PDM을 사용하여 방화벽 간 이중 터널 생성

목차

소개

이 문서에서는 Cisco PDM(PIX Device Manager)을 사용하여 두 PIX 방화벽 간의 터널을 구성하는 데 사용하는 절차에 대해 설명합니다. PIX 방화벽은 서로 다른 두 사이트에 배치됩니다. 기본 경로에 도달하지 못할 경우 이중 링크를 통해 터널을 시작하는 것이 좋습니다. IPsec은 IPsec 피어 간에 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증을 제공하는 개방형 표준의 조합입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

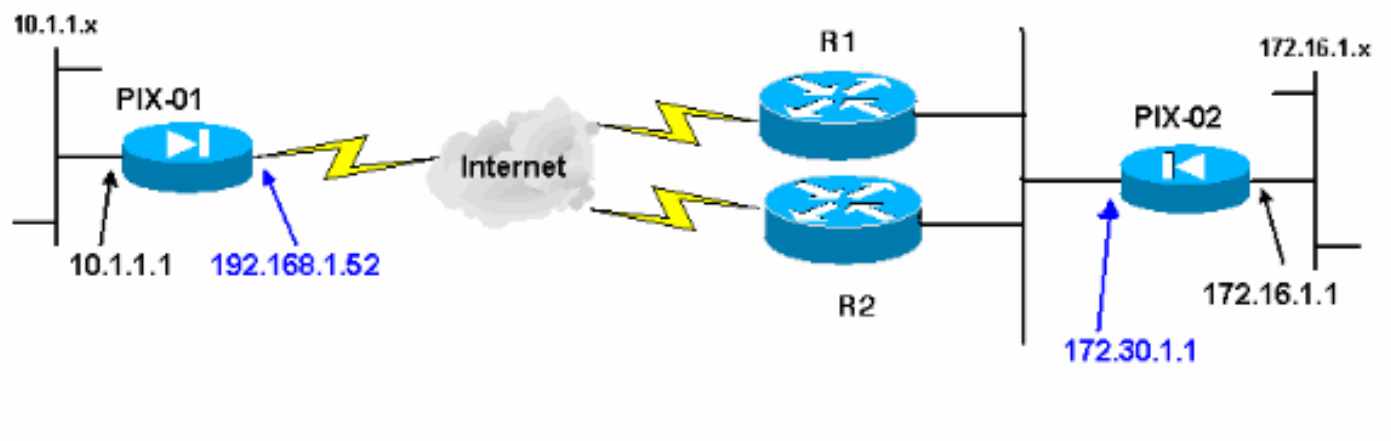
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure PIX 515E Firewalls with 6.x and PDM version 3.0

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 규칙을 참조하십시오.

배경 정보

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

IPsec 터널은 흥미로운 트래픽에 의해 시작됩니다. 트래픽은 IPsec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.

IKE 1단계에서 IPsec 피어는 설정된 IKE SA(Security Association) 정책을 협상합니다. 피어가 인증되면 ISAKMP(Internet Security Association and Key Management Protocol)를 사용하여 보안 터널이 생성됩니다.

IKE 2단계에서 IPsec 피어는 IPsec SA 변형을 협상하기 위해 인증되고 안전한 터널을 사용합니다. 공유 정책의 협상은 IPsec 터널의 설정 방법을 결정합니다.

IPsec 터널이 생성되고 IPsec 변형 집합에 구성된 IPsec 매개변수를 기반으로 IPsec 피어 간에 데이터가 전송됩니다.

IPsec 터널은 IPsec SA가 삭제되거나 수명이 만료될 때 종료됩니다.

참고: 두 IKE 단계의 SA가 피어에서 일치하지 않으면 두 PIX 간의 IPsec 협상이 실패합니다.

구성

이 절차에서는 흥미로운 트래픽이 있을 때 터널을 트리거하도록 PIX 방화벽 중 하나의 컨피그레이션을 안내합니다. 이 컨피그레이션을 사용하면 PIX-01과 PIX-02에서 라우터 1(R1)까지 연결되지 않은 경우 라우터 2(R2)를 통해 백업 링크를 통해 터널을 설정할 수 있습니다. 이 문서에서는 PDM을 사용하는 PIX-01의 컨피그레이션을 보여 줍니다. 유사한 행에서 PIX-02를 구성할 수 있습니다.

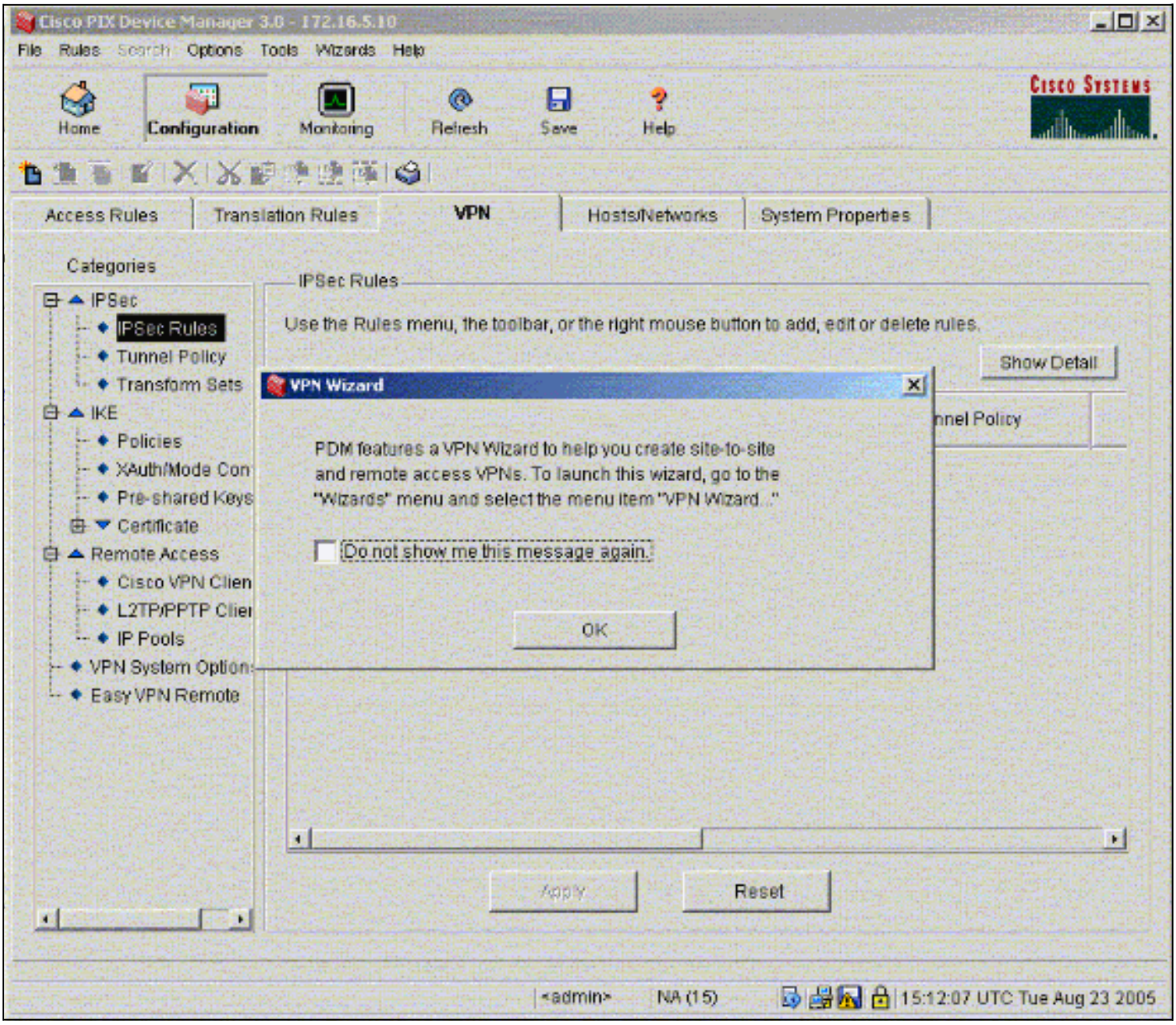
이 문서에서는 라우팅을 이미 구성한 것으로 가정합니다.

한 번에 하나의 링크만 작동하려면 R2는 192.168.1.0 네트워크뿐만 아니라 172.30.0.0 네트워크에도 더 나쁜 메트릭을 광고합니다. 예를 들어, 라우팅에 RIP를 사용하는 경우 R2는 다른 네트워크 광고와 별도로 이 컨피그레이션을 가집니다.

```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

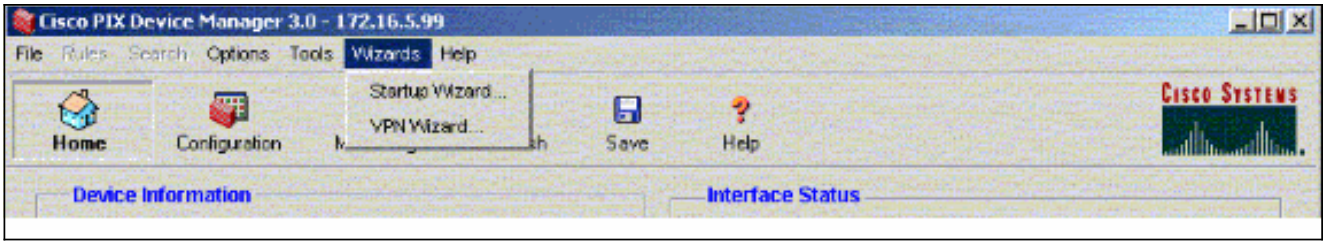
구성 절차

PDM을 **시작하려면 https://<Inside_IP_Address_on_PIX>를** 입력하고 처음으로 VPN 탭을 클릭하면 자동 VPN 마법사에 대한 정보가 표시됩니다.



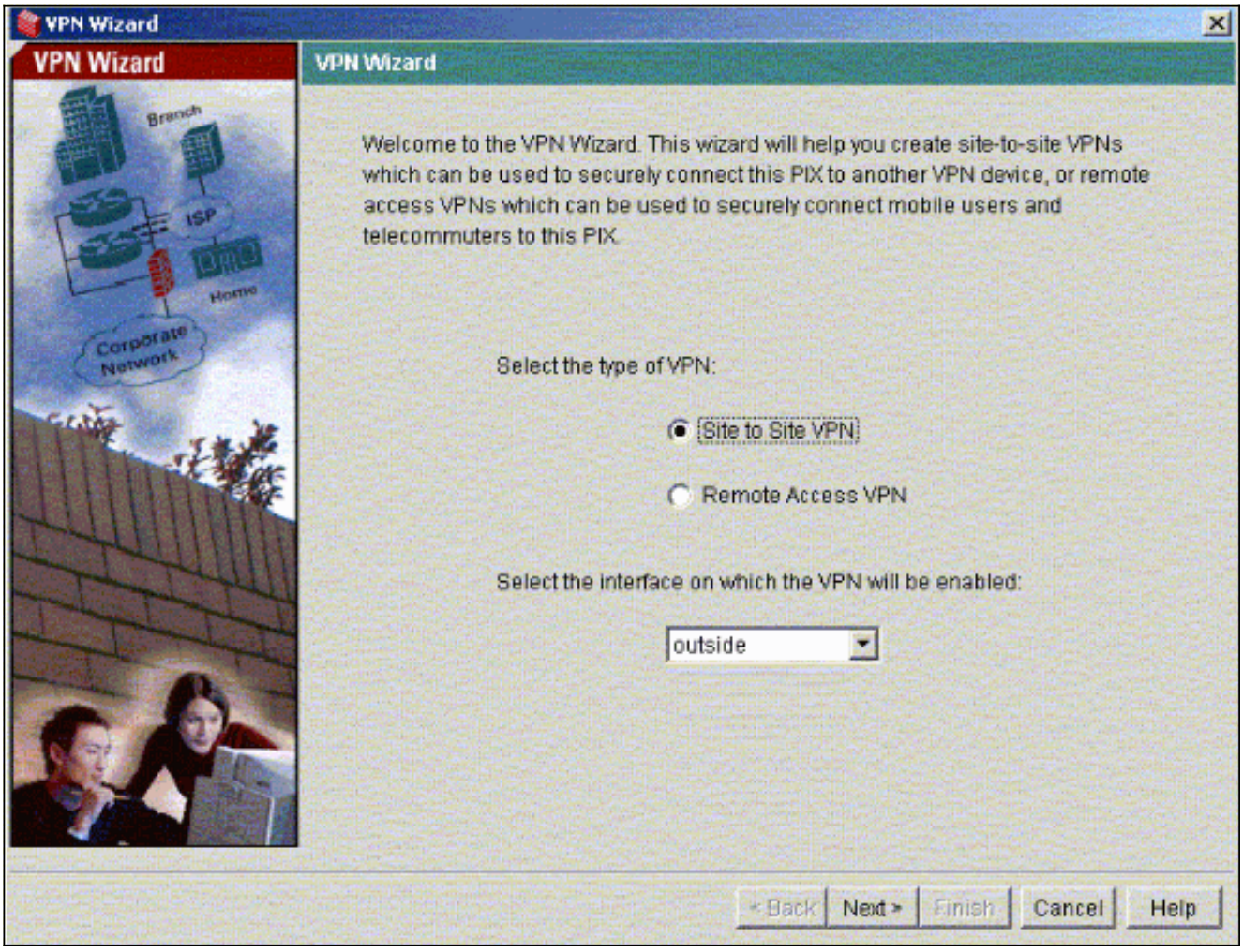
1. Wizards **> VPN Wizard를 선택합니다**

.



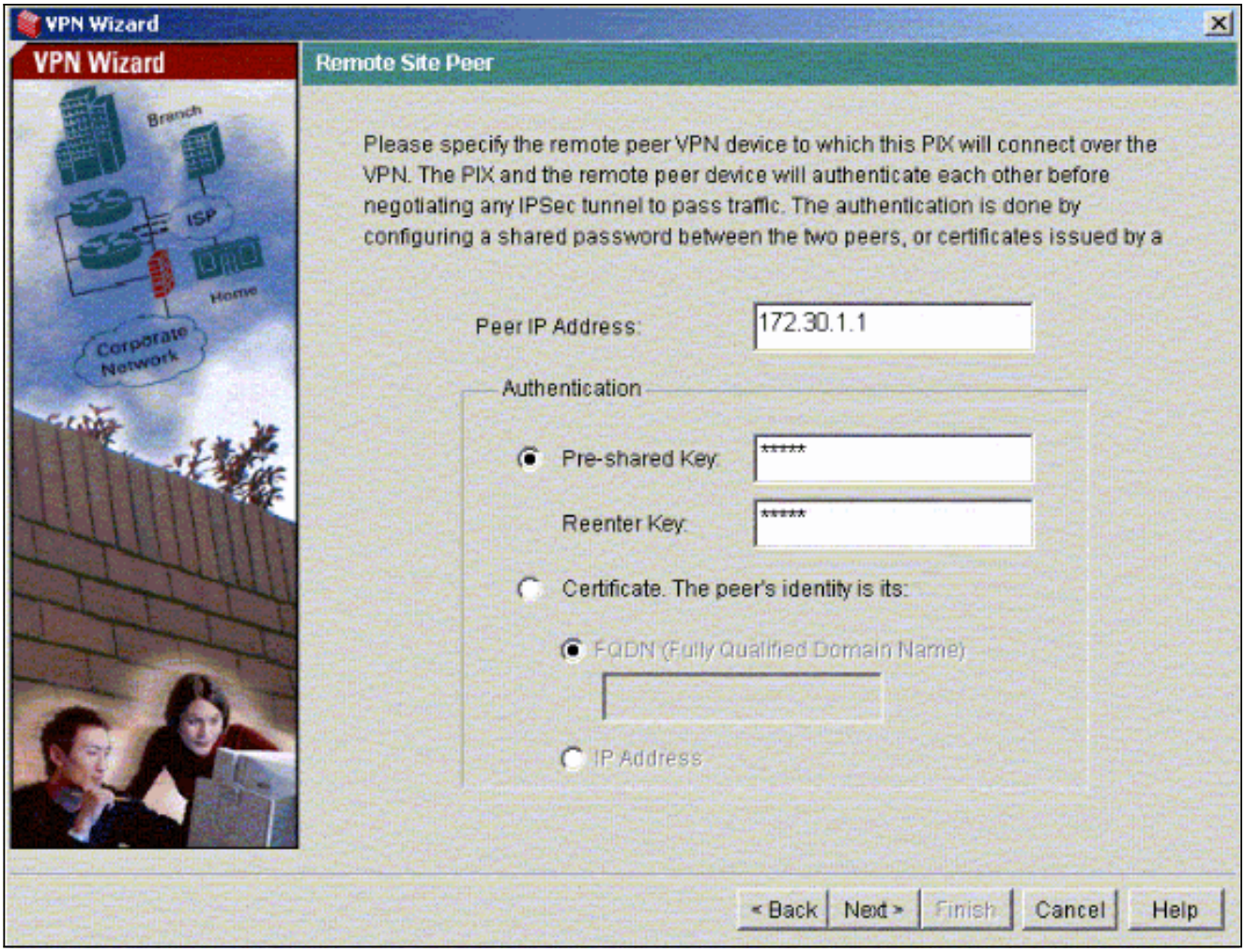
2. VPN 마법사가 시작되고 구성할 VPN 유형을 묻는 메시지를 표시합니다. Site-**to-Site VPN**을 선택하고 **외부** 인터페이스를 VPN이 활성화될 인터페이스로 선택하고 **Next**(다음)를 클릭합니다

.



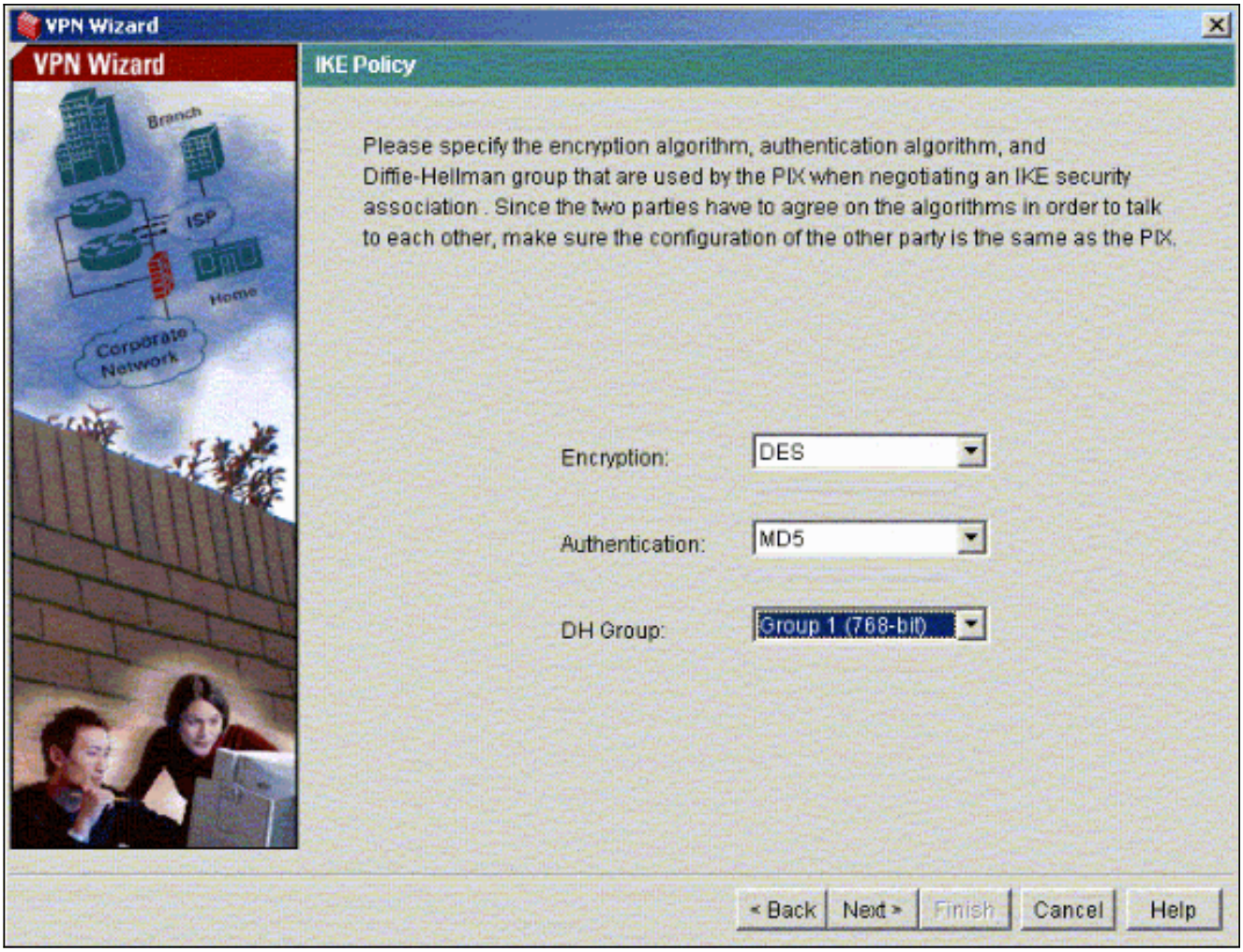
3. IPsec 터널이 종료되어야 하는 Peer IP 주소를 입력합니다. 이 예에서 터널은 PIX-02의 외부 인터페이스에서 끝납니다. **다음**을 클릭합니다

.



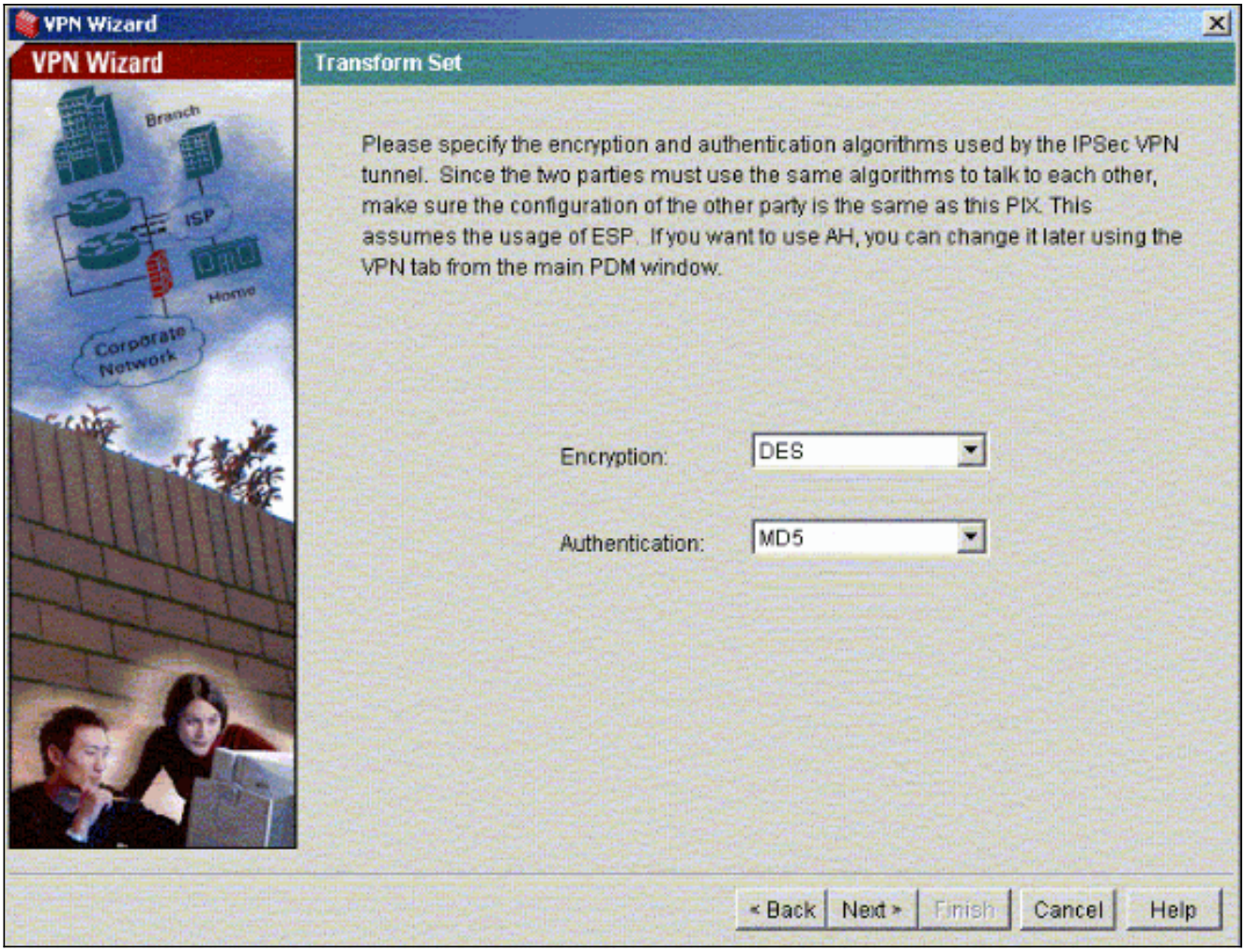
4. 사용할 IKE 정책 매개변수를 입력하고 Next(**다음**)를 클릭합니다

.



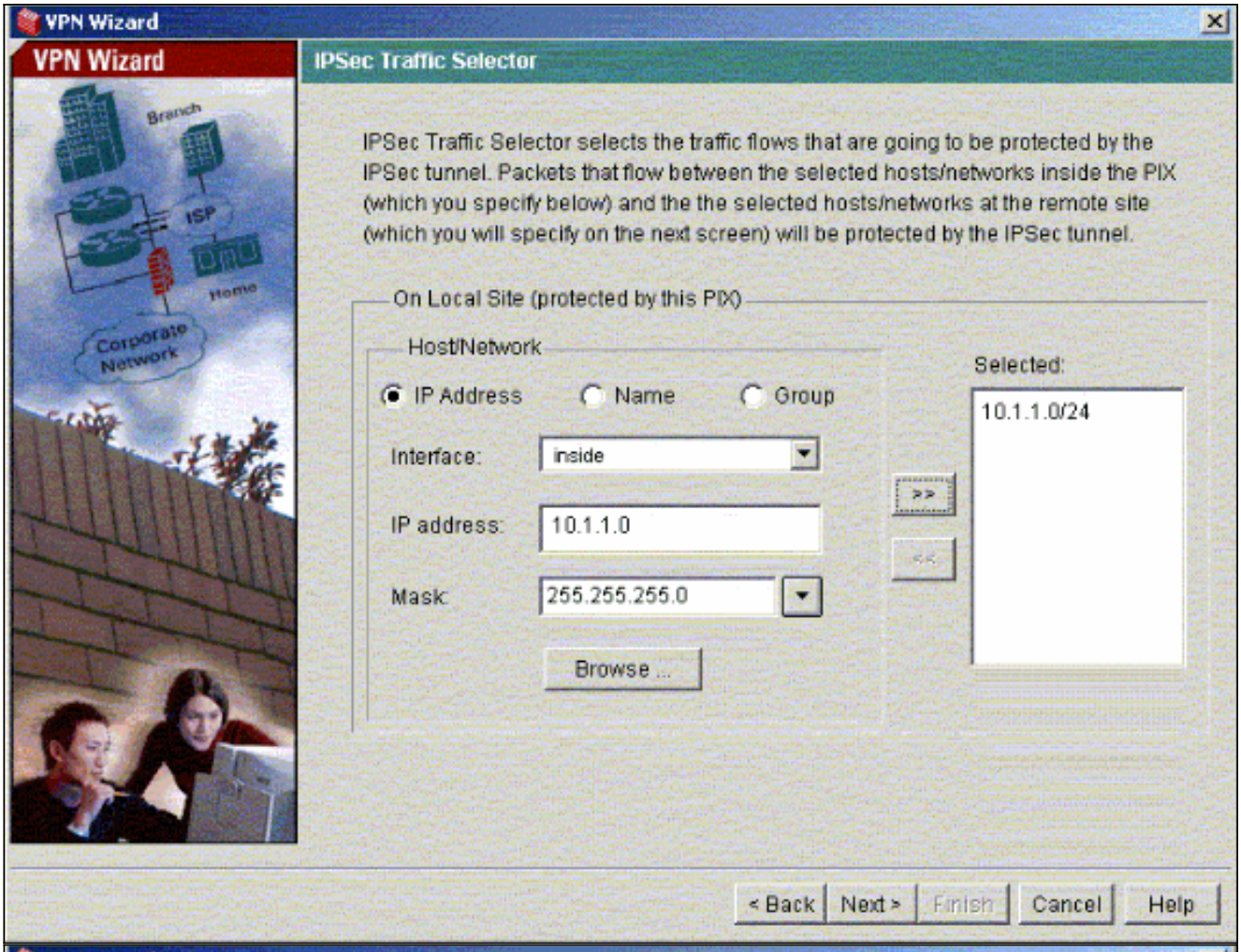
5. 변형 집합에 대한 암호화 및 인증 매개변수를 제공하고 **Next**를 클릭합니다

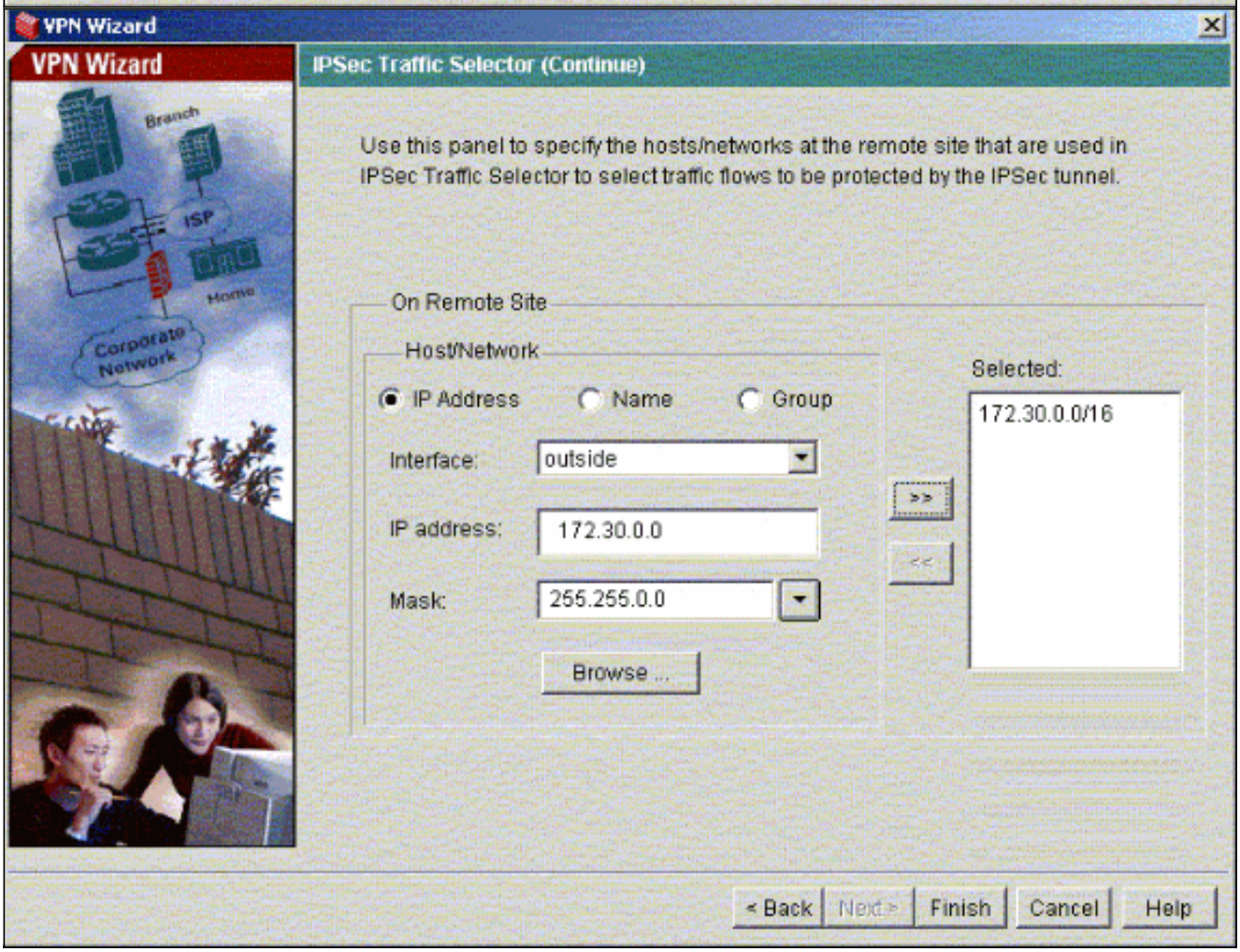
.



6. 보호해야 할 흥미로운 트래픽을 선택하려면 IPsec을 사용하여 보호해야 하는 로컬 네트워크 및 원격 네트워크를 선택합니다

.


VPN Wizard
VPN Wizard
IPSec Traffic Selector
Branch
ISP
Home
Corporate Network
IPSec Traffic Selector selects the traffic flows that are going to be protected by the IPSec tunnel. Packets that flow between the selected hosts/networks inside the PIX (which you specify below) and the the selected hosts/networks at the remote site (which you will specify on the next screen) will be protected by the IPSec tunnel.
On Local Site (protected by this PIX)
Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.1.1.0
Mask:
255.255.255.0
Browse ...
Selected:
10.1.1.0/24
>>
<<
< Back
Next >
Finish
Cancel
Help

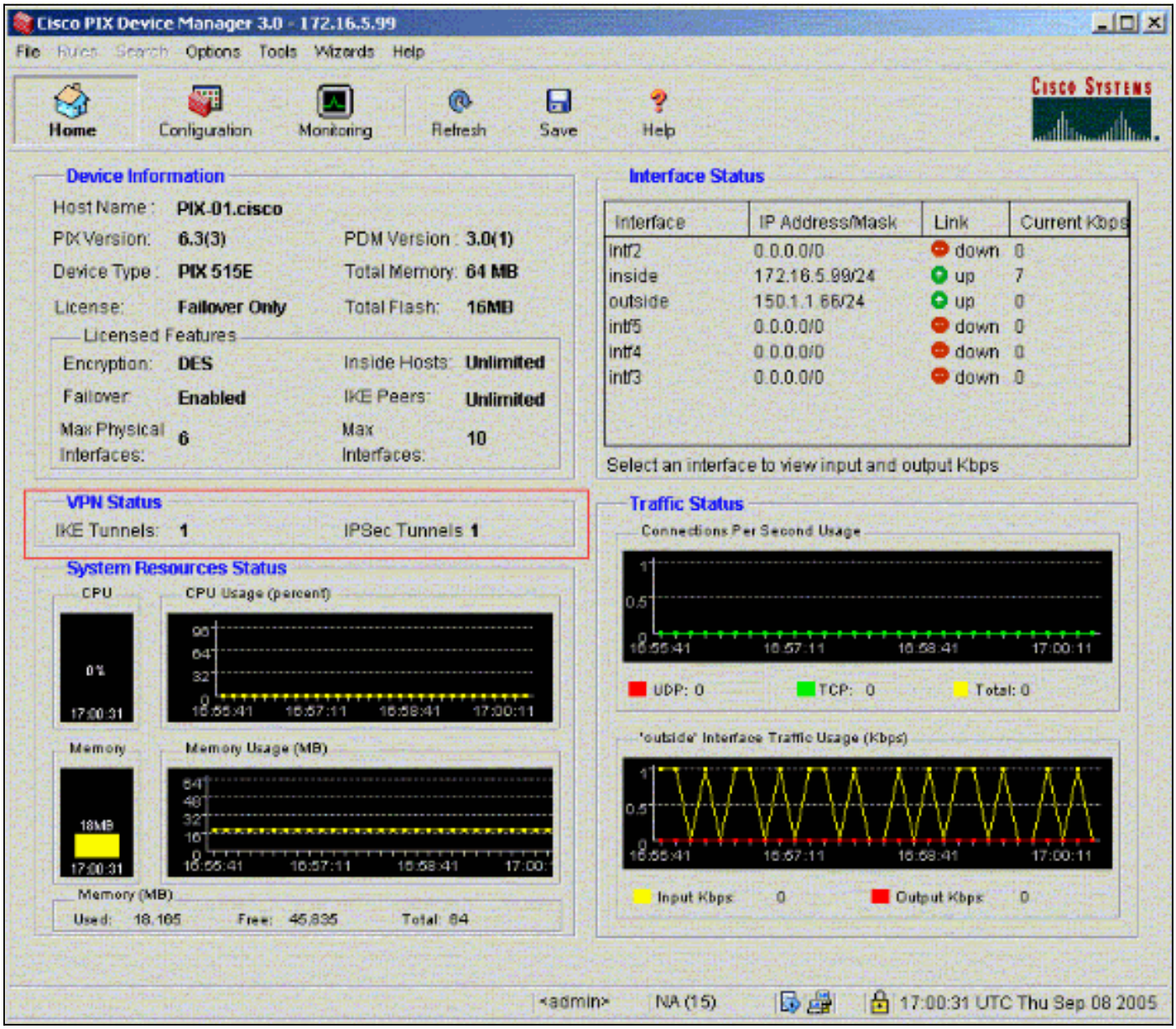

VPN Wizard
VPN Wizard
IPSec Traffic Selector (Continue)
Branch
ISP
Home
Corporate Network
Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.
On Remote Site
Host/Network
IP Address
Name
Group
Interface:
outside
IP address:
172.30.0.0
Mask:
255.255.0.0
Browse ...
Selected:
172.30.0.0/16
>>
<<
< Back
Next >
Finish
Cancel
Help

다음을 확인합니다.

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

이를 확인하려면 흥미로운 트래픽이 있을 때 R2를 통해 PIX-01과 PIX-02 사이에 터널이 설정된 R1 직렬 인터페이스를 종료합니다.

PDM의 **Home(홈)**에서 **VPN Status(VPN 상태)**(빨간색으로 강조 표시)를 확인하여 터널의 구조를 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.

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

PDM을 사용하는 PIX 방화벽 컨피그레이션에 대한 자세한 내용은 Cisco PIX Device Manager 3.0을 참조하십시오.

문제 해결

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

관련 정보

- IPsec을 사용하여 단순 PIX-to-PIX VPN 터널 구성
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems