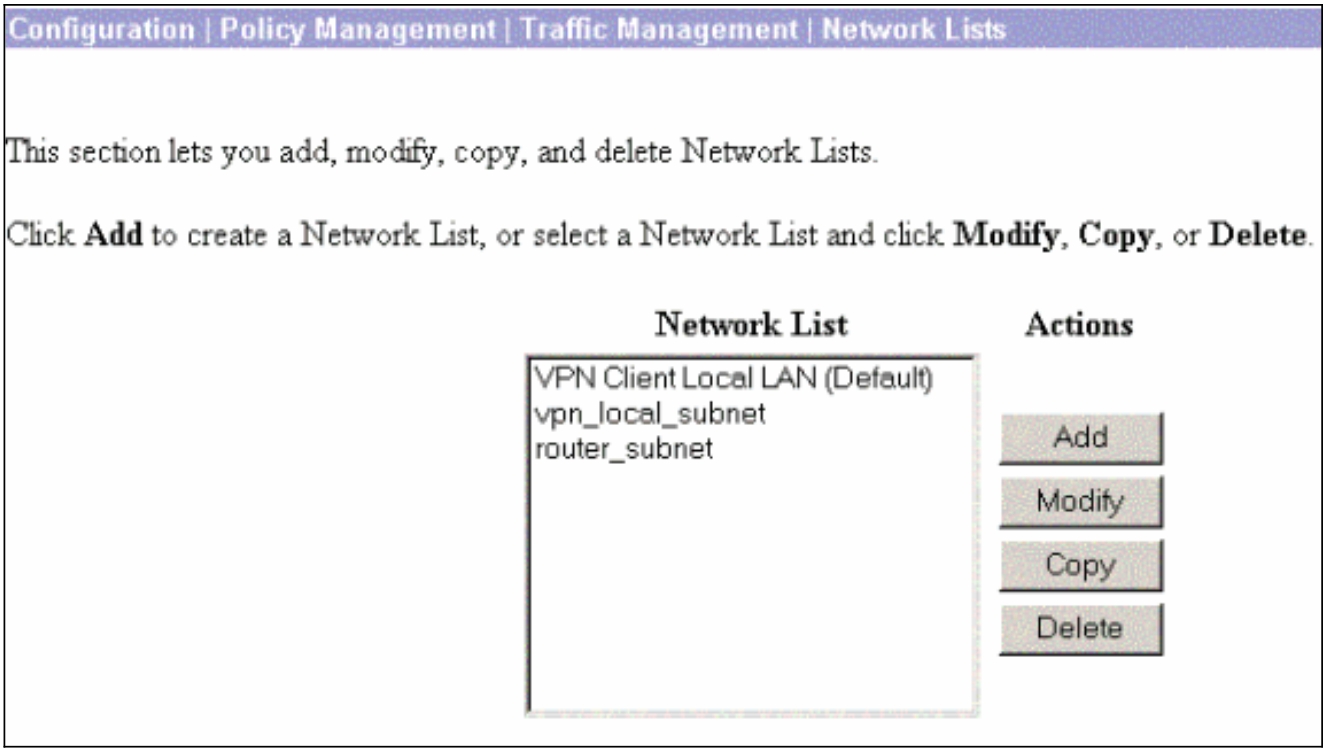
다음은 원격 네트워크입니다

.



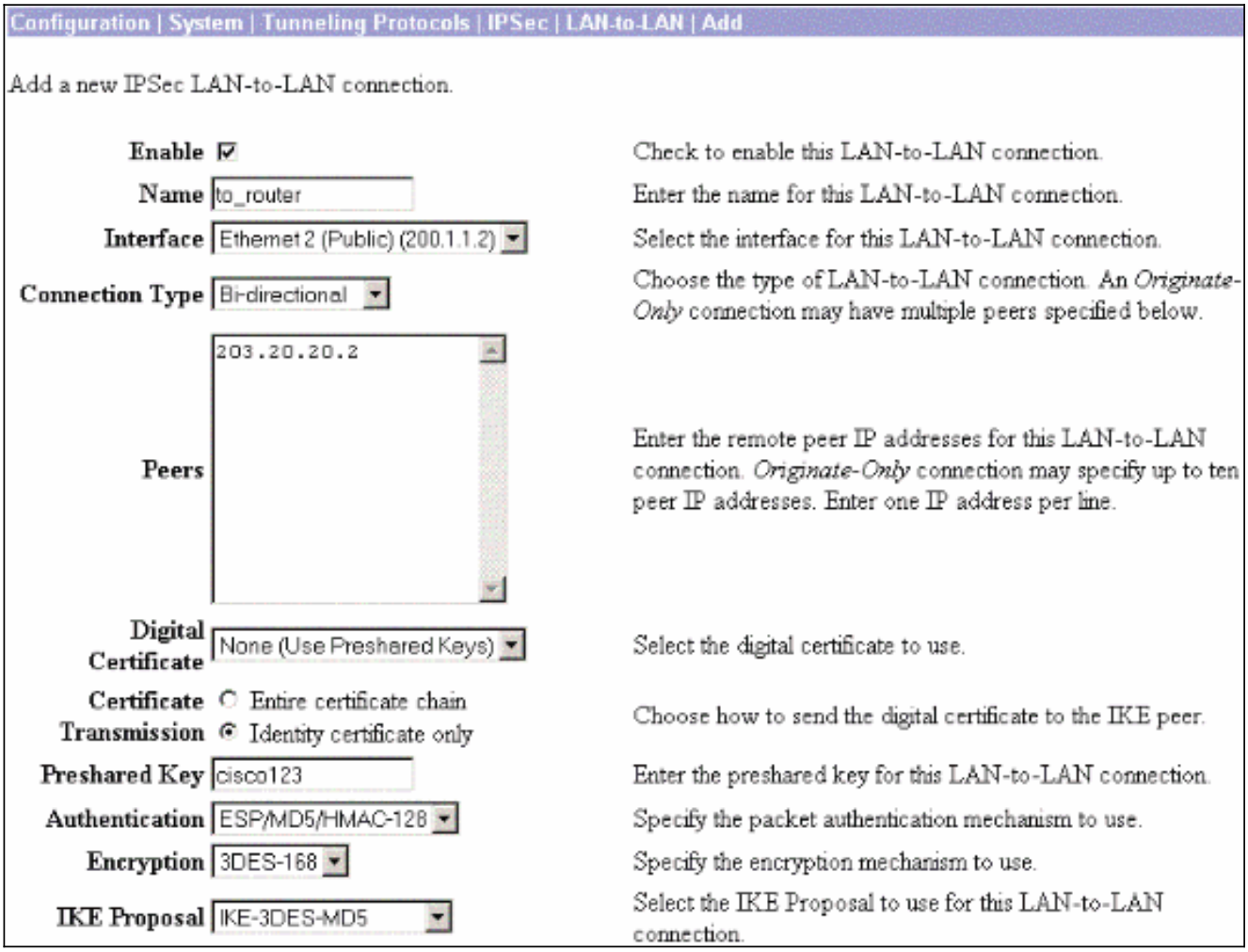
4. 완료되면 다음 두 네트워크 목록이 표시됩니다.**참고:** IPsec 터널이 나타나지 않으면 흥미로운 트래픽이 양쪽에서 일치하는지 확인합니다. 흥미로운 트래픽은 라우터와 PIX 상자의 액세스 목록에 의해 정의됩니다. VPN Concentrator의 네트워크 목록에 의해 정의됩니다

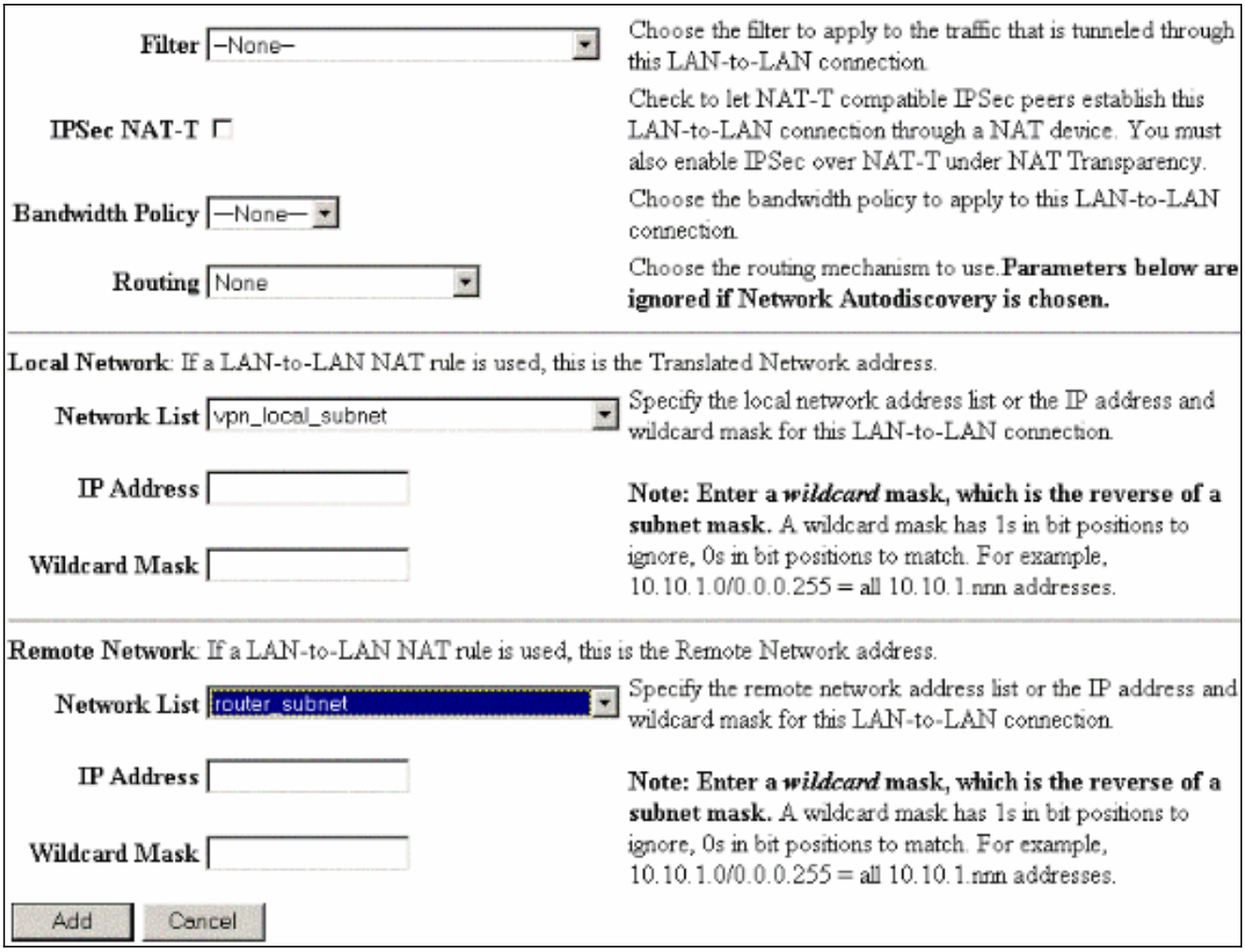
.



5. Configuration(**컨피그레이션**) > **System(시스템) Tunneling Protocols(터널링 프로토콜) > IPSec LAN-to-LAN**을 선택하고 LAN-to-LAN 터널을 정의합니다

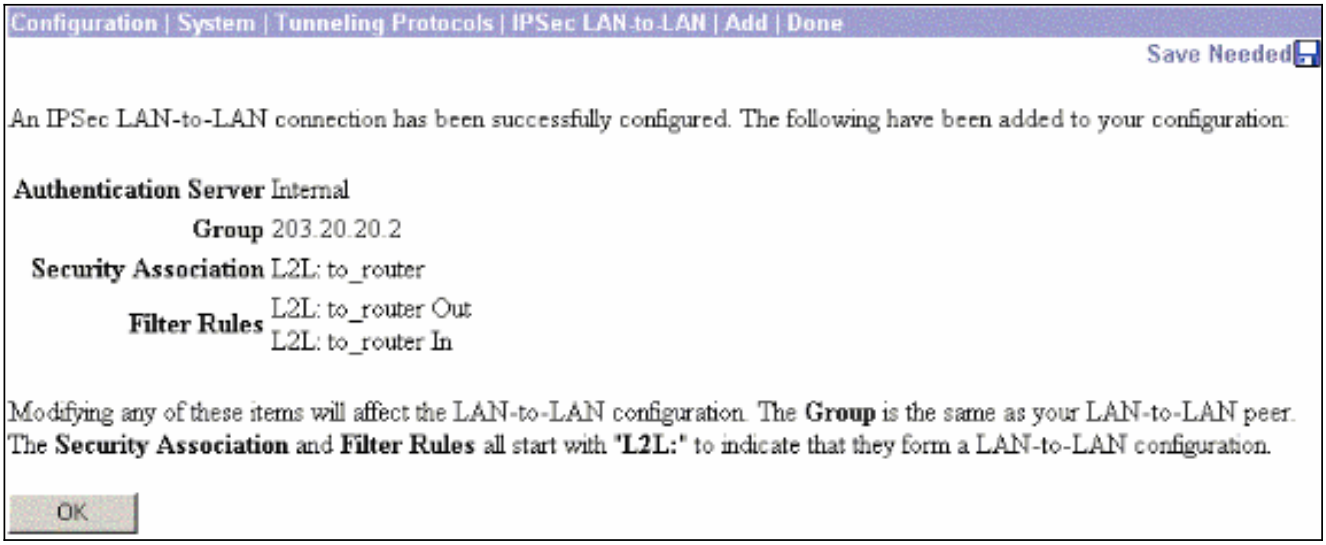
.





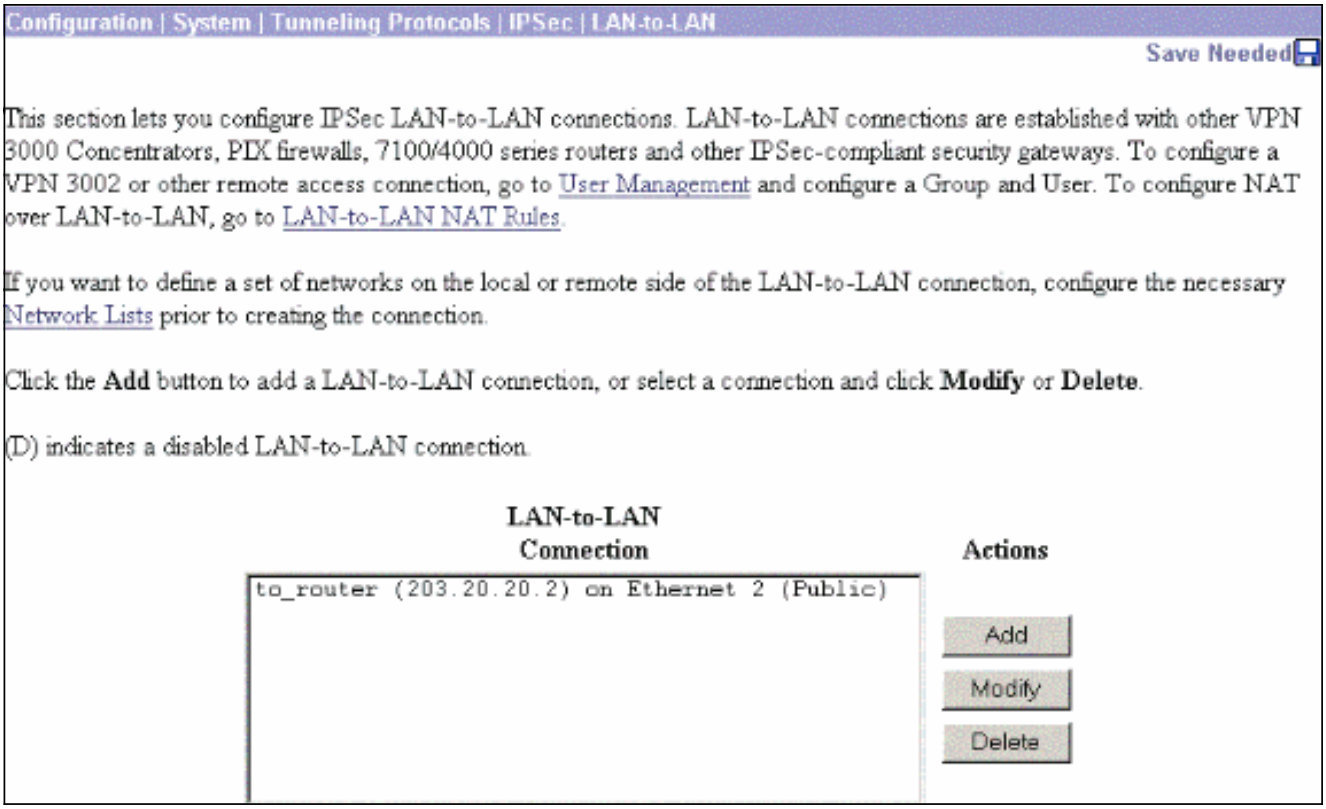
6. Apply(**적용**)를 클릭하면 LAN-to-LAN 터널 컨피그레이션의 결과로 자동으로 생성되는 다른 컨피그레이션과 함께 이 창이 표시됩니다

.



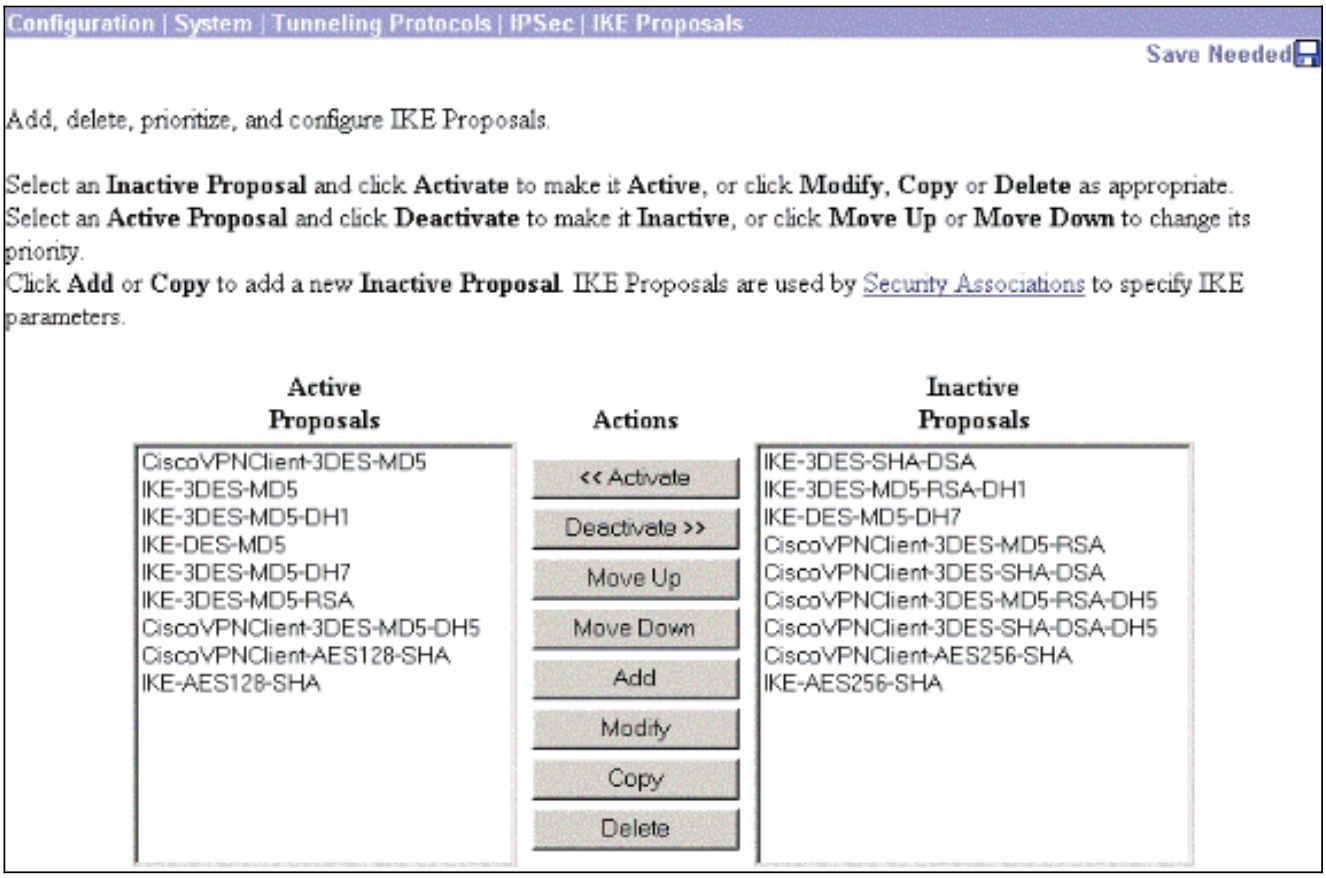
이전에 생성한 LAN-to-LAN IPsec 매개 변수는 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) **> IPSec LAN-to-LAN에서** 보거나 수정할 수 있습니다

.



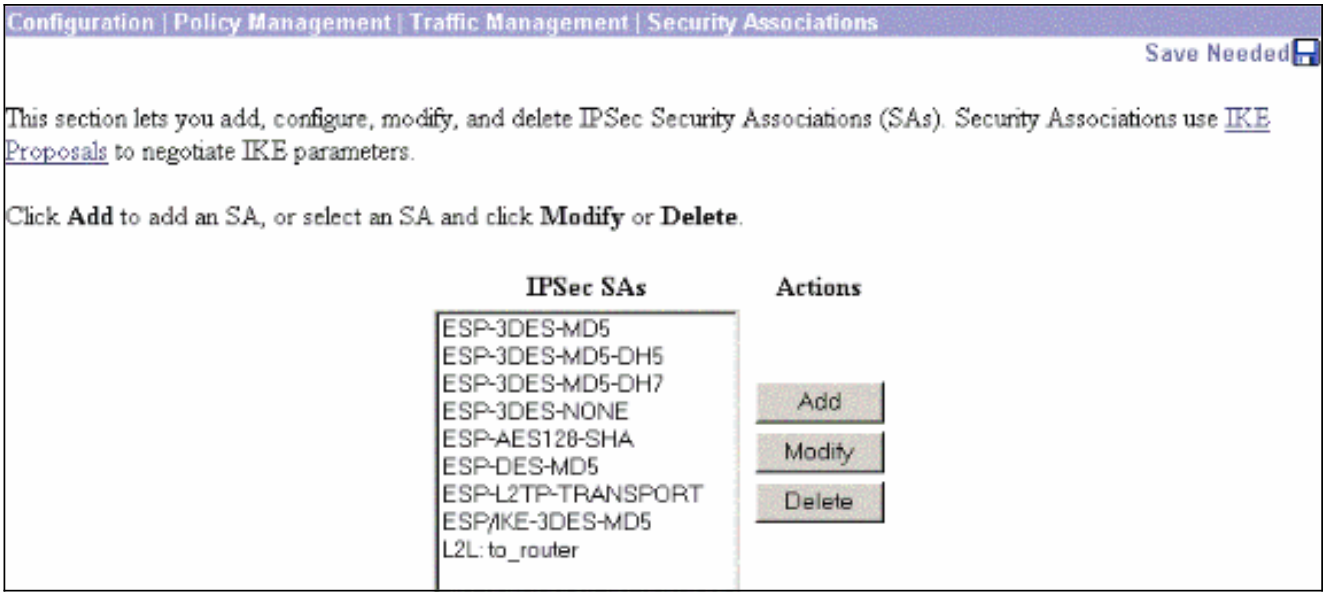
7. Configuration(**컨피그레이션**) > **System(시스템) Tunneling Protocols(터널링 프로토콜)** > **IPSec > IKE Proposals(IKE 제안)**를 선택하여 활성 IKE 제안을 확인합니다

.



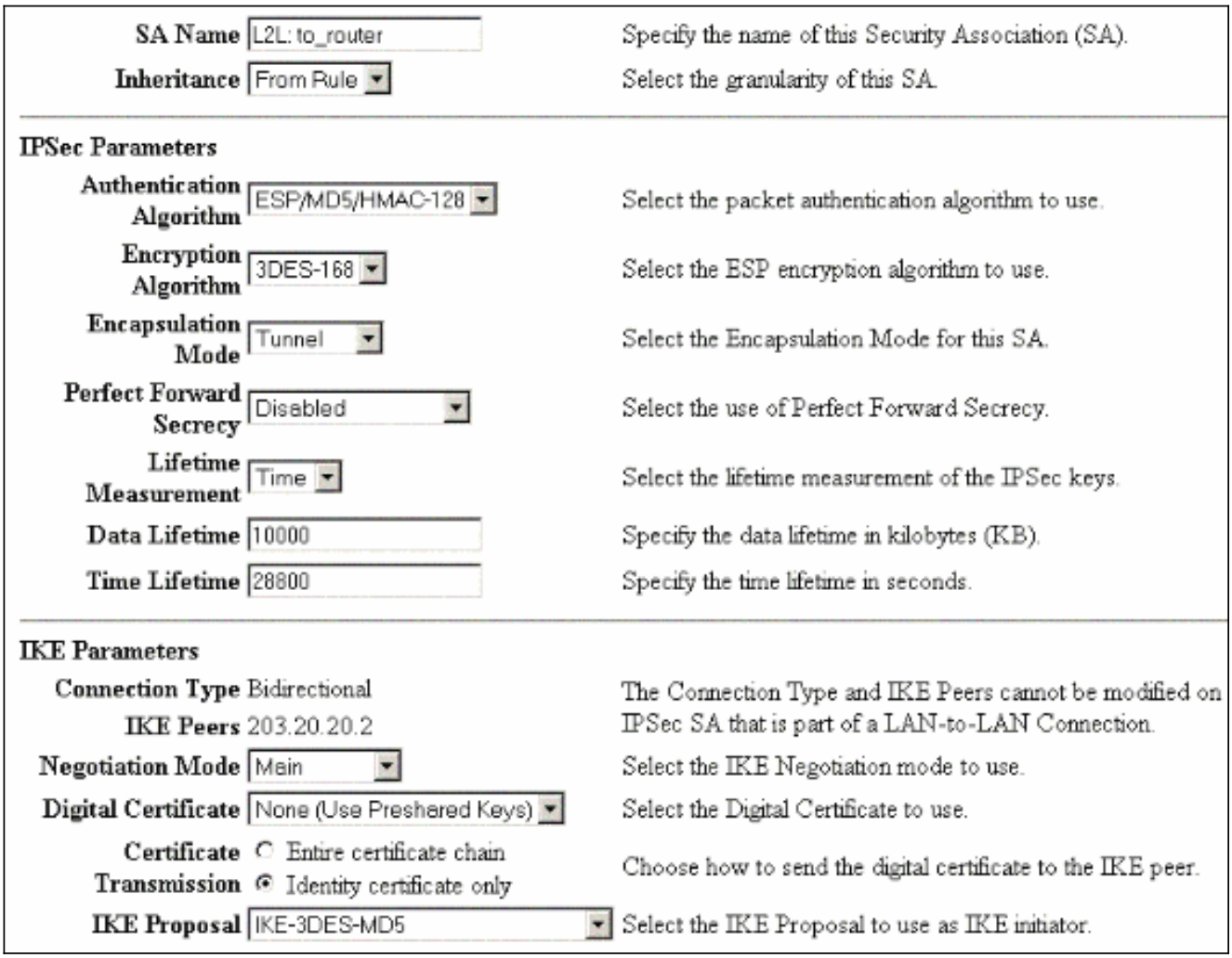
8. Configuration(**컨피그레이션**) > **Policy Management(정책 관리)** > Traffic Management(**트래픽 관리**) > **Security Associations(보안 연결)**를 선택하여 보안 연결 목록을 확인합니다

.



9. 보안 연결 이름을 클릭한 다음 **수정**을 클릭하여 보안 연결을 확인합니다

.



다음을 확인합니다.

이 섹션에서는 이 컨피그레이션에 사용된 **show** 명령을 나열합니다.

라우터에서

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

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

- **show crypto ipsec sa** - 현재 보안 연결에서 사용하는 설정을 표시합니다.
- **show crypto isakmp sa** - 피어의 현재 모든 인터넷 키 교환 보안 연결을 표시합니다.
- **show crypto engine connection active(암호화 엔진 연결 활성** 표시) - 모든 암호화 엔진에 대한 현재 활성 암호화 세션 연결을 표시합니다.

IOS Command Lookup Tool(등록된 고객만)을 사용하여 특정 명령에 대한 자세한 내용을 볼 수 있습니다.

VPN Concentrator에서

로깅을 켜려면 **Configuration > System > Events > Classes > Modify를 선택합니다.** 다음 옵션을 사용할 수 있습니다.

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

기록할 심각도 = 1-13

콘솔에 대한 심각도 = 1-3

Monitoring(**모니터링**) > **Event Log(이벤트 로그**)를 선택하여 이벤트 로그를 검색합니다.

문제 해결

라우터에서

debug 명령을 시도하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

문제 - 터널을 시작할 수 없습니다.

오류 메시지

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

솔루션

원하는 동시 로그인 수를 구성하거나 이 SA에 대해 동시 로그인을 5로 설정하려면 이 작업을 완료합니다.

Configuration(**구성) > User Management(사용자 관리) > Groups(그룹) > Modify 10.19.187.229 > General(일반) > Simultaneouts Logins(동시 로그인)**로 이동하여 로그인 수를 5로 변경합니다.

PFS

IPsec 협상에서 PFS(Perfect Forward Secrecy)는 각 새 암호화 키가 이전 키와 관련이 없도록 합니다. 두 터널 피어에서 PFS를 활성화 또는 비활성화합니다. 그렇지 않으면 라우터에 LAN-to-LAN(L2L) IPsec 터널이 설정되지 않습니다.

이 암호화 맵 항목에 대해 새 보안 연결이 요청될 때 IPsec이 PFS를 요청하도록 지정하거나, 새 보안 연결에 대한 요청을 받을 때 IPsec에서 PFS를 요구하도록 지정하려면 암호화 맵 컨피그레이션 모드에서 **set pfs** 명령을 사용합니다. IPsec에서 PFS를 요청하지 않도록 지정하려면 이 명령의 **no** 형식을 사용합니다.

```
set pfs [group1 | group2]
no set pfs
```

set pfs 명령의 **경우**:

- *group1* - 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 768비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.
- *group2* **-** 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 1024비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.

기본적으로 PFS는 요청되지 않습니다. 이 명령으로 지정된 그룹이 없으면 *group1***이** 기본값으로 사용됩니다.

예:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

set pfs 명령에 대한 자세한 내용은 Cisco IOS Security Command Reference를 **참조하십시오**.

관련 정보

- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- Cisco VPN 3000 Series Concentrator
- Cisco VPN 3002 하드웨어 클라이언트
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems