PDM 구성을 사용하여 두 PIX 간 LAN-to-LAN VPN 터널 예

목차

소개

이 문서에서는 Cisco PDM(PIX Device Manager)을 사용하여 두 PIX 방화벽 간에 VPN 터널을 구성하는 절차에 대해 설명합니다.PDM은 GUI를 사용하여 PIX 방화벽을 설정, 구성 및 모니터링하는 데 도움이 되도록 설계된 브라우저 기반 구성 도구입니다.PIX 방화벽은 서로 다른 두 사이트에 배치됩니다.

터널은 IPsec을 사용하여 형성됩니다.IPsec은 IPsec 피어 간에 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증을 제공하는 개방형 표준의 조합입니다.

사전 요구 사항

요구 사항

이 문서에 대한 요구 사항이 없습니다.

사용되는 구성 요소

이 문서의 정보는 6.x 및 PDM 버전 3.0이 포함된 Cisco Secure PIX 515E Firewalls를 기반으로 합니다.

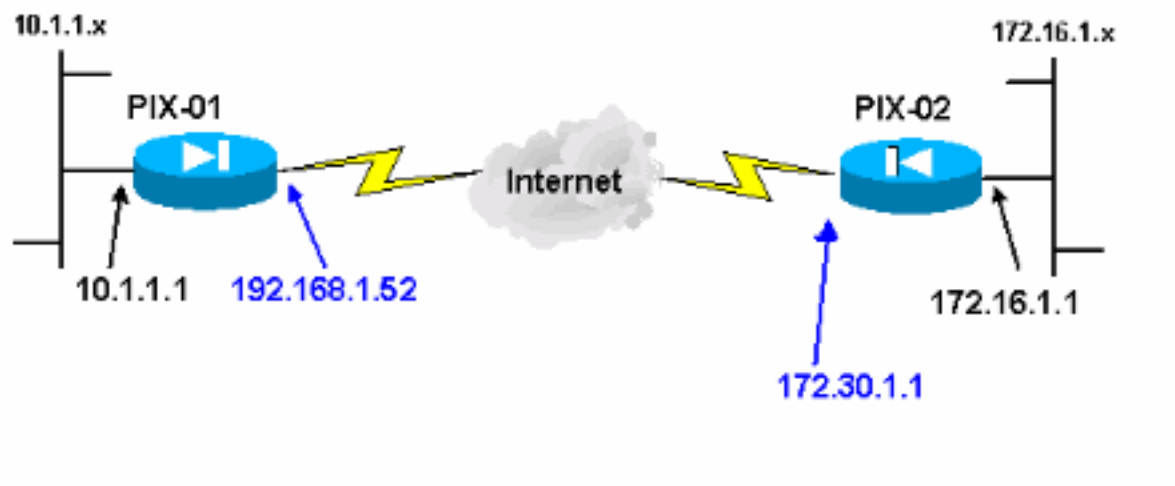
CLI(Command Line Interface)를 사용하여 두 PIX 디바이스 간 VPN 터널 컨피그레이션에 대한 컨피그레이션 예는 IPsec을 사용하여 단순 PIX-to-PIX VPN 터널 구성을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 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 규칙을 참조하십시오.

배경 정보

IPsec 협상은 5단계로 나눌 수 있으며 2개의 IKE(Internet Key Exchange) 단계를 포함합니다.

1. IPsec 터널은 흥미로운 트래픽에 의해 시작됩니다.트래픽은 IPsec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.
2. 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.
3. IKE 2단계에서 IPsec 피어는 IPsec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다.공유 정책의 협상은 IPsec 터널의 설정 방법을 결정합니다.
4. IPsec 터널이 생성되고 IPsec 변형 집합에 구성된 IPsec 매개변수를 기반으로 IPsec 피어 간에 데이터가 전송됩니다.
5. IPsec 터널은 IPsec SA가 삭제되거나 수명이 만료될 때 종료됩니다.**참고:** 두 IKE 단계의 SA가 피어에서 일치하지 않으면 두 PIX 간의 IPsec 협상이 실패합니다.

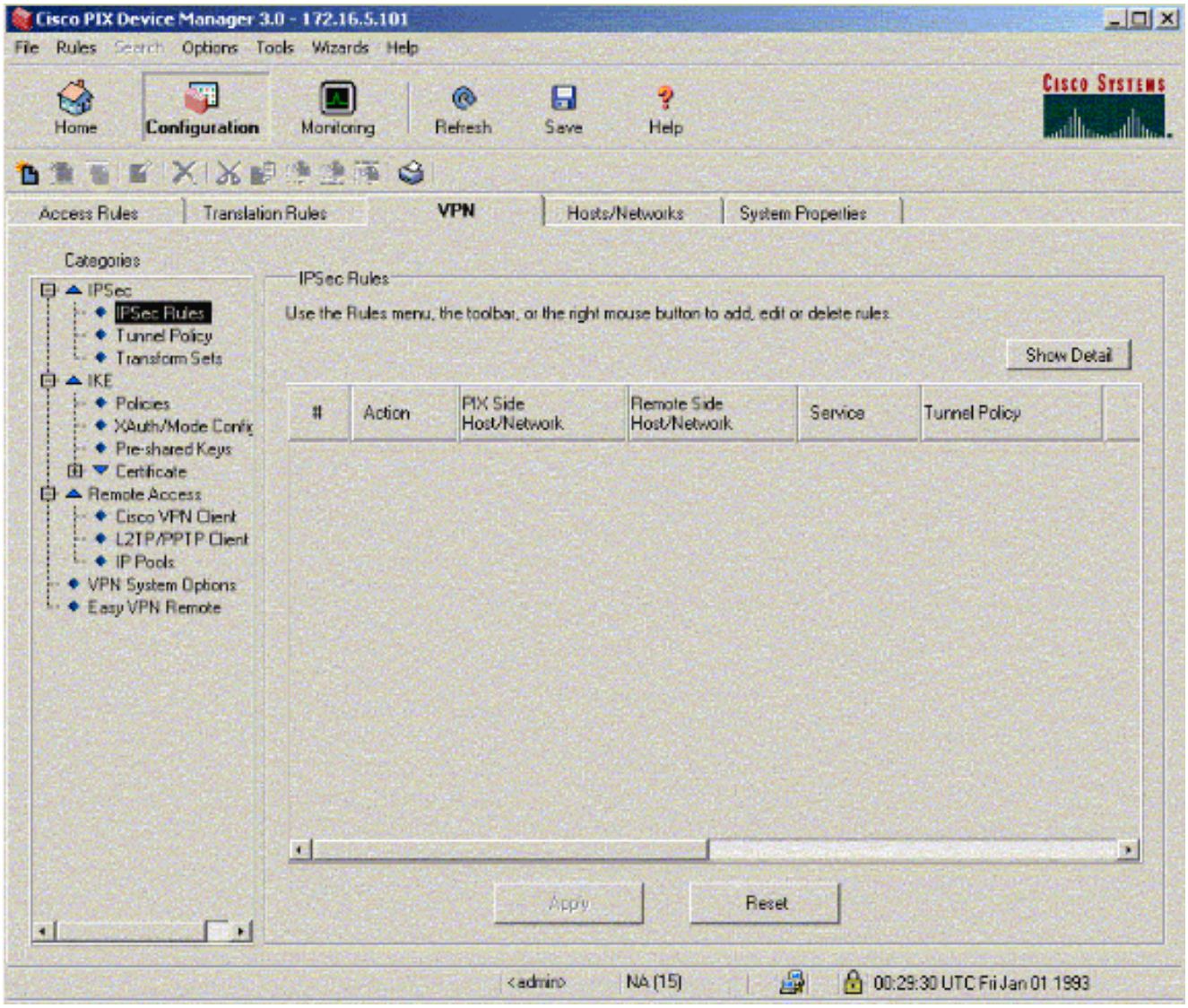
구성 절차

PIX의 CLI에 있는 다른 일반 컨피그레이션 외에, **http server enable** 및 **http server <local_ip> <mask> <interface>** 명령을 사용합니다. 여기서 ***<local_ip> 및 <mask>는 PDM이 설치된 워크스테이션의 IP 주소와 마스크입니다.***이 문서의 컨피그레이션은 PIX-01에 대한 것입니다. PIX-02는 주소가 서로 다른 동일한 단계를 사용하여 구성할 수 있습니다.

다음 단계를 완료하십시오.

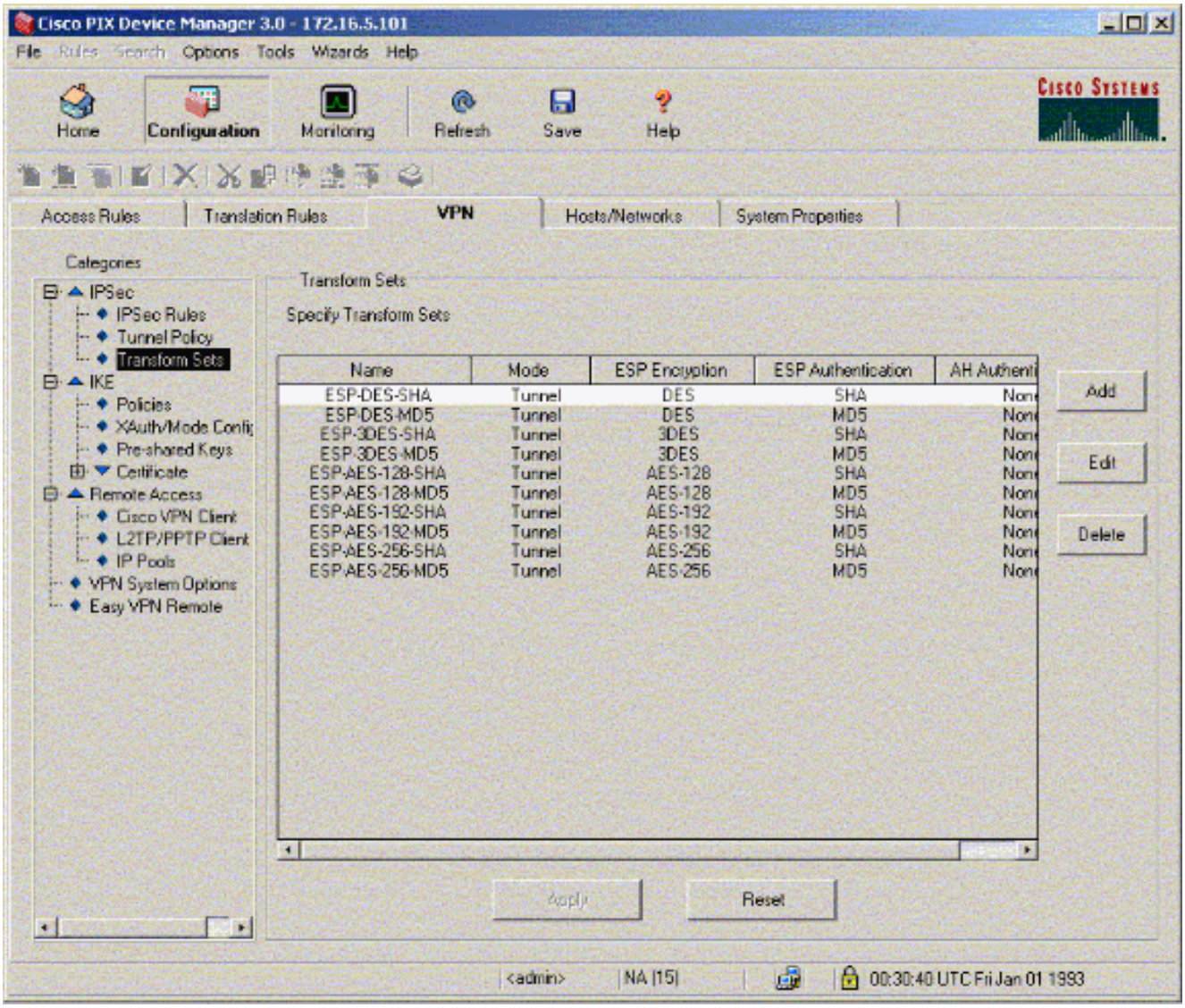
1. 브라우저를 열고 https://**<Inside_IP_Address_of_PIX>를 입력하여 PDM**의 PIX에 액세스합니다.
2. Configuration(**컨피그레이션**)을 클릭하고 VPN 탭으로 이동합니다

.



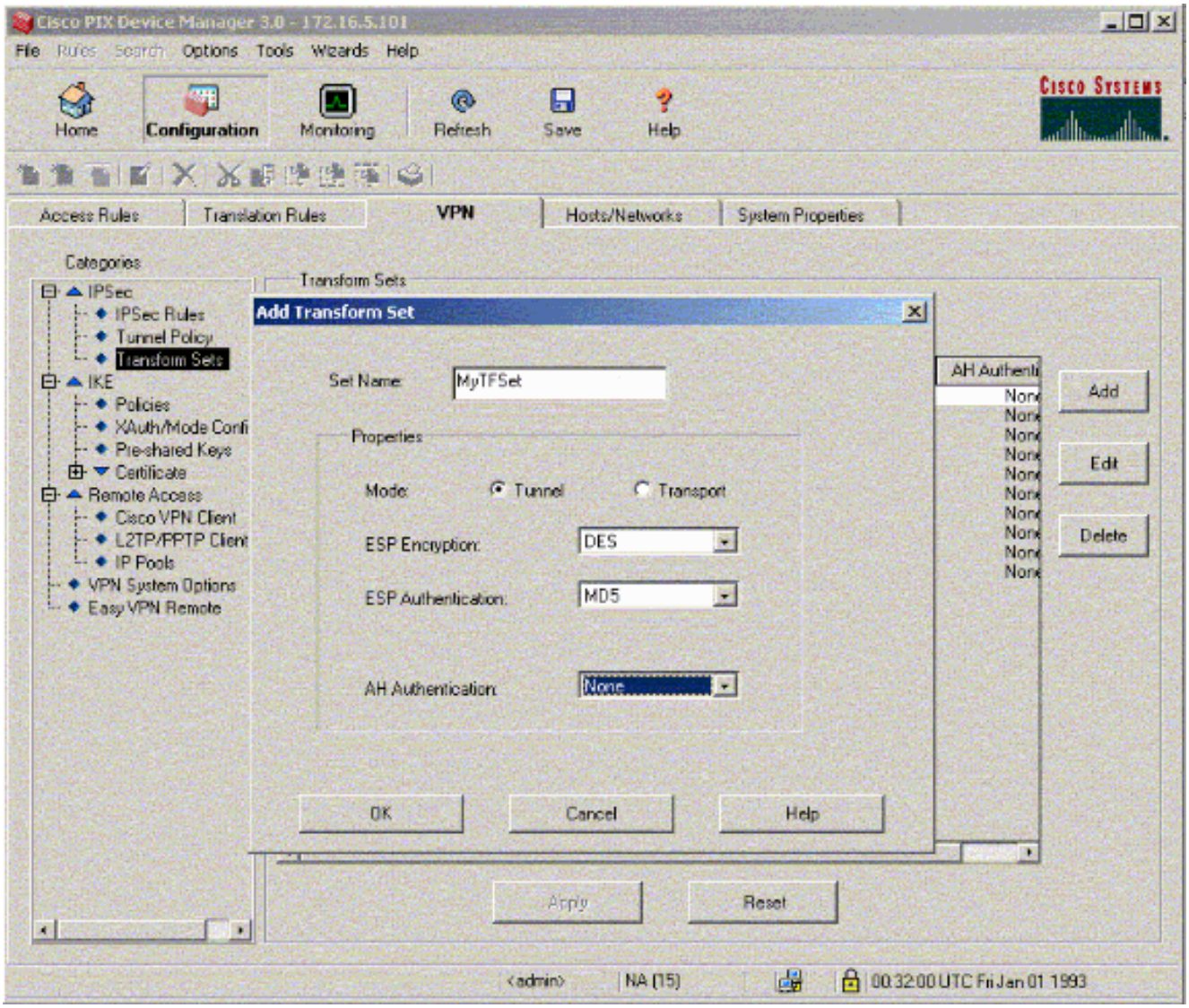
3. IPSec 아래의 Transform Sets를 클릭하여 변형 집합을 생성합니다

.



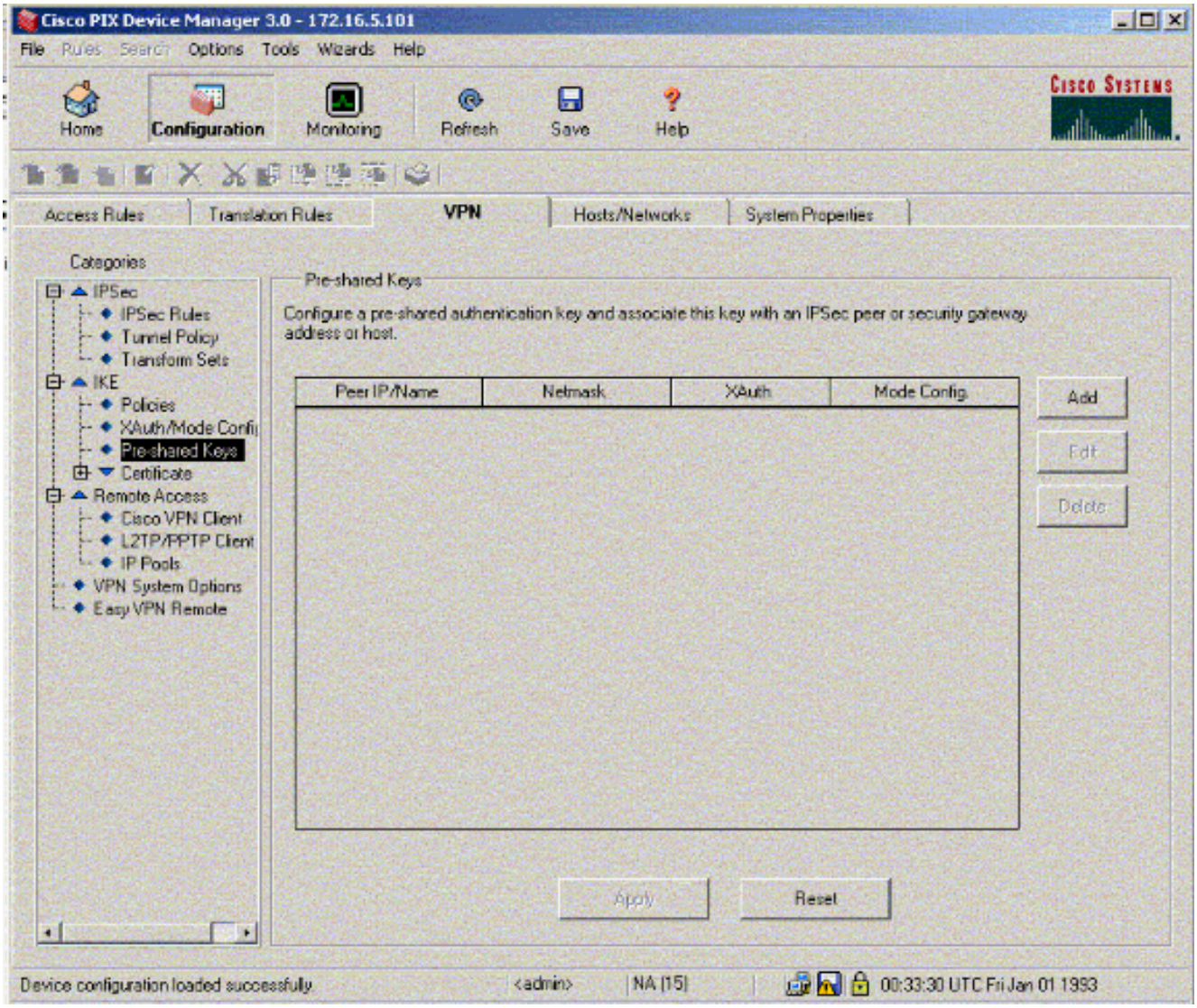
4. Add(**추가**)를 클릭하고 적절한 옵션을 모두 선택한 다음 **OK(확인)**를 클릭하여 새 변형 집합을 생성합니다

.



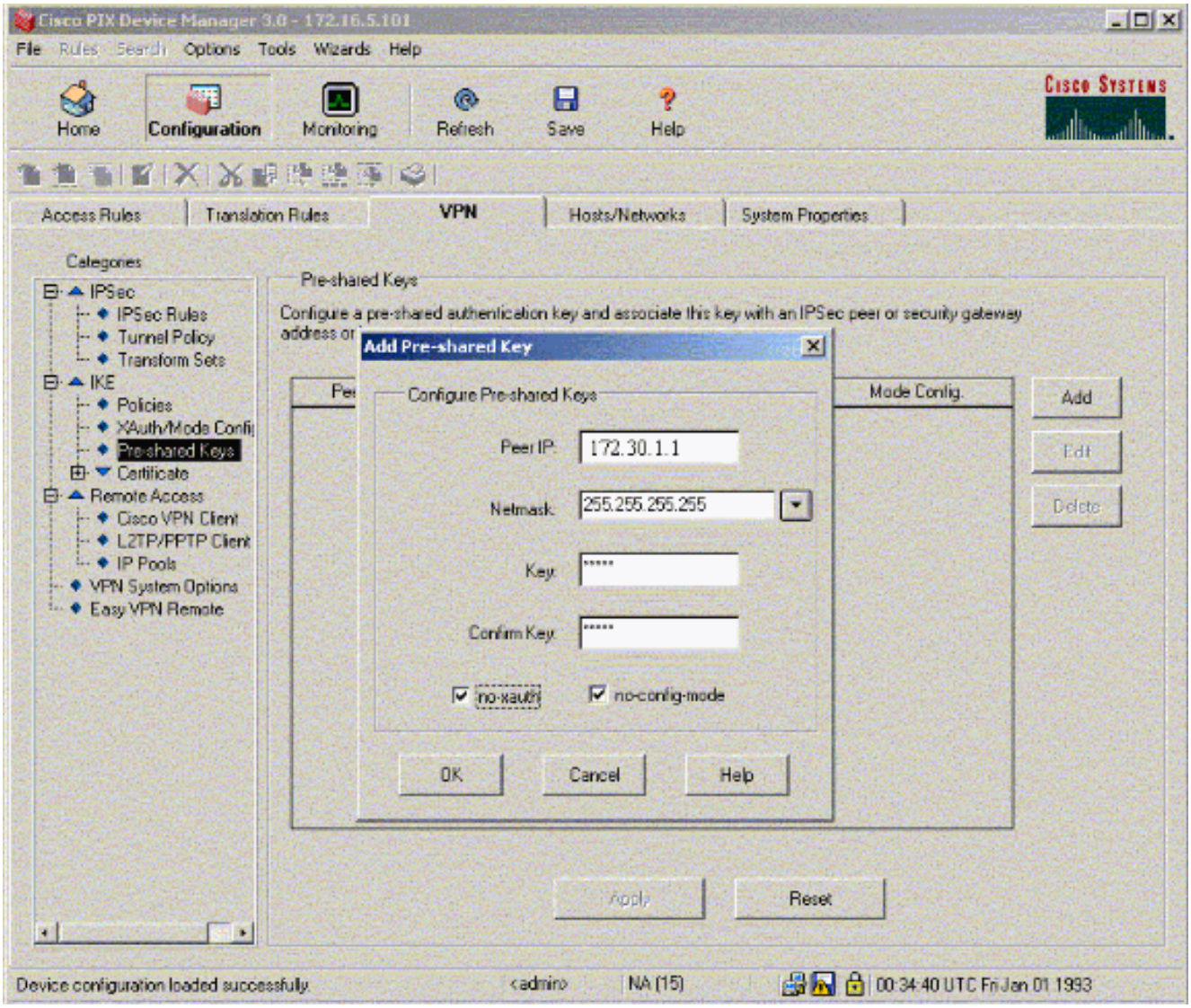
5. 사전 공유 키를 **구성하려면 IKE** 아래에서 Pre-Shared Keys를 클릭합니다

.



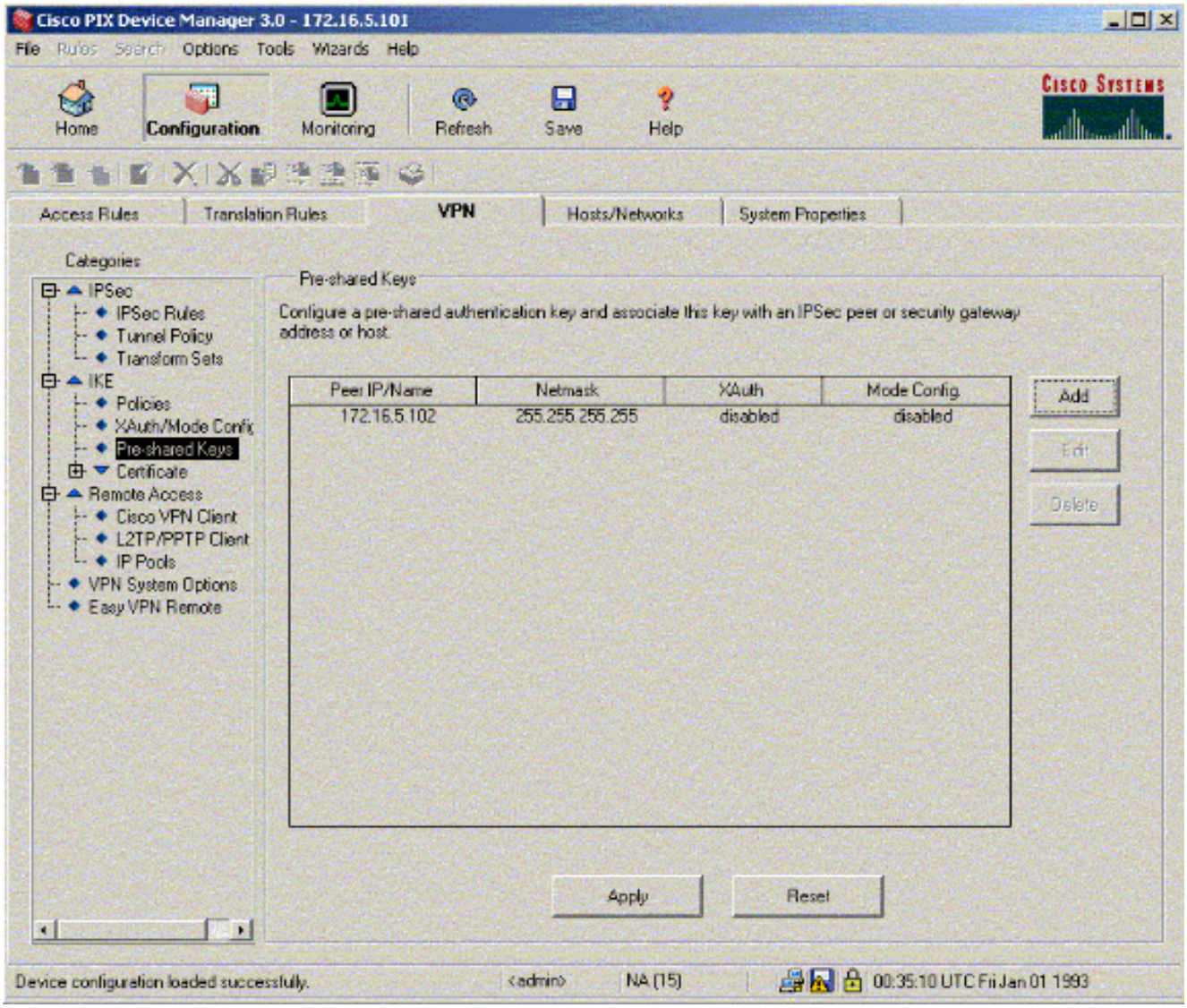
6. Add(**추가**)를 클릭하여 새 사전 공유 키를 추가합니다

.



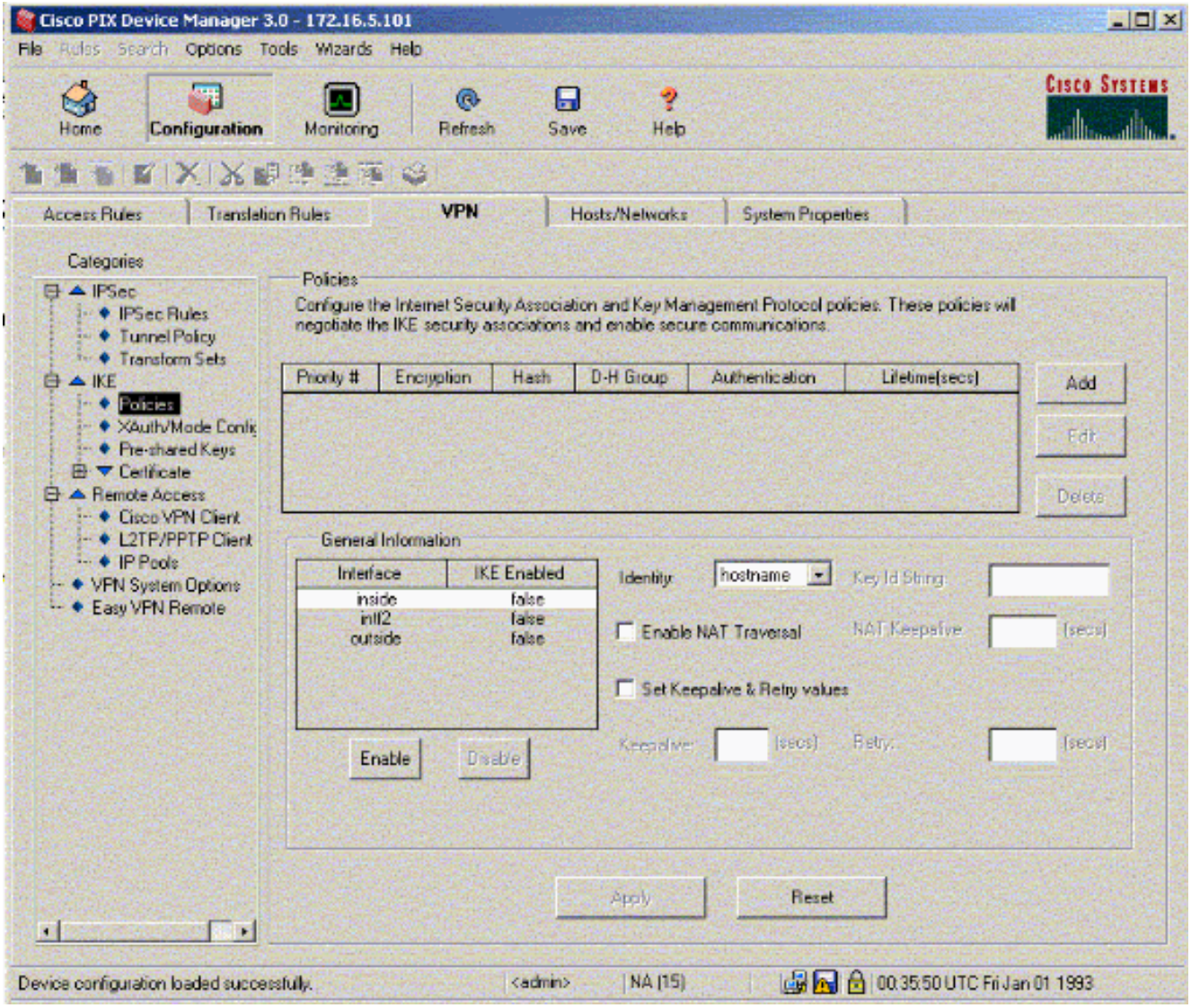
이 창에는 터널 연결의 암호인 키가 표시됩니다.터널의 양쪽에서 일치해야 합니다

.



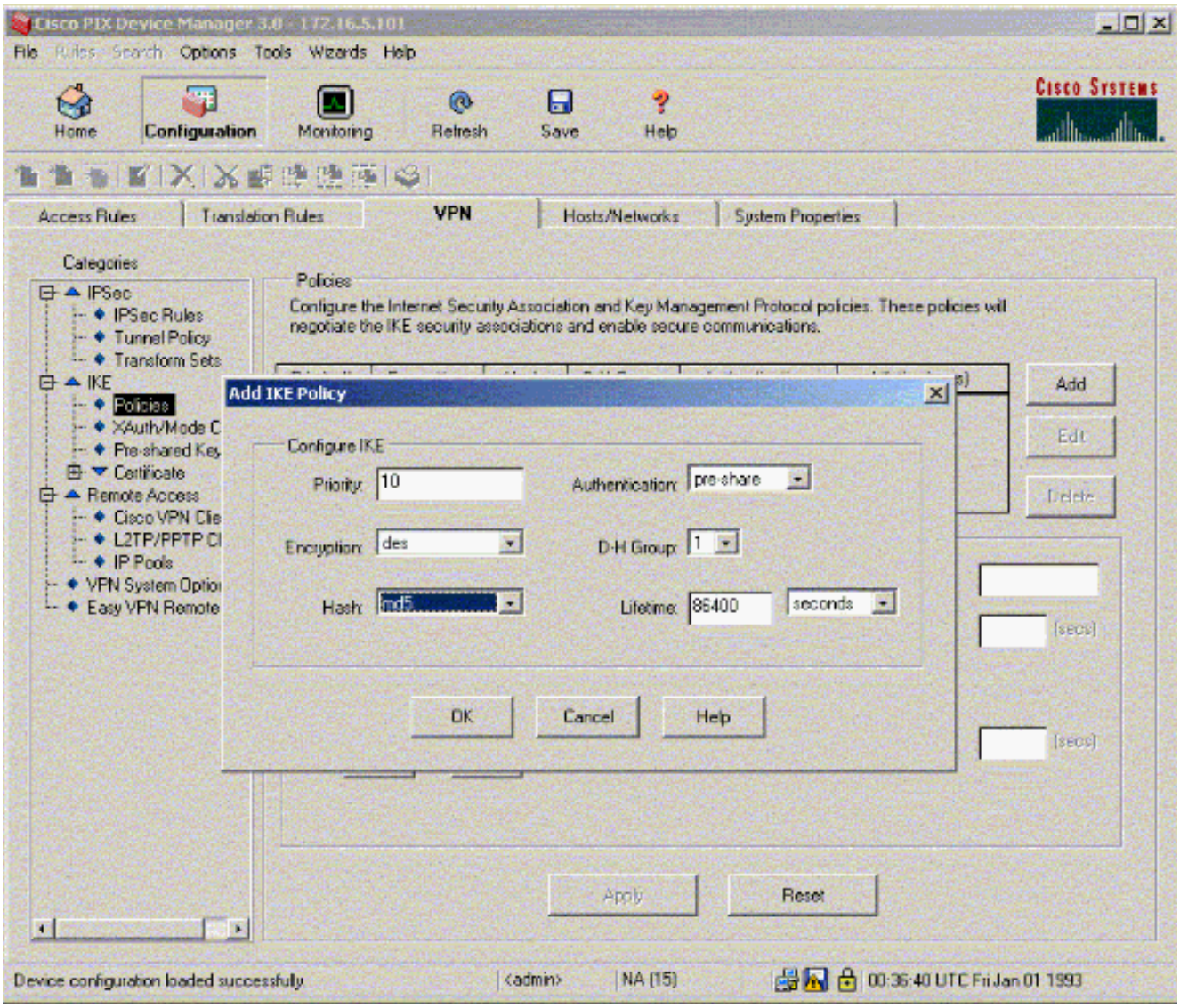
7. 정책을 구성하려면 IKE 아래에서 Policies(정책)를 클릭합니다

.



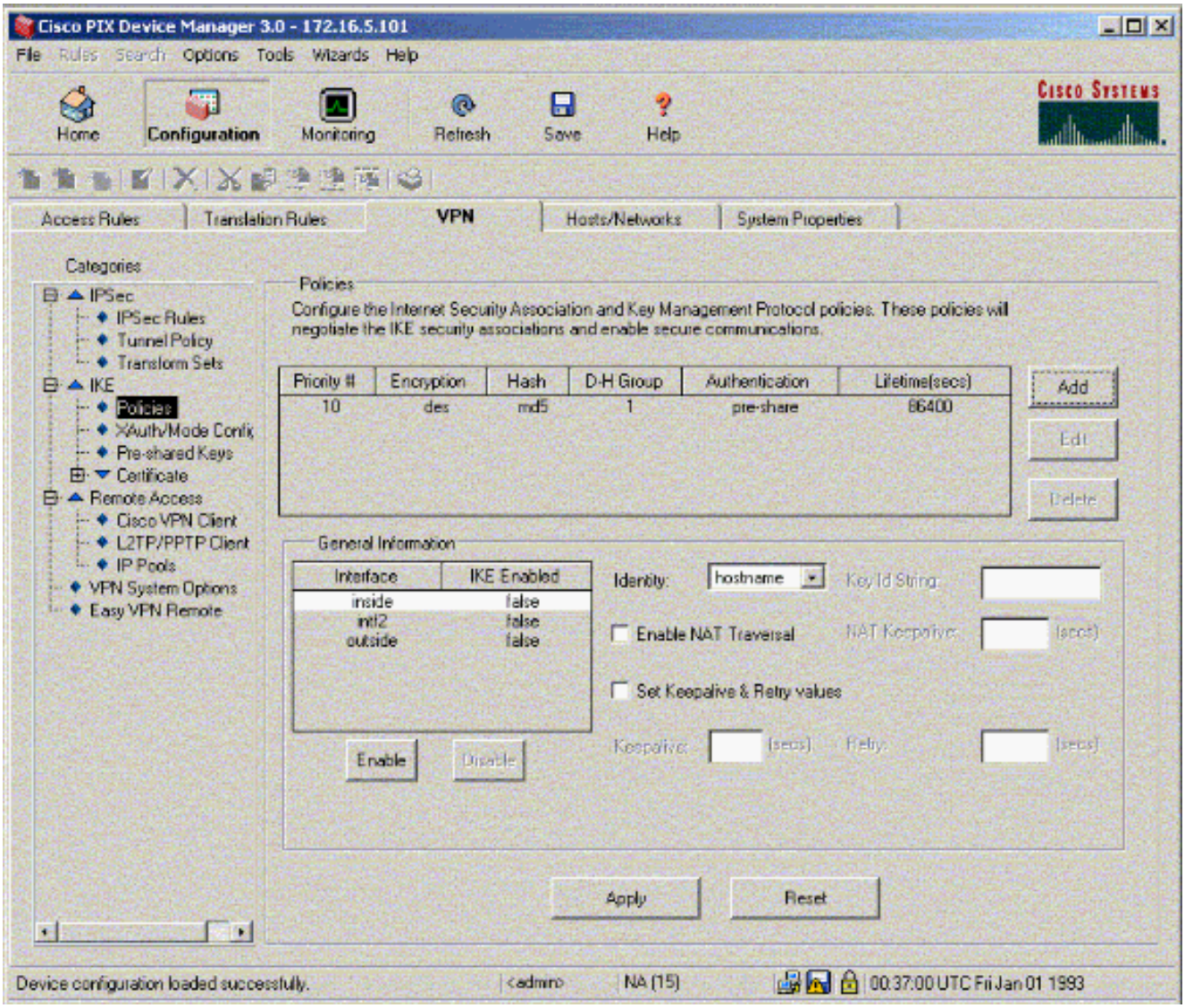
8. Add(**추가**)를 클릭하고 적절한 필드를 입력합니다

.



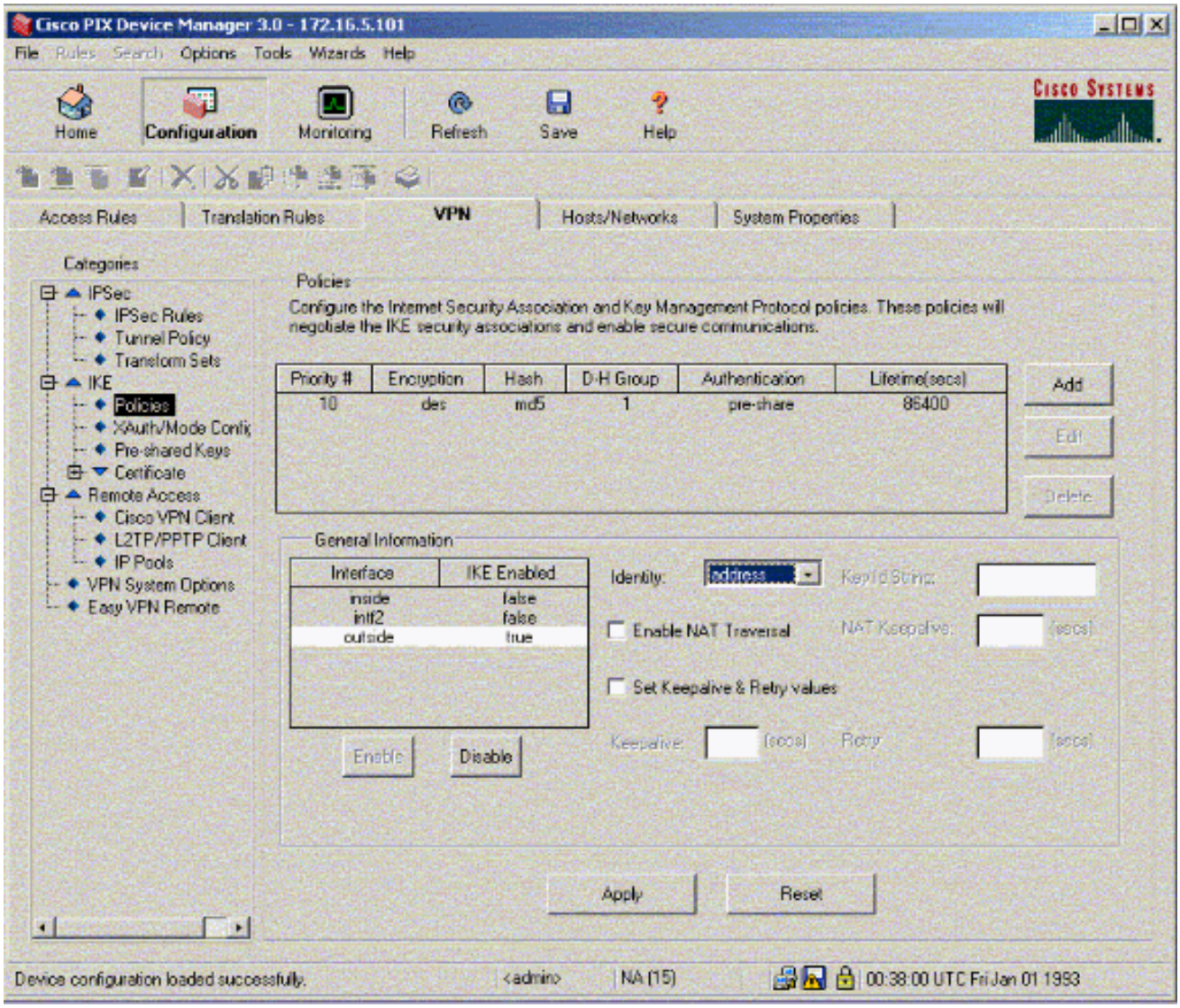
9. OK(**확인**)를 클릭하여 새 정책을 추가합니다

.



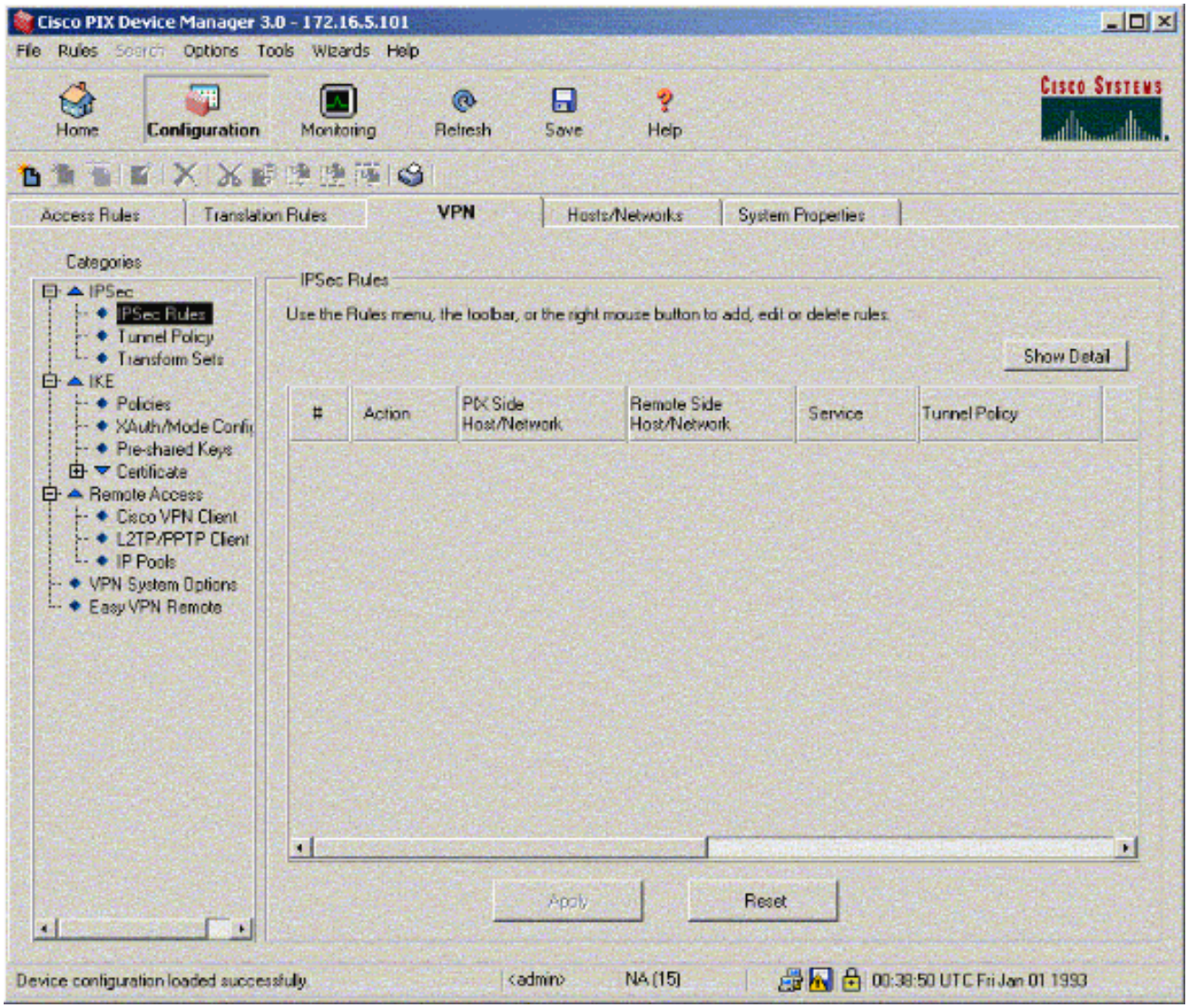
10. **외부** 인터페이스를 선택하고 **Enable**을 클릭한 다음 Identity 풀다운 메뉴에서 **주소**를 선택합니다

.



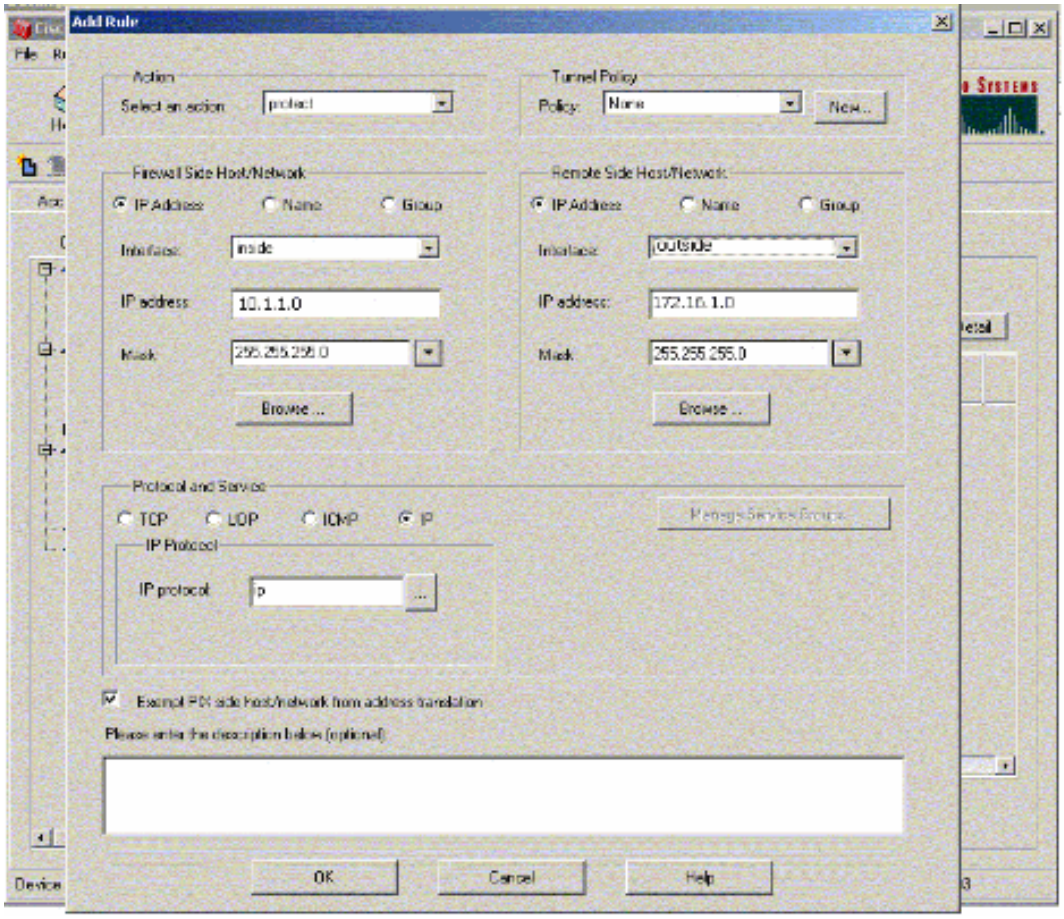
11. IPSec에서 **IPSec 규칙**을 클릭하여 IPsec 규칙을 생성합니다

.



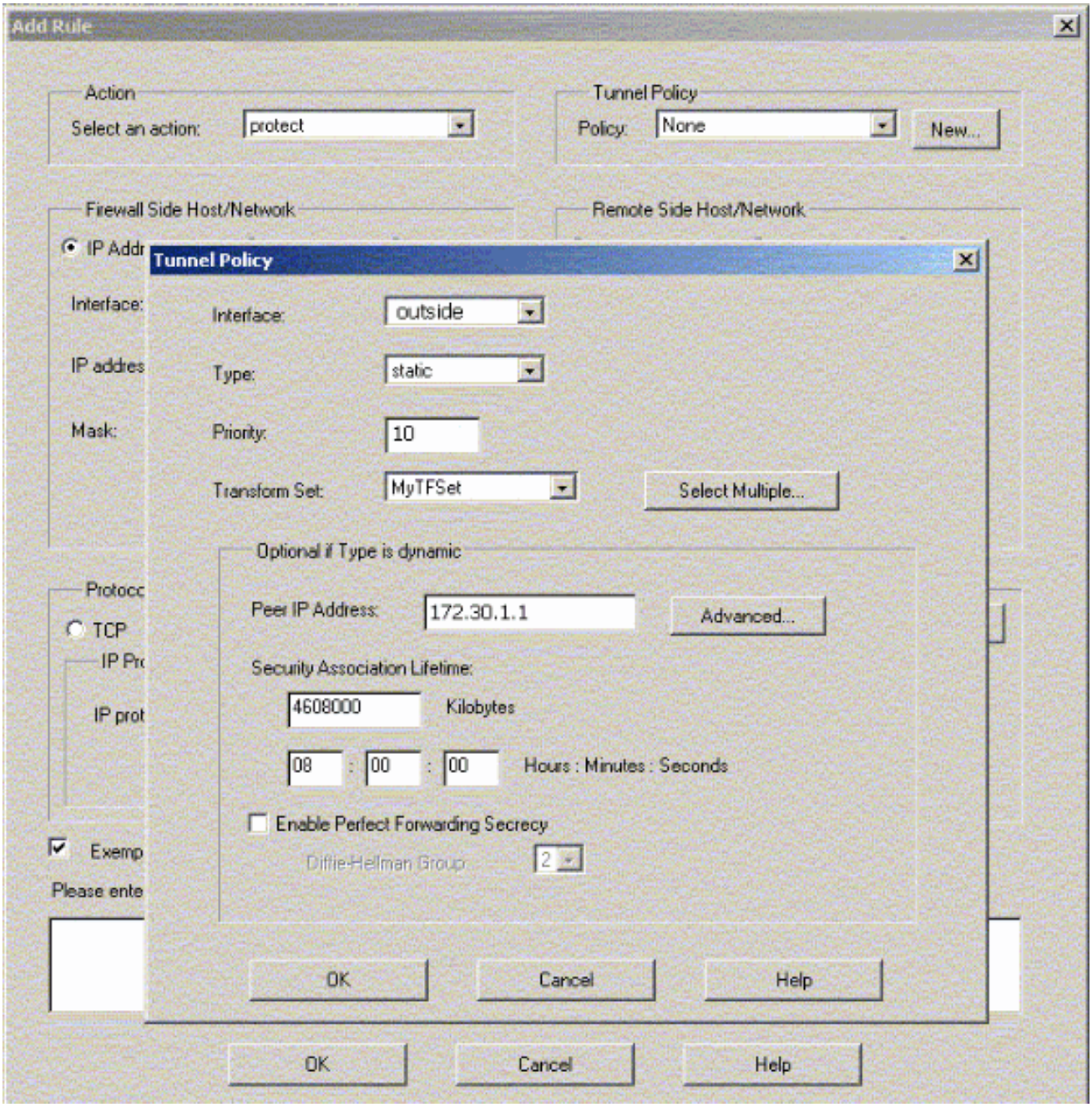
12. 해당 필드를 입력합니다

.



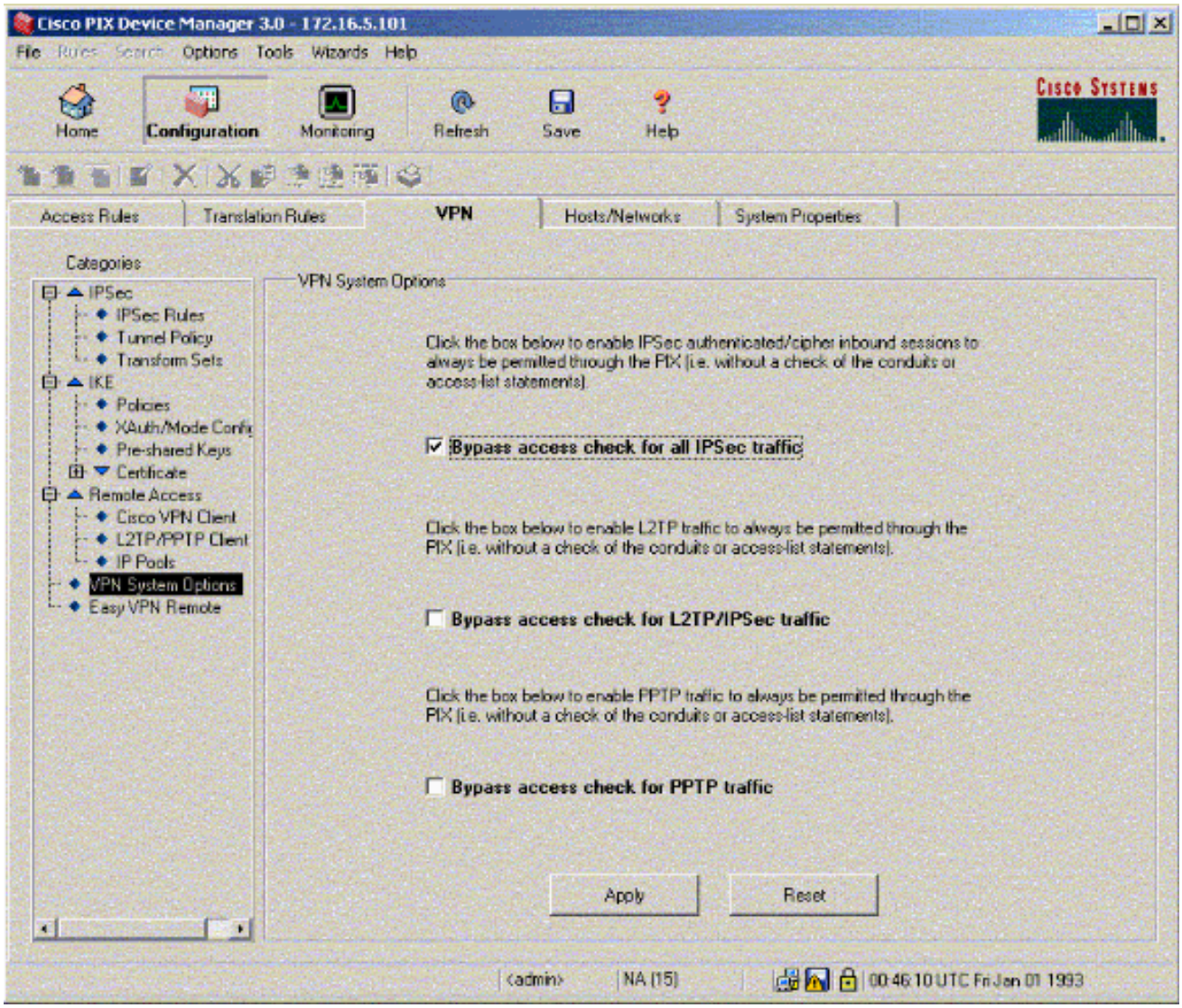
13. Tunnel **Policy**(터널 정책)에서 New(새로 만들기)를 클릭합니다.Tunnel Policy 창이 나타납니다.해당 필드를 입력합니다

.



14. OK(**확인**)를 클릭하여 구성된 IPsec 규칙을 확인합니다.
15. VPN **Systems Options(VPN 시스템 옵션)**를 클릭하고 **모든 IPSec 트래픽에 대한 Bypass access check(액세스 우회 확인)를 선택합니다**

.

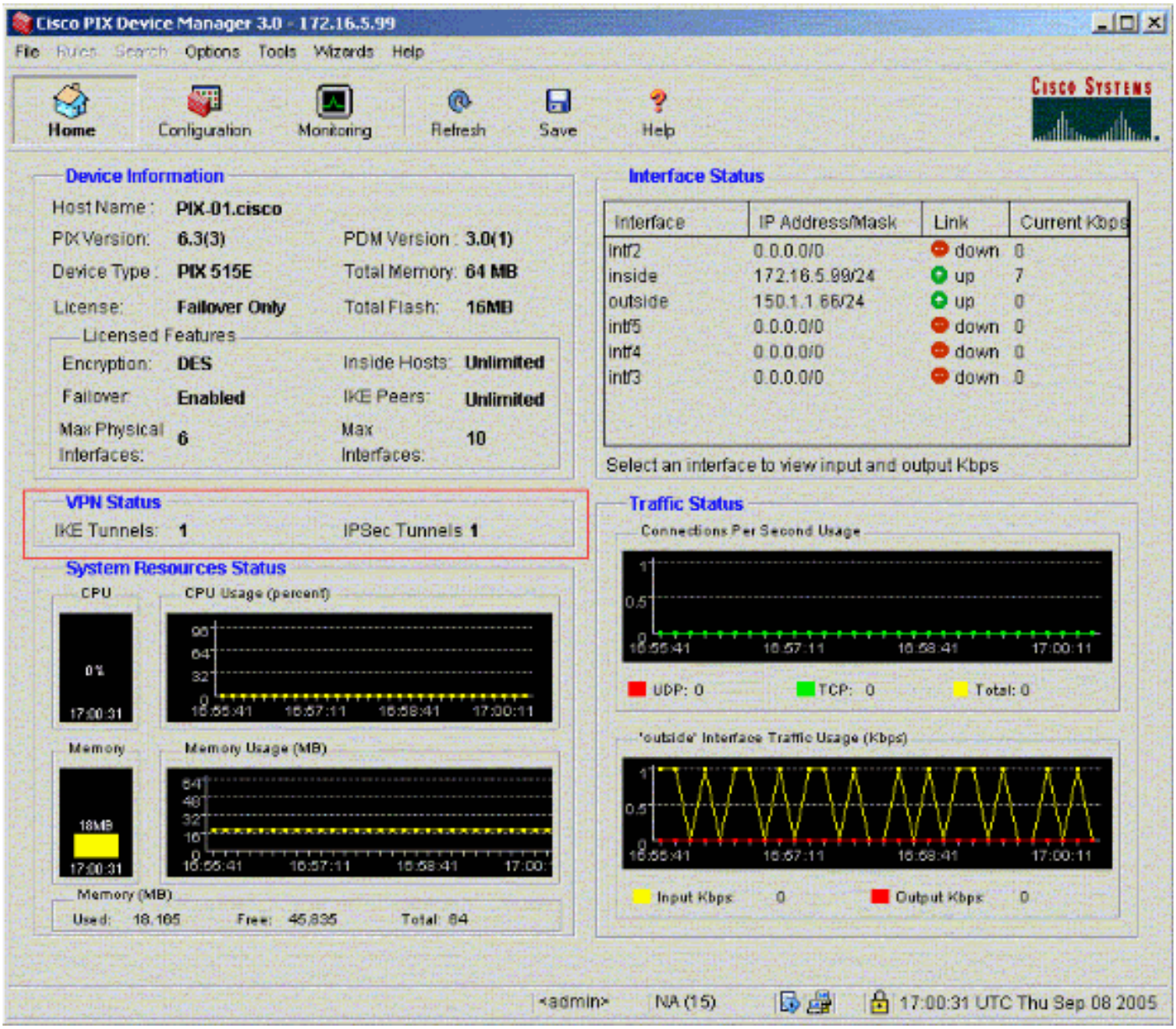


다음을 확인합니다.

피어에 대한 흥미로운 트래픽이 있는 경우 터널은 PIX-01과 PIX-02 사이에 설정됩니다.

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

PDM의 Home(홈)에서 VPN Status(VPN 상태)를 보고(빨간색으로 강조 표시됨) 터널을 확인합니다
.



PDM의 도구 아래에서 CLI를 사용하여 터널 구성을 확인할 수도 있습니다.show crypto isakmp **sa** 명령을 실행하여 터널 구성을 확인하고 **show crypto ipsec sa** 명령을 실행하여 캡슐화, 암호화 등의 패킷 수를 확인합니다.

참고: PIX의 내부 인터페이스는 management-access 명령이 전역 확인 모드에서 구성되지 않는 한 터널을 형성하기 위해 ping할 수 없습니다.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- PDM을 사용하여 방화벽 간 이중 터널 생성
- Cisco Secure PIX Firewall 명령 참조

- RFC(Request for Comments)
- Cisco PIX 방화벽 소프트웨어