PIX/ASA 7.x 이상:인터넷 컨피그레이션으로 여러 내부 네트워크 연결 예

목차

소개

이 문서에서는 CLI(Command Line Interface) 또는 ASDM(Adaptive Security Device Manager) 5.x 이상을 사용하여 인터넷에 연결하는 여러 내부 네트워크(또는 외부 네트워크)를 사용하는 PIX/ASA Security Appliance 버전 7.x 이상에 대한 샘플 컨피그레이션을 제공합니다.

PIX/ASA를 통한 연결 설정 및 문제 해결 방법에 대한 자세한 내용은 Cisco Security Appliance를 통한 연결 설정 및 문제 해결을 참조하십시오.

공통 PIX 명령에 대한 자세한 내용은 PIX에서 nat, global, static, waller 및 access-list Commands 및 Port Redirection(Forwarding) 사용을 참조하십시오.

참고: 다른 ASDM 버전의 일부 옵션은 ASDM 5.1의 옵션과 다를 수 있습니다. 자세한 내용은 ASDM 문서를 참조하십시오.

사전 요구 사항

요구 사항

PIX 방화벽 뒤에 둘 이상의 내부 네트워크를 추가할 경우 다음 사항에 유의하십시오.

- PIX는 보조 주소 지정을 지원하지 않습니다.
- 기존 네트워크와 새로 추가된 네트워크 간의 라우팅을 달성하려면 PIX 뒤에서 라우터를 사용해야 합니다.
- 모든 호스트의 기본 게이트웨이는 내부 라우터를 가리켜야 합니다.
- PIX를 가리키는 내부 라우터에 기본 경로를 추가합니다.
- 내부 라우터에서 ARP(Address Resolution Protocol) 캐시를 지웁니다.

ASDM에서 디바이스를 구성하도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용 을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX Security Appliance 515E(소프트웨어 버전 7.1 포함)
- ASDM 5.1
- Cisco IOS® Software 릴리스 12.3(7)T가 포함된 Cisco 라우터

참고: 이 문서는 PIX/ASA 소프트웨어 버전 8.x 및 Cisco IOS Software 릴리스 12.4로 수정되었습니다.

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.

관련 제품

이 컨피그레이션은 Cisco ASA Security Appliance 버전 7.x 이상에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

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

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

배경 정보

이 시나리오에서는 3개의 내부 네트워크(10.1.1.0/24, 10.2.1.0/24 및 10.3.1.0/24)이 PIX를 통해 인터넷(또는 외부 네트워크)에 연결됩니다.내부 네트워크는 PIX의 내부 인터페이스에 연결됩니다.인터넷 연결은 PIX의 외부 인터페이스에 연결된 라우터를 통해 이루어집니다.PIX에는 IP 주소 172.16.1.1/24이 있습니다.

고정 경로는 내부 네트워크에서 인터넷으로 패킷을 라우팅하는 데 사용되며 그 반대의 경우도 마찬가지입니다.고정 경로를 사용하는 대신 RIP(Routing Information Protocol) 또는 OSPF(Open Shortest Path First)와 같은 동적 라우팅 프로토콜을 사용할 수도 있습니다.

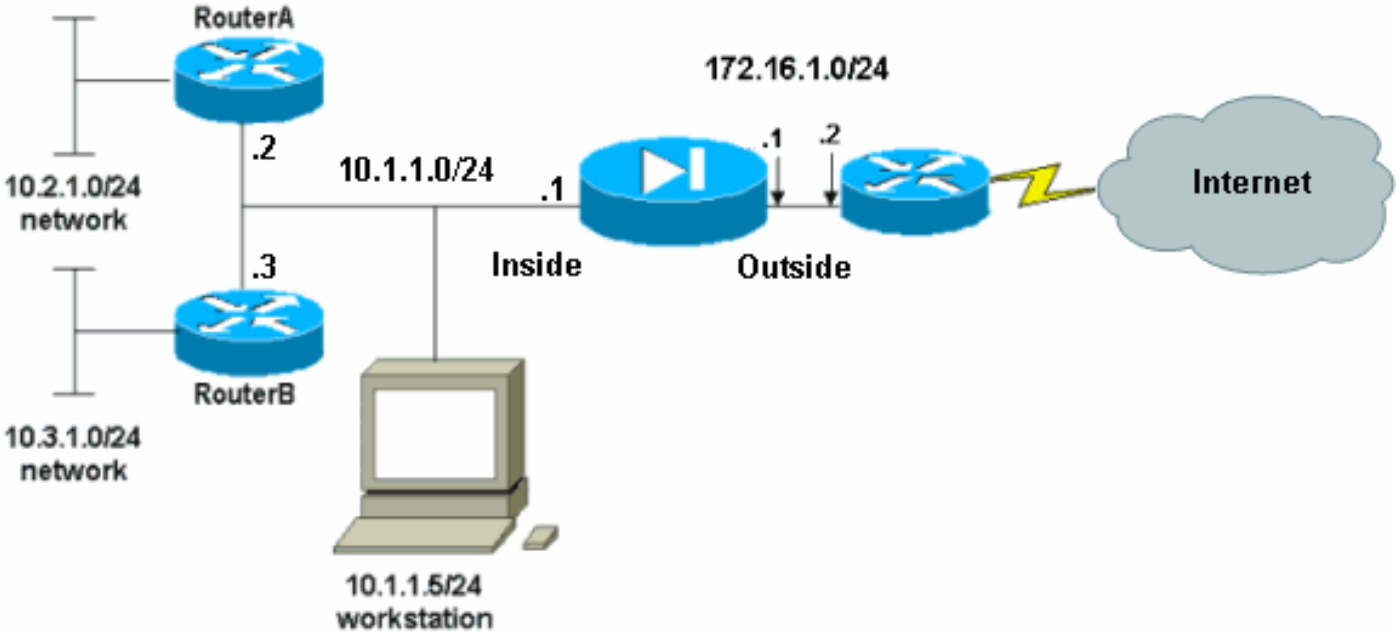
내부 호스트는 동적 NAT(IP 주소 풀 - 172.16.1.5~172.16.1.10)을 사용하여 PIX의 내부 네트워크를 변환하여 인터넷과 통신합니다. IP 주소 풀이 모두 사용되면 PIX는 내부 호스트를 PAT(IP 주소 172.16.1.4 사용)하여 인터넷에 연결합니다.

NAT/PAT에 대한 자세한 내용은 PIX/ASA 7.x NAT 및 PAT 문을 참조하십시오.

참고: 고정 NAT가 외부 IP(global_IP) 주소를 변환하기 위해 사용하는 경우 변환이 발생할 수 있습니다.따라서 고정 변환에서 IP 주소 대신 키워드 인터페이스를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



10.1.1.0 네트워크에 있는 호스트의 기본 게이트웨이는 RouterA를 가리킵니다.RouterB에서 RouterA를 가리키는 기본 경로가 추가됩니다.RouterA에는 PIX 내부 인터페이스를 가리키는 기본 경로가 있습니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- RouterA 컨피그레이션
- RouterB 컨피그레이션
- PIX Security Appliance 7.1 컨피그레이션ASDM을 사용한 PIX 컨피그레이션PIX Security Appliance CLI 컨피그레이션

RouterA 컨피그레이션
RouterA#**show running-config** Building configuration...

```
Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
 ip address 10.2.1.1 255.255.255.0
 half-duplex
!

interface Ethernet2/1
 ip address 10.1.1.2 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#
```

RouterB 컨피그레이션

```
RouterB#show running-config
Building configuration...
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 speed auto
!

interface Ethernet1/0
 ip address 10.3.1.1 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
```

```
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

PIX Security Appliance 컨피그레이션에 ASDM을 사용하되 디바이스를 부트스트랩하지 않은 경우 다음 단계를 완료합니다.

1. 콘솔을 PIX로 연결합니다.
2. 지워진 컨피그레이션에서 대화형 프롬프트를 사용하여 워크스테이션 10.1.1.5에서 PIX를 관리할 ASDM을 활성화합니다.

PIX Security Appliance 7.1 컨피그레이션

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
commands
         INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
         INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
```

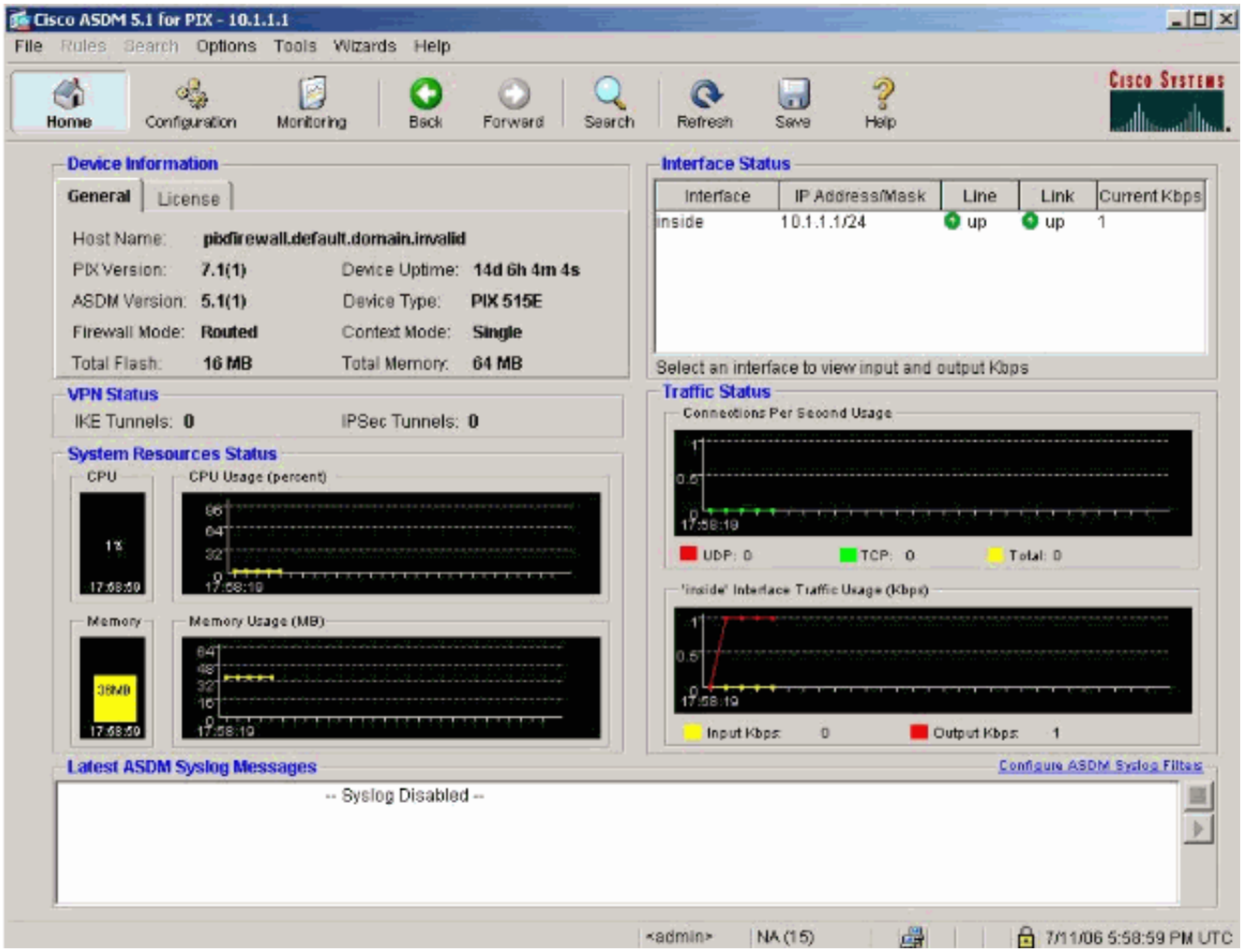
```
        INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
        INFO: converting 'fixup protocol rsh 514' to
MPF commands
        INFO: converting 'fixup protocol rtsp 554' to
MPF commands
        INFO: converting 'fixup protocol sip 5060' to
MPF commands
        INFO: converting 'fixup protocol skinny 2000'
to MPF commands
        INFO: converting 'fixup protocol smtp 25' to
MPF commands
        INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
        INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
        INFO: converting 'fixup protocol tftp 69' to
MPF commands
        INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
        INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
        OZ-PIX>
```

ASDM을 사용한 PIX 컨피그레이션

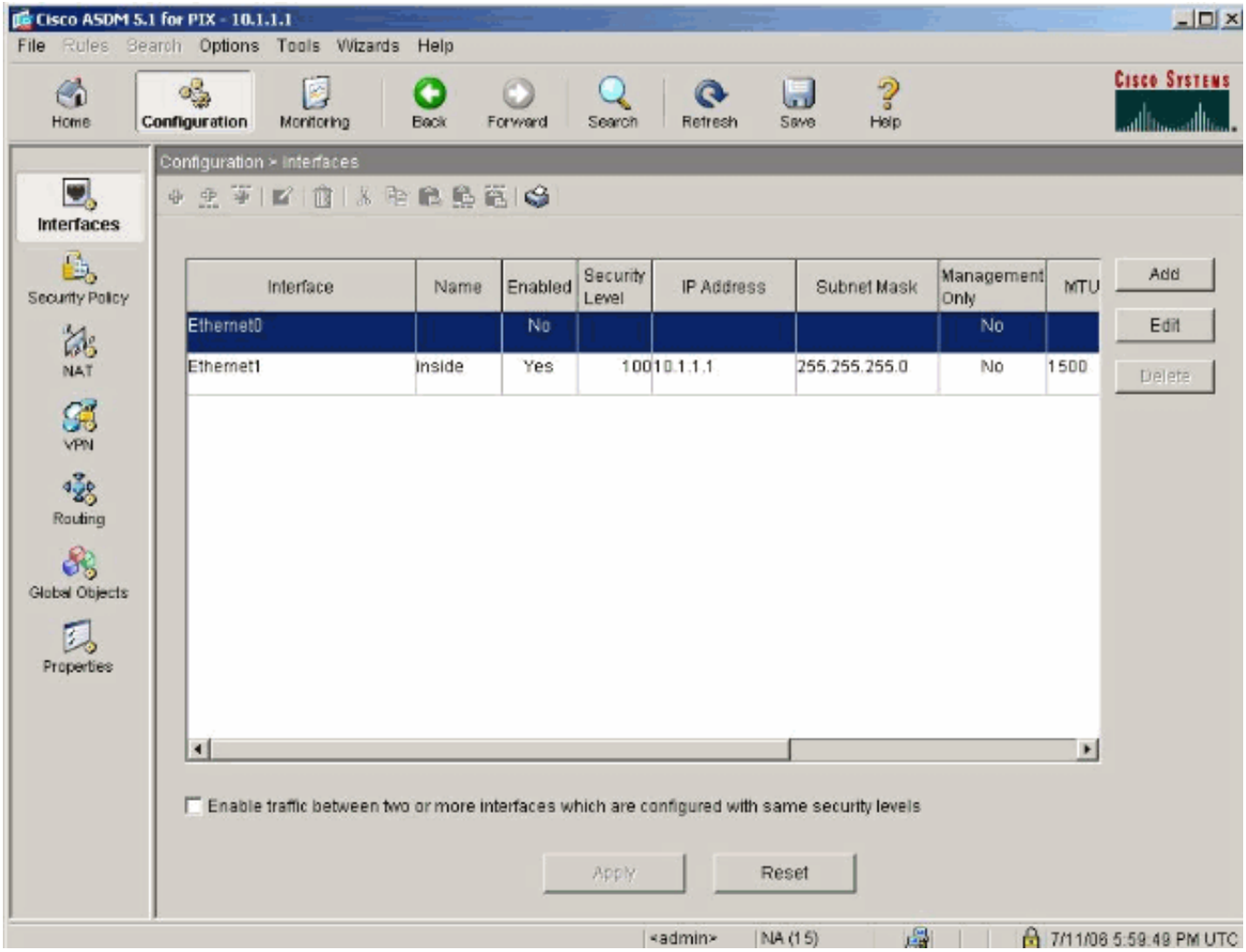
ASDM GUI를 통해 구성하려면 다음 단계를 완료합니다.

1. 워크스테이션 10.1.1.5에서 ADSM을 사용할 웹 브라우저를 엽니다(이 예에서는 https://10.1.1.1).
2. 인증서 프롬프트**에서 예**를 클릭합니다.
3. 이전에 구성한 대로 enable 비밀번호로 로그인합니다.
4. PC에서 ASDM을 처음 실행하는 경우 ASDM Launcher 또는 ASDM을 Java 앱으로 사용하라는 메시지가 표시됩니다.이 예에서는 ASDM Launcher가 선택되어 설치됩니다.
5. ASDM Home(ASDM 홈) 창으로 이동하여 Configuration(컨피그레이션)을 **클릭합니다**.



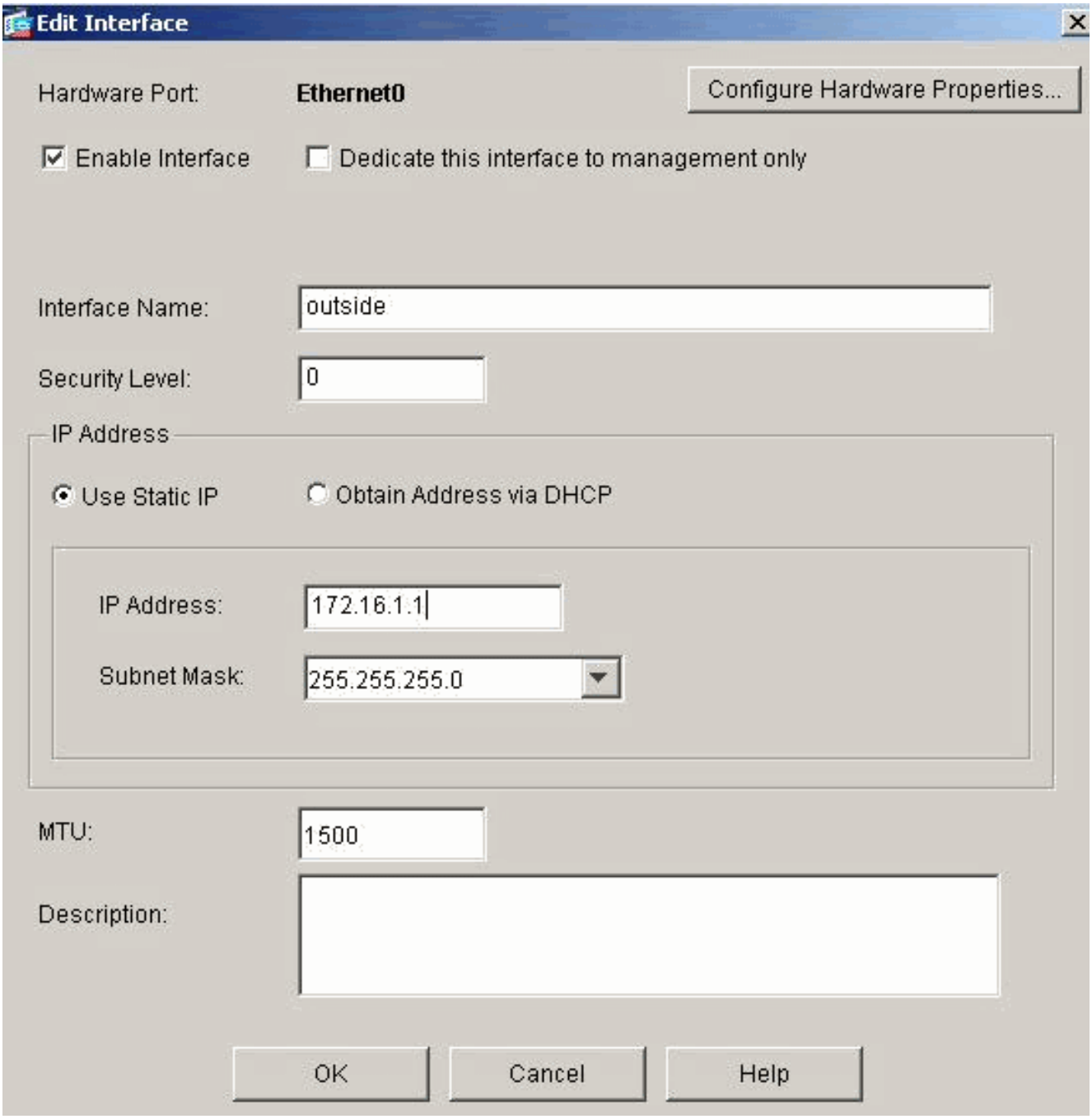
6. 외부 인터페이스를 구성하려면 **Interface > Edit**를 선택합니다

.



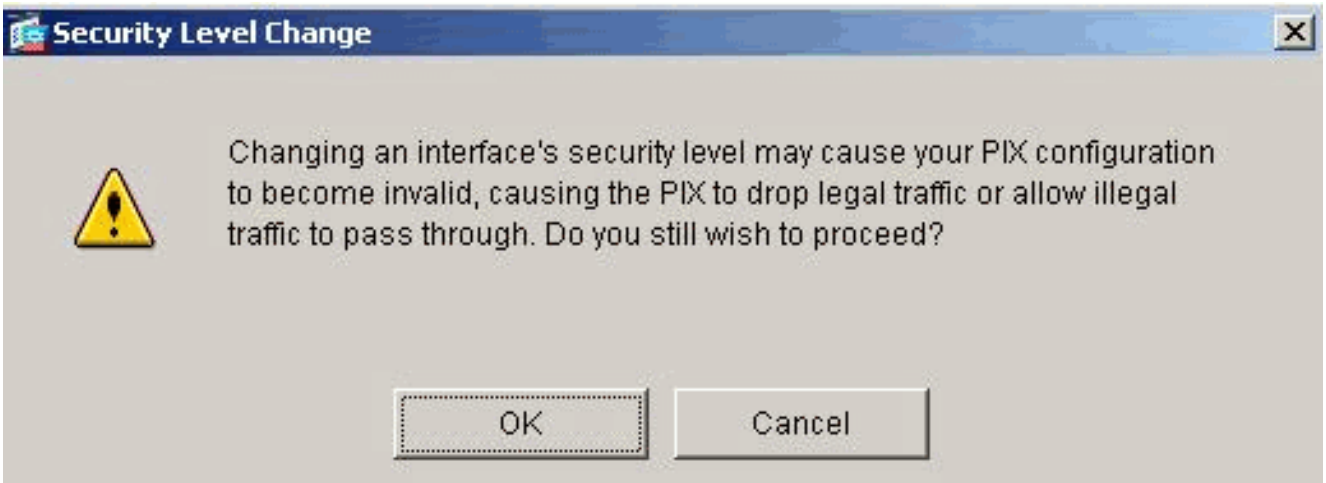
7. 인터페이스 세부사항을 입력하고 완료되면 **OK**(확인)를 클릭합니다

.



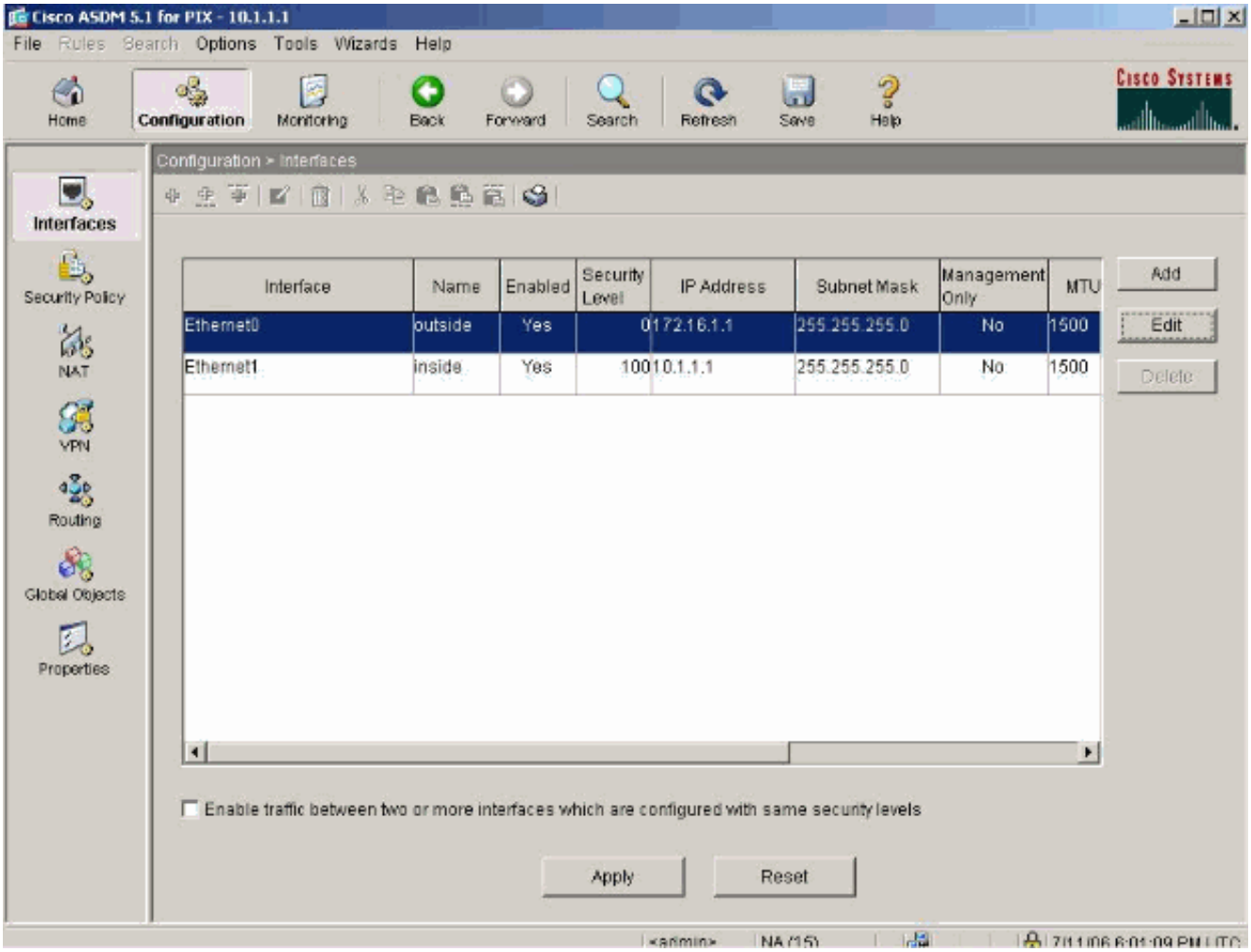
8. Security Level Change 대화 상자에서 OK를 클릭합니다

.



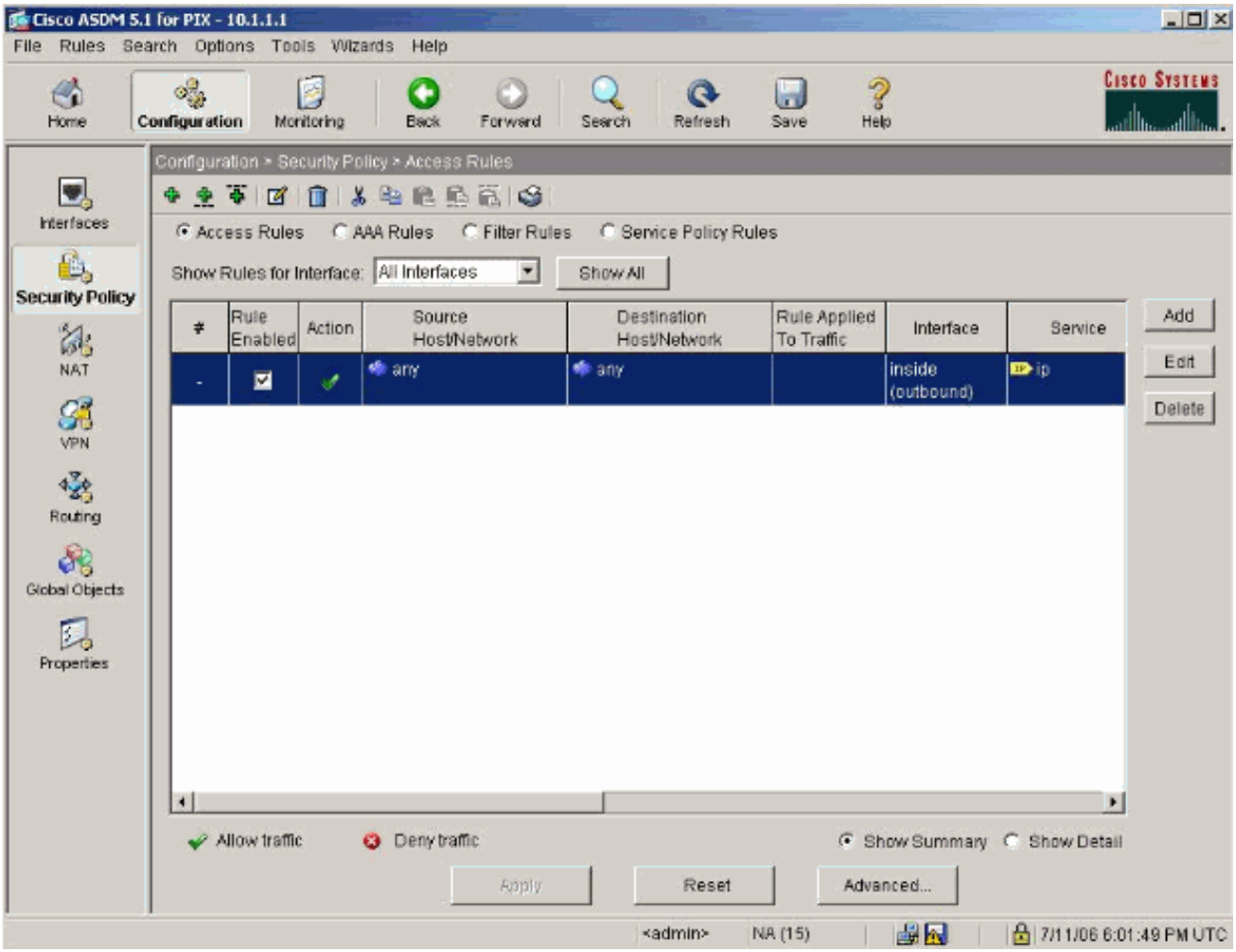
9. Apply(**적용**)를 클릭하여 인터페이스 컨피그레이션을 적용합니다.컨피그레이션이 PIX에 푸시됩니다

.



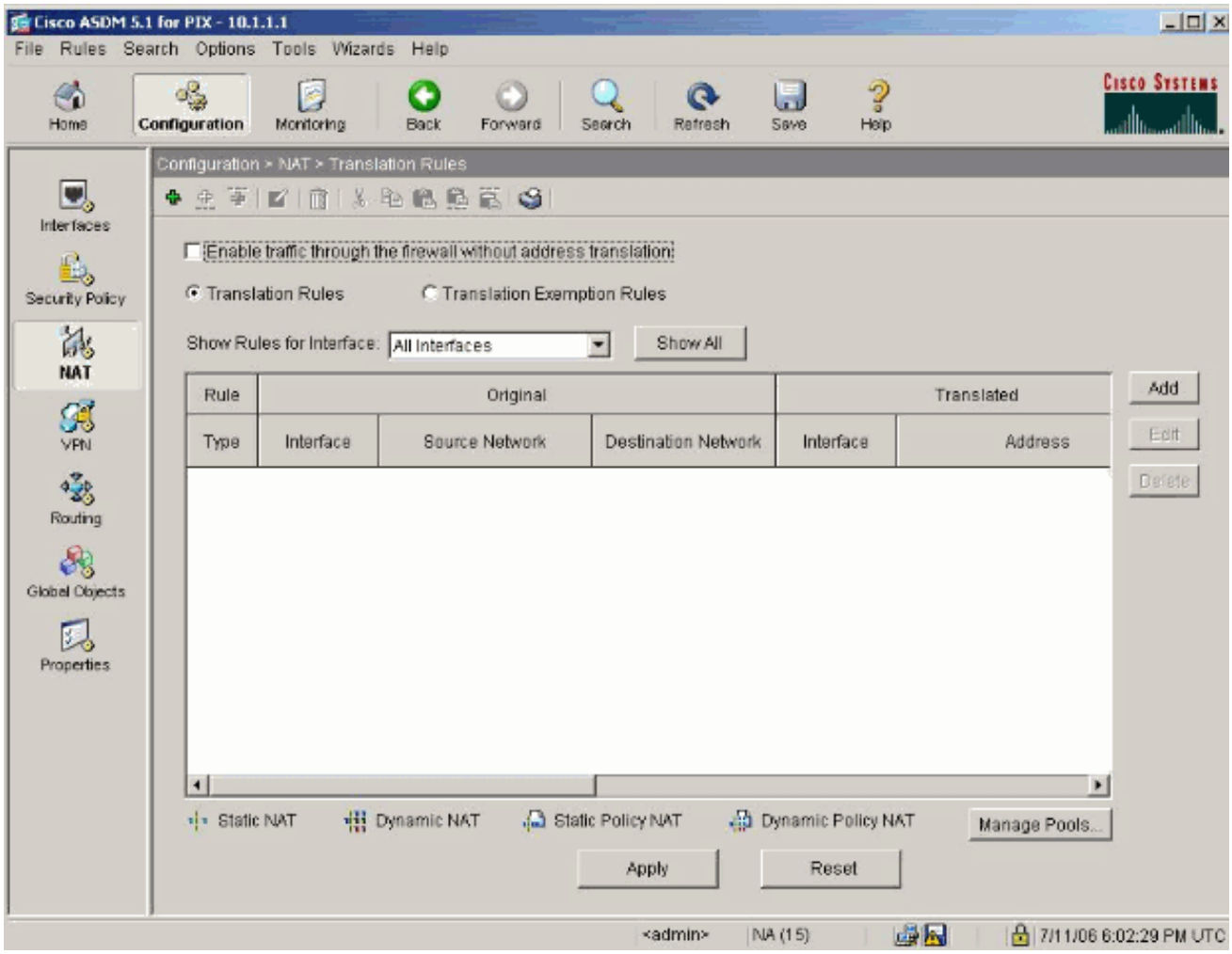
10. 사용된 보안 정책 규칙을 검토하려면 Features(기능) 탭에서 Security Policy(보안 정책)를 선택합니다.이 예에서는 기본 내부 규칙이 사용됩니다

.

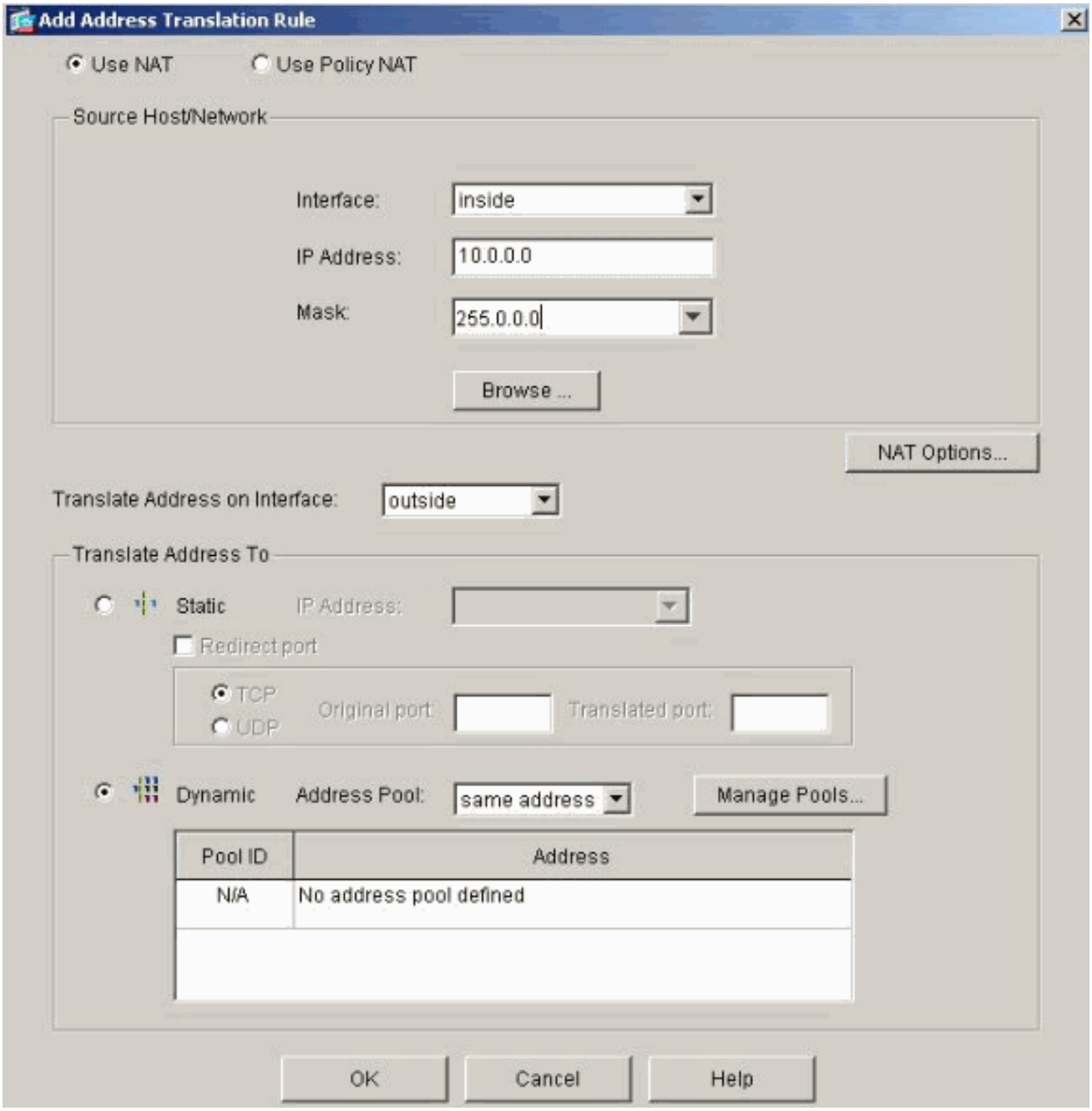


11. 이 예에서는 NAT가 사용됩니다.Enable traffic through the firewall without address translation(**주소 변환 없이 방화벽을 통과하는 트래픽 활성화**) 확인란을 선택 취소하고 **Add(추가)를** 클릭하여 NAT 규칙을 구성합니다

.

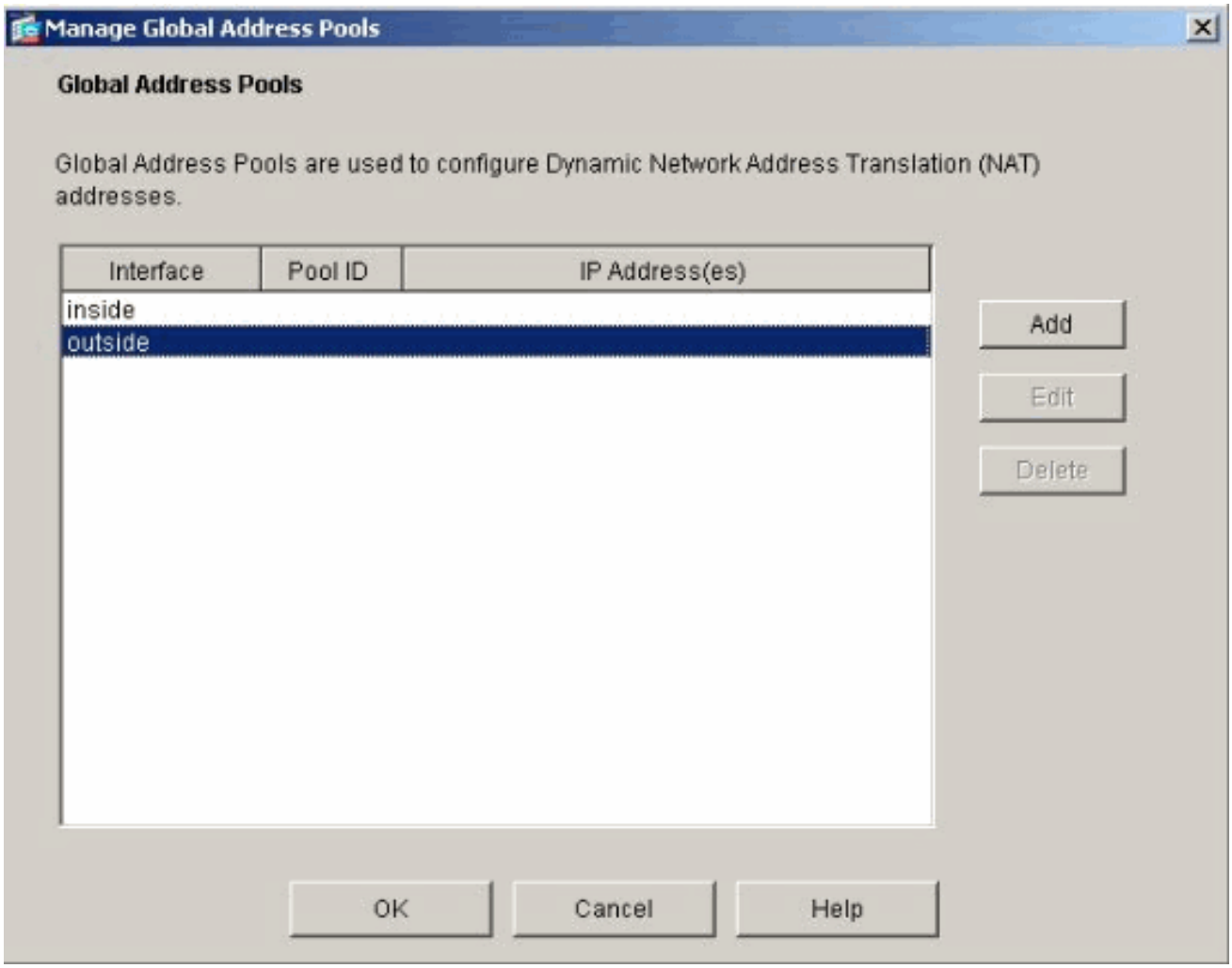


12. 소스 네트워크를 구성합니다.이 예에서는 IP 주소에 10.0.0.0이 사용되고 마스크에 255.0.0.0이 사용됩니다.NAT 풀 주소를 정의하려면 Manage Pools(풀 관리)를 클릭합니다 .



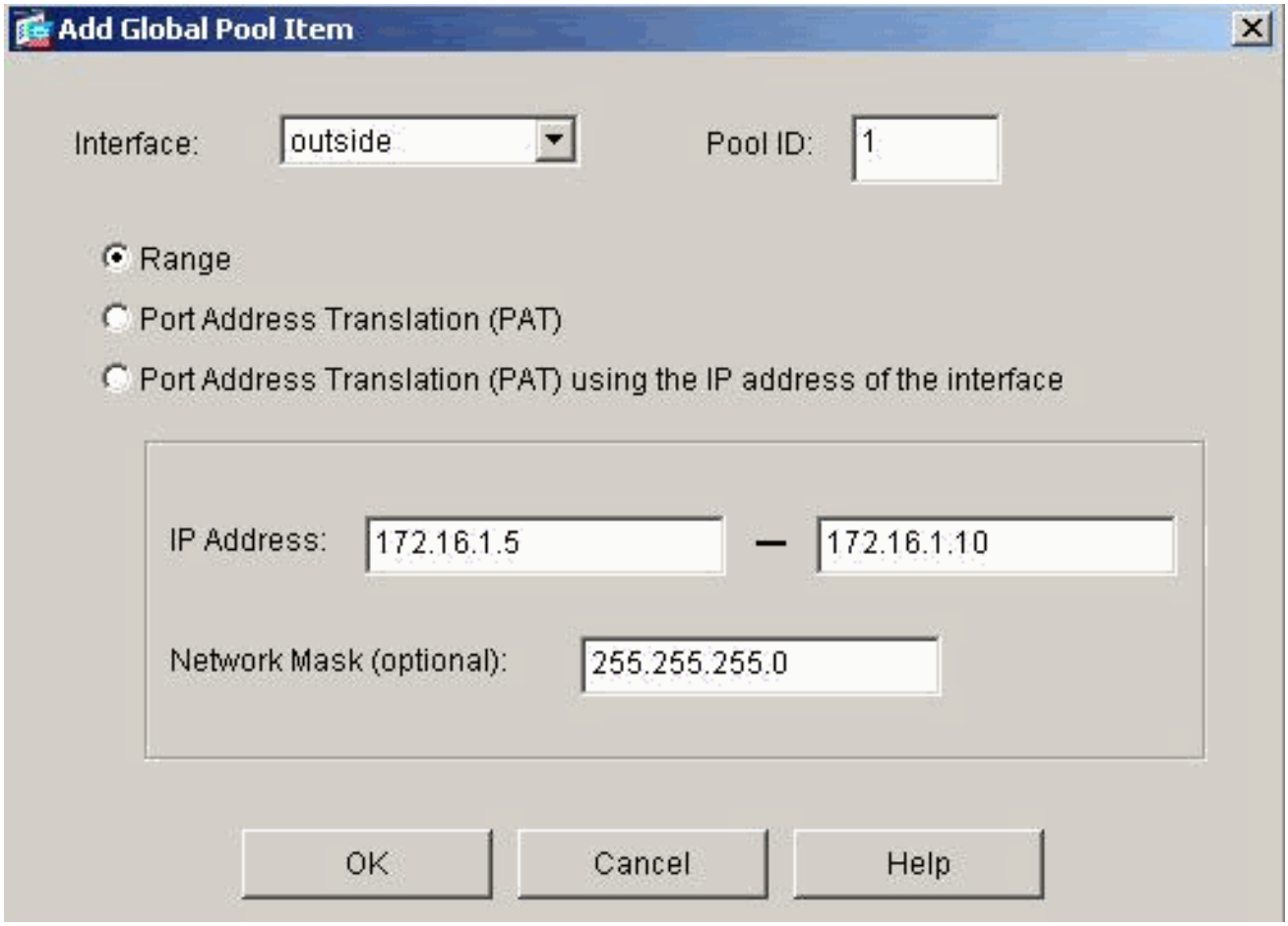
13. 외부 인터페이스를 선택하고 Add를 **클릭합니다**

.

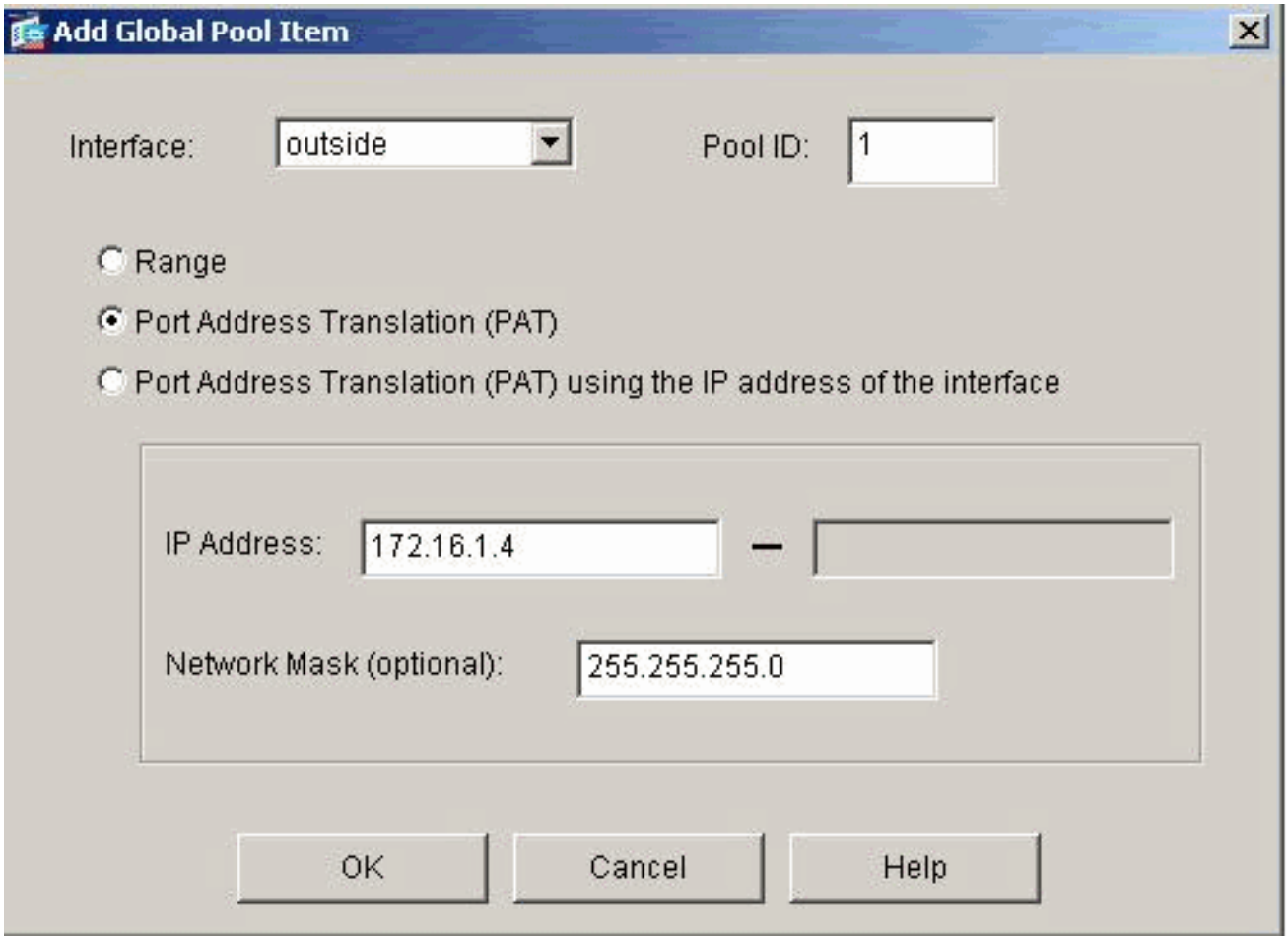


14. 이 예에서는 범위 및 PAT 주소 풀이 구성됩니다.범위 NAT 풀 주소를 구성하고 **OK**를 클릭합니다

.

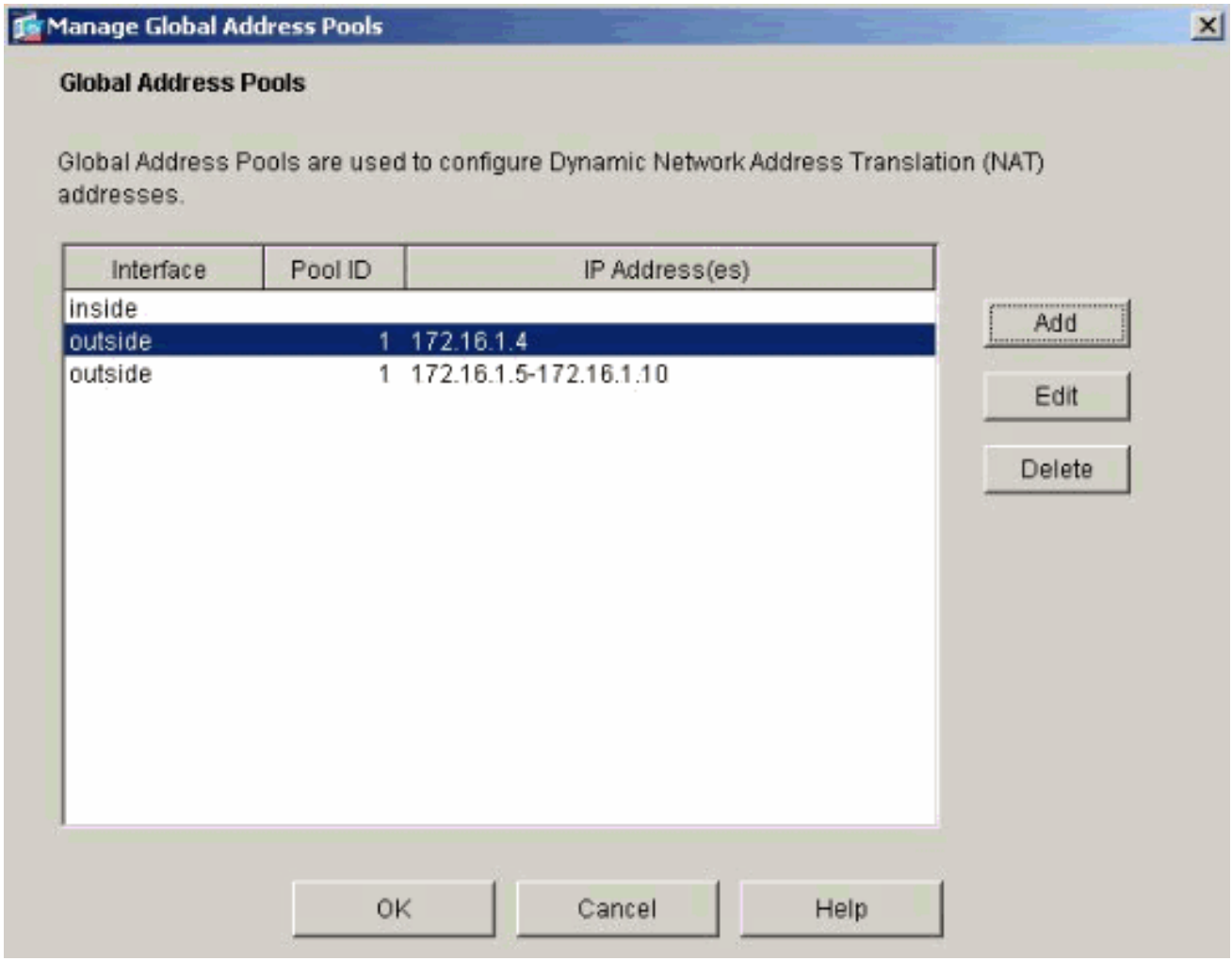


15. PAT 주소를 구성하려면 13단계에서 외부 인터페이스를 선택합니다.OK(확인)를 **클릭합니다**
.



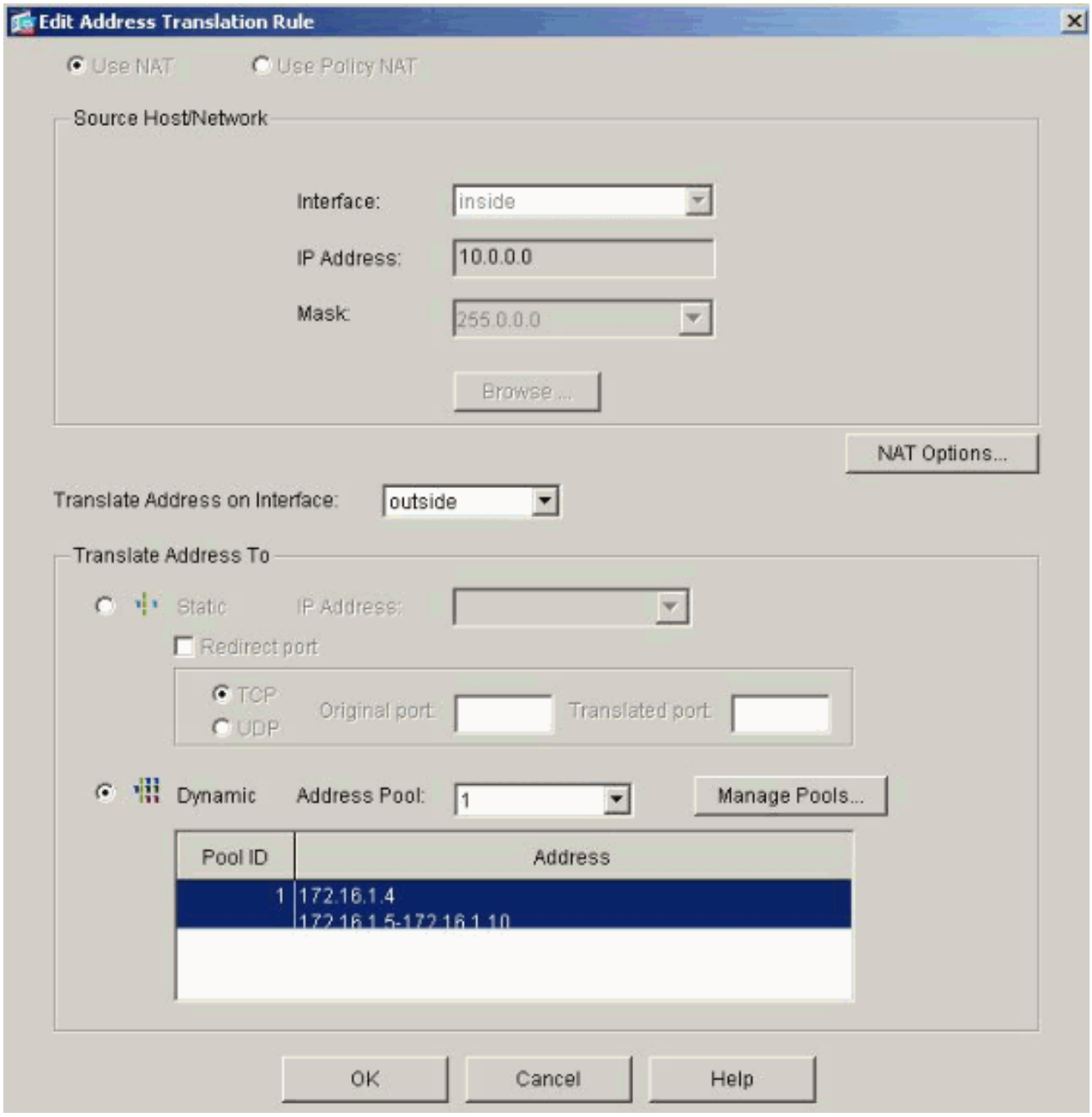
계속하려면 **OK**(확인)를 클릭합니다

.



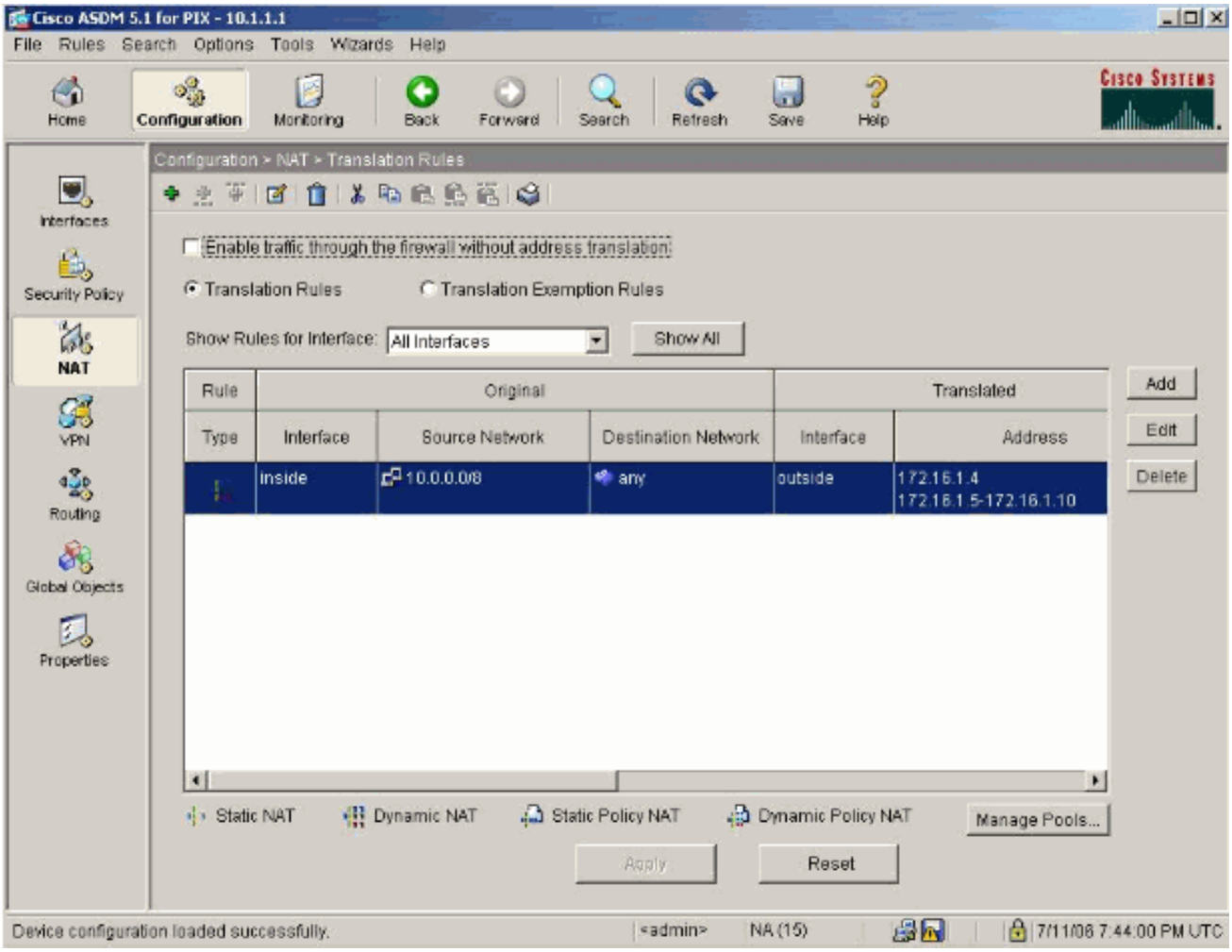
16. Edit Address Translation Rule(주소 변환 규칙 수정) 창에서 구성된 소스 네트워크에서 사용할 풀 ID를 선택합니다.**확인**을 **클릭합니다**

.



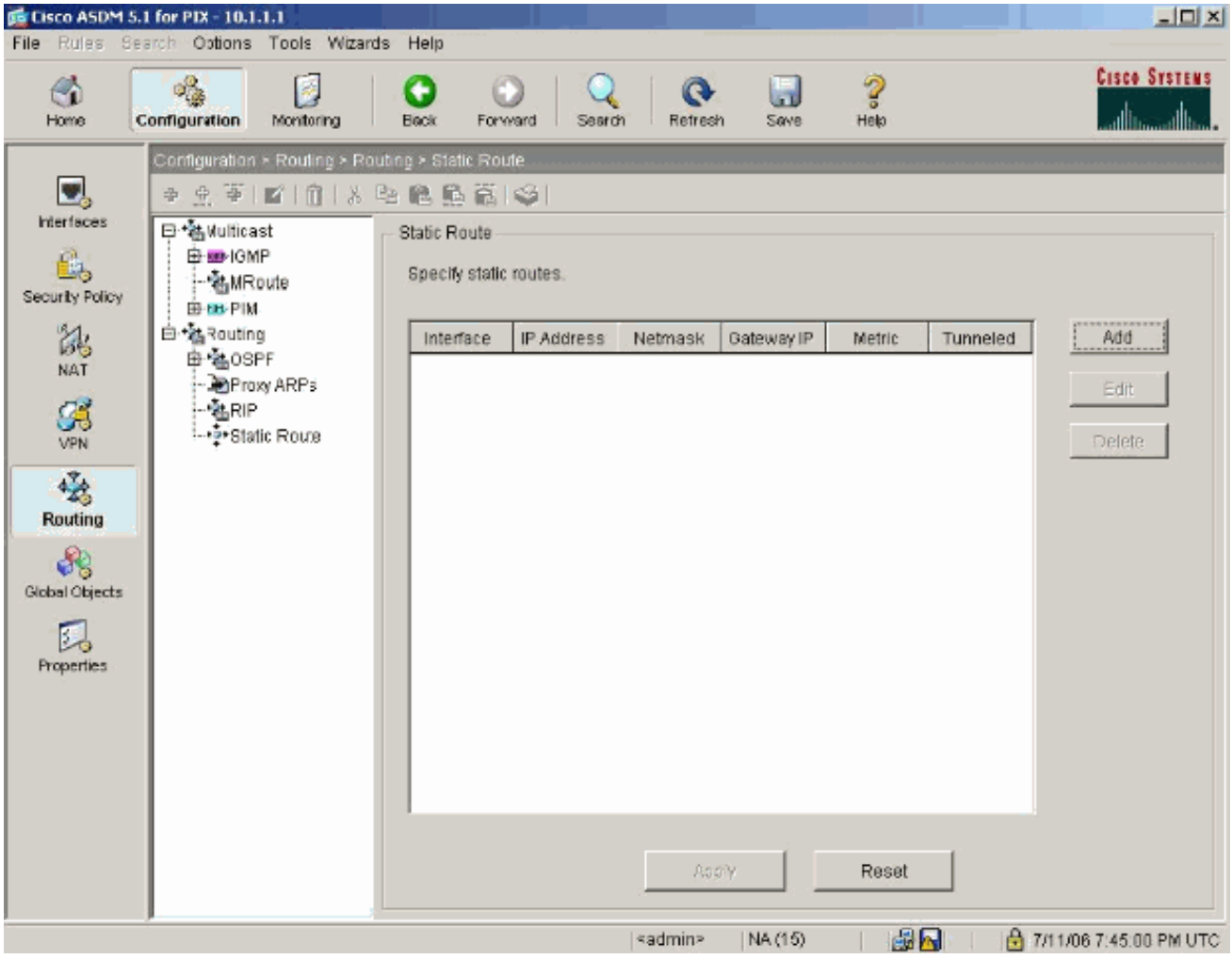
17. Apply(**적용**)를 클릭하여 구성된 NAT 규칙을 PIX로 푸시합니다

.

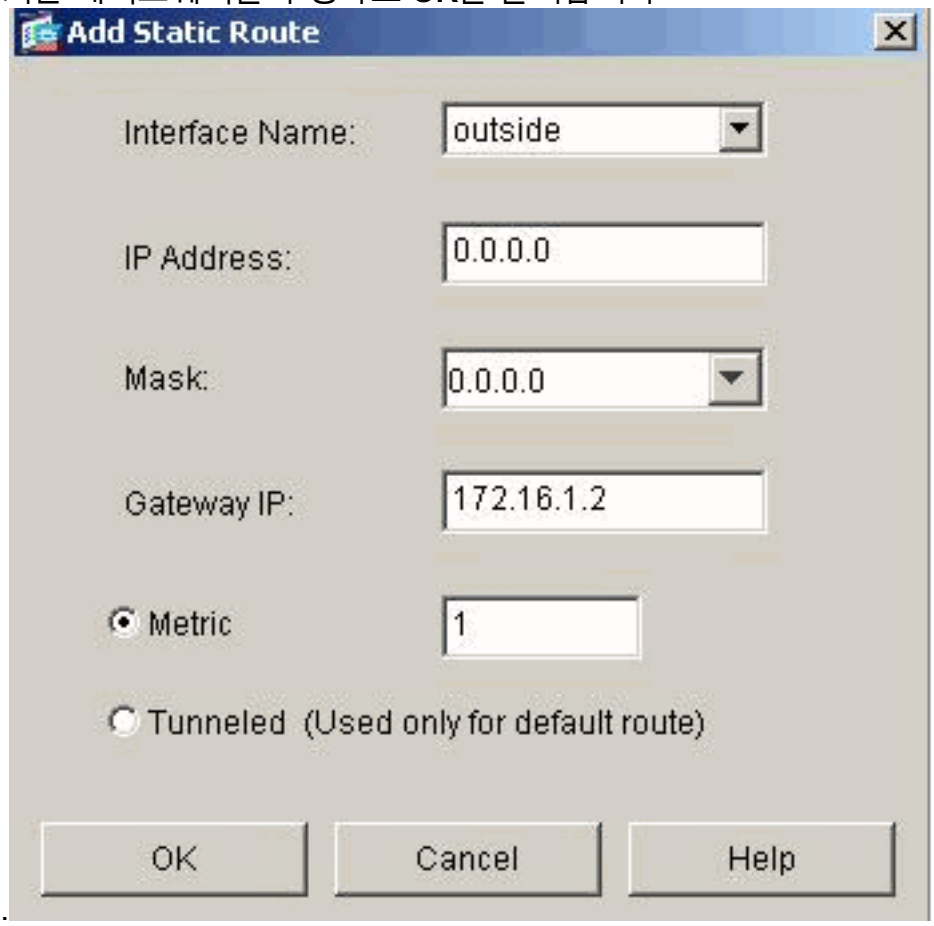


18. 이 예에서는 고정 경로가 사용됩니다.Routing(**라우팅**)을 클릭하고 **Static Route(고정 경로)**를 선택하고 Add(추가)를 **클릭합니다**

.

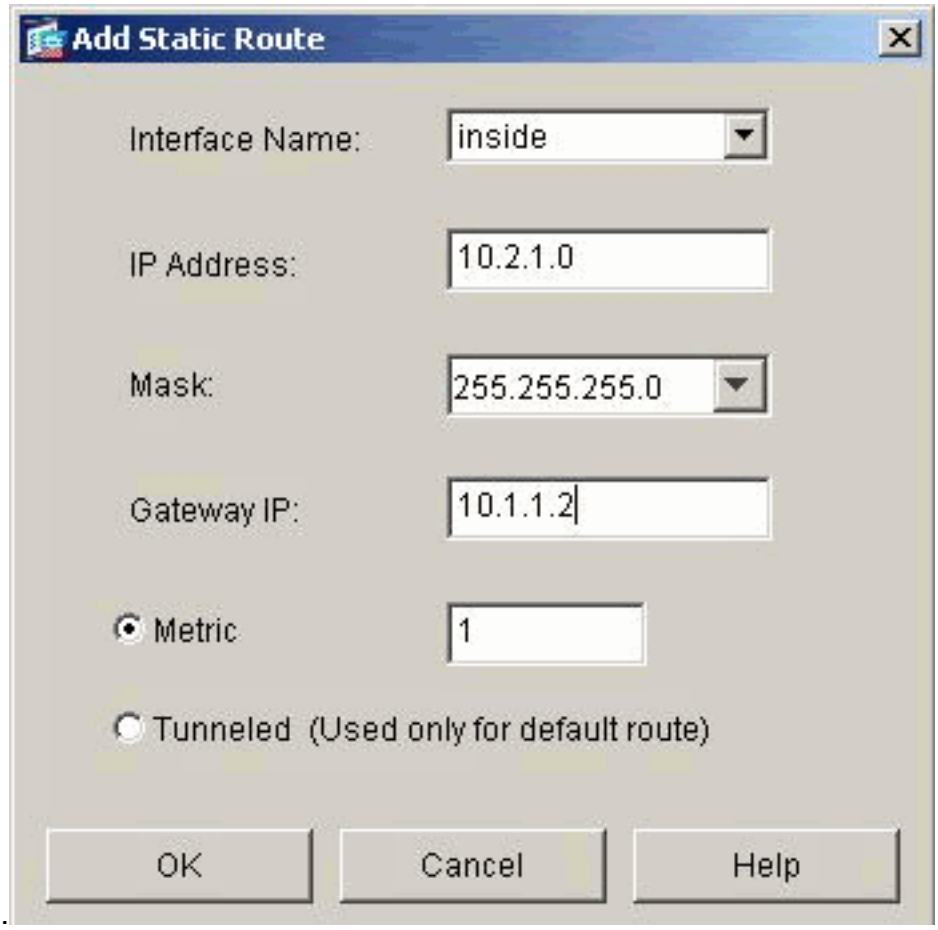


19. 기본 게이트웨이를 구성하고 **OK**를 클릭합니다

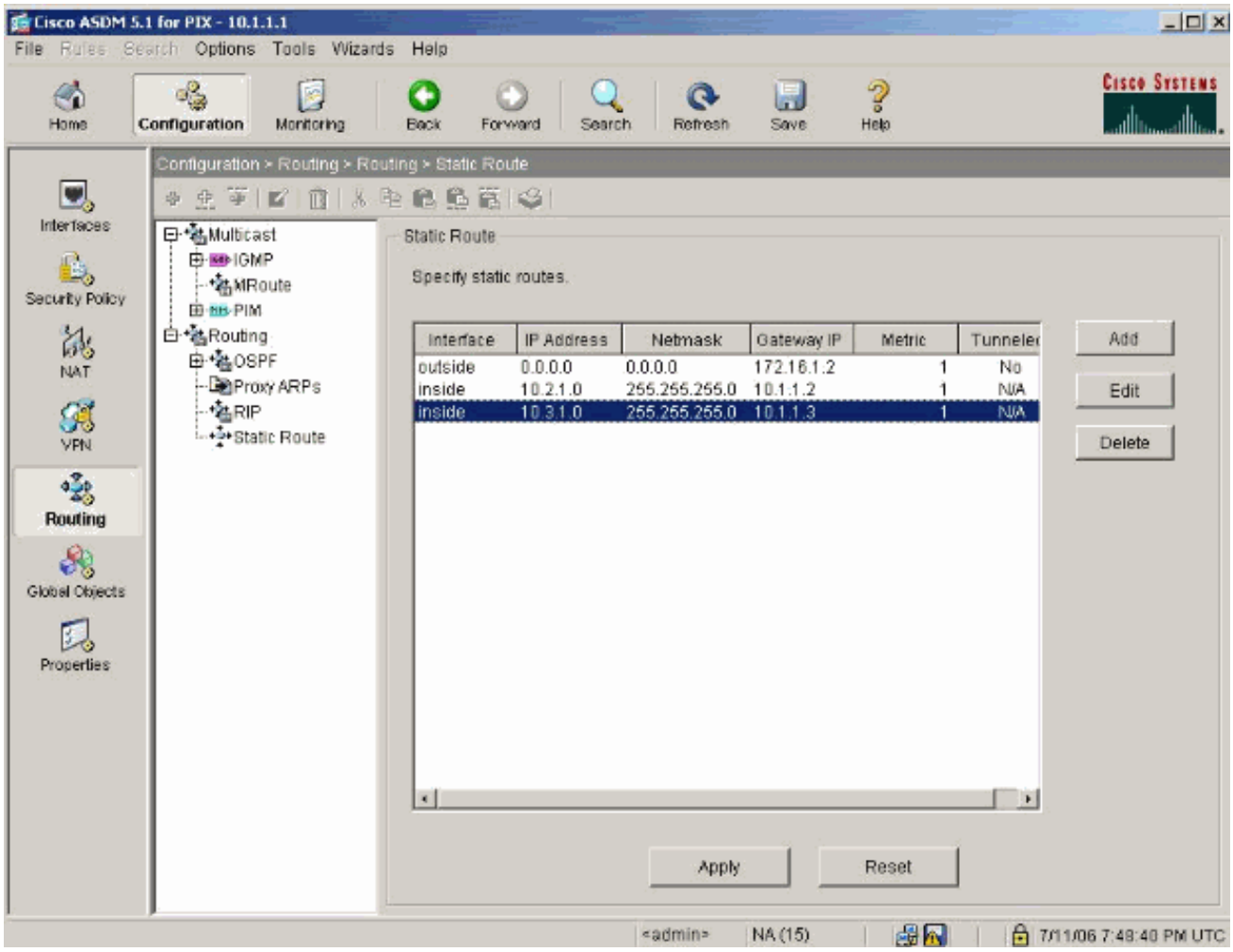


.

20. Add(**추가**)를 클릭하고 내부 네트워크에 경로를 추가합니다



21. 올바른 경로가 구성되었는지 확인하고 Apply를 **클릭합니다**
.



CLI를 사용한 PIX 컨피그레이션

이제 ASDM GUI를 통한 구성이 완료되었습니다.

CLI를 통해 이 컨피그레이션을 볼 수 있습니다.

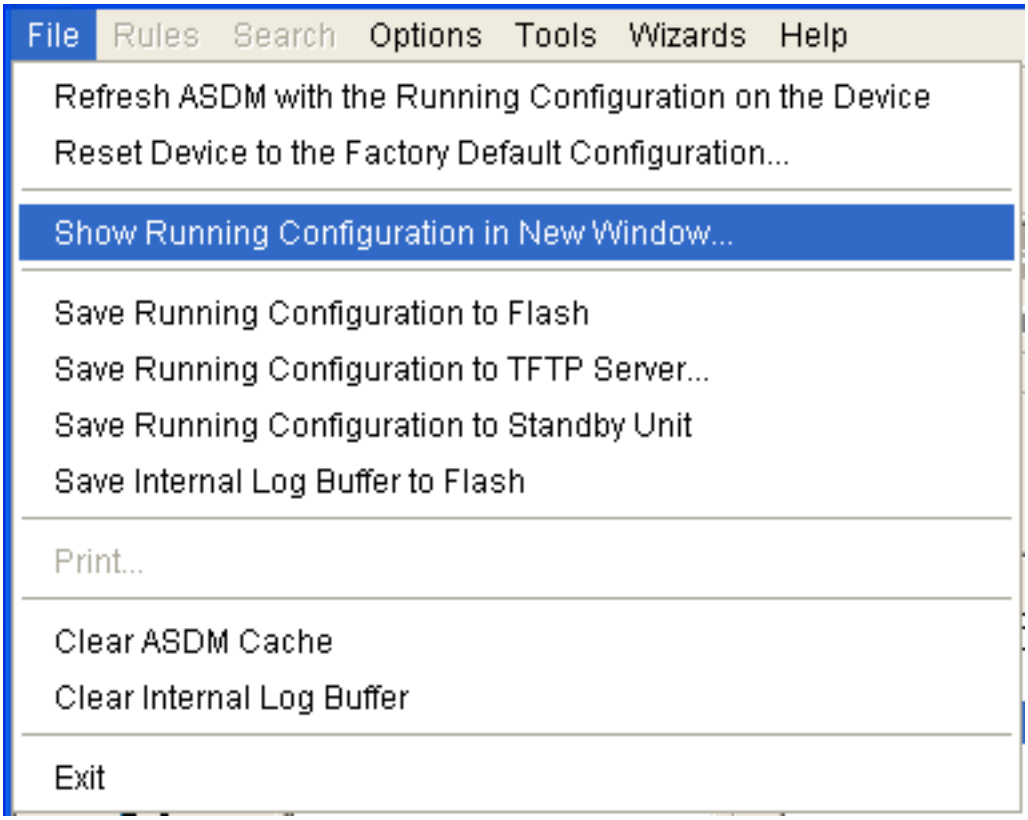
PIX 보안 어플라이언스 CLI

```
pixfirewall(config)#write terminal
PIX Version 7.0(0)102
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!--- Enforce a strict NAT for all the traffic through
the Security appliance global (outside) 1 172.16.1.5-
```

```
172.16.1.10 netmask 255.255.255.0
!--- Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0
!--- Define a single IP address 172.16.1.4 with NAT ID 1
to be used for PAT nat (inside) 1 10.0.0.0 255.0.0.0
!--- Define the inside networks with same NAT ID 1 used
in the global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
!--- Configure static routes for routing the packets
towards the internal network route outside 0.0.0.0
0.0.0.0 172.16.1.2 1
!--- Configure static route for routing the packets
towards the Internet (or External network) timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute http
server enable
!--- Enable the HTTP server on PIX for ASDM access http
10.1.1.5 255.255.255.255 inside
!--- Enable HTTP access from host 10.1.1.5 to configure
PIX using ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

ASDM**에서 CLI 컨피그레이션을** 보려면 File(파일) > Show Running Configuration in New Window(새 창에서 실행 중인 컨피그레이션 표시)를 선택합니다.



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

문제 해결 명령

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

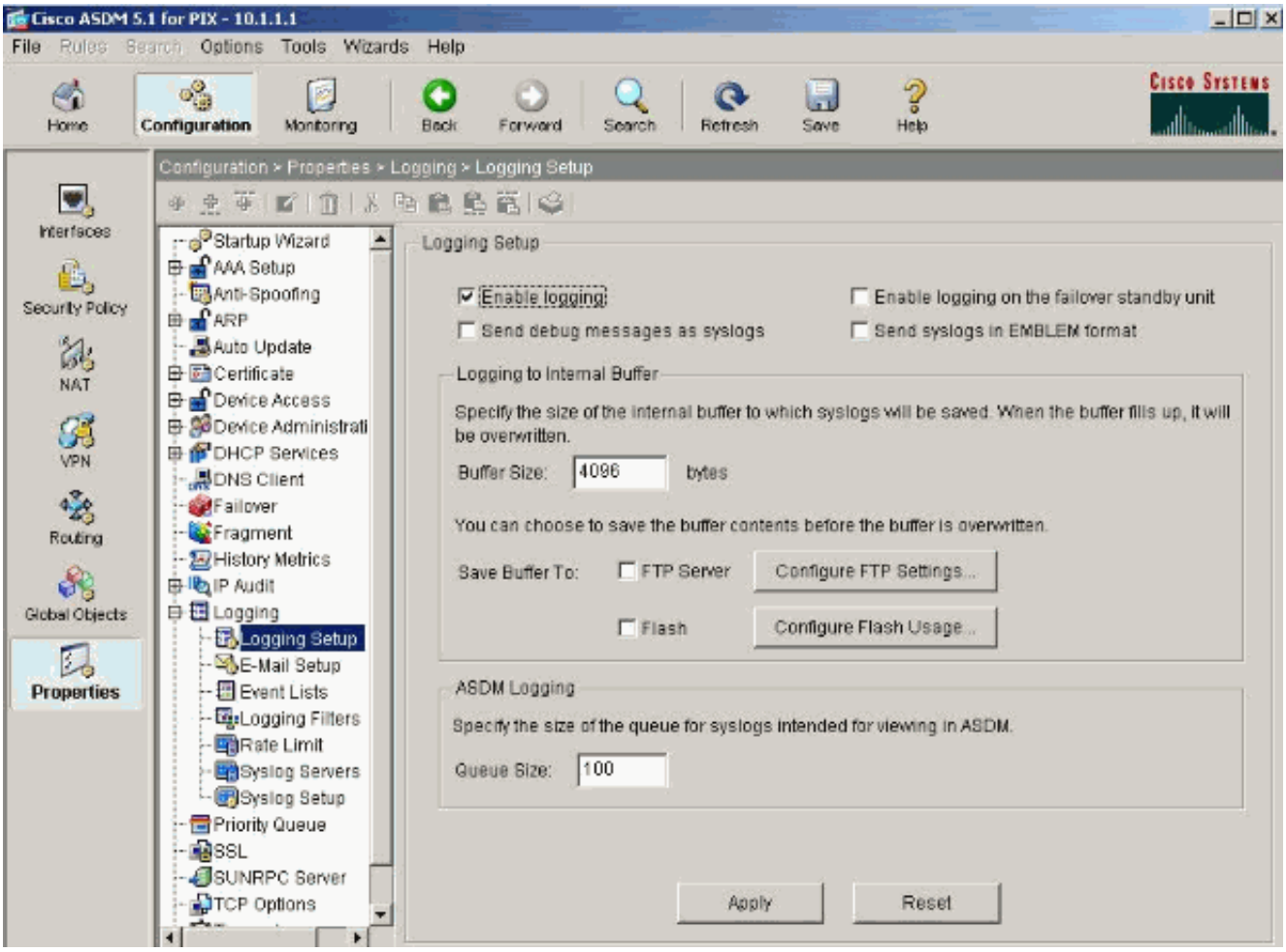
참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug icmp trace** - 호스트의 ICMP 요청이 PIX에 도달하는지 여부를 표시합니다.이 디버그를 실행하려면 컨피그레이션에서 ICMP를 허용하려면 **access-list** 명령을 추가해야 합니다.
- **logging buffer debugging(로깅 버퍼 디버깅)** - PIX를 통과하는 호스트에 설정 및 거부된 연결을 표시합니다.정보는 PIX 로그 버퍼에 저장되며 **show log** 명령을 사용하여 출력을 볼 수 있습니다.

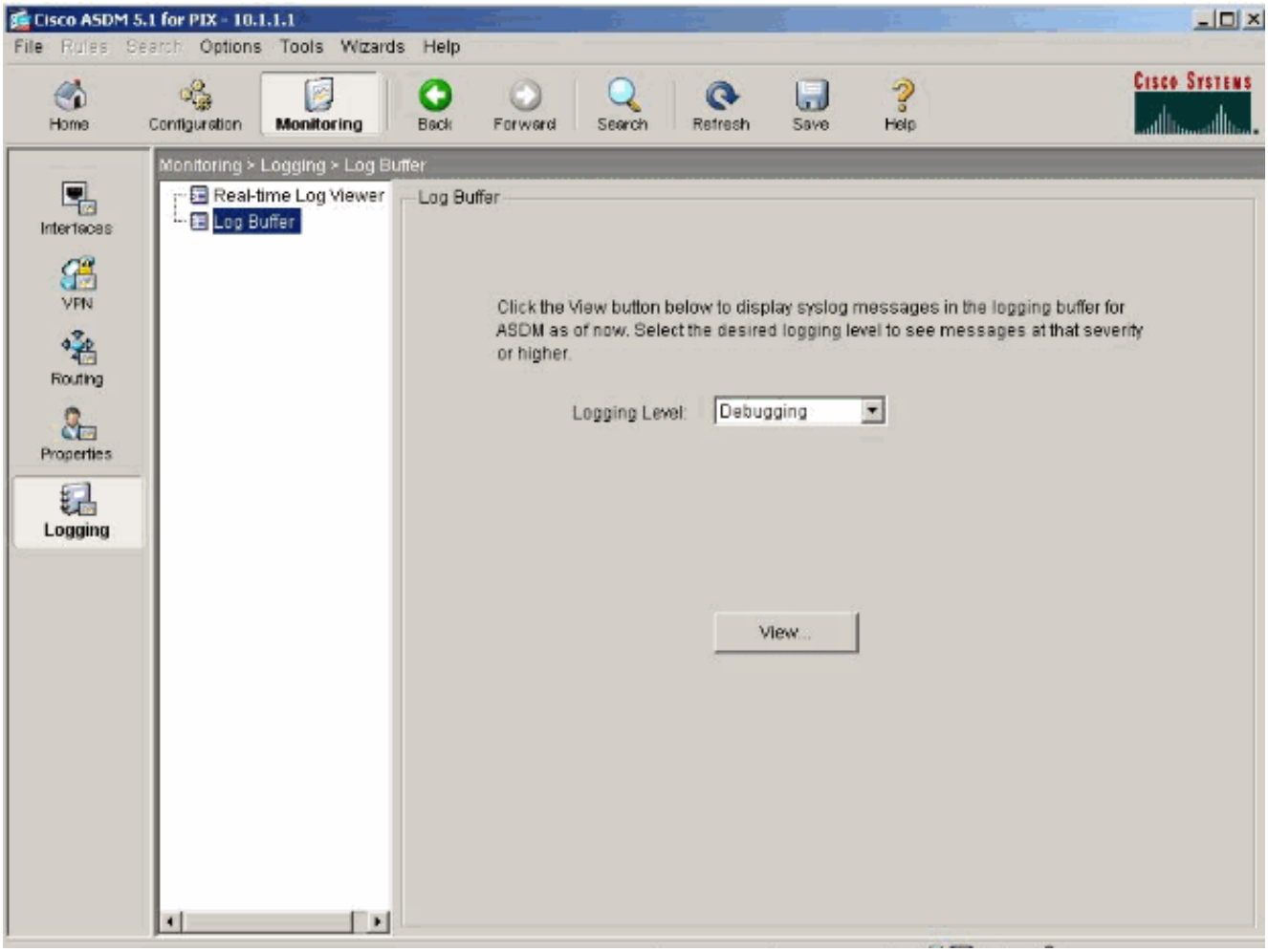
문제 해결 절차

ASDM을 사용하여 로깅을 활성화하고 로그를 볼 수도 있습니다.

1. Configuration(**구성) > Properties(속성) > Logging(로깅) > Logging Setup(로깅 설정)을 선택하고 Enable Logging(로깅 활성화**)을 선택하고 Apply(적용)를 **클릭합니다**

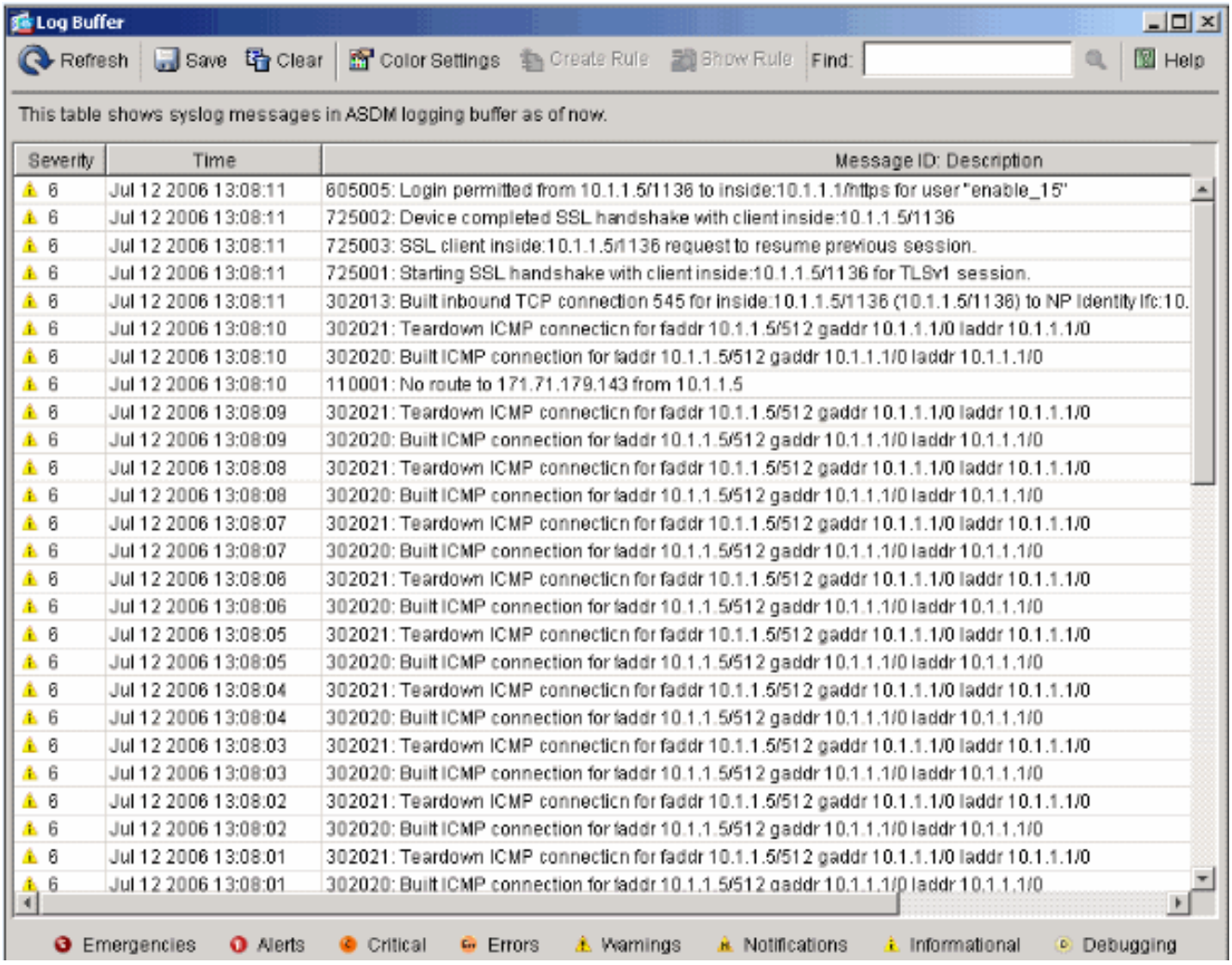


2. Monitoring(**모니터링) > Logging(로깅) > Log Buffer(로그 버퍼) > Logging Level(로깅 레벨**)을 선택하고 드롭다운 목록에서 Logging Buffer(로깅 버퍼)를 선택합니다.**보기를 클릭합니다**



3. 다음은 로그 버퍼의 예입니다

.



이름으로 웹 사이트에 액세스할 수 없음

특정 시나리오에서는 내부 네트워크가 웹 브라우저에서 이름(IP 주소와 함께 작동)을 사용하여 인터넷 웹 사이트에 액세스할 수 없습니다.이 문제는 일반적이며 DNS 서버가 정의되지 않은 경우, 특히 PIX/ASA가 DHCP 서버인 경우 발생합니다.또한 PIX/ASA에서 DNS 서버를 푸시할 수 없거나 DNS 서버에 연결할 수 없는 경우에도 이 문제가 발생할 수 있습니다.

관련 정보

- Cisco PIX 500 Series 보안 어플라이언스
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Secure PIX Firewall 명령 참조
- Cisco Adaptive Security Device Manager
- Cisco ASDM(Adaptive Security Device Manager) 문제 해결 및 알림
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems