PIX/ASA 7.x:nat, global, static 및 access-list 명령을 사용하는 포트 리디렉션(전달)

목차

소개

Cisco PIX Security Appliance 버전 7.0을 구현할 때 보안을 최대화하려면 nat **control**, nat, **global**, static, access-list 및 access-**group 명령**을 사용할 때 보안 인터페이스가 더 높은 인터페이스와 낮은 보안 인터페이스 간에 패킷이 전달되는 방식을 이해하는 것이 중요합니다.이 문서에서는 명령줄 인터페이스 또는 ASDM(Adaptive Security Device Manager)을 사용하여 PIX 소프트웨어 버전 7.x에서 포트 리디렉션(포워딩) 및 외부 NAT(Network Address Translation) 기능을 구성하는 방법과 이러한 명령의 차이점을 설명합니다.

참고: ASDM 5.2 이상의 일부 옵션은 ASDM 5.1의 옵션과 다르게 나타날 수 있습니다. 자세한 내용은 ASDM 문서를 참조하십시오.

사전 요구 사항

요구 사항

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX 500 Series Security Appliance Software 버전 7.0 이상
- ASDM 버전 5.x 이상

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.

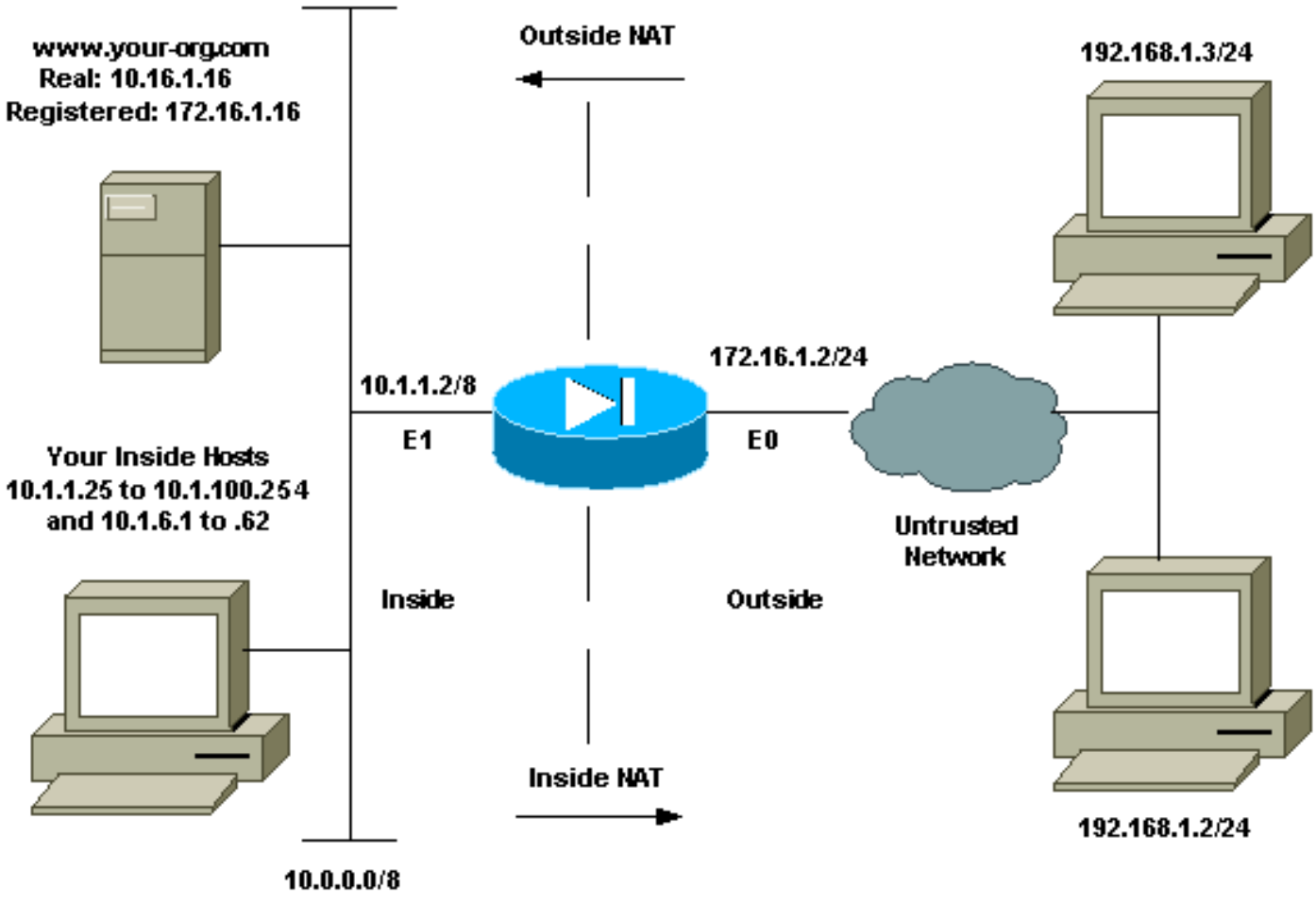
관련 제품

Cisco ASA Security Appliance 버전 7.x 이상에서 이 컨피그레이션을 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

네트워크 다이어그램



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

초기 컨피그레이션

인터페이스 이름은 다음과 같습니다.

- **interface ethernet 0** - nameif outside
- **interface ethernet 1** - nameif inside

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

아웃바운드 액세스 허용

아웃바운드 액세스는 상위 보안 수준 인터페이스에서 하위 보안 수준 인터페이스로의 연결을 설명합니다.여기에는 내부, 외부, 내부, DMZ(Demilitarized Zones), DMZ에서 외부 연결이 포함됩니다.또한 연결 소스 인터페이스의 보안 수준이 대상보다 높은 경우 한 DMZ에서 다른 DMZ로의 연결을 포함할 수 있습니다.PIX 인터페이스에서 "보안 수준" 컨피그레이션을 검토하여 이를 확인합니다.

다음 예에서는 보안 레벨 및 인터페이스 이름 컨피그레이션을 보여줍니다.

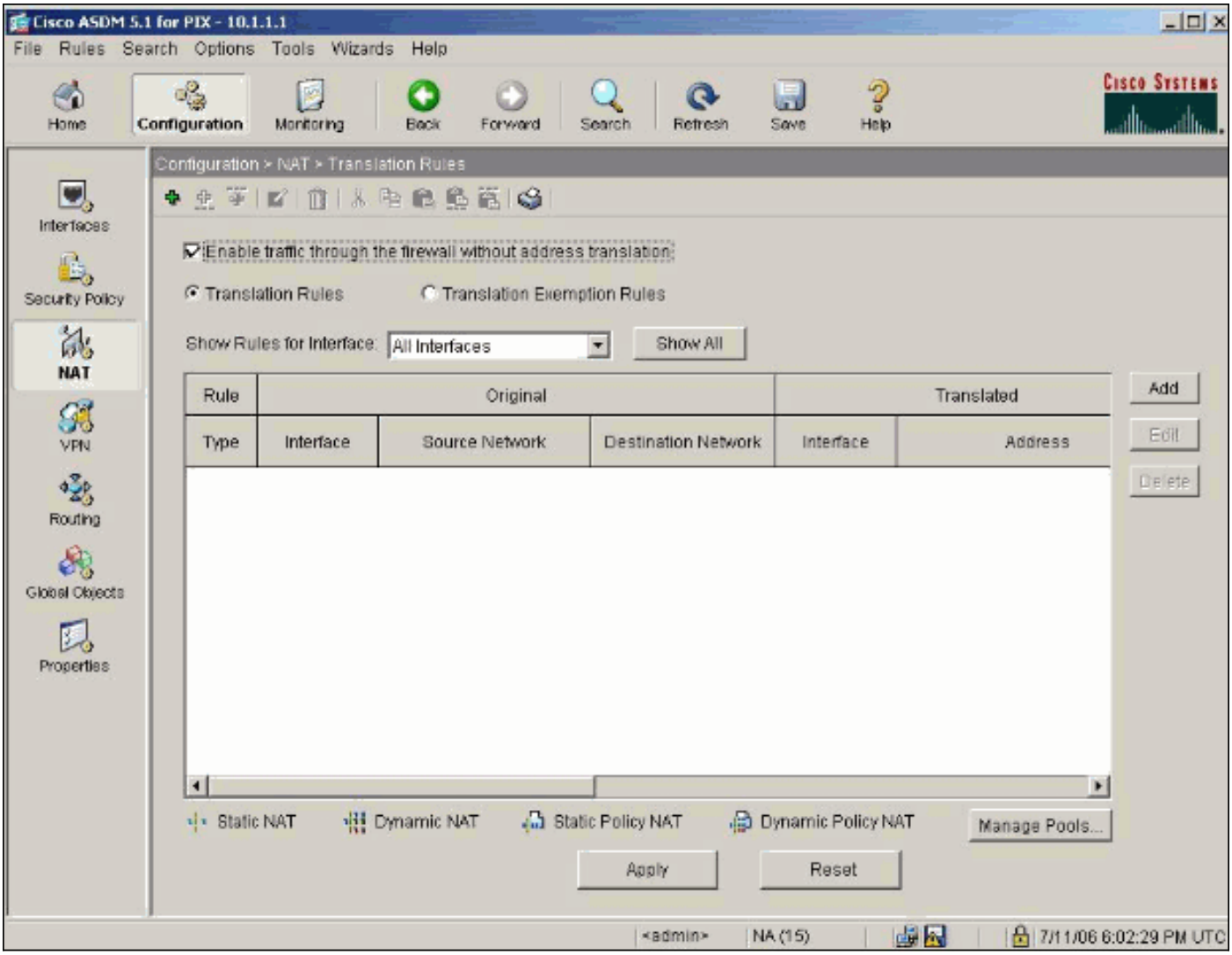
```
pix(config)#interface ethernet 0
pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit
```

PIX 7.0에는 nat-control 명령이 도입됩니다.외부 통신에 NAT가 필요한지 여부를 지정하기 위해 컨피그레이션 모드에서 nat-control 명령을 사용할 수 있습니다.NAT 컨트롤이 활성화된 경우 이전 버전의 PIX 소프트웨어와 마찬가지로 아웃바운드 트래픽을 허용하려면 NAT 규칙의 컨피그레이션이 필요합니다.NAT 컨트롤이 비활성화된 경우(nat-control 없음) 내부 호스트는 NAT 규칙의 컨피그레이션 없이 외부 네트워크와 통신할 수 있습니다.그러나 공용 주소가 없는 내부 호스트가 있는 경우 해당 호스트에 대해 NAT를 구성해야 합니다.

ASDM을 사용하여 NAT 제어를 구성하려면 ASDM Home(ASDM 홈) 창에서 Configuration(컨피그레이션) 탭을 선택하고 기능 메뉴에서 **NAT**를 선택합니다.

변환 없이 방화벽을 통과하는 트래픽을 활성화합니다.이 옵션은 PIX 버전 7.0(1)에 도입되었습니다.이 옵션을 선택하면 컨피그레이션에서 nat-control 명령이 실행되지 않습니다.이 명령은 방화벽을 통과하는 데 변환이 필요하지 않음을 의미합니다.이 옵션은 일반적으로 내부 호스트에 공용 IP 주소가 있거나 네트워크 토폴로지에서 내부 호스트를 IP 주소로 변환할 필요가 없는 경우에만 선택됩니다.

내부 호스트에 전용 IP 주소가 있는 경우 내부 호스트가 공용 IP 주소로 변환되어 인터넷에 액세스할 수 있도록 이 옵션을 선택하지 않아야 합니다.



NAT 제어를 통한 아웃바운드 액세스를 허용하려면 두 가지 정책이 필요합니다.첫 번째는 변환 방법입니다.이는 static 명령을 사용하는 정적 변환이거나 nat/**전역** 규칙을 사용하는 동적 변환일 수 있습니다.NAT 컨트롤이 비활성화되어 있고 내부 호스트에 공용 주소가 있는 경우에는 이 작업이 필요하지 않습니다.

아웃바운드 액세스에 대한 다른 요구 사항(NAT 제어 활성화 또는 비활성화 여부에 적용)은 ACL(Access Control List)이 있는 경우입니다.ACL이 있는 경우 특정 프로토콜 및 포트를 사용하여 소스 호스트가 대상 호스트에 액세스할 수 있도록 허용해야 합니다.기본적으로 PIX를 통한 아웃바운드 연결에 대한 액세스 제한은 없습니다.즉, 소스 인터페이스에 대해 구성된 ACL이 없으면 기본적으로 변환 방법이 구성된 경우 아웃바운드 연결이 허용됩니다.

내부 호스트에서 NAT를 사용하여 외부 네트워크에 액세스 허용

이 컨피그레이션에서는 서브넷 10.1.6.0/24의 모든 호스트가 외부에 액세스할 수 있습니다.이를 수행하려면 이 절차에 설명된 대로 **nat** 및 **전역** 명령을 사용합니다.

1. NAT에 포함할 내부 그룹을 정의합니다.

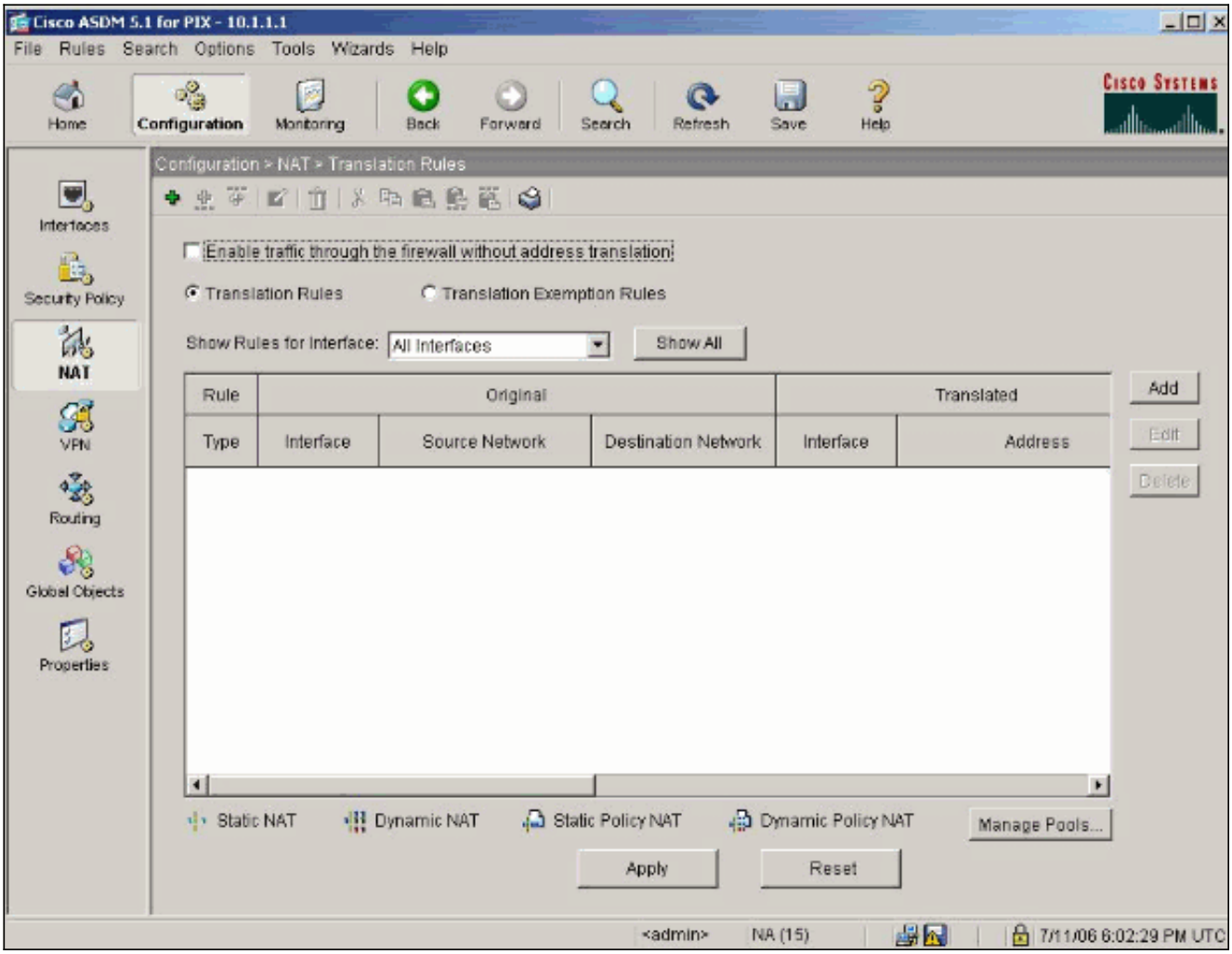
```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. NAT 문에 정의된 호스트가 변환될 외부 인터페이스의 주소 풀을 지정합니다.

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

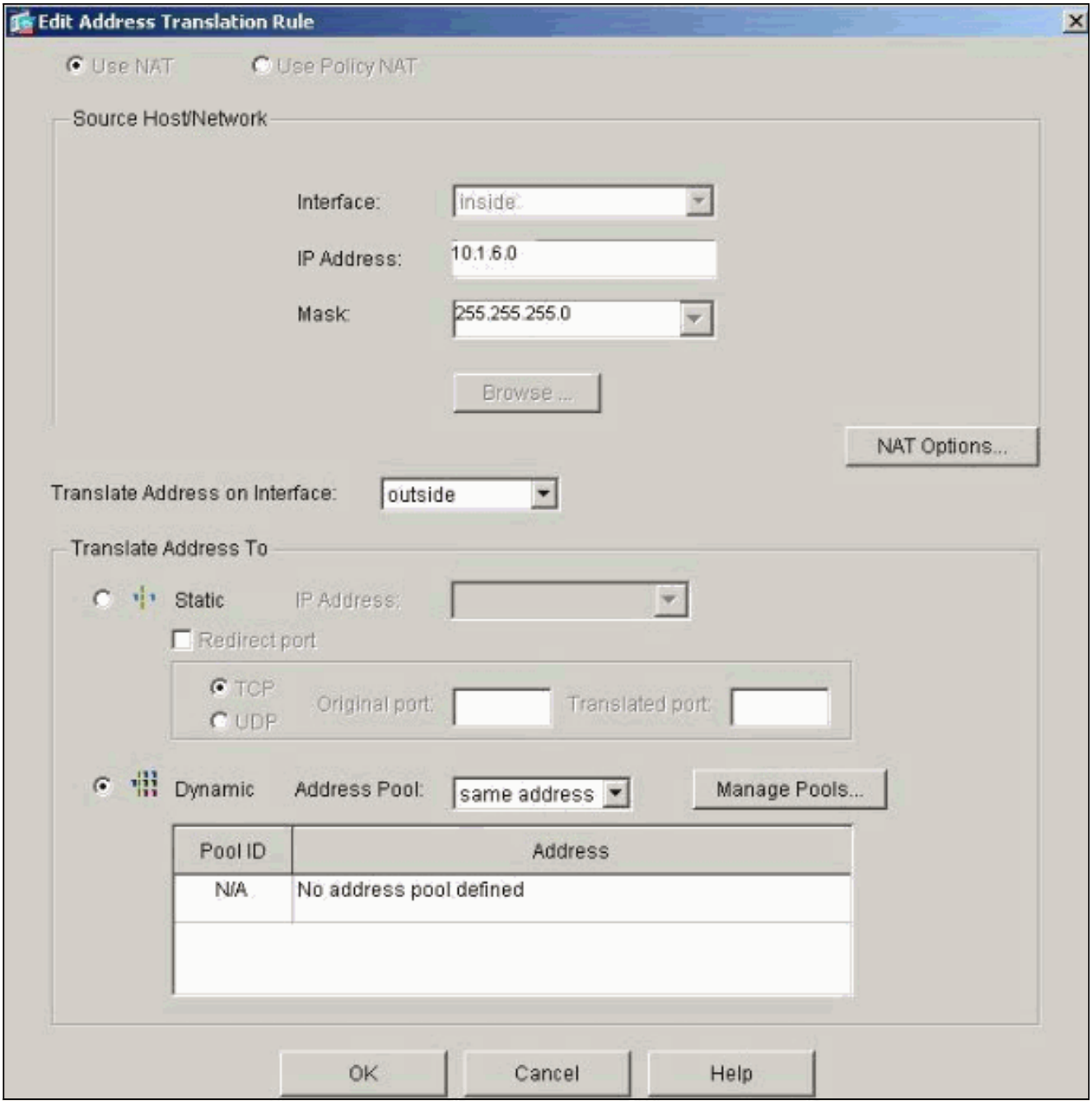
3. 전역 주소 풀을 생성하려면 ASDM을 사용합니다.Configuration **> Features > NAT**를 선택하고 **Enable traffic through the firewall without address translation**의 **선택을 취소합니다**.그런 다음 **Add**를 클릭하여 NAT 규칙을 구성합니다

.



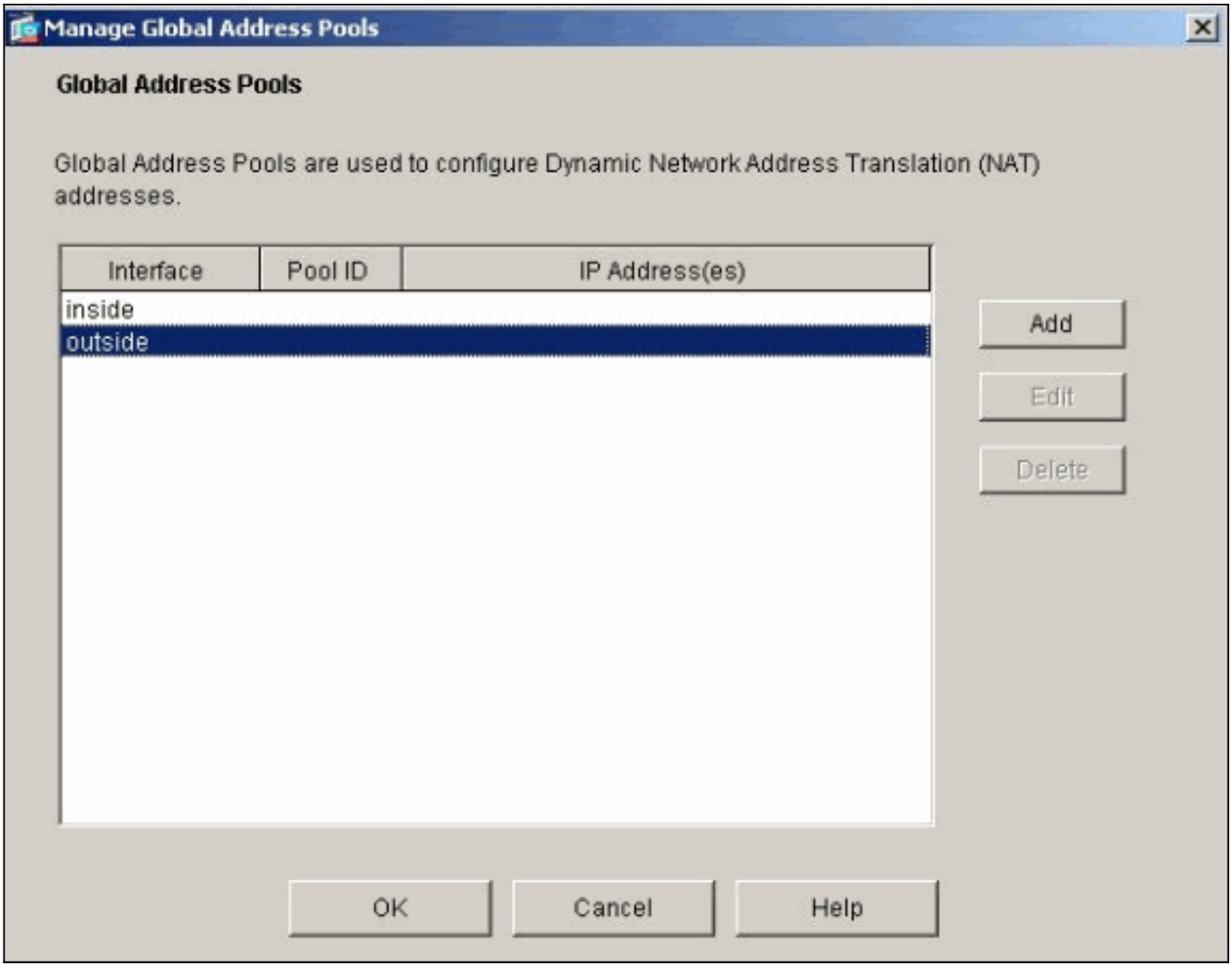
4. NAT **풀** 주소를 정의하려면 Manage Pools(풀 관리)를 클릭합니다

.



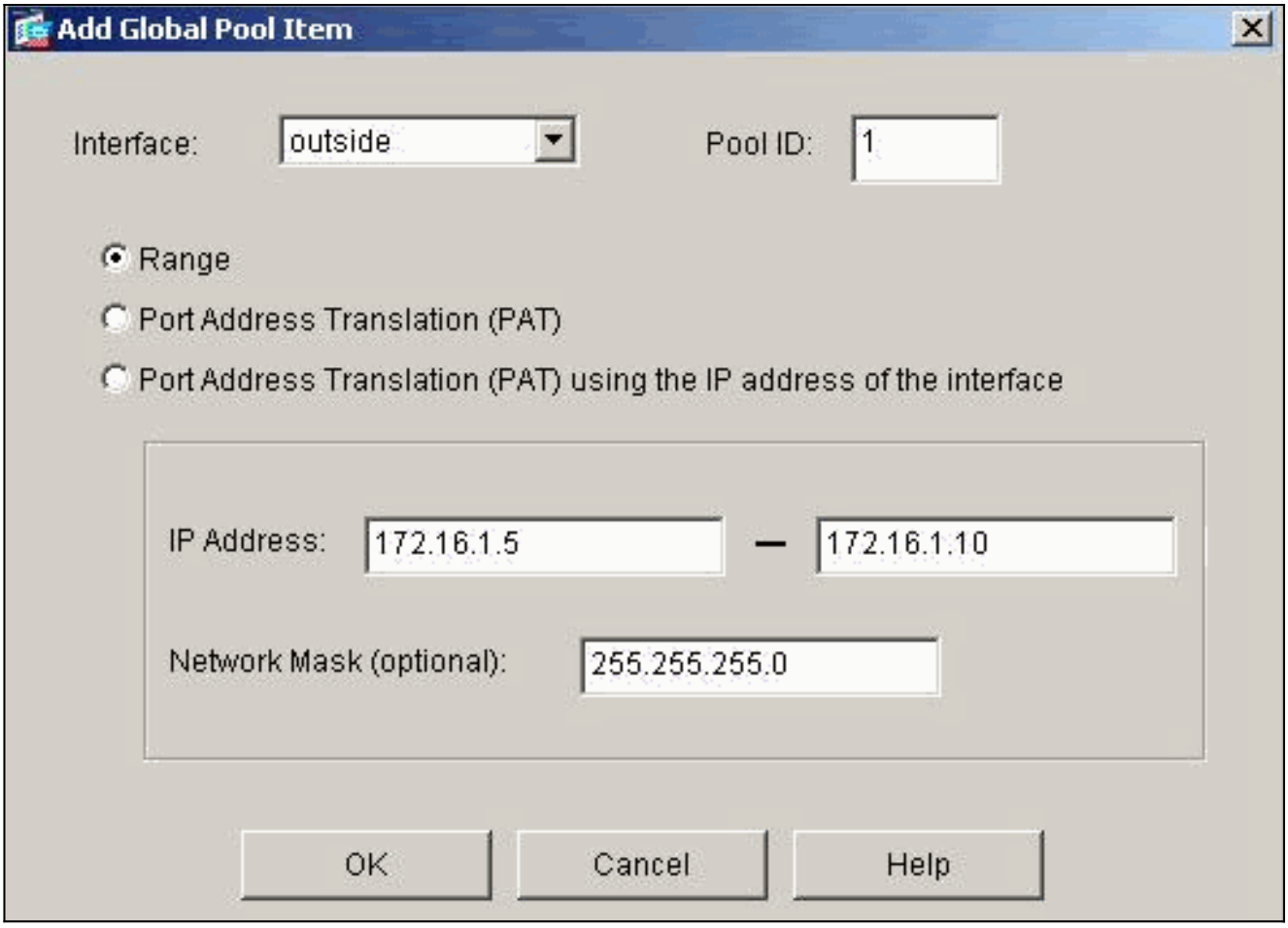
5. Outside(**외부) > Add(추가**)를 선택하고 주소 풀을 지정할 범위를 선택합니다

.



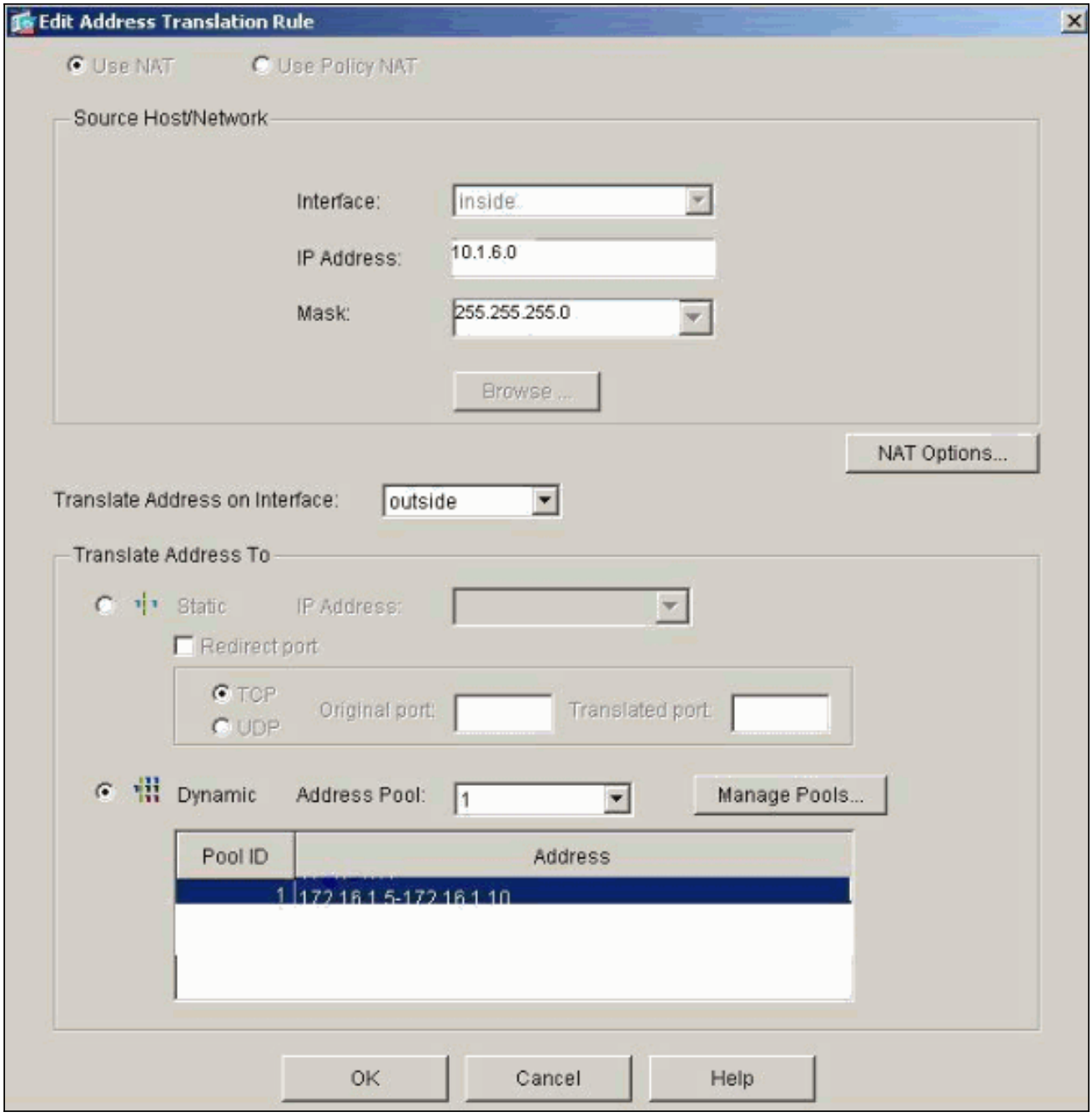
6. 주소 범위를 입력하고 풀 ID를 입력한 다음 **확인**을 클릭합니다

.



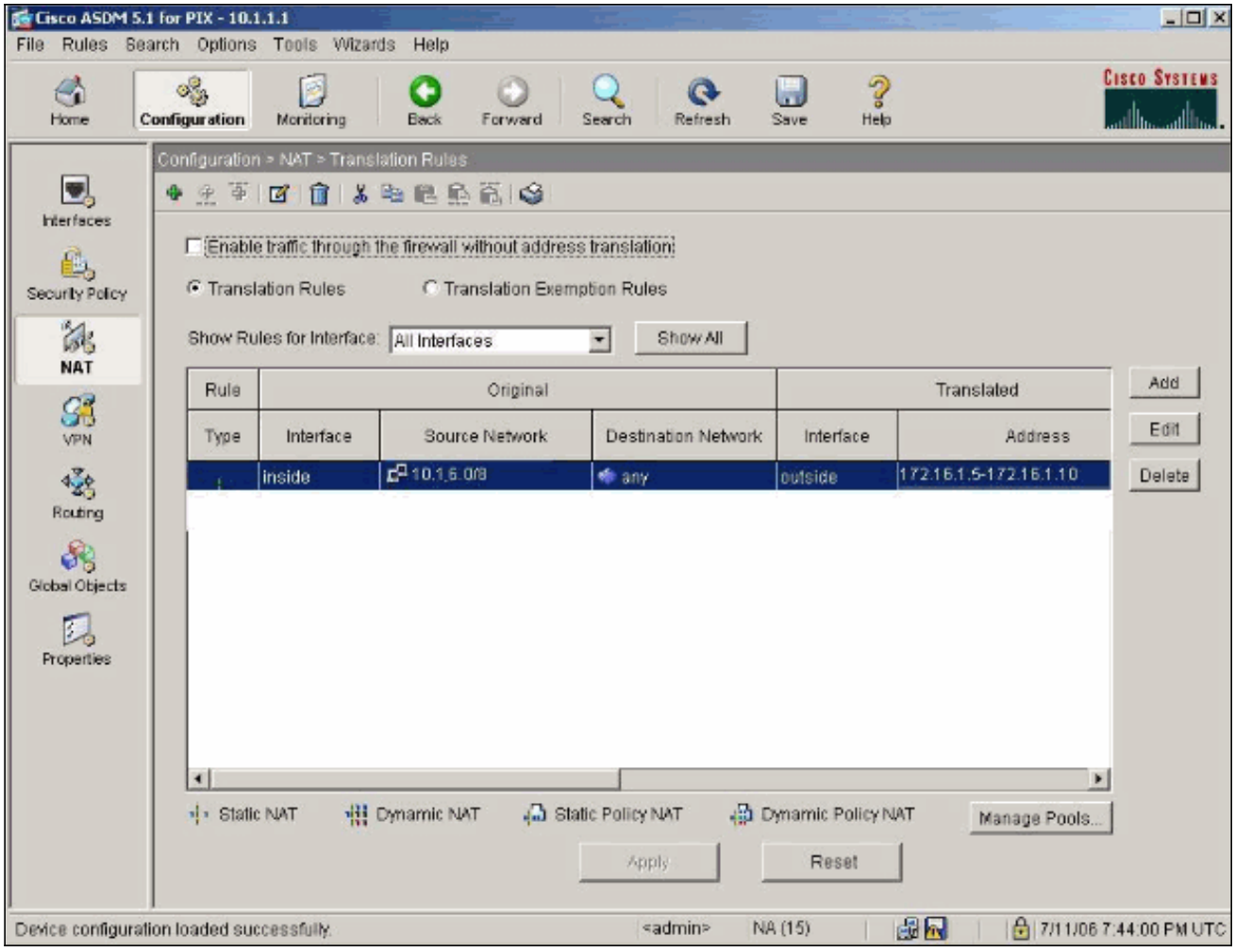
7. 변환 **규칙을** 생성하려면 Configuration > Features > NAT > Translation Rules를 선택합니다.
8. Source Interface로 Inside를 선택하고 NAT할 주소를 입력합니다.
9. Translate Address on Interface(인터페이스에서 주소 변환)에서 **Outside(외부)**를 선택하고 **Dynamic(동적)**을 선택한 다음 방금 구성한 주소 풀을 선택합니다.
10. **확인을 클릭합니다**

.



11. 변환은 Translation Rules at Configuration > Features **> NAT > Translation Rules**에 나타납니다

.



이제 내부 호스트가 외부 네트워크에 액세스할 수 있습니다.내부 호스트가 외부로 연결을 시작할 때 전역 풀의 주소로 변환됩니다.주소는 처음에 변환된 상태로 전역 풀에서 할당되고 풀의 가장 낮은 주소로 시작합니다.예를 들어 호스트 10.1.6.25이 외부로 연결을 처음 시작하는 경우 주소 172.16.1.5을 수신하고 다음 호스트 아웃은 172.16.1.6을 수신합니다.이는 정적 변환이 아니며, timeout xlate hh:mm:ss 명령에 의해 정의된 비활성 기간 후 변환 시간**이 초과됩니다**.풀에 주소가 있는 것보다 더 많은 내부 호스트가 있는 경우 풀의 최종 주소가 PAT(Port Address Translation)에 사용됩니다.

PAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용

내부 호스트에서 번역을 위해 단일 공용 주소를 공유하려면 PAT를 사용합니다.**global 문**이 하나의 주소를 지정하면 해당 주소는 포트 변환됩니다.PIX는 인터페이스당 하나의 포트 변환을 허용하며, 이 변환은 단일 전역 주소에 대해 최대 65,535개의 활성 xlate 객체를 지원합니다.내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스할 수 있도록 하려면 다음 단계를 완료하십시오.

1. PAT에 포함할 내부 그룹을 정의합니다(0 0을 사용할 경우 모든 내부 호스트를 선택합니다).

   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```

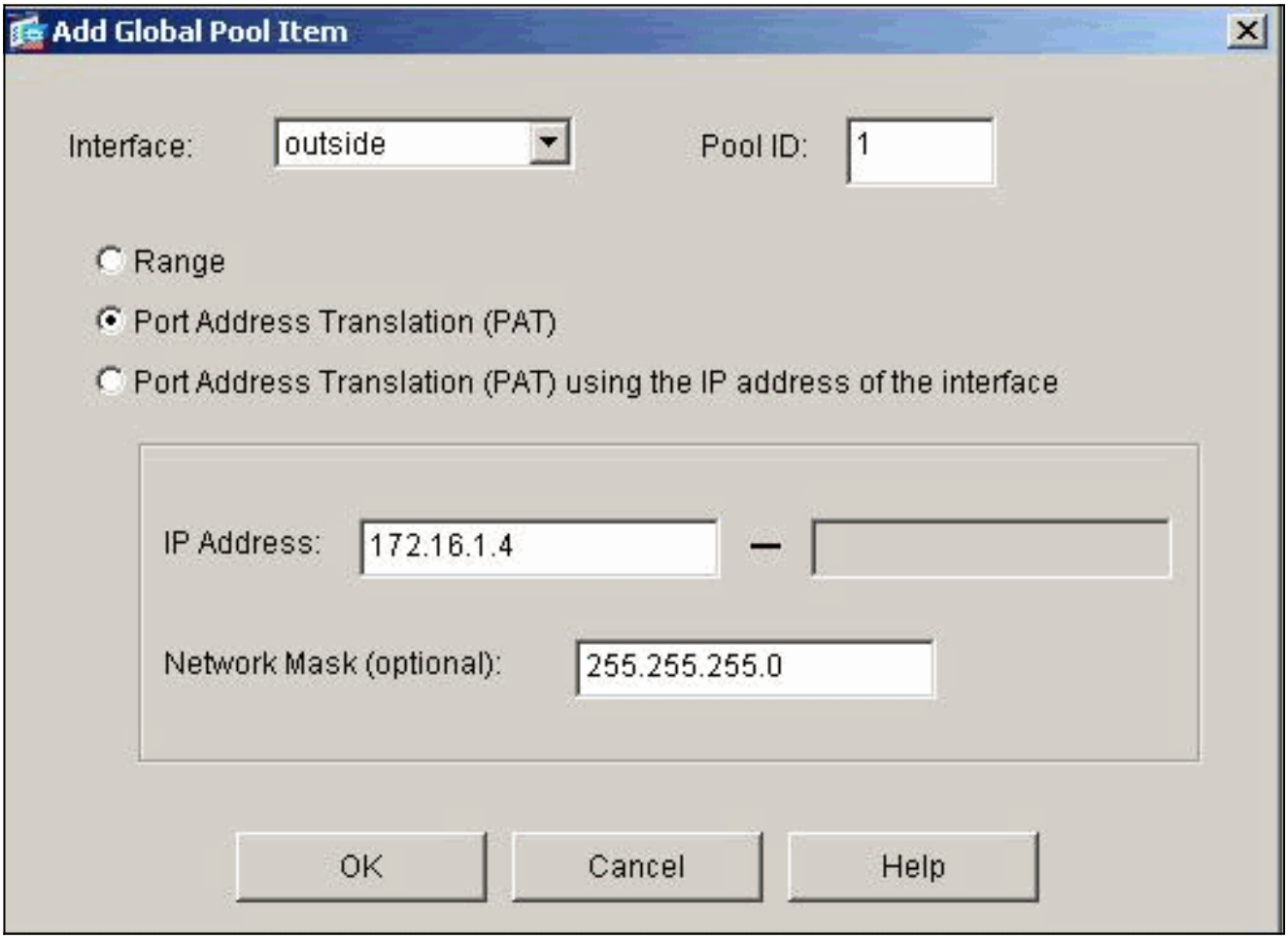
2. PAT에 사용할 전역 주소를 지정합니다.인터페이스 주소가 될 수 있습니다.

   ```
   global (outside) 1 172.16.1.4 netmask 255.255.255.0
   ```

3. ASDM에서 **Configuration > Features > NAT**를 선택하고 **Enable traffic through the firewall without address translation의 선택을 취소합니다**.
4. NAT 규칙을 구성하려면 Add를 클릭합니다.
5. PAT 주소를 구성하려면 Manage Pools를 선택합니다.

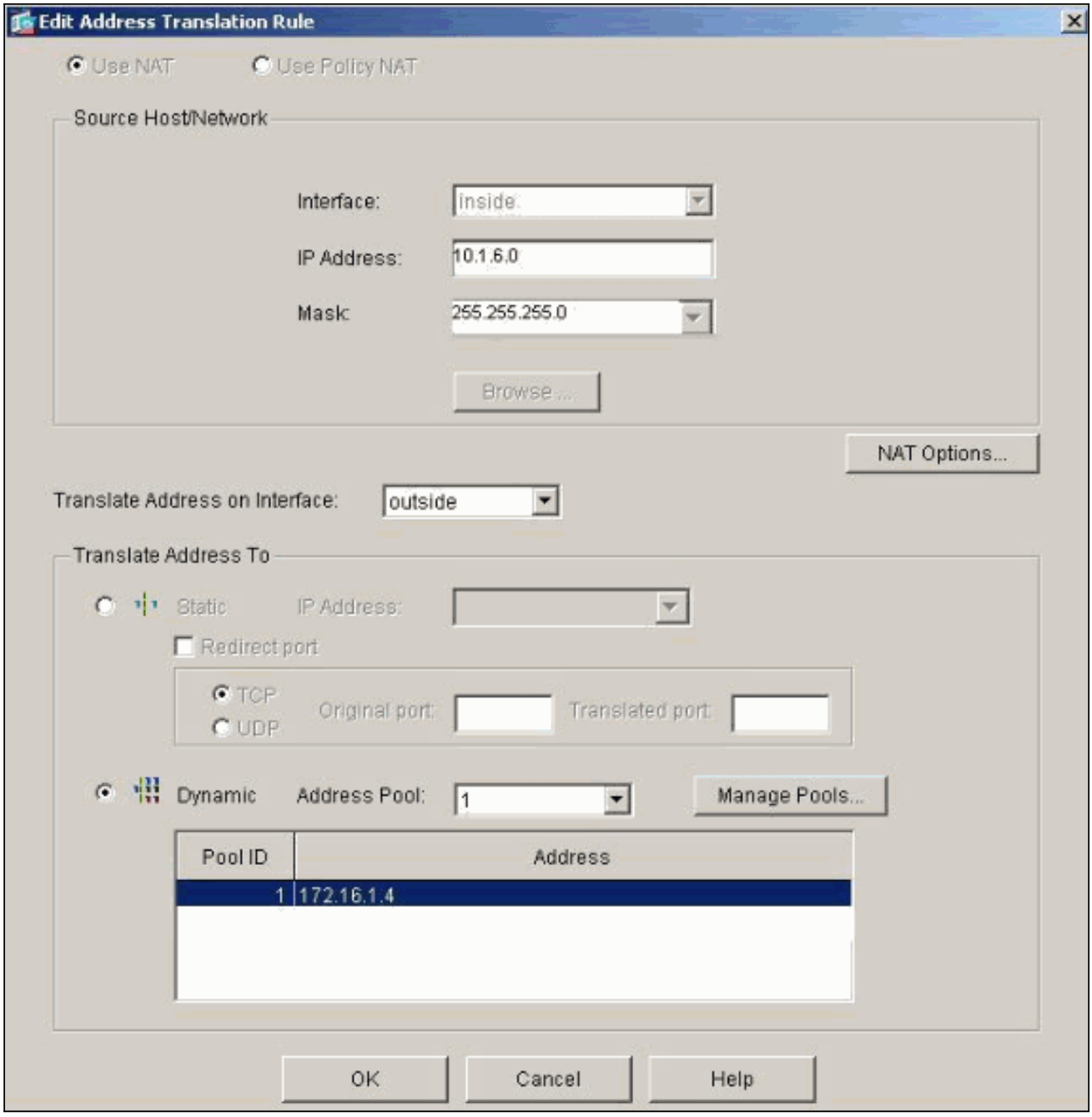
6. PAT에 대한 단일 주소를 구성하려면 **Outside > Add**(추가)를 선택하고 **Port Address Translation (PAT)**을 클릭합니다.
7. 주소, 풀 ID를 입력하고 **확인**을 클릭합니다

.



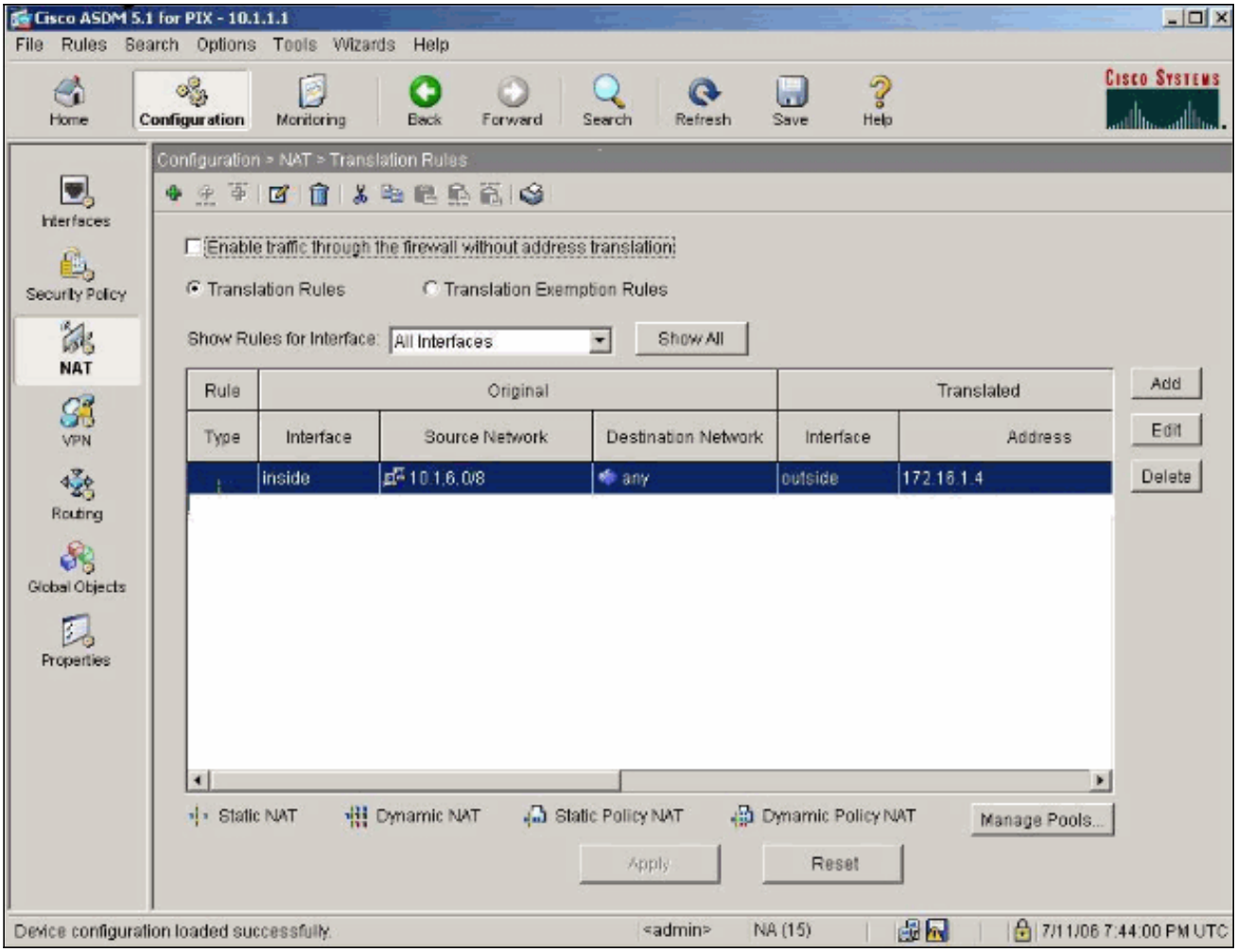
8. 변환 **규칙을** 생성하려면 Configuration > Features > NAT > Translation Rules를 선택합니다.
9. **내부**를 소스 인터페이스로 선택하고 NAT할 주소를 입력합니다.
10. Translate Address on Interface(인터페이스에서 주소 변환)에서 **outside(외부)**를 선택하고 **Dynamic(동적)**을 선택한 다음 방금 구성한 주소 풀을 선택합니다.**확인을 클릭합니다**

.



11. 변환은 Translation Rules at Configuration > Features **> NAT > Translation Rules**에 나타납니다

.



PAT를 사용할 때 고려해야 할 몇 가지 사항이 있습니다.

- PAT에 대해 지정하는 IP 주소는 다른 전역 주소 풀에 있을 수 없습니다.
- PAT는 H.323 애플리케이션, 캐싱 이름 서버 및 PPTP(Point-to-Point Tunneling Protocol)에서 작동하지 않습니다.PAT는 DNS(Domain Name Service), FTP 및 패시브 FTP, HTTP, 메일, RPC(remote-procedure call), rshell, 텔넷, URL 필터링, 아웃바운드 traceroute에서 작동합니다 .
- 방화벽을 통해 멀티미디어 애플리케이션을 실행해야 할 경우 PAT를 사용하지 마십시오.멀티미디어 애플리케이션은 PAT에서 제공하는 포트 매핑과 충돌할 수 있습니다.
- PAT 소프트웨어 릴리스 4.2(2)에서 PAT 기능은 역순으로 도착하는 IP 데이터 패킷에서 작동하지 않습니다.PIX 소프트웨어 릴리스 4.2(3)는 이 문제를 해결합니다.
- global 명령으로 지정된 전역 주소 풀의 IP 주소는 PIX를 통해 모든 외부 네트워크 주소에 액세스할 수 있도록 하려면 역방향 DNS 항목이 필요합니다.역방향 DNS 매핑을 생성하려면 각 전역 주소에 대한 주소-이름 매핑 파일에서 DNS 포인터(PTR) 레코드를 사용합니다.PTR 항목이 없으면 사이트가 느리거나 간헐적인 인터넷 연결을 경험할 수 있으며 FTP 요청이 지속적으로 실패합니다.예를 들어 글로벌 IP 주소가 192.168.1.3이고 PIX 보안 어플라이언스의 도메인 이름이 pix.caguana.com인 경우 PTR 레코드는 다음과 같습니다.

```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
 4.1.1.175.in-addr.arpa. IN PTR
pix4.caguana.com & so on.
```

외부 네트워크에 대한 내부 호스트 액세스 제한

소스 호스트에 대해 정의된 유효한 변환 방법이 있고 소스 PIX 인터페이스에 대해 정의된 ACL이 없는 경우 기본적으로 아웃바운드 연결이 허용됩니다.그러나 경우에 따라 소스, 대상, 프로토콜 및/또

는 포트를 기반으로 아웃바운드 액세스를 제한해야 합니다.이를 위해 access-**list** 명령으로 ACL을 구성하고 **access-group** 명령을 사용하여 연결 소스 PIX 인터페이스에 적용합니다.인바운드 및 아웃바운드 방향 모두에서 PIX 7.0 ACL을 적용할 수 있습니다.이 절차는 한 서브넷에 대해 아웃바운드 HTTP 액세스를 허용하지만, 모든 사용자에게 다른 모든 IP 트래픽을 허용하는 동시에 외부에 대한 다른 모든 호스트의 HTTP 액세스를 거부하는 예입니다.

1. ACL을 정의합니다.

   ```
   access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
   access-list acl_outbound deny tcp any any eq www
   access-list acl_outbound permit ip any any
   ```

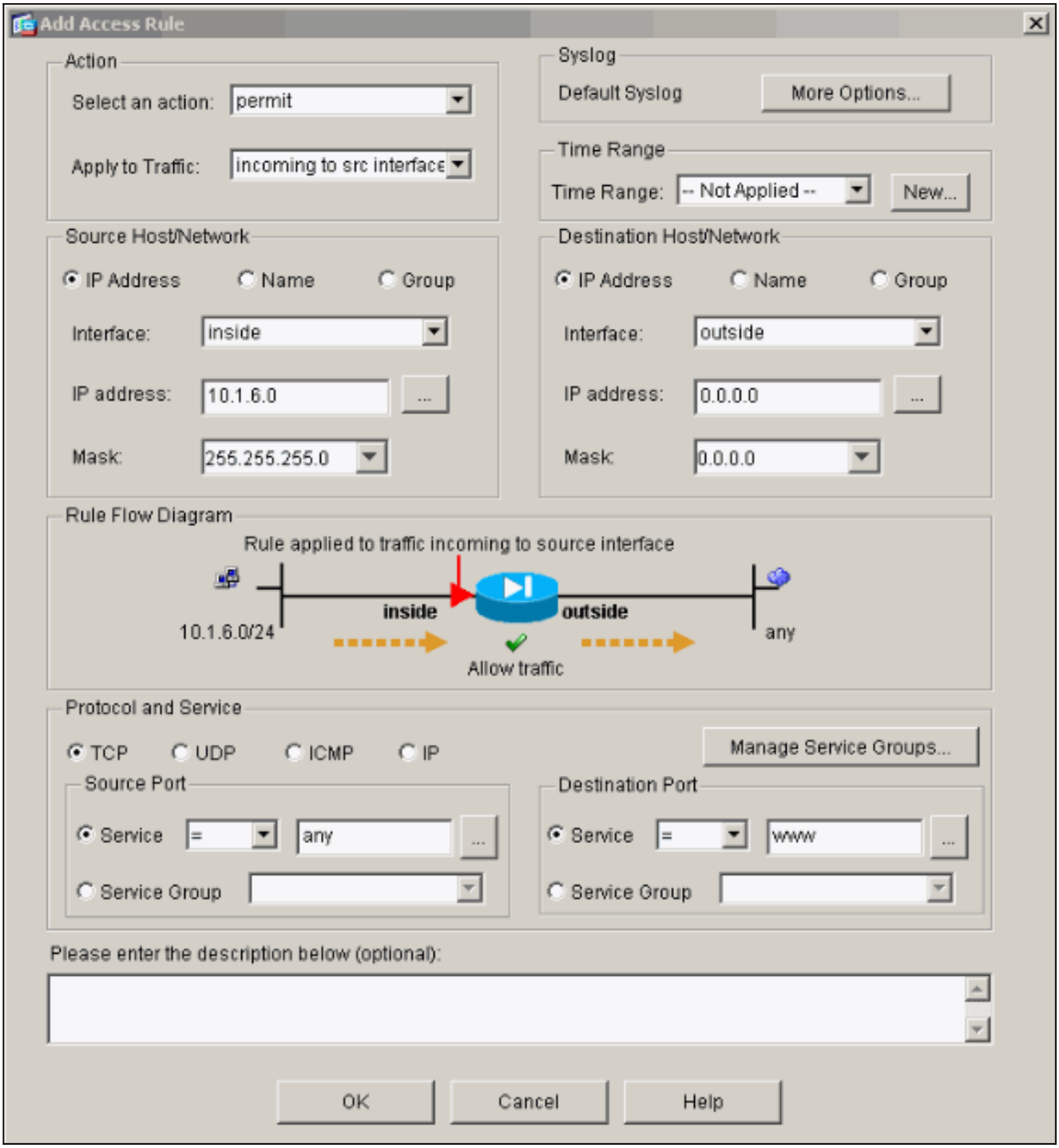
   참고: PIX ACL은 Cisco IOS® 라우터의 ACL과 다릅니다. PIX는 Cisco IOS와 같은 와일드카드 마스크를 사용하지 않습니다.ACL 정의에서 일반 서브넷 마스크를 사용합니다.Cisco IOS 라우터와 마찬가지로 PIX ACL은 ACL의 끝에 암시적 "deny all(모두 거부)"이 있습니다.**참고:** 새 액세스 목록 항목은 기존 ACE의 끝에 추가됩니다.먼저 특정 ACE를 처리해야 하는 경우 access-list에서 `line` 키워드를 사용할 수 있습니다.다음은 명령 요약의 예입니다.

   ```
   access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
   ```

2. 내부 인터페이스에 ACL을 적용합니다.

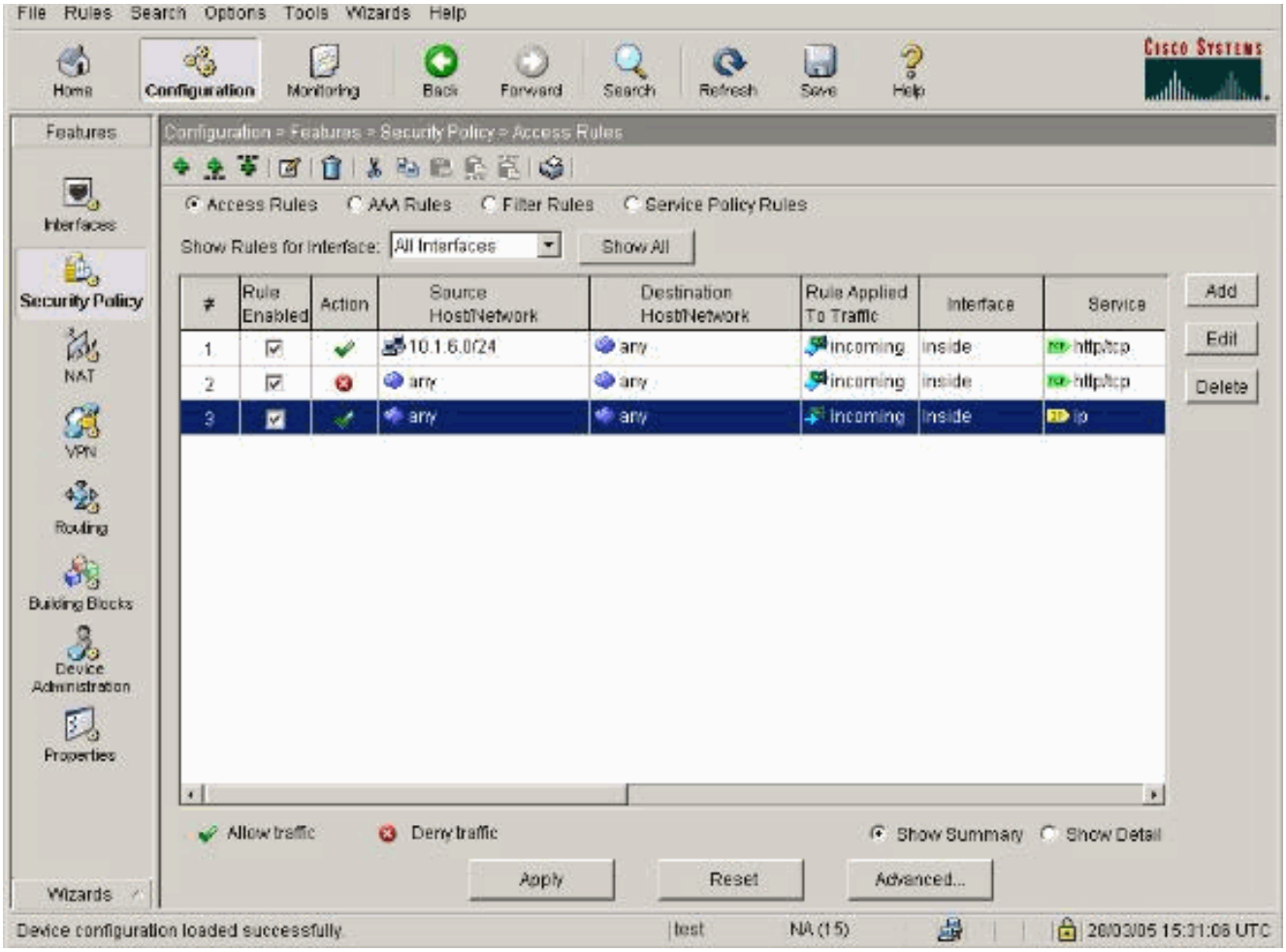
   ```
   access-group acl_outbound in interface inside
   ```

3. 1단계에서 첫 번째 액세스 목록 항목을 구성하여 10.1.6.0/24의 HTTP 트래픽을 허용하려면 ASDM을 사용합니다. Configuration(구성) **> Features(기능) > Security Policy(보안 정책) > Access Rules(액세스 규칙)를 선택합니다**.
4. Add(**추가**)를 클릭하고 이 창에 표시되는 정보를 입력한 다음 **OK**(확인)를 클릭합니다
   .



5. 세 개의 액세스 목록 항목을 입력한 후 이러한 규칙을 표시하려면 **Configuration > Feature > Security Policy > Access Rules**를 선택합니다

.



신뢰할 수 없는 호스트에서 신뢰할 수 있는 네트워크의 호스트에 액세스 허용

대부분의 조직은 신뢰할 수 없는 호스트가 신뢰할 수 있는 네트워크의 리소스에 액세스하도록 허용해야 합니다.일반적인 예는 내부 웹 서버입니다.기본적으로 PIX는 외부 호스트에서 내부 호스트로의 연결을 거부합니다.NAT 제어 모드에서 이 연결을 허용하려면 **access-list** 및 **access-group** 명령과 함께 static 명령을 사용합니다.NAT 컨트롤이 비활성화된 경우 변환이 수행되지 않을 경우 **access-list** 및 **access-group** 명령만 필요합니다.

access-group 명령을 사용하여 인터페이스에 ACL을 적용합니다.이 명령은 ACL을 인터페이스와 연결하여 특정 방향으로 흐르는 트래픽을 검사합니다.

내부 호스트를 아웃하는 **nat** 및 **전역** 명령과 달리 static 명령은 적절한 ACL/그룹을 추가할 경우 내부 호스트 외부 및 외부 호스트를 허용하는 양방향 변환을 생성합니다.

이 문서에 표시된 PAT 컨피그레이션 예에서 외부 호스트가 전역 주소에 연결을 시도할 경우 내부 호스트 수천 개에서 사용할 수 있습니다.static 명령은 일대일 매핑을 생성합니다.access-**list** 명령은 내부 호스트에 허용되는 연결 유형을 정의하며, 하위 보안 호스트가 상위 보안 호스트에 연결될 때 항상 필요합니다.access-**list** 명령은 포트 및 프로토콜을 모두 기반으로 하며 시스템 관리자가 원하는 사항을 기반으로 매우 허용하거나 매우 제한적일 수 있습니다.

이 문서의 네트워크 다이어그램은 신뢰할 수 없는 호스트가 내부 웹 서버에 연결되도록 PIX를 구성하고, 신뢰할 수 없는 호스트 192.168.1.1이 동일한 시스템의 FTP 서비스에 액세스하도록 허용하기 위해 이러한 명령을 사용하는 방법을 보여줍니다.

PIX 버전 7.0 이상에서 ACL 사용

ACL을 사용하여 PIX 소프트웨어 버전 7.0 이상에 대해 다음 단계를 완료합니다.

1. NAT 컨트롤이 활성화된 경우 내부 웹 서버에서 외부/전역 주소에 대한 고정 주소 변환을 정의합니다.

   ```
   static (inside, outside)  172.16.1.16 10.16.1.16
   ```

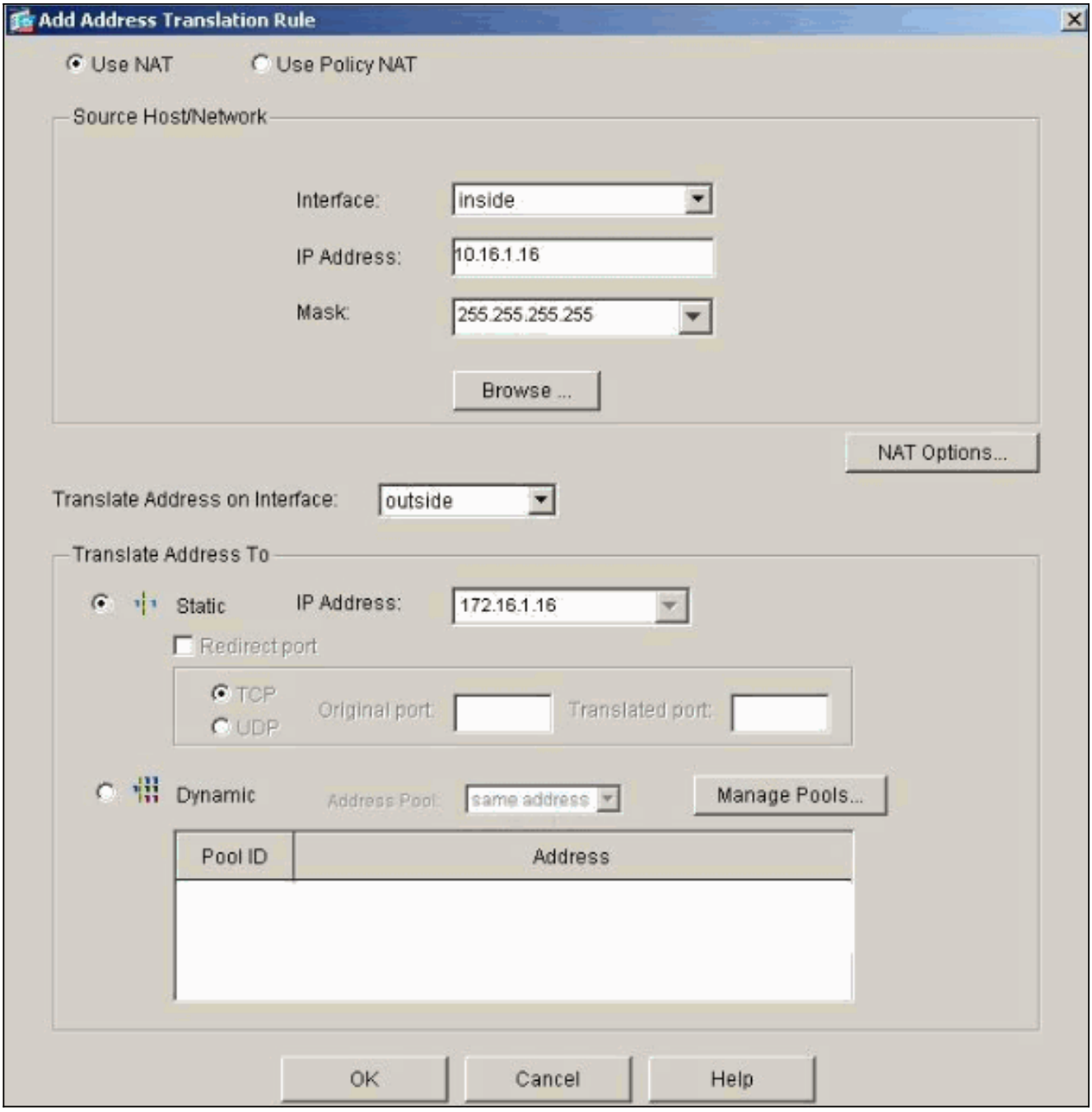
2. 웹/FTP 서버에 어떤 포트를 연결할 수 있는지 정의합니다.

   ```
   access-list 101 permit tcp any host  172.16.1.16 eq www
   access-list 101 permit tcp host  192.168.1.1 host  172.16.1.16 eq ftp
   ```

3. 외부 인터페이스에 ACL을 적용합니다.

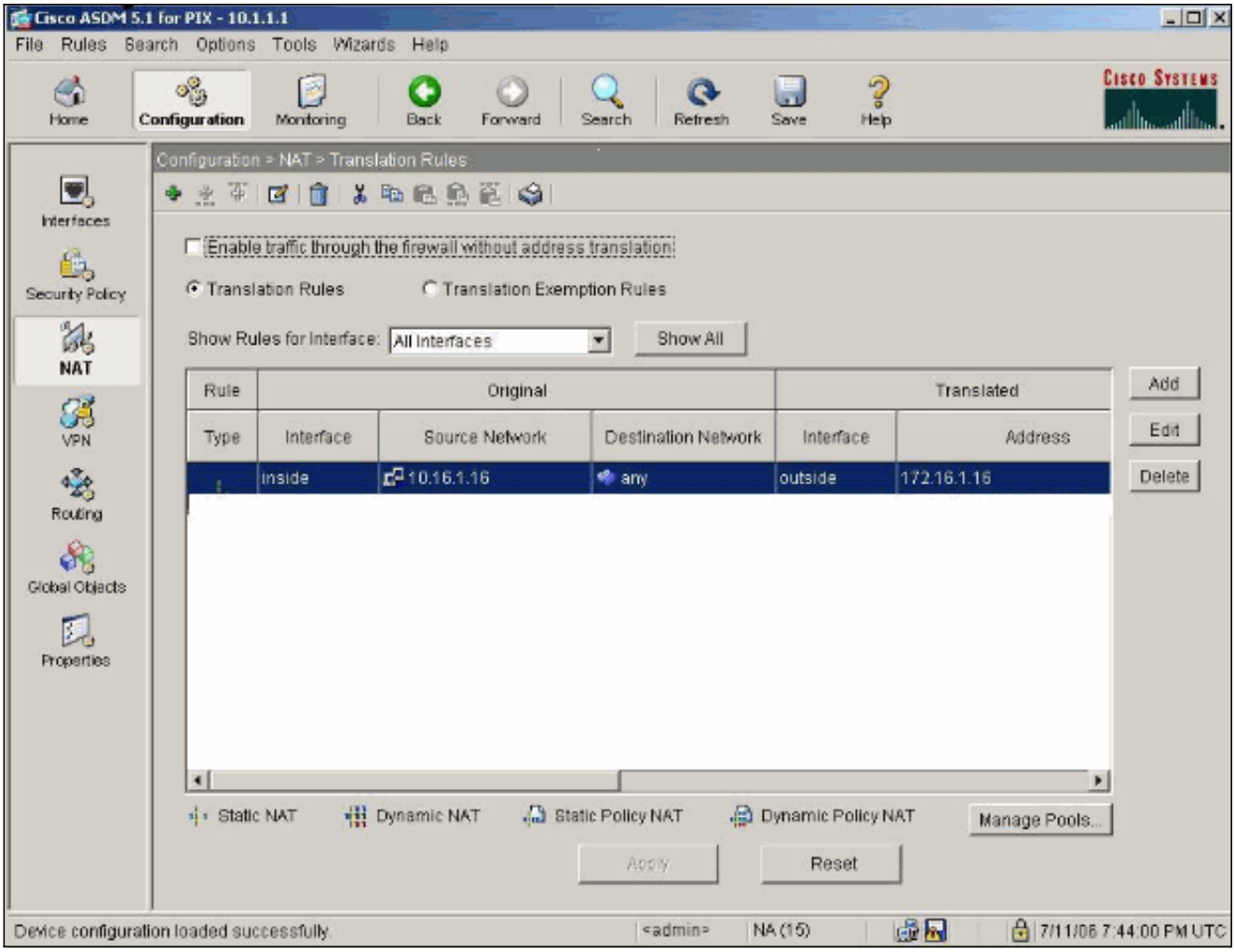
   ```
   access-group 101 in interface outside
   ```

4. ASDM**을** 사용하여 이 고정 변환을 생성하려면 Configuration > Features > NAT를 선택하고 Add를 클릭합니다.
5. **내부**를 소스 인터페이스로 선택하고 고정 변환을 생성할 내부 주소를 입력합니다.
6. Static**을** 선택하고 IP 주소 필드에 변환할 외부 주소를 입력합니다.**확인**을 **클릭합니다**
   .



7. 변환은 Configuration(컨피그레이션) > Features(기능) **> NAT > Translation Rules(변환 규칙)를** 선택할 때 Translation Rules(변환 규칙)**에 나타납니다**

.



8. **액세스 목록** 항목을 입력하려면 Restrict Inside Hosts Access to Outside Networks(외부 네트워크에 대한 내부 호스트 액세스 제한) 절차를 사용합니다.**참고:** 이러한 명령을 구현할 때는 주의해야 합니다.**access-list 101 permit ip any any** 명령을 구현하면 활성 변환이 있는 한 신뢰할 수 없는 네트워크의 모든 호스트가 IP를 사용하여 신뢰할 수 있는 네트워크의 모든 호스트에 액세스할 수 있습니다.

특정 호스트/네트워크에 대해 NAT 비활성화

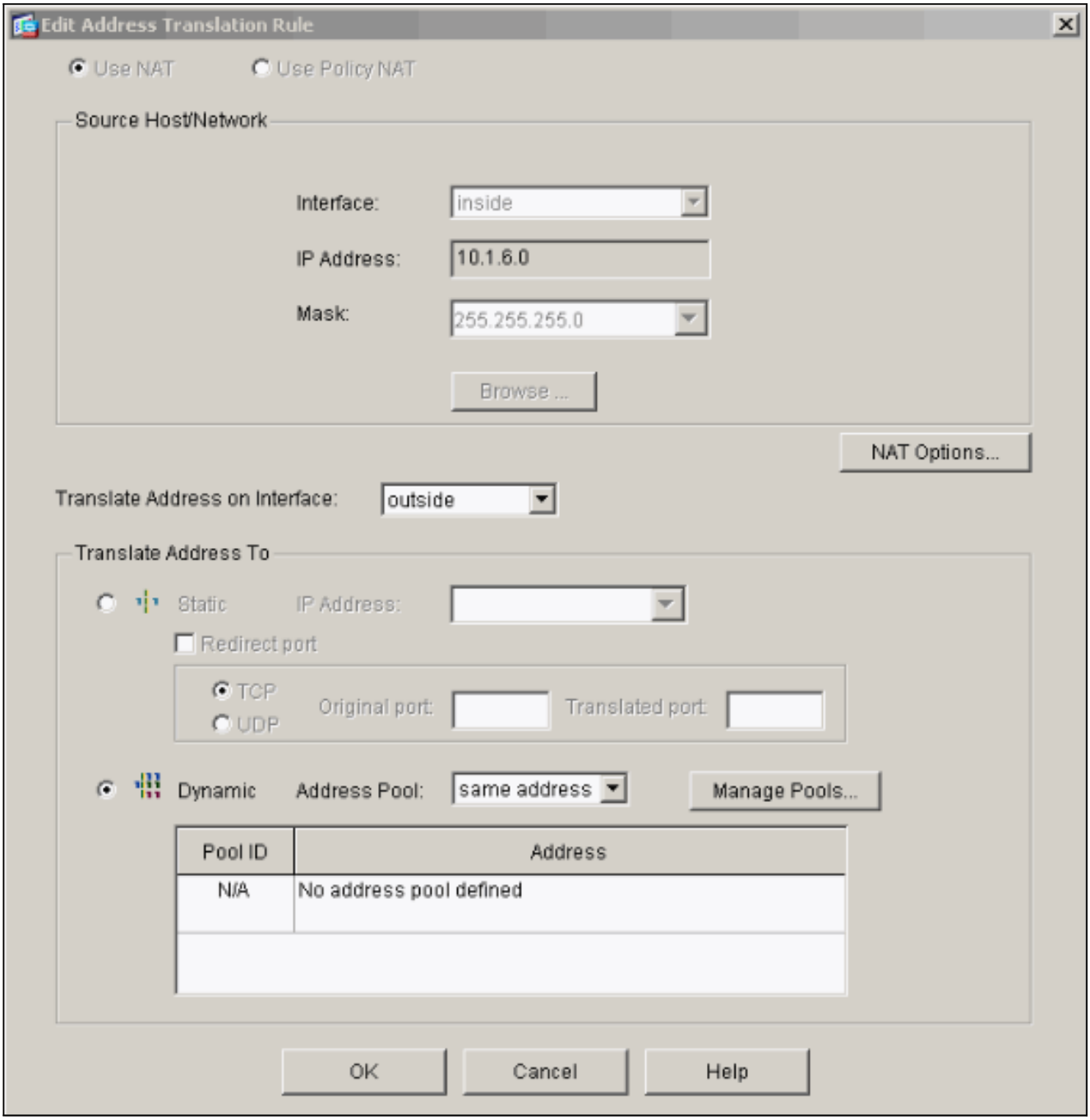
NAT 컨트롤을 사용하고 내부 네트워크에 일부 공용 주소가 있는 경우 이러한 특정 내부 호스트가 변환 없이 외부로 나가도록 하려면 nat **0** 또는 **static** 명령을 사용하여 해당 호스트에 대해 NAT를 비활성화할 수 있습니다.

다음은 nat 명령의 **예입니다**.

```
nat (inside) 0 10.1.6.0 255.255.255.0
```

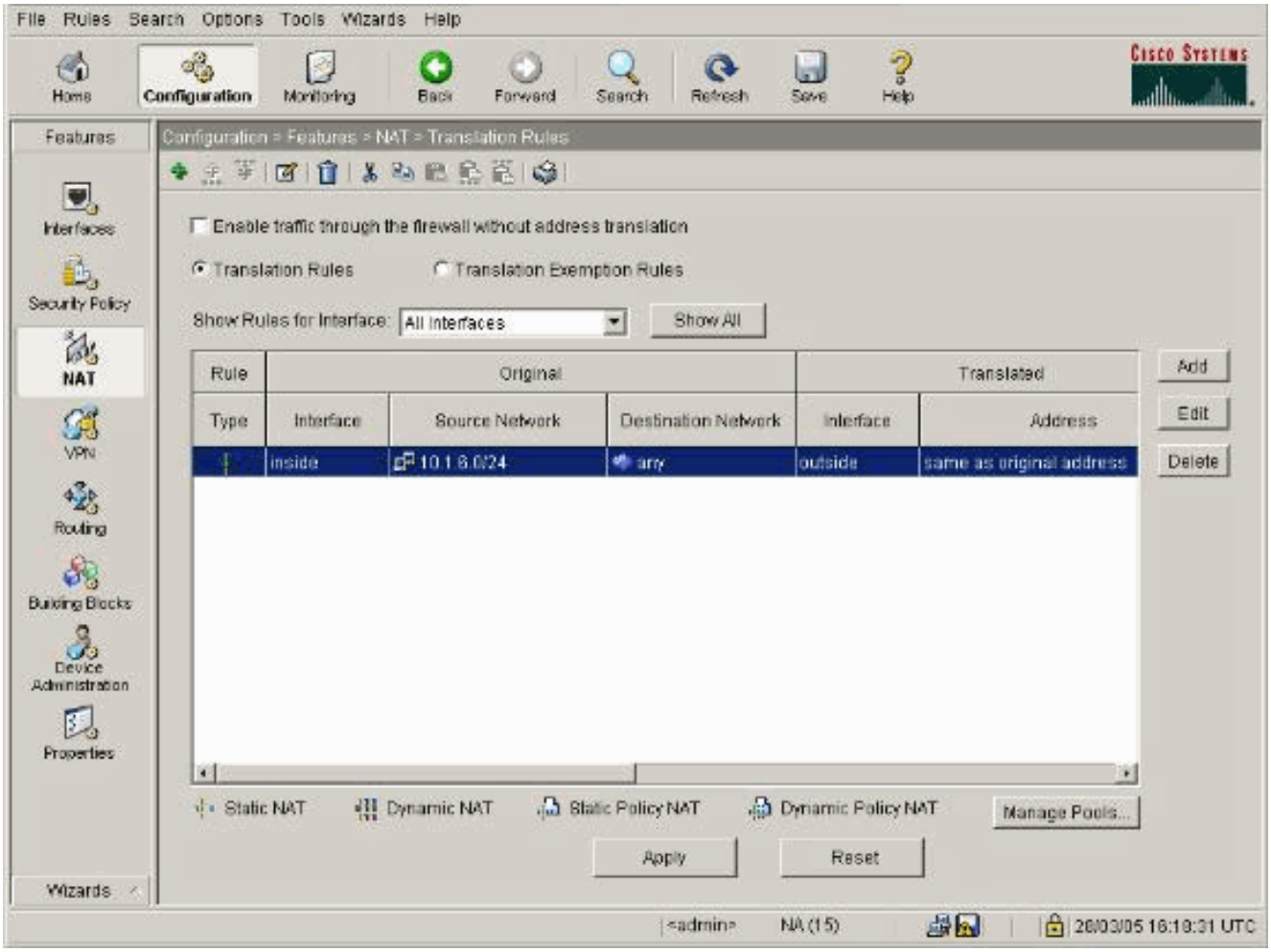
ASDM을 사용하여 특정 호스트/네트워크에 대해 NAT를 비활성화하려면 다음 단계를 완료합니다.

1. Configuration(**컨피그레이션**) > **Features(기능)** > **NAT**를 선택하고 Add(**추가**)를 클릭합니다.
2. **내부**를 소스 인터페이스로 선택하고 고정 변환을 생성할 내부 주소/네트워크를 입력합니다.
3. Dynamic(**동적**)을 선택하고 주소 풀에 대해 동일한 주소를 선택합니다.**확인**을 **클릭합니다**
.



4. Configuration(컨피그레이션) > Features(기능) **> NAT > Translation Rules(변환 규칙)를** 선택하면 새 규칙이 Translation Rules**에** 나타납니다

.

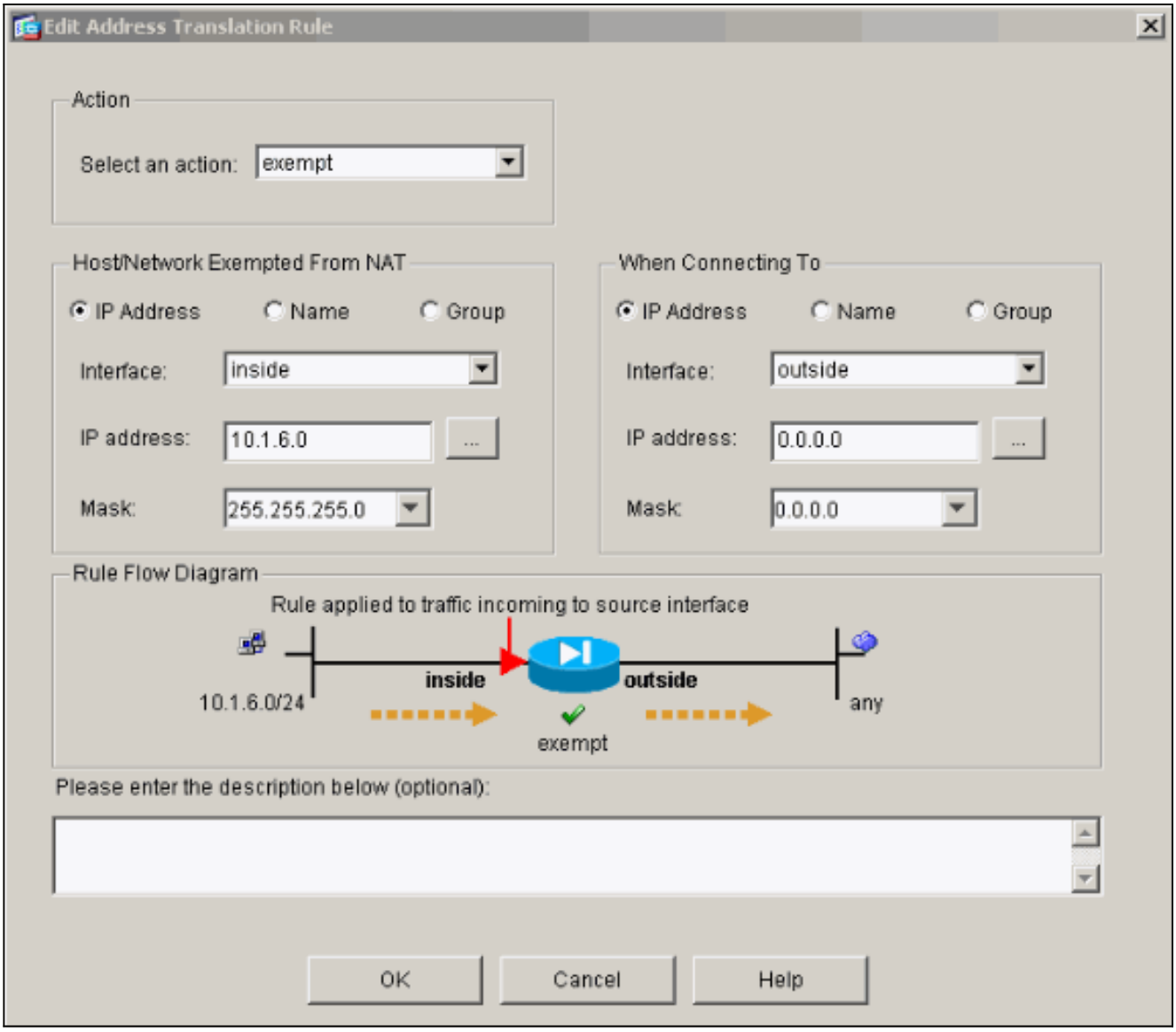


5. 변환해서는 안 되는 트래픽을 더욱 정밀하게 제어할 수 있는 ACL을 사용할 경우(소스/대상에 따라) 다음 명령을 사용합니다.

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

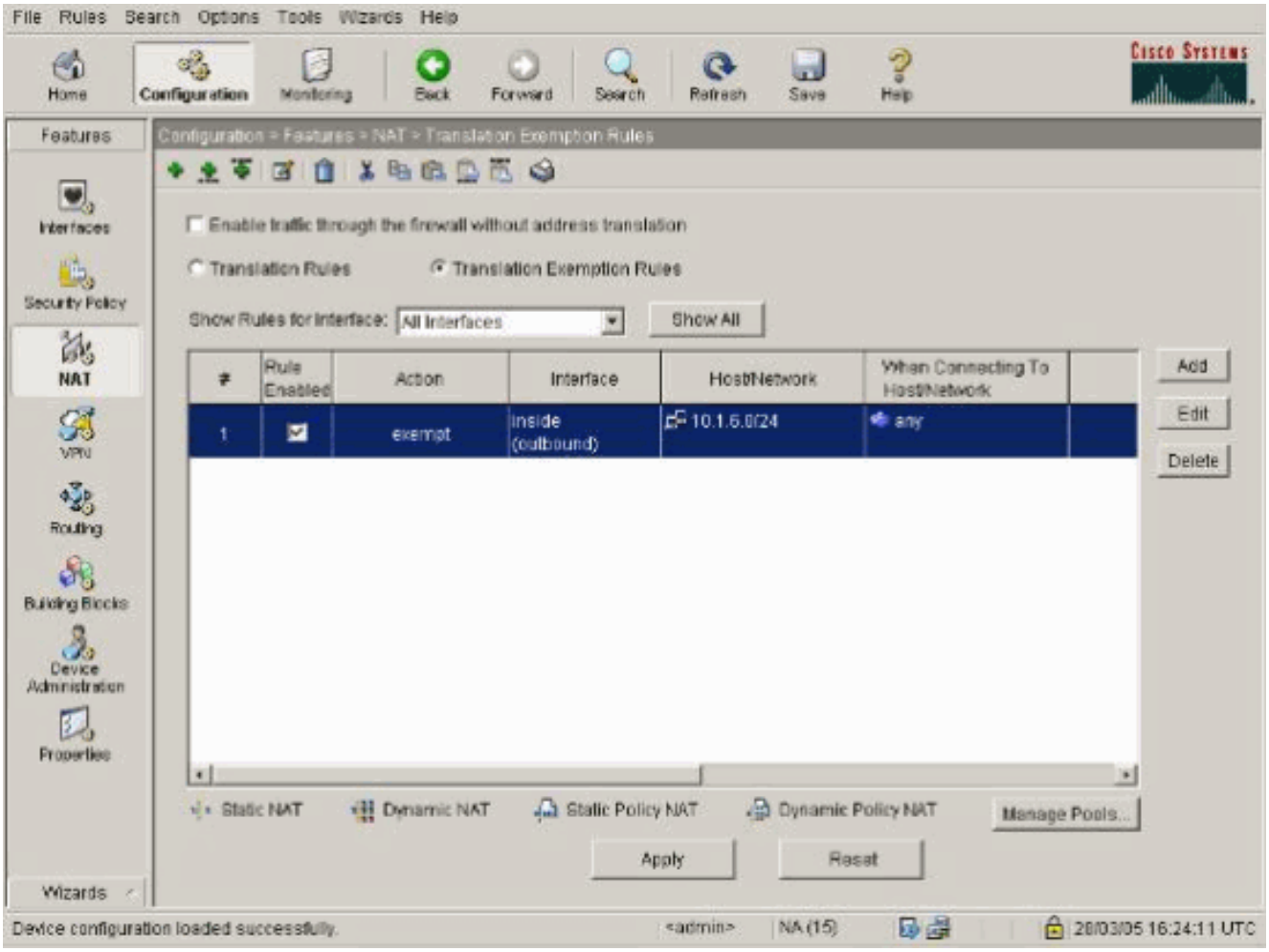
6. ASDM을 사용하고 Configuration(구성) **> Features(기능) > NAT > Translation Rules(변환 규칙)를** 선택합니다.
7. Translation **Exemption Rules(번역 예외 규칙)**를 선택하고 Add(추가)를 **클릭합니다**.이 예에서는 10.1.6.0/24 네트워크에서 변환되지 않도록 트래픽을 제외하는 방법을 보여 줍니다

.



8. 새 규칙을 표시하려면 **Configuration > Features > NAT > Translation Exemption Rules**를 선택합니다

.

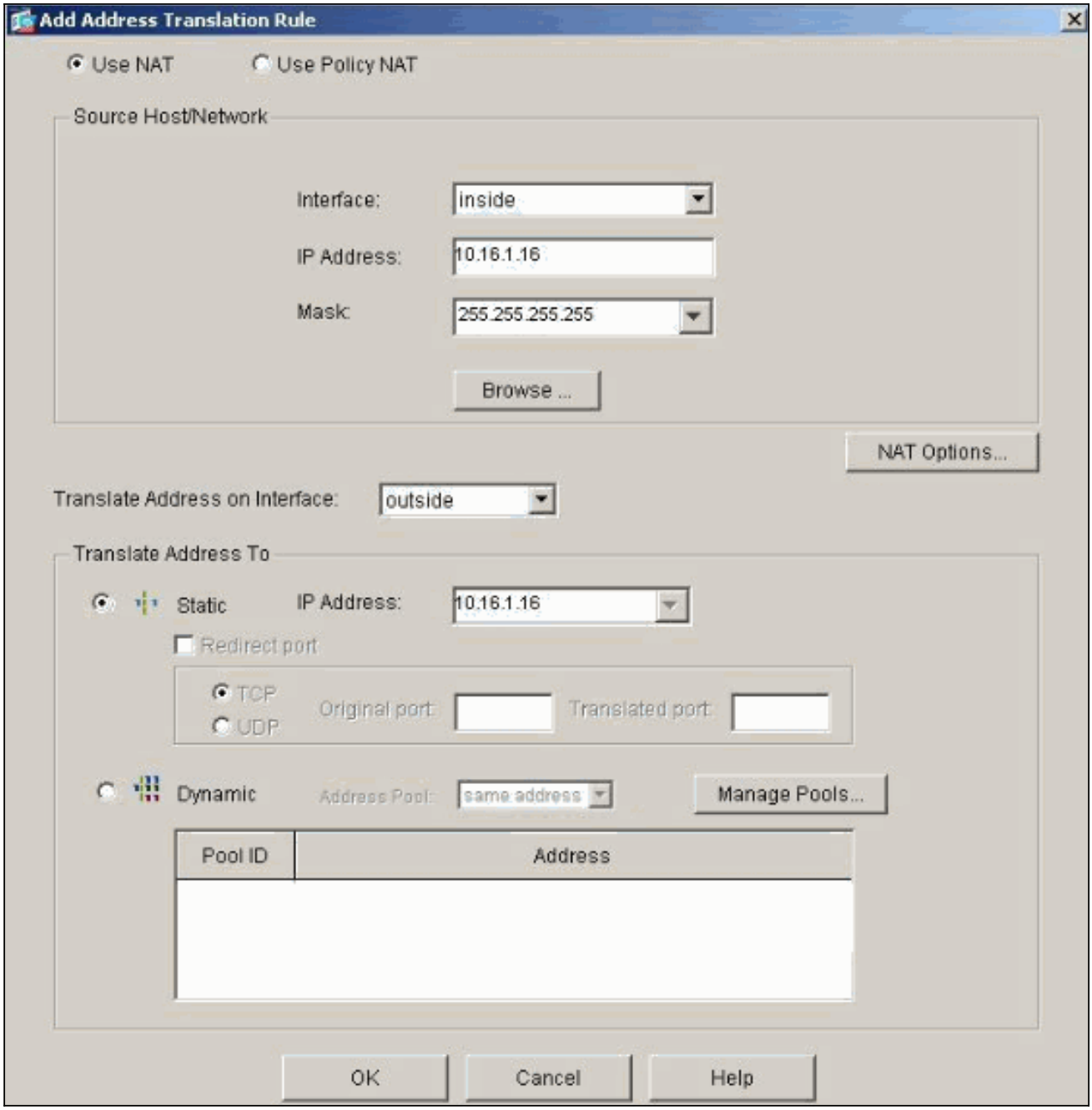


9. 이 예와 같이 웹 서버에 대한 **static** 명령이 변경됩니다.

```
static (inside, outside) 10.16.1.16 10.16.1.16
```

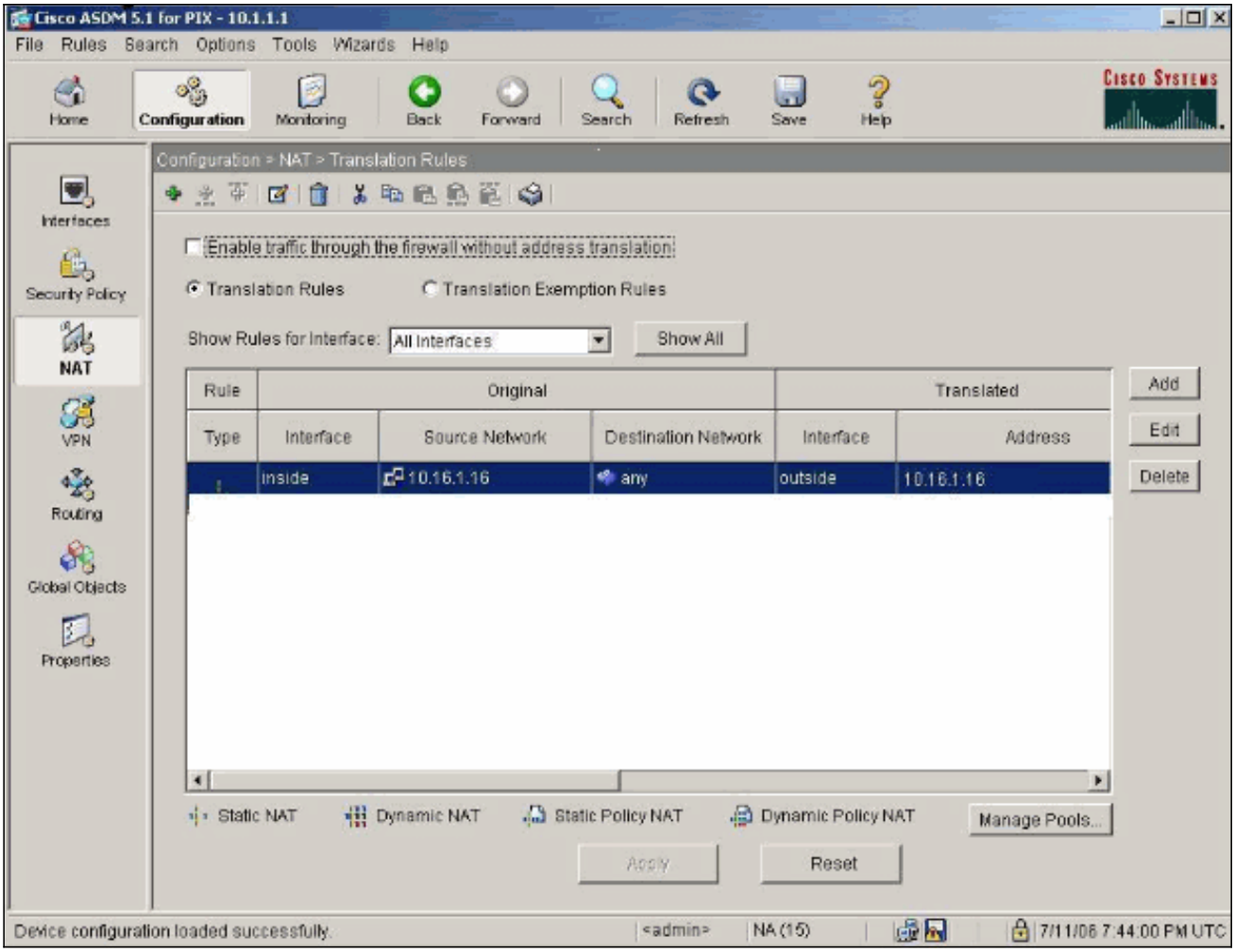
10. ASDM에서 Configuration(구성) **> Features(기능) > NAT > Translation Rules(변환 규칙)**를 선택합니다.
11. Translation **Rules**를 선택하고 Add를 **클릭합니다**.소스 주소 정보를 입력하고 Static을 **선택합니다**.IP Address 필드에 동일한 주소를 입력합니다

.



12. 변환은 Configuration(컨피그레이션) > Features(기능) **> NAT > Translation Rules(변환 규칙)를** 선택할 때 Translation Rules(변환 규칙)**에 나타납니다**

.



13. ACL을 사용하는 경우 다음 명령을 사용합니다.

```
access-list 102 permit tcp any host 10.16.1.16 eq www
access-group 102 in interface outside
```

ASDM에서 ACL의 컨피그레이션에 대한 자세한 내용은 이 문서의 Restrict Inside Hosts Access to Outside Networks 섹션을 참조하십시오.네트워크/마스크를 사용하는 경우와 반대로 네트워크/마스크를 지정할 때 nat **0**을 사용하는 경우의 차이점에 유의하십시오. 네트워크/마스크를 사용하는 ACL에서는 내부 전용 연결을 시작할 수 있습니다.ACL을 nat **0**으로 사용하면 인바운드 또는 아웃바운드 트래픽에 의한 연결 시작을 허용합니다.연결 문제가 발생하지 않도록 하려면 PIX 인터페이스가 서로 다른 서브넷에 있어야 합니다.

정학을 사용한 포트 리디렉션(전달)

PIX 6.0에서는 외부 사용자가 특정 IP 주소/포트에 연결하고 PIX가 트래픽을 적절한 내부 서버/포트로 리디렉션하도록 하기 위해 포트 리디렉션(전달) 기능이 추가되었습니다.static 명령이 수정되었습니다.공유 주소는 고유한 주소, 공유 아웃바운드 PAT 주소 또는 외부 인터페이스와 공유될 수 있습니다.이 기능은 PIX 7.0에서 사용할 수 있습니다.

참고: 공간 제한으로 인해 두 행에 명령이 표시됩니다.

static *[(internal_if_name, external_if_name)] {global_ip|interface}local_ip [netmask mask] [max_conns [emb_limit [norandomseq]]]*

static *[(internal_if_name, external_if_name)] {tcp|udp} {global_ip|interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]*

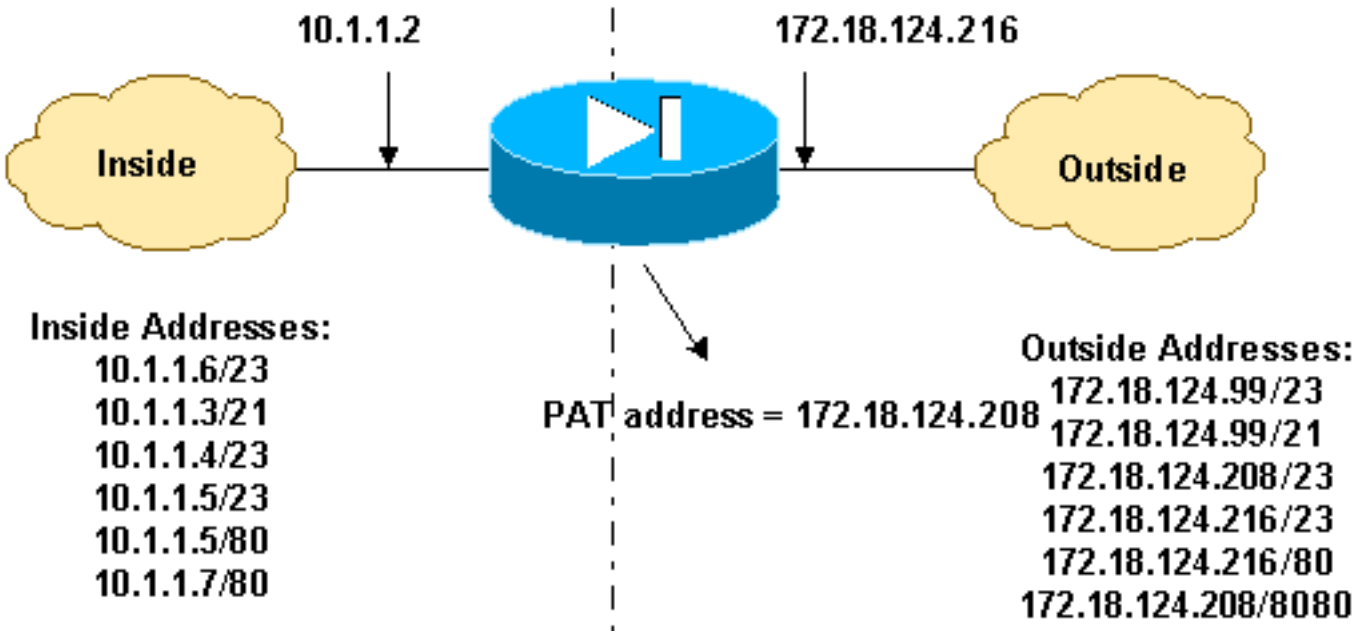
참고: 고정 NAT가 외부 IP(global_IP) 주소를 변환하기 위해 사용하는 경우 변환이 발생할 수 있습니다.따라서 고정 변환에서 IP 주소 대신 키워드 **인터페이스**를 사용합니다.

다음 포트 리디렉션(전달)은 다음 네트워크 예에 나와 있습니다.

- 외부 사용자는 텔넷 요청을 고유한 IP 주소 172.18.124.99으로 디렉션합니다. 이 주소는 PIX가 10.1.1.6으로 리디렉션됩니다.
- 외부 사용자는 고유한 IP 주소 172.18.124.99에 FTP 요청을 전송하며, PIX는 10.1.1.3으로 리디렉션합니다.
- 외부 사용자는 텔넷 요청을 PAT 주소 172.18.124.208에 전달하며, PIX는 10.1.1.4으로 리디렉션합니다.
- 외부 사용자는 PIX가 10.1.1.5으로 리디렉션하는 IP 주소 172.18.124.216 외부의 PIX에 텔넷 요청을 보냅니다.
- 외부 사용자는 PIX가 10.1.1.5으로 리디렉션하는 IP 주소 172.18.124.216 외부의 PIX에 HTTP 요청을 보냅니다.
- 외부 사용자는 PAT 주소 172.18.124.208에 HTTP 포트 8080을 직접 요청합니다. 이 요청은 PIX가 10.1.1.7 포트 80으로 리디렉션됩니다.

이 예에서는 ACL 100을 사용하여 내부 또는 외부에서 일부 사용자의 액세스를 차단합니다. 이 단계는 선택 사항입니다.ACL이 없는 모든 트래픽은 아웃바운드로 허용됩니다.

네트워크 다이어그램 - 포트 리디렉션(전달)



부분 PIX 컨피그레이션 - 포트 리디렉션

이 부분 컨피그레이션은 정적 포트 리디렉션(전달) 사용을 보여줍니다. 포트 리디렉션(전달) 네트워크 다이어그램을 참조하십시오.

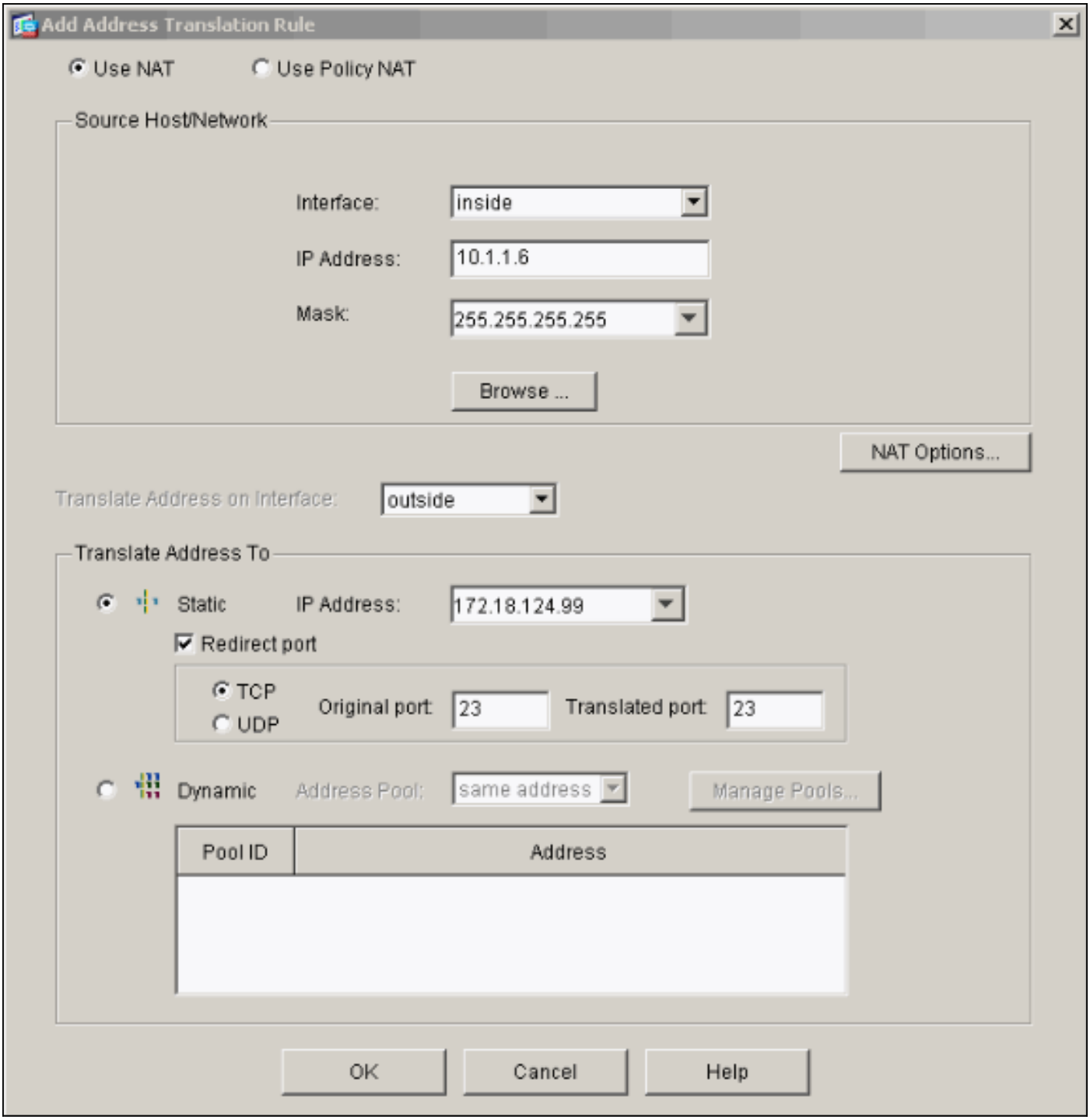
부분 PIX 7.x 구성 - 포트 리디렉션(전달)
`fixup protocol ftp 21` `!--- Use of an outbound ACL is optional.` `access-list 100 permit tcp 10.1.1.0 255.255.255.128 any eq www access-`

```
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

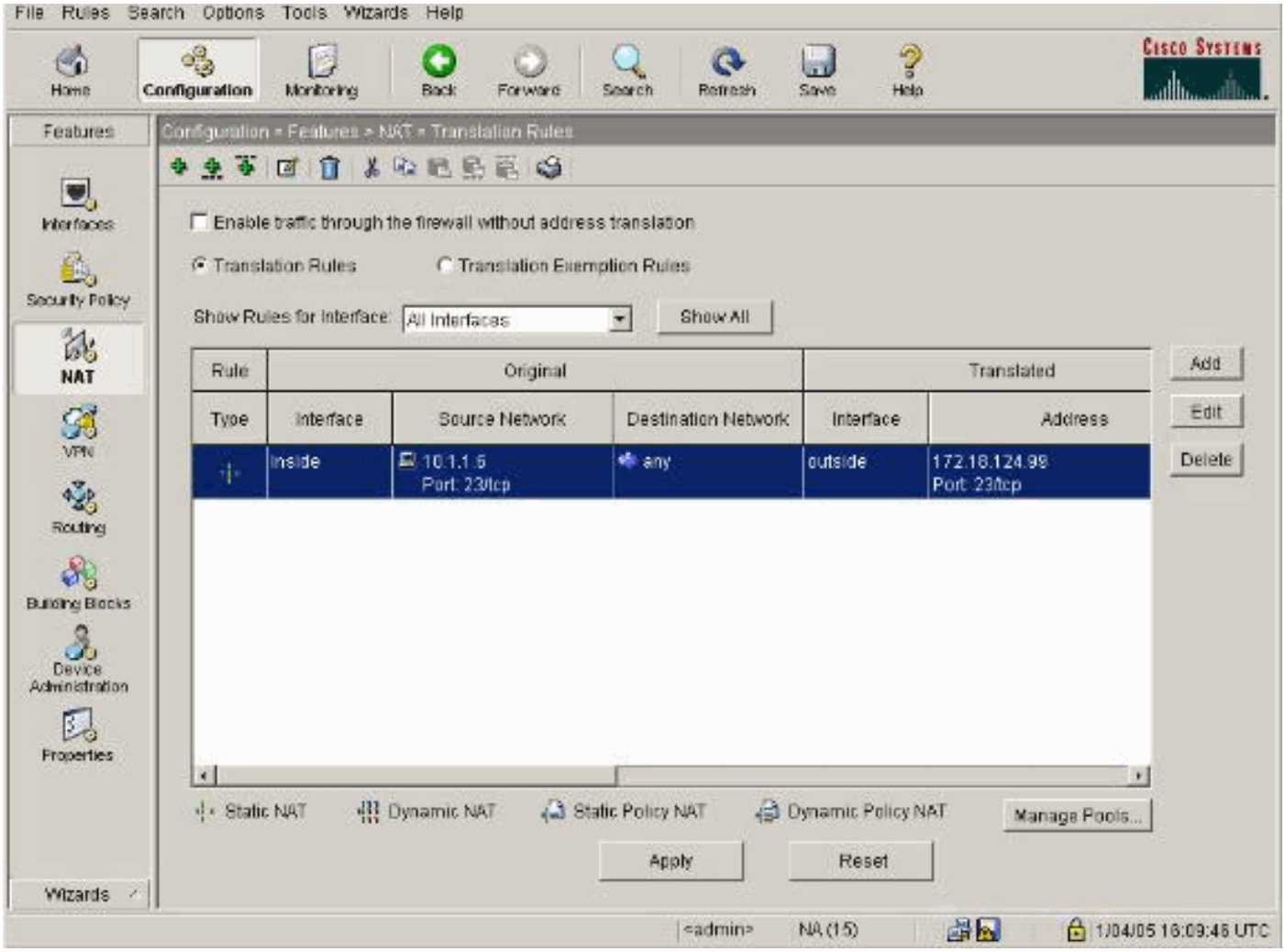
참고: PIX/ASA가 sysopt noproxyarp **outside** 명령으로 구성된 경우 방화벽에서 PIX/ASA의 proxyarp 및 고정 NAT 변환을 수행할 수 없습니다.이 문제를 해결하려면 PIX/ASA 컨피그레이션**에서 sysopt noproxyarp outside** 명령을 제거한 다음 무상 ARP를 사용하여 ARP 엔트리를 업데이트합니다.이를 통해 고정 NAT 엔트리가 제대로 작동합니다.

이 절차는 외부 사용자가 텔넷 요청을 고유한 IP 주소 172.18.124.99에 직접 전달하도록 허용하는 Port Redirection(Forwarding)을 구성하는 방법의 예입니다. 이는 PIX가 10.1.1.6으로 리디렉션합니다.

1. ASDM을 사용하고 Configuration(구성) **> Features(기능) > NAT > Translation Rules(변환 규칙)를** 선택합니다.
2. Translation **Rules를** 선택하고 Add를 **클릭합니다**.
3. Source Host/Network의 경우 내부 IP 주소에 대한 정보를 입력합니다.
4. Translate Address To에서 Static을 선택하고 외부 IP 주소를 입력하고 Redirect **port를 선택합니다**.
5. 사전 변환 및 사후 변환 포트 정보를 입력합니다(이 예에서는 포트 23을 유지 관리합니다). **확인을 클릭합니다**.



변환은 Configuration(컨피그레이션) > Features(기능) **> NAT > Translation Rules(변환 규칙)를** 선택할 때 Translation Rules(변환 규칙)**에 나타납니다**.



Static을 사용하여 TCP/UDP 세션 제한

TCP 또는 UDP 세션을 PIX/ASA에 배치된 내부 서버로 제한하려면 **static** 명령을 사용합니다.

전체 서브넷에 대한 최대 동시 TCP 및 UDP 연결 수를 지정합니다.기본값은 0이며, 이는 무제한 연결을 의미합니다(유휴 연결은 timeout conn 명령에 지정된 유휴 시간 제한 후 **닫힙니다**). 이 옵션은 외부 NAT에는 적용되지 않습니다.보안 어플라이언스는 상위 보안 인터페이스에서 하위 보안 인터페이스로의 연결만 추적합니다.

원시 연결 수를 제한하면 DoS 공격으로부터 보호됩니다.보안 어플라이언스는 초기 제한을 사용하여 TCP 가로채기를 트리거합니다. 이는 TCP SYN 패킷으로 인터페이스를 플러딩하여 시행된 DoS 공격으로부터 내부 시스템을 보호합니다.원시 연결은 소스와 대상 간의 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다.이 옵션은 외부 NAT에는 적용되지 않습니다.TCP 가로채기 기능은 보안 수준이 높은 호스트 또는 서버에만 적용됩니다.외부 NAT에 대한 원시 제한을 설정하면 원시 제한이 무시됩니다.

예를 들면 다음과 같습니다.

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100
!--- The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is
500, default is 0 which means unlimited !--- connections. Idle connections are closed after the
time specified !--- by the timeout conn command !--- The maximum number of embryonic connections
per host is 100.
```

%PIX-3-201002:{static|xlate} global_address에 너무 많은 연결이 있습니다.conn nconn

연결 관련 메시지입니다.이 메시지는 지정된 고정 주소에 대한 최대 연결 수를 초과할 때 기록됩니다.econns 변수는 최대 원시 연결 수이며 nconn은 정적 또는 xlate에 허용되는 최대 연결 수입니다.

권장되는 작업은 정적 주소에 대한 연결에 적용되는 제한을 확인하기 위해 **show static** 명령을 사용하는 것입니다.제한을 구성할 수 있습니다.

%ASA-3-201011:인터페이스 Outside에서 인바운드 패킷의 연결 제한이 10.1.26.51/2393에서 10.0.86.155/135까지 10.00/1000을 초과했습니다.

이 오류 메시지는 Cisco 버그 ID CSCsg52106(등록된 고객만 해당) 때문입니다. 자세한 내용은 이 버그를 참조하십시오.

시간 기반 액세스 목록

시간 범위 생성은 디바이스에 대한 액세스를 제한하지 않습니다.**time-range** 명령은 시간 범위만 정의합니다.시간 범위가 정의되면 트래픽 규칙 또는 작업에 연결할 수 있습니다.

시간 기반 ACL을 구현하려면 **time-range** 명령을 사용하여 요일과 주의 특정 시간을 정의합니다.그런 다음 **access-list extended time-range** 명령을 **사용하여** 시간 범위를 ACL에 바인딩합니다.

시간 범위는 보안 어플라이언스의 시스템 클럭에 의존합니다.그러나 이 기능은 NTP 동기화에서 가장 잘 작동합니다.

시간 범위를 생성하고 시간 범위 컨피그레이션 모드를 입력한 후 **absolute** 및 **periodic** 명령으로 시간 범위 매개변수를 정의할 수 있습니다.**time-range** 명령 absolute 및 periodic 키워드에 대한 기본 설정을 복원하려면 time-range 컨피그레이션 모드에서 **default** 명령을 사용합니다.

시간 기반 ACL을 구현하려면 **time-range** 명령을 사용하여 요일과 주의 특정 시간을 정의합니다.그런 다음 **access-list extended** 명령을 **사용하여** 시간 범위를 ACL에 바인딩합니다.다음 예에서는 "Sales"라는 ACL을 "New York Minute"라는 시간 범위에 바인딩합니다.

이 예에서는 "New York Minute"라는 시간 범위를 만들고 시간 범위 컨피그레이션 모드를 시작합니다.

```
hostname(config)#time-range New_York_Minute
hostname(config-time-range)#periodic weekdays 07:00 to 19:00
hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute
hostname(config)#access-group Sales in interface inside
```

기술 지원 케이스를 열 경우 수집할 정보

여전히 도움이 필요하고 Cisco 기술 지원 서비스에 케이스를 열려면 PIX Security Appliance 문제 해결을 위해 이 정보를 포함해야 합니다.
• 문제 설명 및 관련 토폴로지 세부사항 • 케이스를 열기 전에 트러블슈팅에 사용한 단계. • **show tech-support** 명령의 출력입니다.

- logging buffered debugging 명령이 실행된 후 **show log** 명령의 출력 또는 문제를 보여 주는 콘솔 캡처(사용 가능한 경우)

수집된 데이터를 압축되지 않은 일반 텍스트 형식(.txt)으로 케이스에 첨부합니다. TAC Service Request Tool(등록된 고객만)에서 케이스에 정보를 첨부할 수 있습니다. TAC 서비스 요청 툴(등록된 고객만 해당)에 액세스할 수 없는 경우 메시지 제목 줄에 케이스 번호가 포함된 이메일 첨부 파일의 정보를 attach@cisco.com으로 보낼 수 있습니다.

관련 정보

- PIX Security Appliance 지원 페이지
- PIX 명령 참조
- Cisco ASDM(Adaptive Security Device Manager) 문제 해결 및 알림
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems