PIX/ASA 7.x 및 FWSM:NAT 및 PAT 문

목차

소개

이 문서에서는 Cisco PIX/ASA Security Appliances의 기본 NAT(Network Address Translation) 및 PAT(Port Address Translation) 컨피그레이션의 예를 제공합니다.간소화된 네트워크 다이어그램이 제공됩니다.자세한 내용은 PIX/ASA 소프트웨어 버전에 대한 PIX/ASA 설명서를 참조하십시오.

PIX **5.x 이상**의 nat, **전역**,**정적**,**배관** 및 **access-list 명령 및 포트 리디렉션(전달)에** 대한 자세한 내용은 PIX에서 nat, global, static**, and access-list 명령 및 Port Redirection (Forwarding)을 참조하십시오.**

Cisco Secure PIX Firewall의 기본 NAT 및 PAT 컨피그레이션의 예에 대한 자세한 내용은 Cisco Secure PIX Firewall에서 NAT 및 PAT 문 사용을 참조하십시오.

ASA 버전 8.3 이상의 NAT 컨피그레이션에 대한 자세한 내용은 NAT 정보를 참조하십시오.

참고: 투명 모드의 NAT는 PIX/ASA 버전 8.x에서 지원됩니다.자세한 내용은 투명 모드의 NAT를 참조하십시오.

사전 요구 사항

요구 사항

이 문서의 독자는 Cisco PIX/ASA Security Appliance에 대해 잘 알고 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco PIX 500 Series Security Appliance Software 버전 7.0 이상을 기반으로 합니다.

참고: 이 문서는 PIX/ASA 버전 8.x로 수정되었습니다.

참고: 이 문서에서 사용되는 명령은 FWSM(Firewall Service Module)에 적용됩니다.

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 규칙을 참조하십시오.

nat-control 명령

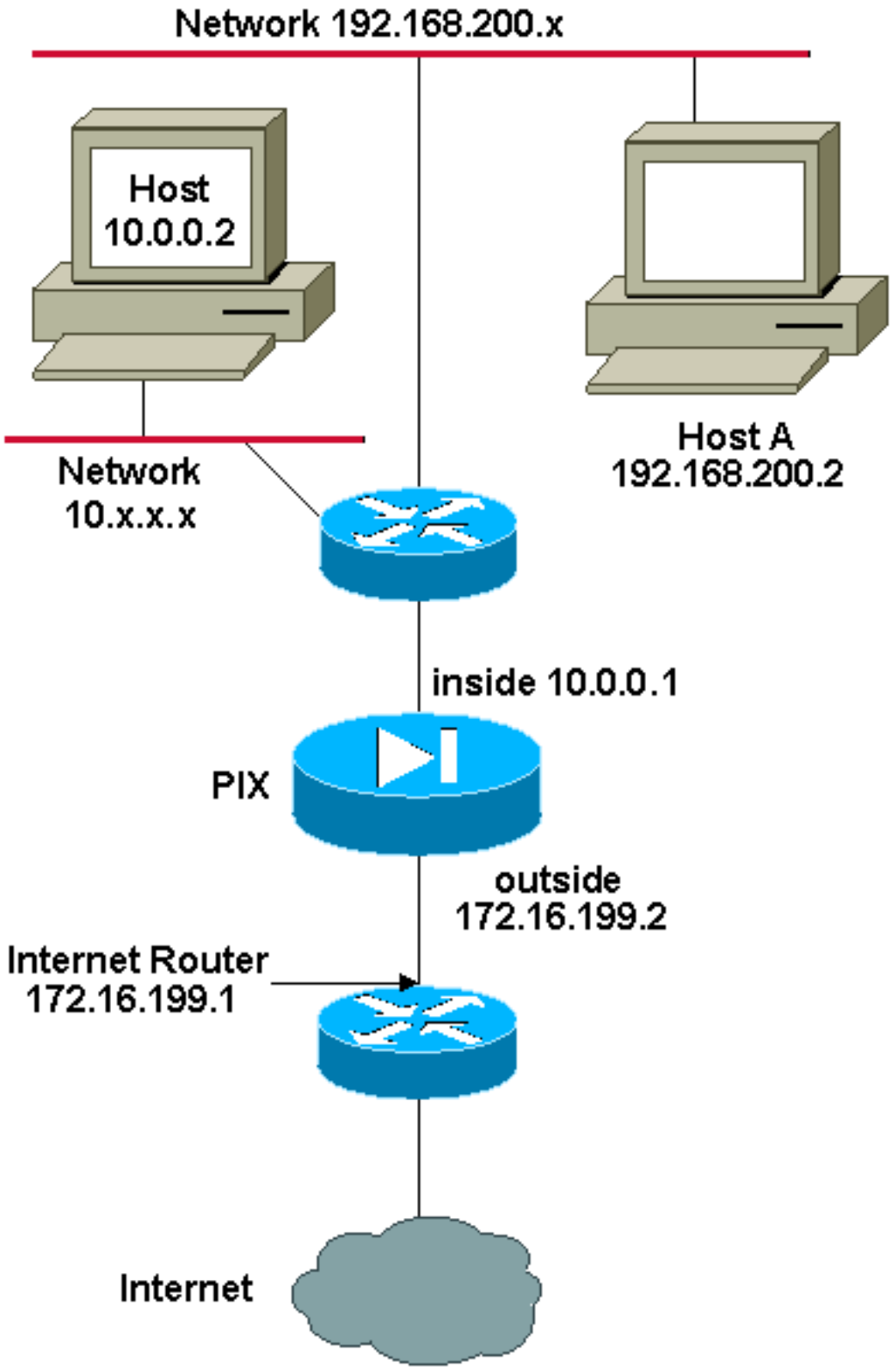
PIX/ASA의 nat-**control** 명령은 방화벽을 통과하는 모든 트래픽에 해당 트래픽이 방화벽을 통과하도록 특정 변환 항목(일치하는 **전역** 또는 **static** 문이 있는 **nat 문**)이 있어야 한다고 지정합니다.nat-**control** 명령은 변환 동작이 7.0 이전 버전의 PIX 방화벽 버전과 동일한지 확인합니다. PIX/ASA 버전 7.0 이상의 기본 컨피그레이션은 **no nat-control** 명령의 사양입니다.PIX/ASA 버전 7.0 이상에서는 nat-**control** 명령을 실행할 때 이 동작을 변경할 수 있습니다.

nat **제어**가 비활성화된 경우 PIX/ASA는 컨피그레이션에서 특정 변환 항목이 없는 상위 보안 인터페이스에서 하위 인터페이스로 패킷을 전달합니다.낮은 보안 인터페이스에서 상위 인터페이스로 트래픽을 전달하려면 액세스 목록을 사용하여 트래픽을 허용합니다.그런 다음 PIX/ASA가 트래픽을 전달합니다.이 문서에서는 nat-control이 활성화된 PIX/ASA 보안 어플라이언스 동작**에** 초점을 맞춥니다.

참고: PIX/ASA에서 nat-control 문을 제거하거나 비활성화하려면 보안 어플라이언스에서 모든 NAT 문을 제거해야 합니다.일반적으로 NAT 제어를 해제하기 전에 NAT를 제거해야 합니다.PIX/ASA에서 NAT 문이 예상대로 작동하도록 재구성해야 합니다.

NAT 0을 사용하는 다중 NAT 문

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 ISP는 네트워크 관리자에게 172.16.199.1~172.16.199.63 범위의 주소를 제공합니다. 네트워크 관리자는 인터넷 라우터의 내부 인터페이스에 172.16.199.1을 할당하고 PIX/ASA의 외부 인터페이스172.16.199.2 할당합니다.

네트워크 관리자는 192.168.200.0/24네트워크에 클래스 C 주소를 이미 할당했으며 인터넷에 액세스하기 위해 이러한 주소를 사용하는 워크스테이션이 있습니다.이 워크스테이션은 번역할 주소가 아닙니다.그러나 새 워크스테이션에는 10.0.0.0/8 네트워크에 주소가 할당되며 번역할 필요가 있습

니다.

이 네트워크 설계를 수용하려면 네트워크 관리자가 PIX/ASA 컨피그레이션에서 NAT 문 2개와 글로벌 풀 1개를 다음 출력에 표시된 대로 사용해야 합니다.

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

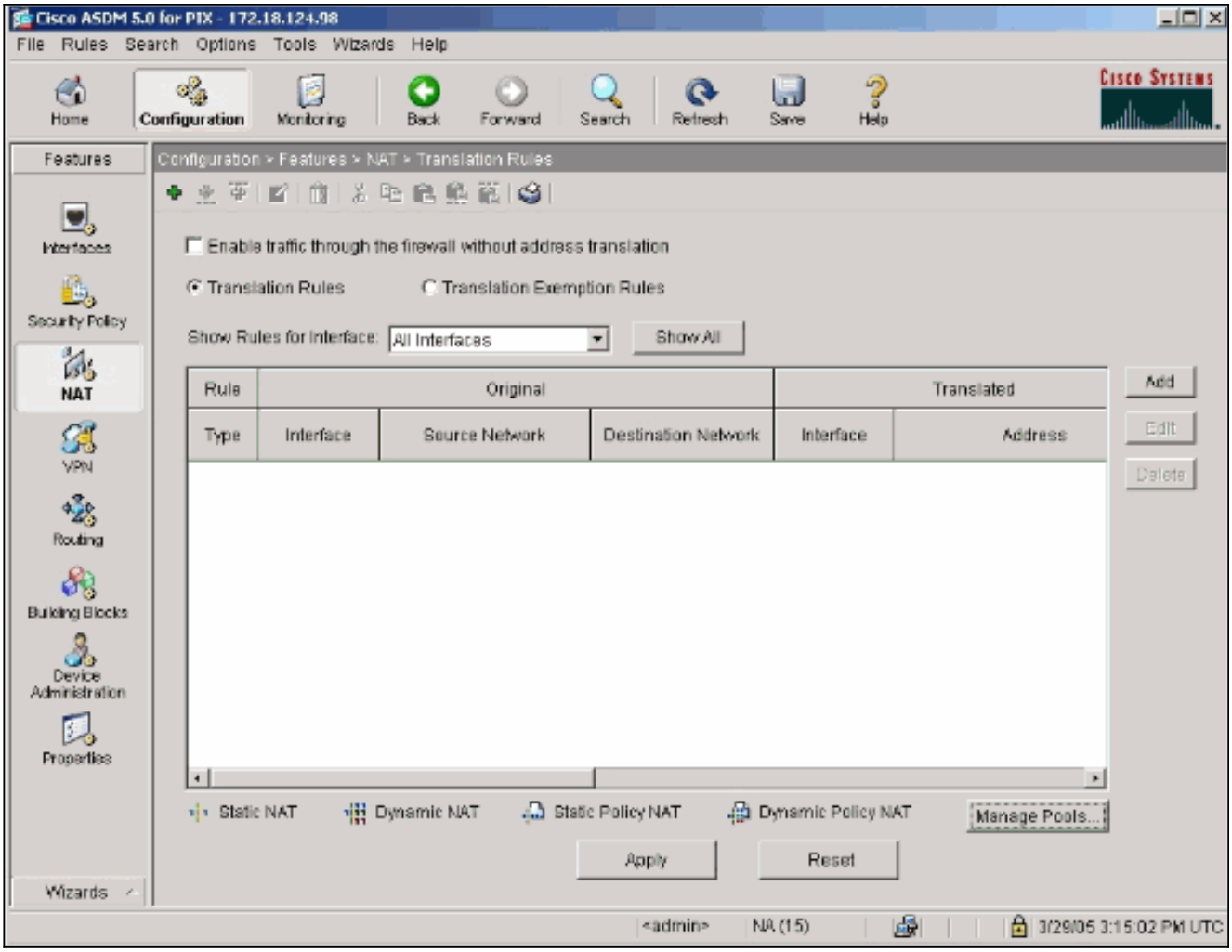
이 컨피그레이션은 192.168.200.0/24 네트워크의 아웃바운드 트래픽의 소스 주소를 변환하지 않습니다.10.0.0.0/8 네트워크의 소스 주소를 172.16.199.3~172.16.199.62 범위의 주소로 변환합니다.

이러한 단계에서는 ASDM(Adaptive Security Device Manager)을 사용하여 동일한 컨피그레이션을 적용하는 방법에 대해 설명합니다.

참고: CLI 또는 ASDM을 통해 모든 컨피그레이션 변경을 수행합니다.컨피그레이션 변경에 CLI와 ASDM을 모두 사용하면 ASDM에서 적용하는 것과 관련하여 매우 잘못된 동작이 발생합니다.이는 버그가 아니지만 ASDM의 작동 방식 때문에 발생합니다.

참고: ASDM을 열면 PIX/ASA에서 현재 컨피그레이션을 가져오고 변경 사항을 적용하고 적용할 때 해당 컨피그레이션에서 작동합니다.ASDM 세션이 열려 있는 동안 PIX/ASA에서 변경이 이루어진 경우 ASDM은 더 이상 PIX/ASA의 현재 컨피그레이션인 "생각하는 것"과 함께 작동하지 않습니다 .CLI를 통해 컨피그레이션을 변경하는 경우 ASDM 세션을 닫아야 합니다.GUI를 통해 작업하려면 ASDM을 다시 엽니다.

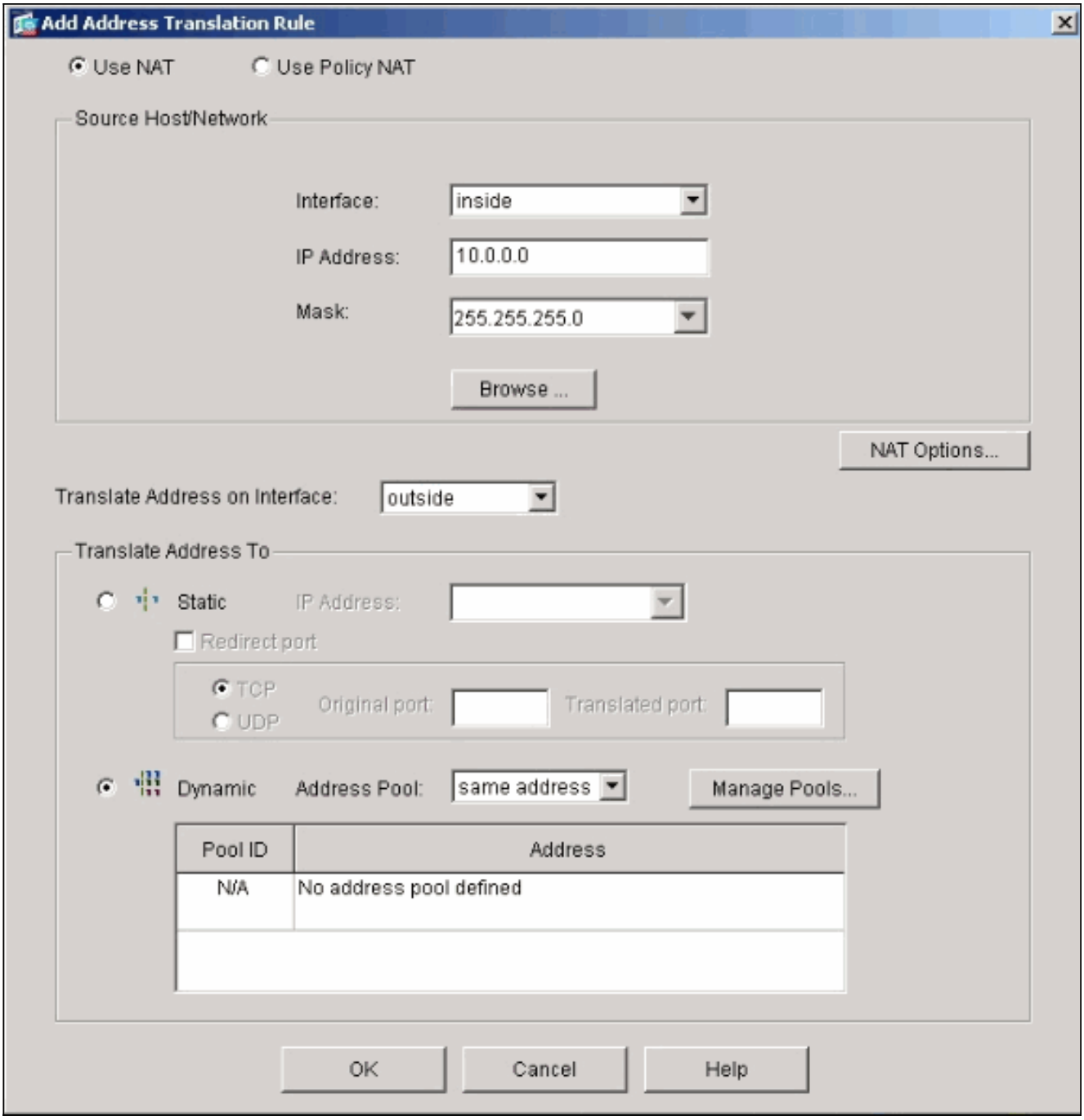
1. ASDM을 시작하고 Configuration(컨피그레이션) 탭으로 이동한 다음 NAT를 **클릭합니다**.
2. 새 규칙을 생성하려면 Add를 클릭합니다
   .



사용자가 이 NAT 항목에 대한 NAT 옵션을 변경할 수 있는 새 창이 나타납니다.이 예에서는 특정 10.0.0.0/24 네트워크에서 소싱된 내부 인터페이스에 도착하는 패킷에 대해 NAT를 수행합니다.PIX/ASA는 이러한 패킷을 외부 인터페이스의 동적 IP 풀로 변환합니다.NAT에 대한 트래픽을 설명하는 정보를 입력한 후 변환된 트래픽에 대한 IP 주소 풀을 정의합니다.

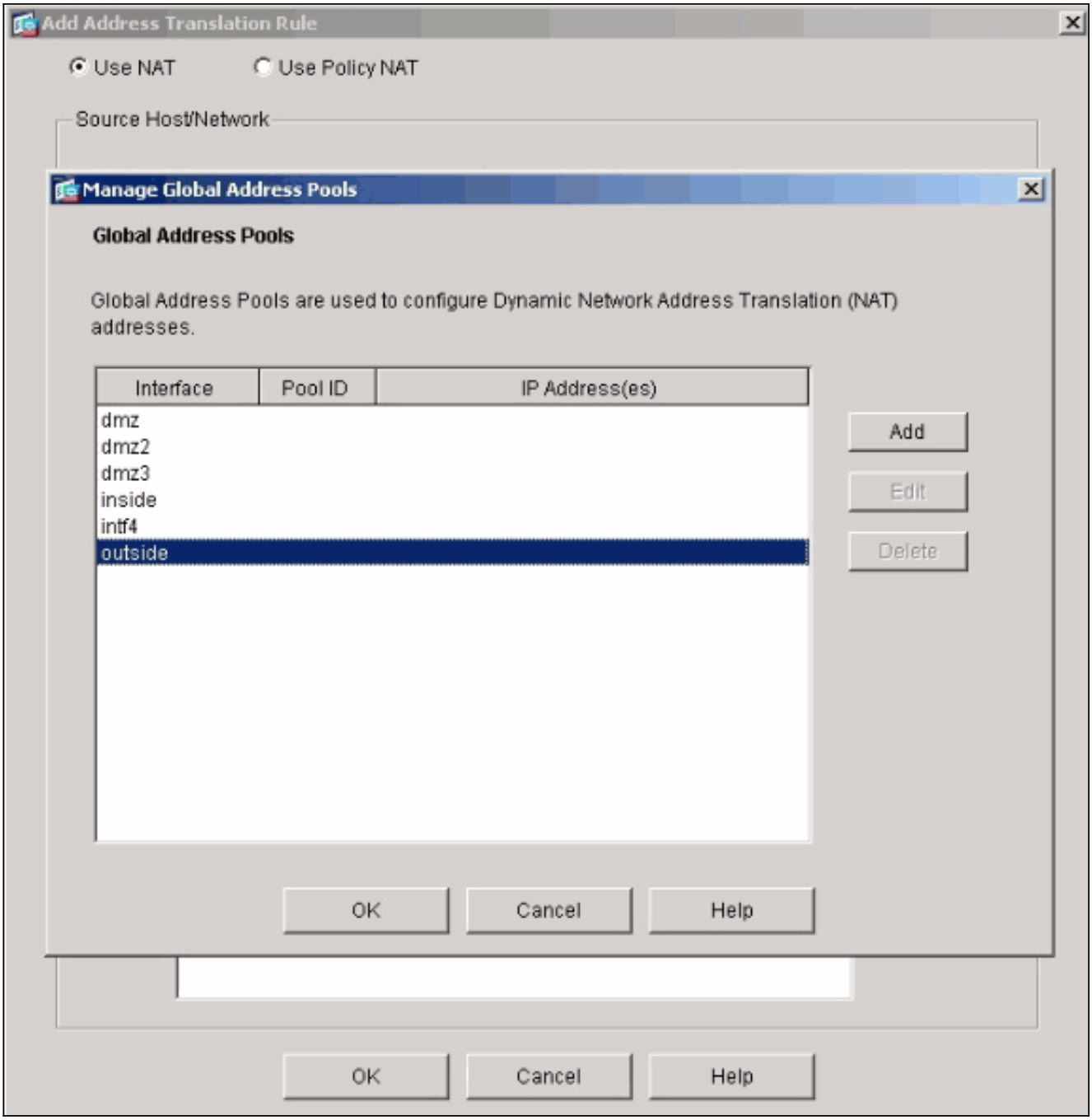
3. 새 IP 풀을 추가하려면 Manage Pools를 클릭합니다

.



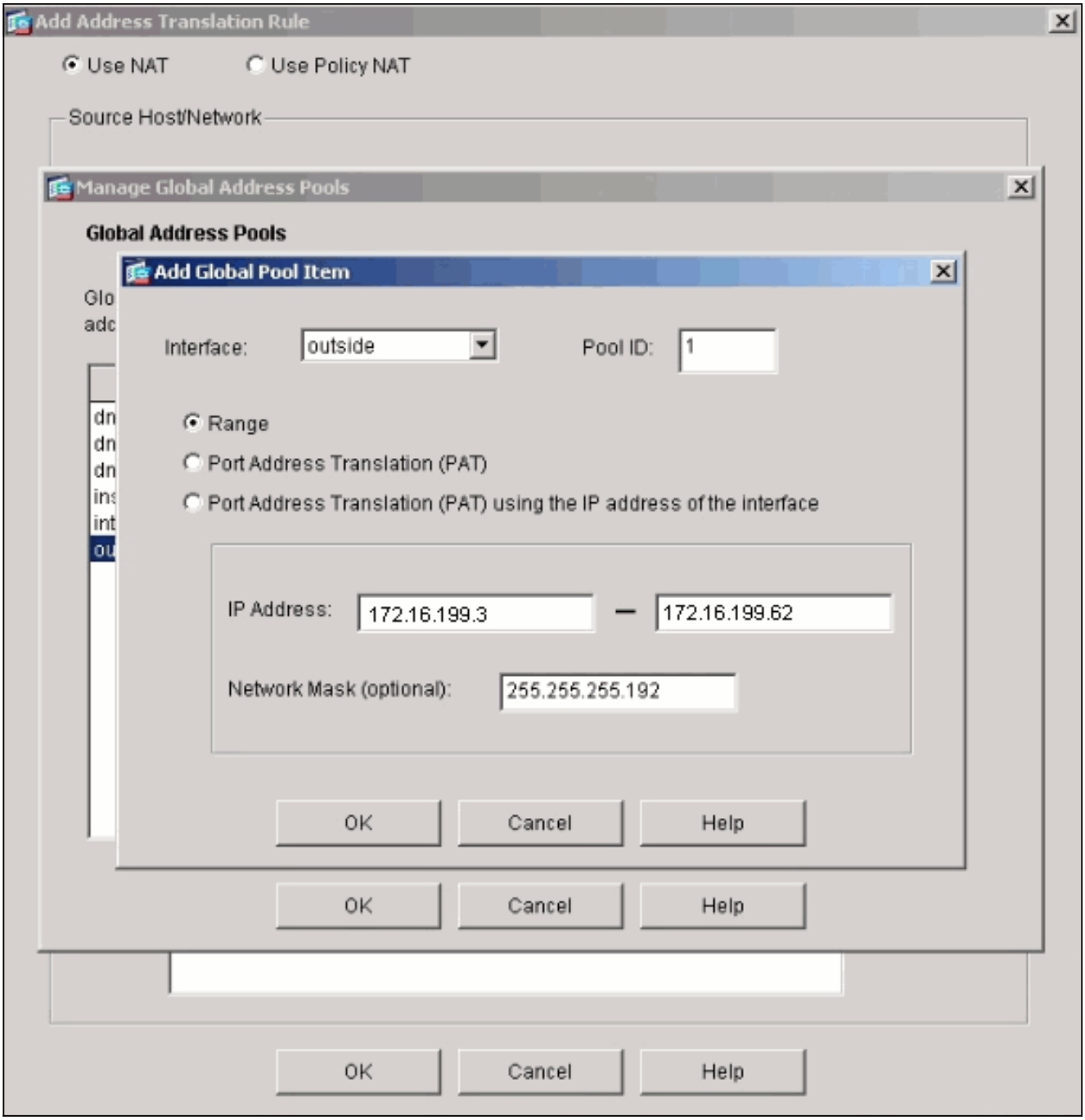
4. **outside**를 선택하고 Add를 **클릭합니다**

.

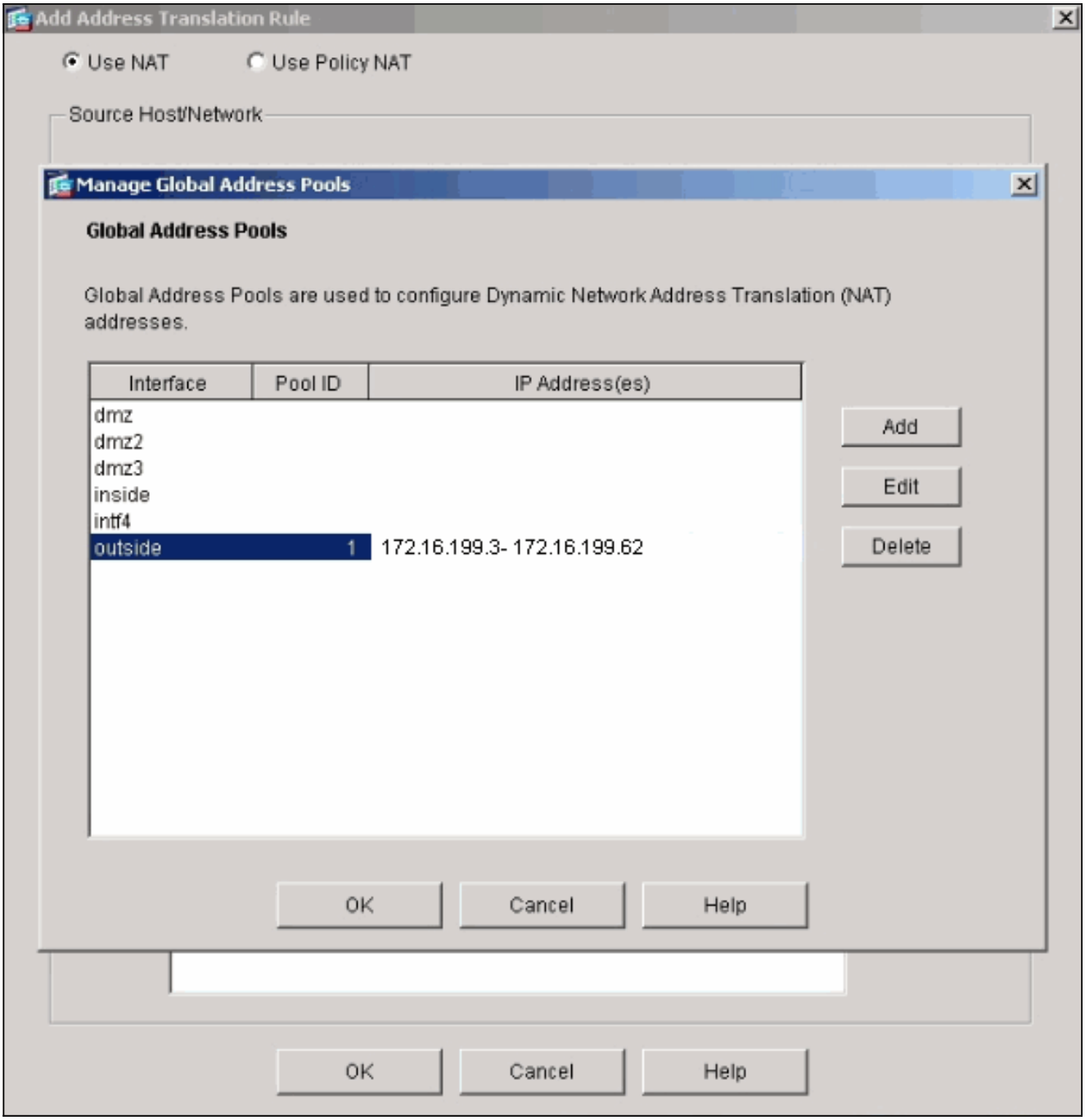


5. 풀의 IP 범위를 지정하고 풀에 고유한 정수 ID 번호를 지정합니다

.

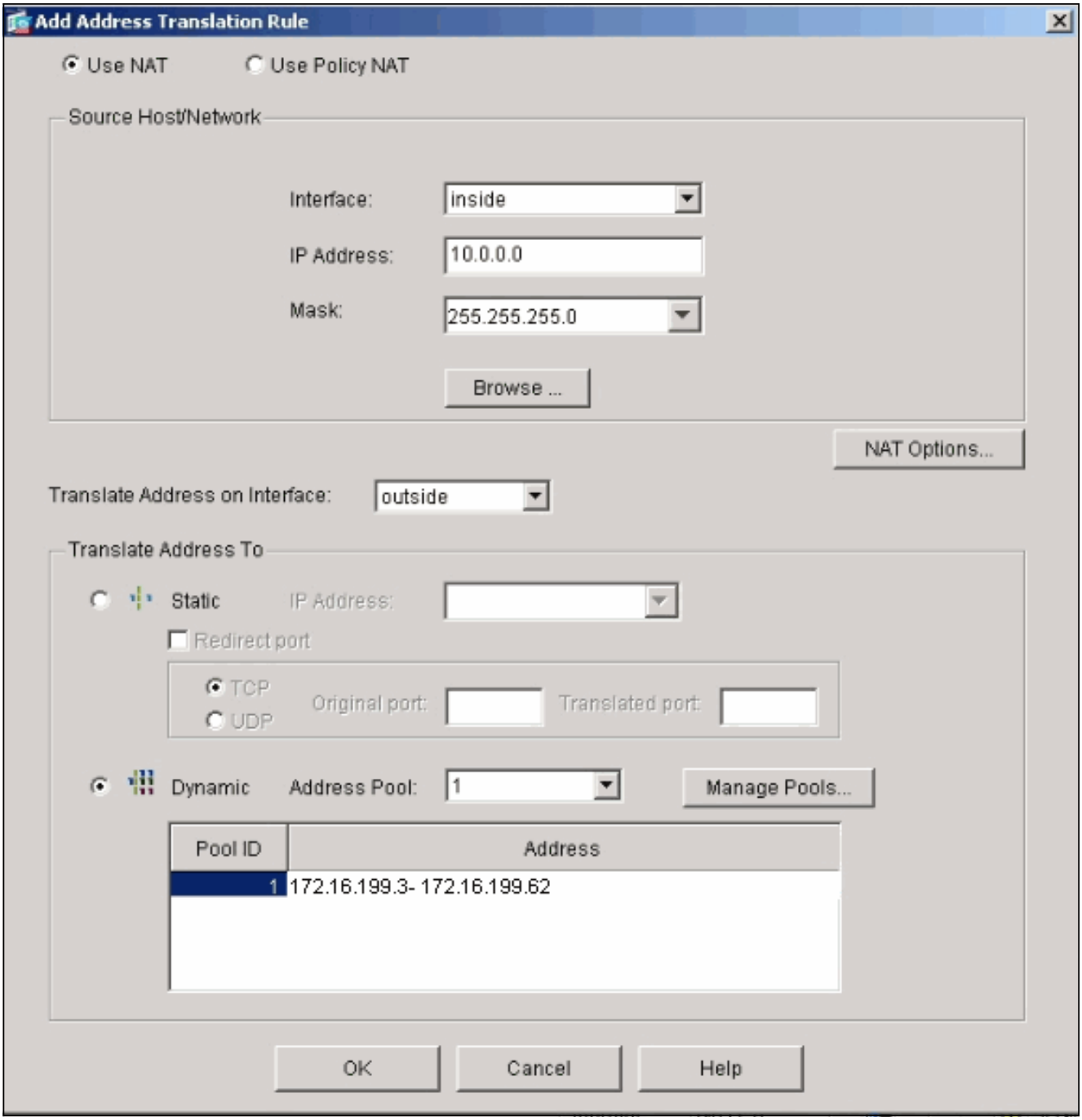


6. 적절한 값을 입력하고 확인을 **클릭합니다**.외부 인터페이스에 대해 새 풀이 정의됩니다
.



7. 풀을 정의한 후 **OK**를 클릭하여 NAT Rule 컨피그레이션 창으로 돌아갑니다.Address Pool(주소 풀) 드롭다운 목록에서 방금 생성한 올바른 풀을 선택해야 합니다

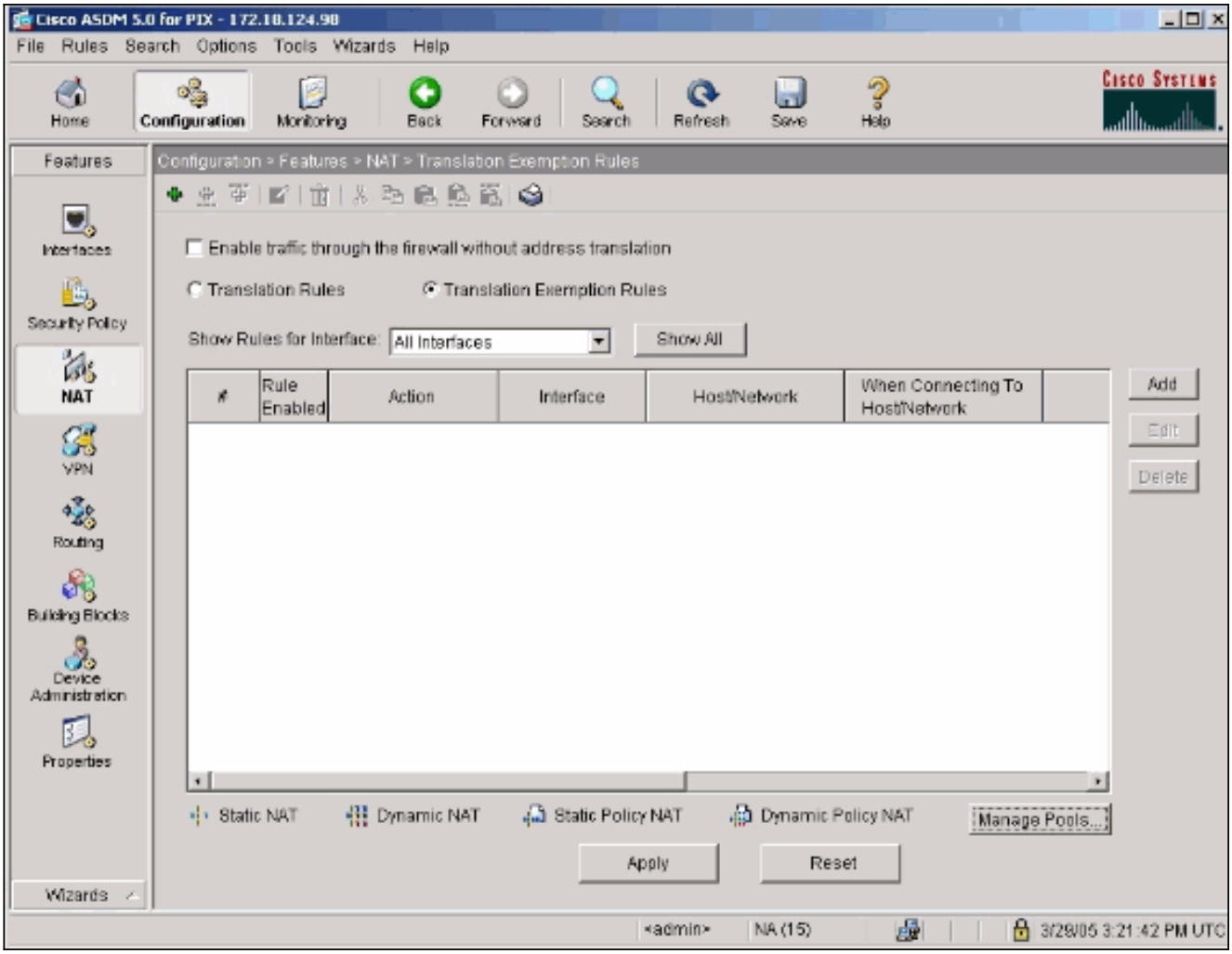
.



이제 보안 어플라이언스를 통해 NAT 변환을 생성했습니다.그러나 NAT에 연결되지 않는 트래픽을 지정하는 NAT 엔트리를 생성해야 합니다.

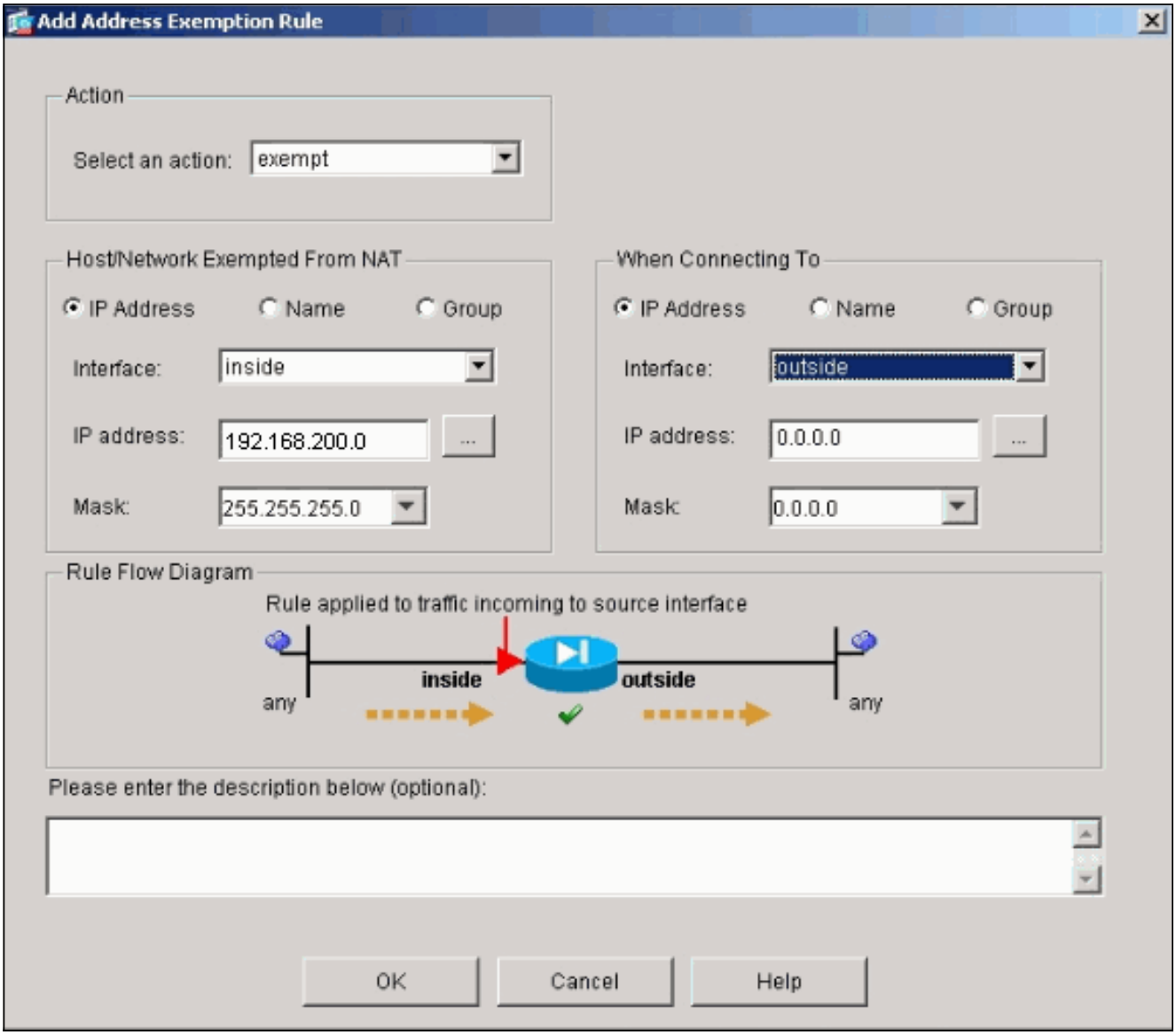
8. 창 맨 위에 있는 **Translation Exemption Rules**를 클릭한 다음 **Add**를 클릭하여 새 규칙을 생성합니다

.



9. *내부* 인터페이스를 소스로 선택하고 **192.168.200.0/24** 서브넷을 지정합니다."연결 시" 값을 기본값으로 둡니다

.



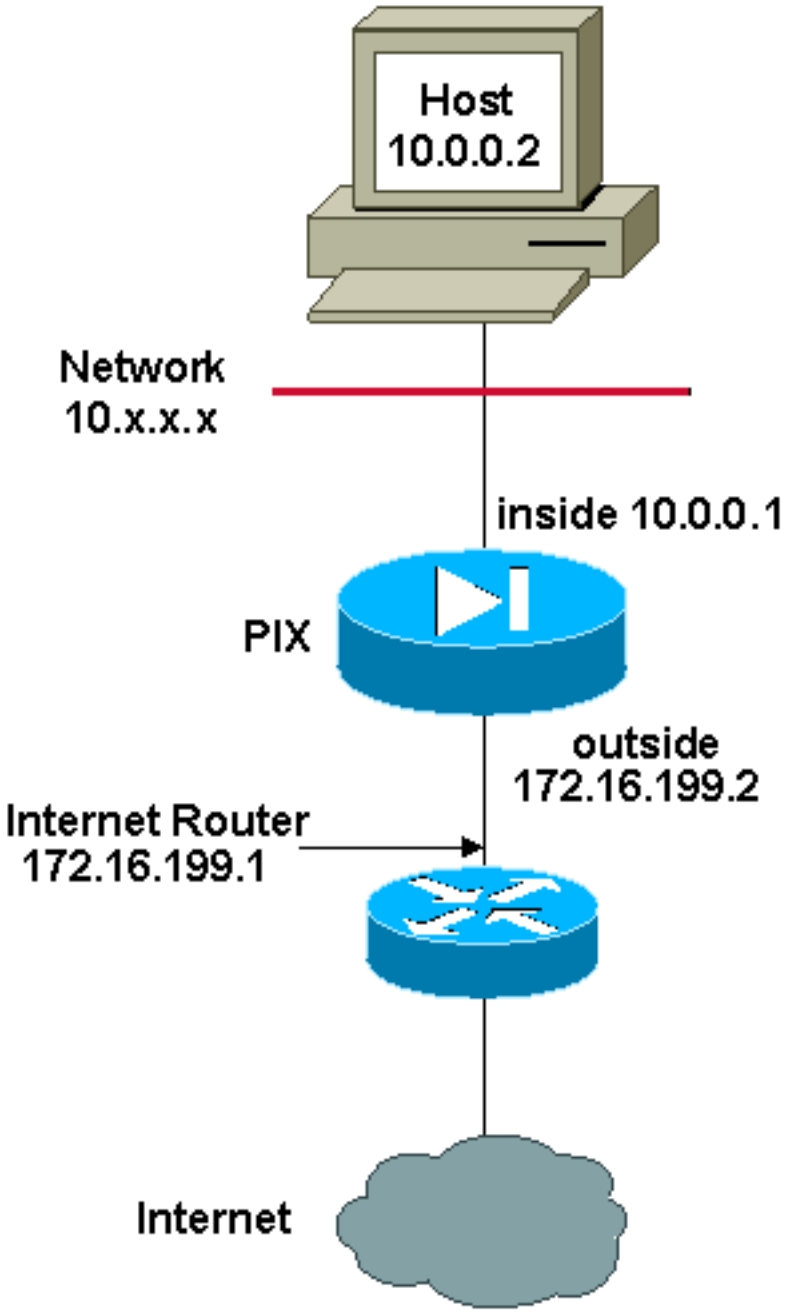
이제 NAT 규칙이 정의됩니다.

10. 보안 어플라이언스의 현재 실행 중인 컨피그레이션에 변경 사항을 적용하려면 Apply를 클릭합니다.이 출력은 PIX/ASA 컨피그레이션에 적용된 실제 추가 사항을 보여줍니다.수동 방법에서 입력한 명령과 약간 다르지만 같습니다.

```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

여러 글로벌 풀

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 네트워크 관리자는 인터넷에 등록하는 두 가지 범위의 IP 주소를 가집니다.네트워크 관리자는 10.0.0.0/8 범위에 있는 모든 내부 주소를 등록된 주소로 변환해야 합니다.네트워크 관리자가 사용해야 하는 IP 주소의 범위는 172.16.199.1~172.16.199.62 및 192.168.150.1~192.168.150.254입니다. 네트워크 관리자는 다음을 사용하여 이 작업을 수행할 수 있습니다.

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

동적 NAT에서는 동일한 인터페이스를 글로벌에서 사용할 때 우선하는 명령문이 더 구체적입니다.

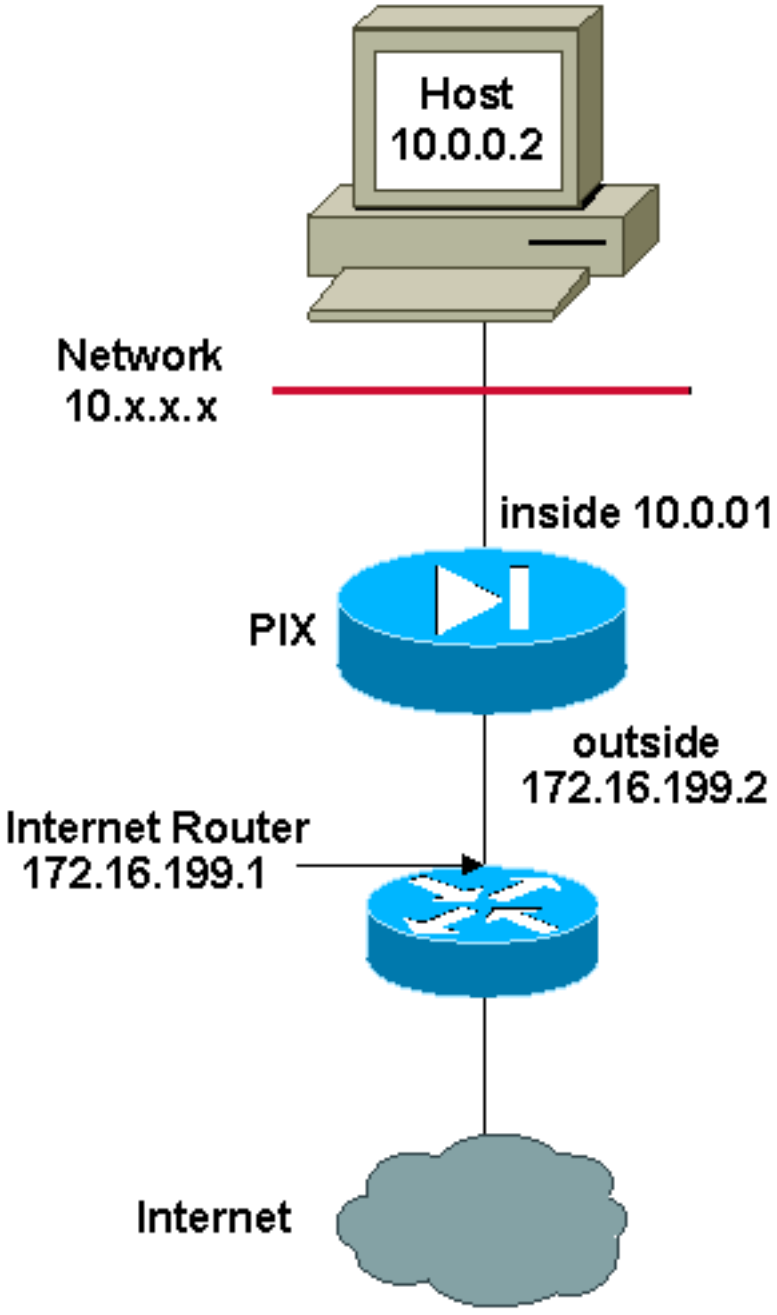
```
nat (inside) 1 10.0.0.0 255.0.0.0
```

```
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```
내부 네트워크가 10.1.0.0인 경우 NAT 전역 2가 변환에 더 특화되어 1보다 우선합니다.

참고: 와일드카드 주소 지정 체계가 NAT 문에 사용됩니다.이 명령문은 PIX/ASA가 인터넷으로 이동할 때 내부 소스 주소를 변환하도록 지시합니다.이 명령의 주소는 원하는 경우 더 구체적일 수 있습니다.

NAT와 PAT 글로벌 명령문 혼합

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 ISP는 네트워크 관리자에게 회사 사용을 위해 172.16.199.1~172.16.199.63 범위의 주소

를 제공합니다.네트워크 관리자는 인터넷 라우터의 내부 인터페이스에는 172.16.199.1을, PIX/ASA의 외부 인터페이스에는 172.16.199.2을 사용하도록 결정합니다.NAT 풀에 사용할 172.16.199.3~172.16.199.62이 남아 있습니다.그러나 네트워크 관리자는 PIX/ASA를 탈퇴하려는 사람이 한 번에 60명 이상 있을 수 있다는 사실을 알고 있습니다.따라서 네트워크 관리자는 172.16.199.62을 가져와서 여러 사용자가 동시에 하나의 주소를 공유할 수 있도록 PAT 주소로 지정합니다.

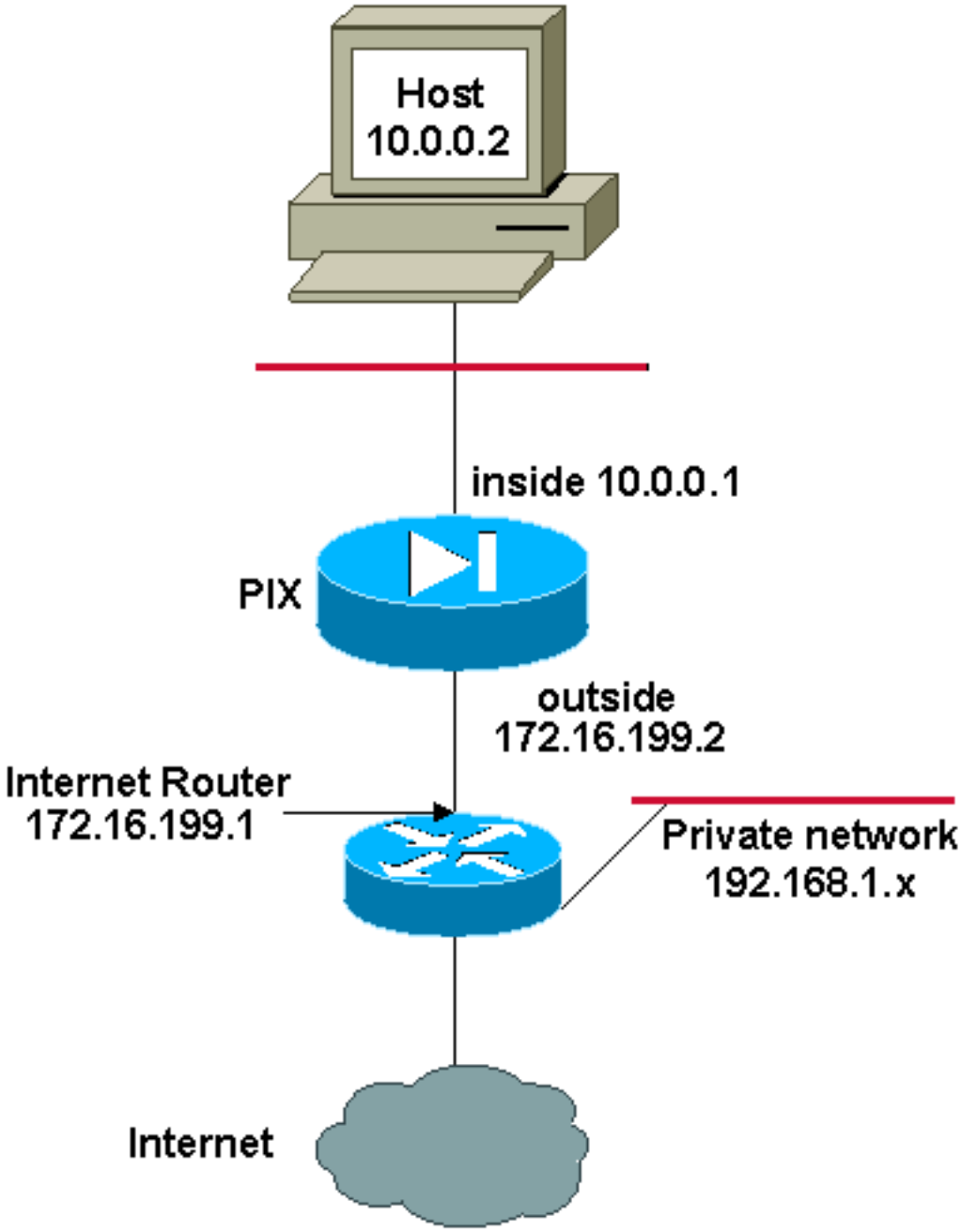
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

이 명령은 PIX/ASA에서 처음 59명의 내부 사용자가 PIX/ASA를 통과하도록 소스 주소를 172.16.199.3~172.16.199.61으로 변환하도록 지시합니다.이러한 주소가 모두 소진되면 PIX는 NAT 풀의 주소 중 하나가 사용 가능해질 때까지 모든 후속 소스 주소를 172.16.199.62으로 변환합니다.

참고: 와일드카드 주소 지정 체계가 NAT 문에 사용됩니다.이 명령문은 PIX/ASA가 인터넷으로 이동할 때 내부 소스 주소를 변환하도록 지시합니다.이 명령의 주소는 원하는 경우 더 구체적일 수 있습니다.

NAT 0 액세스 목록이 있는 다중 NAT 문

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

이 예에서 ISP는 네트워크 관리자에게 172.16.199.1~172.16.199.63 범위의 주소를 제공합니다. 네트워크 관리자는 인터넷 라우터의 내부 인터페이스에 172.16.199.1을 할당하고 PIX/ASA의 외부 인터페이스에 172.16.199.2을 할당합니다.

그러나 이 시나리오에서는 다른 프라이빗 LAN 세그먼트가 인터넷 라우터에서 분리됩니다.네트워크 관리자는 이 두 네트워크의 호스트가 서로 통신할 때 전역 풀의 주소를 낭비하지 않습니다.네트워크 관리자는 모든 내부 사용자(10.0.0.0/8)이 인터넷으로 이동할 때 여전히 소스 주소를 변환해야 합니다.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list 101
```

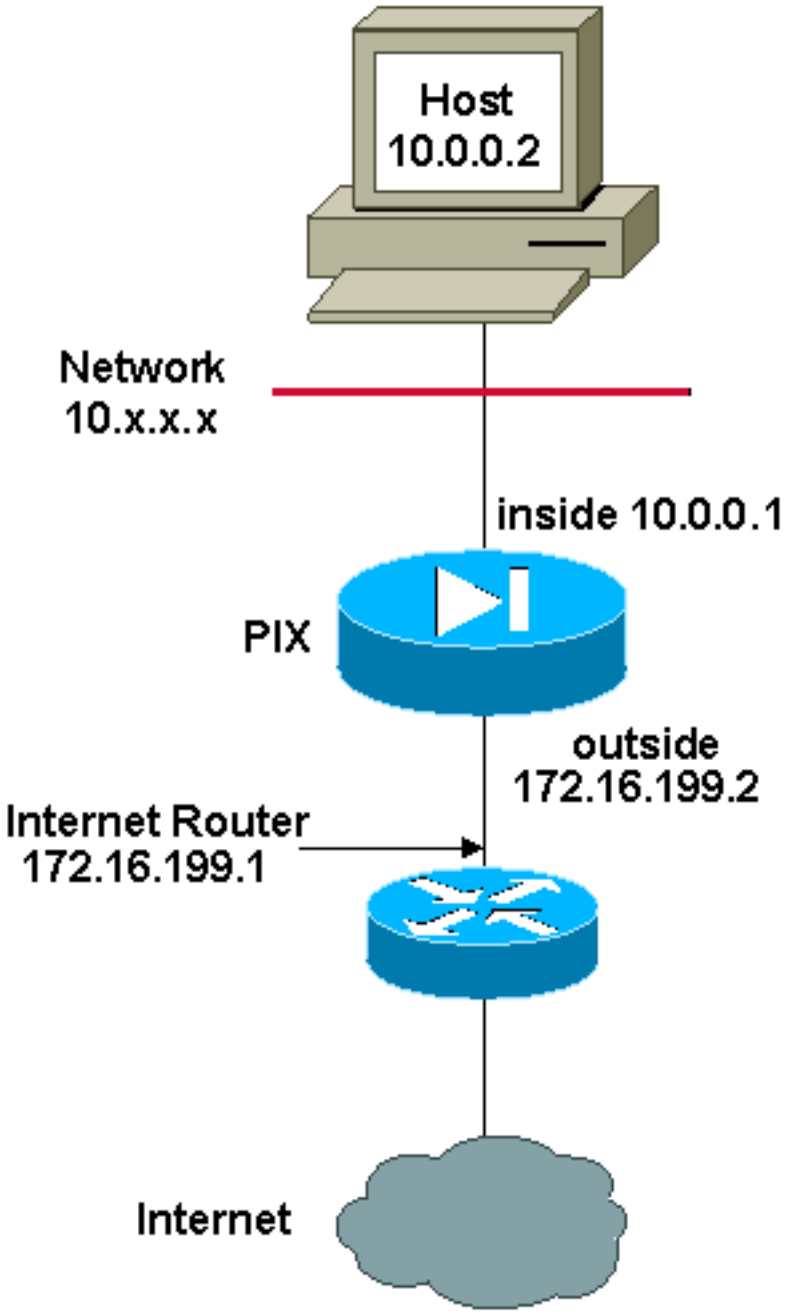
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

이 컨피그레이션은 소스 주소가 10.0.0.0/8이고 대상 주소가 192.168.1.0/24인 주소를 변환하지 않습니다. 10.0.0.0/8 네트워크 내에서 시작된 트래픽에서 소스 주소를 변환하고 192.168.1.0/24 이외의 다른 위치로 향하는 트래픽을 172.16.199.3~172.16.199.62 범위의 주소로 변환합니다.

Cisco 디바이스에서 **write terminal** 명령의 출력이 있는 경우 Output Interpreter Tool(등록된 고객만 해당)을 사용할 수 있습니다.

정책 NAT 사용

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

0이 아닌 NAT ID에 대해 nat 명령과 함께 액세스 목록을 사용할 경우 정책 NAT를 활성화합니다.

참고: 정책 NAT는 버전 6.3.2에서 도입되었습니다.

정책 NAT를 사용하면 액세스 목록에서 소스 및 목적지 주소(또는 포트)를 지정할 때 주소 변환에 대한 로컬 트래픽을 식별할 수 있습니다.일반 NAT는 소스 주소/포트만 사용하는 반면 정책 NAT는 소스 주소와 목적지 주소/포트를 모두 사용합니다.

참고: NAT 면제를 제외한 모든 유형의 NAT 지원 정책 NAT(**nat 0 access-list**).NAT 면제는 로컬 주소를 식별하기 위해 액세스 제어 목록을 사용하지만 포트가 고려되지 않는다는 점에서 정책 NAT와는 다릅니다.

정책 NAT를 사용하면 소스/포트 및 대상/포트 조합이 각 문에 대해 고유한 경우 동일한 로컬 주소를 식별하는 여러 NAT 또는 고정 문을 생성할 수 있습니다.그런 다음 각 소스/포트 및 대상/포트 쌍에 서로 다른 전역 주소를 일치시킬 수 있습니다.

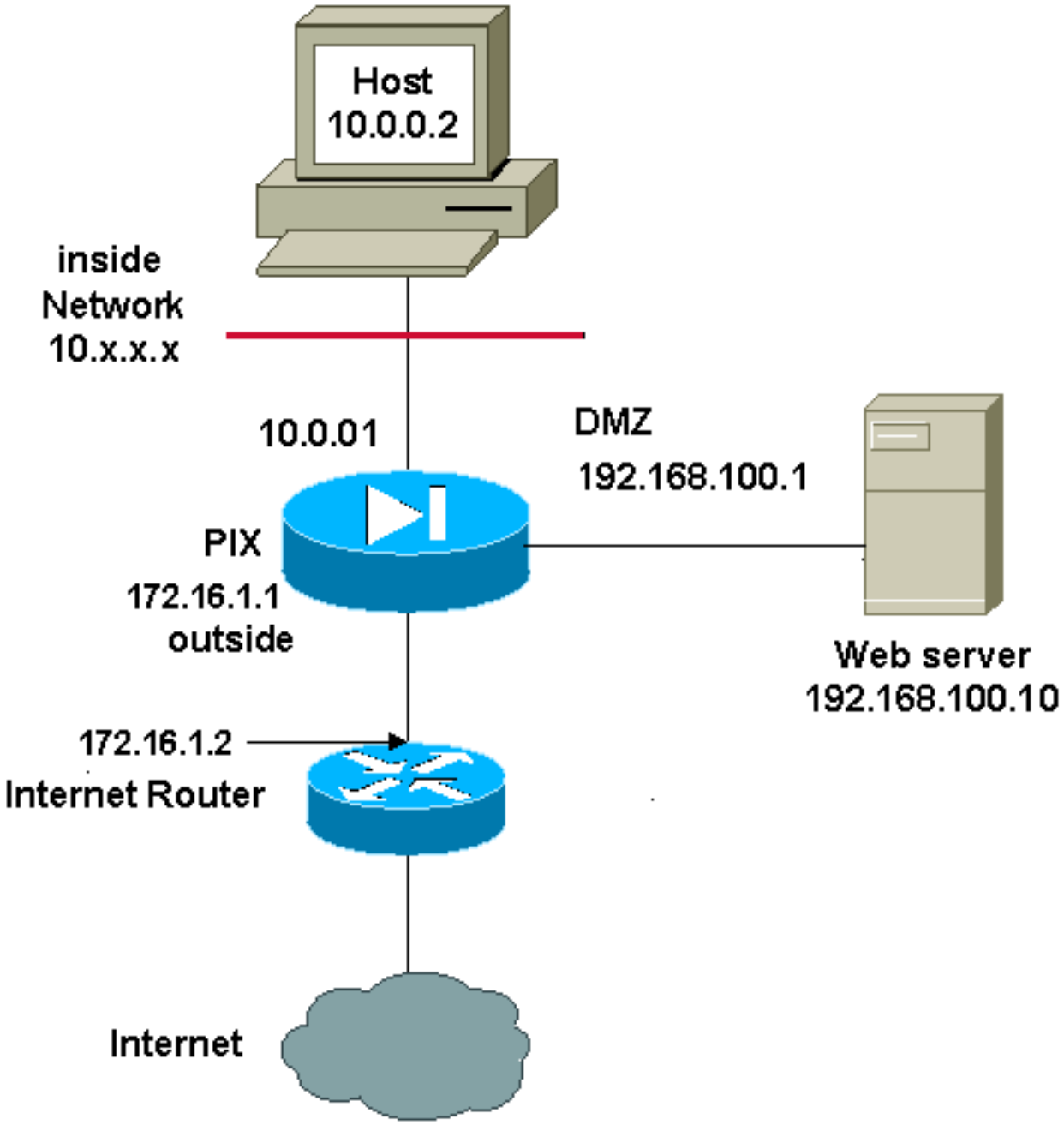
이 예에서 네트워크 관리자는 포트 80(웹) 및 포트 23(텔넷)에 대해 대상 IP 주소 192.168.201.11에 대한 액세스를 제공하지만 두 개의 다른 IP 주소를 소스 주소로 사용해야 합니다.IP 주소 172.16.199.3은 웹의 소스 주소로 사용됩니다.IP 주소 172.16.199.4은 텔넷에 사용되며 10.0.0.0/8 범위에 있는 모든 내부 주소를 변환해야 합니다.네트워크 관리자는 다음을 사용하여 이 작업을 수행할 수 있습니다.

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Output Interpreter Tool(등록된 고객만 해당)을 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다.

고정 NAT

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

고정 NAT 컨피그레이션은 일대일 매핑을 생성하고 특정 주소를 다른 주소로 변환합니다.이 유형의 컨피그레이션은 컨피그레이션이 있는 한 NAT 테이블에 영구 엔트리를 만들고 내부 및 외부 호스트 모두 연결을 시작할 수 있도록 합니다.이는 메일, 웹, FTP 및 기타 애플리케이션 서비스를 제공하는 호스트에 주로 유용합니다.이 예에서 고정 NAT 문은 내부 사용자와 외부 사용자가 DMZ의 웹 서버에 액세스할 수 있도록 구성됩니다.

이 출력은 정적 문이 생성되는 방법을 보여 줍니다.매핑된 IP 주소와 실제 IP 주소의 순서를 확인합니다.

`static (`*`real_interface`*`,`*`mapped_interface`*`) `*`mapped_ip real_ip`* `netmask `*`mask`*

다음은 내부 인터페이스의 사용자에게 DMZ의 서버에 대한 액세스를 제공하기 위해 만들어진 고정 변환입니다.내부 주소와 DMZ에 있는 서버의 주소 간에 매핑을 생성합니다.내부 사용자는 내부 주소를 통해 DMZ의 서버에 액세스할 수 있습니다.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```
다음은 외부 인터페이스의 사용자에게 DMZ의 서버에 대한 액세스를 제공하기 위해 만들어진 고정 변환입니다.외부 주소와 DMZ에 있는 서버의 주소 간에 매핑을 생성합니다.외부 사용자는 외부 주소를 통해 DMZ의 서버에 액세스할 수 있습니다.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```
참고: 외부 인터페이스의 보안 수준이 DMZ보다 낮기 때문에, DMZ의 서버에 대한 외부 액세스를 허용하려면 액세스 목록도 생성해야 합니다.액세스 목록은 사용자에게 정적 변환의 **매핑된 주소**에 대한 액세스 권한을 부여해야 합니다.이 액세스 목록은 최대한 구체적으로 지정하는 것이 좋습니다.이 경우 모든 호스트는 웹 서버의 포트 80(www/http) 및 443(https)에만 액세스할 수 있습니다.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```
그런 다음 액세스 목록을 외부 인터페이스에 적용해야 합니다.

```
access-group OUTSIDE in interface outside
```
access-list 및 access-group 명령에 대한 자세한 내용은 access-list extended and access-group을 참조하십시오.

NAT 우회 방법

이 섹션에서는 NAT를 우회하는 방법에 대해 설명합니다.NAT 제어를 활성화할 때 NAT를 우회할 수 있습니다.NAT를 우회하기 위해 Identity NAT, Static Identity NAT 또는 NAT 예외를 사용할 수 있습니다.

ID NAT 구성

ID NAT는 실제 IP 주소를 동일한 IP 주소로 변환합니다."변환된" 호스트만 NAT 변환을 생성할 수 있으며 응답 트래픽은 다시 허용됩니다.

참고:NAT 컨피그레이션을 변경하고 새 NAT 정보가 사용되기 전에 기존 번역이 시간 초과될 때까지 기다리지 않으려면 **clear xlate** 명령을 사용하여 변환 테이블을 지웁니다.그러나 변환 테이블을 지우면 변환을 사용하는 현재 모든 연결이 끊어집니다.

ID NAT를 구성하려면 다음 명령을 입력합니다.

```
hostname(config)#nat (real_interface) 0 real_ip
 [mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
 udp_max_conns]
```

예를 들어, 내부 10.1.1.0/24 네트워크에 ID NAT를 사용하려면 다음 명령을 입력합니다.

```
hostname(config)#nat (inside) 0 10.1.1.0
 255.255.255.0
```

nat 명령에 대한 자세한 내용은 Cisco Security Appliance 명령 참조 버전 7.2를 **참조하십시오**.

고정 ID NAT 구성

고정 ID NAT는 실제 IP 주소를 동일한 IP 주소로 변환합니다.변환은 항상 활성 상태이며 "변환된" 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.고정 ID NAT를 사용하면 일반 NAT 또는 정책 NAT를 사용할 수 있습니다.정책 NAT를 사용하면 변환할 실제 주소를 결정할 때 실제 및 대상 주소를 식별할 수 있습니다(정책 NAT에 대한 자세한 내용은 정책 NAT 사용 섹션 참조). 예를 들어, 외부 인터페이스에 액세스하고 대상이 서버 A인 경우 내부 주소에 대해 정책 고정 ID NAT를 사용할 수 있지만 외부 서버 B에 액세스할 때는 일반 변환을 사용합니다.

참고:static 명령을 제거할 경우 변환을 사용하는 현재 연결은 영향을 받지 않습니다.이러한 연결을 제거하려면 clear local**-host 명령을 입력합니다.clear xlate** 명령을 사용하여 변환 테이블에서 고정 변환을 지울 수 없습니다.대신 static 명령을 제거해야 합니다.nat 및 global 명령으로 생성된 동적 변환만 clear xlate 명령을 사용하여 제거할 수 있습니다.

정책 고정 ID NAT를 구성하려면 다음 명령을 입력합니다.

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip access-list acl_id [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

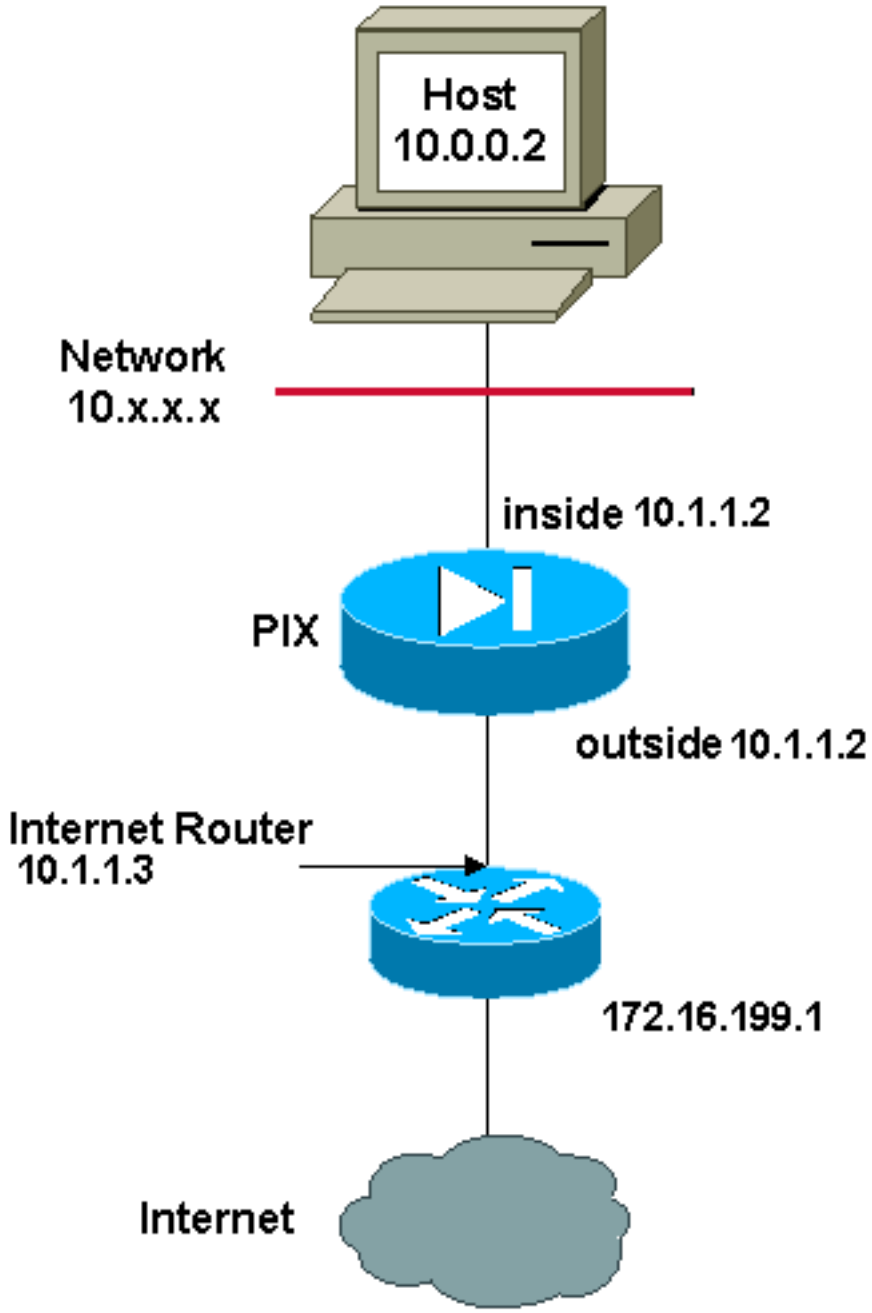
확장 액세스 목록을 만들려면 **access-list extended** 명령을 사용합니다.이 액세스 목록에는 허용 ACE만 포함되어야 합니다.액세스 목록의 소스 주소가 이 명령의 real_ip와 일치하는지 확인합니다.정책 NAT는 inactive 또는 time-range 키워드를 고려하지 않습니다.모든 ACE는 정책 NAT 컨피그레이션에 대해 활성화된 것으로 간주됩니다.자세한 내용은 정책 NAT 사용 섹션을 참조하십시오.

일반 고정 ID NAT를 구성하려면 다음 명령을 입력합니다.

```
hostname(config)#static
 (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
 [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
 udp_max_conns]
```

real_ip 인수 모두에 대해 동일한 IP 주소를 지정합니다.

네트워크 다이어그램



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

예를 들어, 이 명령은 외부에서 액세스할 때 내부 IP 주소(10.1.1.2)에 고정 ID NAT를 사용합니다.

```
hostname(config)#static (inside,outside) 10.1.1.2
 10.1.1.2 netmask 255.255.255.255
```

static 명령에 대한 자세한 내용은 Cisco Security Appliance 명령 참조 버전 7.2를 참조하십시오.

이 명령은 내부에서 액세스할 때 외부 주소(172.16.199.1)에 고정 ID NAT를 사용합니다.

```
hostname(config)#static (outside,inside) 172.16.199.1
 172.16.199.1 netmask 255.255.255.255
```

이 명령은 전체 서브넷을 정적으로 매핑합니다.

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
 netmask 255.255.255.0
```

이 고정 ID 정책 NAT 예는 하나의 목적지 주소에 액세스할 때 ID NAT를 사용하는 단일 실제 주소와 다른 목적지 주소에 액세스할 때 변환을 사용하는 단일 실제 주소를 보여줍니다.

```
hostname(config)#access-list NET1 permit ip host
 10.1.1.3 172.16.199.0 255.255.255.224

hostname(config)#access-list NET2 permit ip host
 10.1.1.3 172.16.199.224 255.255.255.224

hostname(config)#static (inside,outside) 10.1.1.3
 access-list NET1

hostname(config)#static (inside,outside) 172.16.199.1
 access-list NET2
```

참고: static 명령에 대한 자세한 내용은 Cisco ASA 5580 Adaptive Security Appliance 명령 참조 버전 8.1을 참조하십시오.

참고: 액세스 목록에 대한 자세한 내용은 Cisco ASA 5580 Adaptive Security Appliance 명령줄 컨피그레이션 가이드 버전 8.1을 참조하십시오.

NAT 예외 구성

NAT 면제는 변환에서 주소를 제외하며 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있도록 합니다.NAT 면제를 사용하면 제외할 실제 트래픽을 결정할 때 실제 및 대상 주소를 지정할 수 있습니다(정책 NAT와 유사). 따라서 NAT 면제를 사용하여 ID NAT보다 더 효과적으로 제어할 수 있습니다.그러나 정책 NAT와 달리 NAT 면제는 액세스 목록의 포트를 고려하지 않습니다.고정 ID NAT를 사용하여 액세스 목록의 포트를 고려합니다.

참고:NAT 예외 컨피그레이션을 제거하면 NAT 면제를 사용하는 기존 연결은 영향을 받지 않습니다.이러한 연결을 제거하려면 clear local-host 명령을 입력합니다.

NAT 예외를 구성하려면 다음 명령을 입력합니다.

```
hostname(config)#nat (real_interface) 0 access-list
 acl_name [outside]
```

access-list extended 명령을 사용하여 확장 액세스 목록을 생성합니다.이 액세스 목록에는 허용 ACE와 거부 ACE가 모두 포함될 수 있습니다.액세스 목록에서 실제 포트와 대상 포트를 지정하지 마십시오.NAT 면제는 포트를 고려하지 않습니다.NAT 면제에서는 inactive 또는 time-range 키워드도 고려하지 않습니다.모든 ACE는 NAT 예외 컨피그레이션에 대해 활성화된 것으로 간주됩니다.

기본적으로 이 명령은 내부에서 외부로 트래픽을 제외합니다.NAT를 우회하기 위해 외부 간 트래픽이 필요하려면 추가 nat 명령을 추가하고 outside를 입력하여 NAT 인스턴스를 외부 NAT로 식별합니다.외부 인터페이스에 대해 동적 NAT를 구성하고 다른 트래픽을 제외하려는 경우 외부 NAT 예

외를 사용할 수 있습니다.

예를 들어 목적지 주소에 액세스할 때 내부 네트워크를 제외하려면 다음 명령을 입력합니다.

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0
255.255.255.0 any

hostname(config)# nat (inside) 0 access-list
EXEMPT
```

DMZ 네트워크에 동적 외부 NAT를 사용하고 다른 DMZ 네트워크를 제외하려면 다음 명령을 입력합니다.

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0
outside dns

hostname(config)#global (inside) 1
10.1.1.2

hostname(config)#access-list EXEMPT permit ip 10.1.1.0
255.255.255.0 any

hostname(config)#nat (dmz) 0 access-list
EXEMPT
```

서로 다른 두 목적지 주소에 액세스할 때 내부 주소를 제외하려면 다음 명령을 입력합니다.

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
255.255.255.0 172.16.199.0 255.255.255.224

hostname(config)#access-list NET1 permit ip 10.1.1.0
255.255.255.0 172.16.199.224 255.255.255.224

hostname(config)#nat (inside) 0 access-list NET1
```

다음을 확인합니다.

보안 어플라이언스를 통과하는 트래픽은 NAT를 거칠 가능성이 높습니다.PIX/ASA 참조:보안 어플라이언스에서 사용 중인 변환을 확인하기 위해 성능 문제를 모니터링하고 트러블슈팅합니다.

show xlate **count** 명령은 PIX를 통한 현재 및 최대 번역 수를 표시합니다.변환은 내부 주소를 외부 주소에 매핑하는 것으로, NAT와 같은 일대일 매핑 또는 PAT와 같은 다대일 매핑이 될 수 있습니다.이 명령은 **show xlate 명령**의 하위 집합으로, **PIX를** 통해 각 변환을 출력합니다.명령 출력은 명령이 실행될 때 PIX의 활성 변환 수를 나타내는 "사용 중" 변환을 표시합니다."most used"는 전원이 켜진 이후 PIX에서 확인된 최대 변환을 의미합니다.

문제 해결

포트 443에 대한 고정 PAT를 추가할 때 오류 메시지가 수신됨

문제

포트 443에 대해 고정 PAT를 추가하면 다음 오류 메시지가 표시됩니다.

```
[] static (INSIDE,OUTSIDE) tcp interface 443 192.168.1.87 443  255.255.255.255 tcp 0 0 udp 0

 PAT   443   .

:   .
```

솔루션

이 오류 메시지는 ASDM 또는 WEBVPN이 443 포트에서 실행 중일 때 발생합니다.이 문제를 해결하려면 방화벽에 로그인하고 다음 단계 중 하나를 완료하십시오.

- ASDM 포트를 443 이외의 다른 포트로 변경하려면 다음 명령을 실행합니다.
  ```
  ASA(config)#no http server enable
  ASA(config)#http server enable 8080
  ```

- WEBVPN 포트를 443 이외의 포트로 변경하려면 다음 명령을 실행합니다.
  ```
  ASA(config)#webvpn
  ASA(config-webvpn)#enable outside
  ASA(config-webvpn)#port 65010
  ```

이러한 명령을 실행한 후에는 포트 443의 NAT/PAT를 다른 서버에 추가할 수 있어야 합니다.나중에 ASDM을 사용하여 ASA를 관리하려는 경우 새 포트를 8080으로 지정합니다.

오류:매핑된 주소가 기존 고정 주소와 충돌합니다.

문제

ASA에 static 문을 추가하면 다음 오류가 발생합니다.

: .

솔루션

추가하려는 정적 소스에 대한 항목이 이미 없는지 확인합니다.

관련 정보

- PIX 지원 페이지
- PIX 명령 참조
- ASA 지원 페이지
- ASA 명령 참조
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems