ASA 8.2:ASDM을 사용하여 nat, global, static 및 access-list 명령을 사용하는 포트 리디렉션(전달)

목차

소개

이 문서에서는 ASDM을 사용하는 Cisco ASA(Adaptive Security Appliance)에서 포트 리디렉션이 작동하는 방식에 대해 설명합니다.ASA를 통한 트래픽의 액세스 제어 및 변환 규칙의 작동 방식을 처리합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- NAT 개요
- PIX/ASA 7.X:포트 리디렉션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 5500 Series ASA 버전 8.2
- Cisco ASDM 버전 6.3

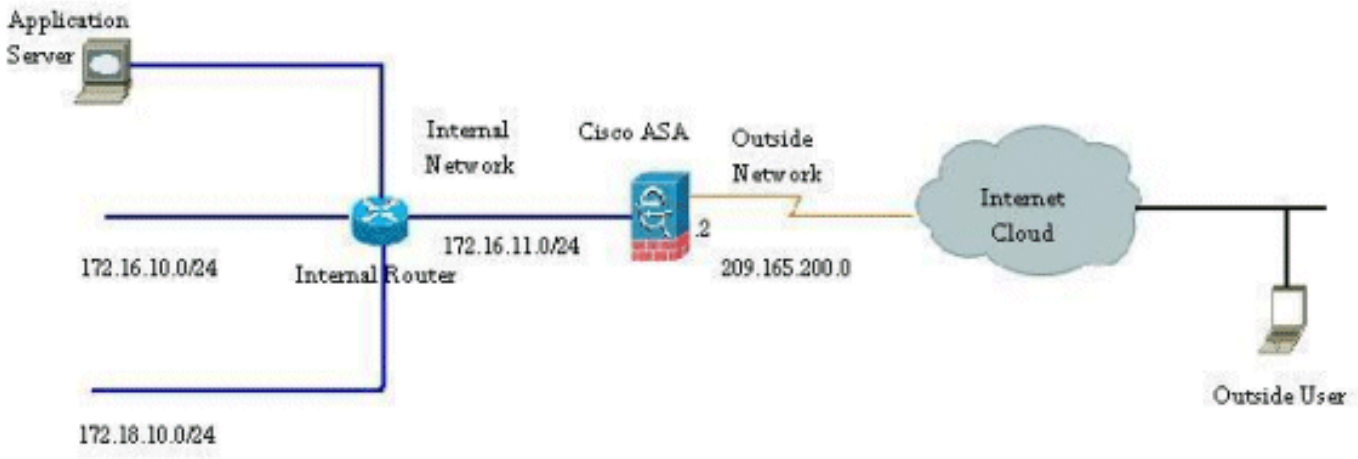
참고: 이 컨피그레이션은 NAT 기능에는 큰 변경 사항이 없으므로 Cisco ASA 소프트웨어 버전 8.0에서 8.2까지만 작동합니다.

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 표기 규칙을 참고하십시오.

네트워크 다이어그램

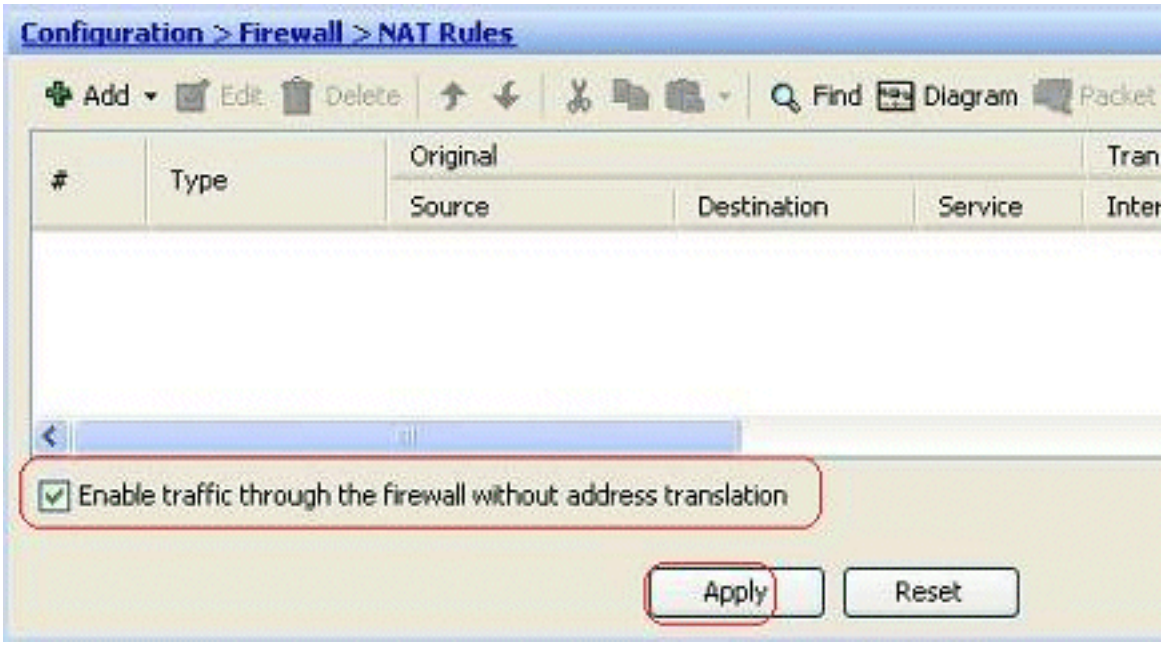


이 컨피그레이션에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

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.

변환 규칙을 구성하지 않으면 Security Appliance를 통과할 수 있는 연결이 없습니다.이 기능을 nat-control이라고 합니다.여기에 표시된 이미지는 주소 변환 없이 ASA를 통한 연결을 허용하기 위해 ASDM을 통해 이 기능을 비활성화하는 방법을 보여줍니다.그러나 변환 규칙이 구성된 경우 이 기능을 비활성화해도 모든 트래픽에 대해 유효한 것은 아니며 주소 변환에서 네트워크를 명시적으로 제외해야 합니다.

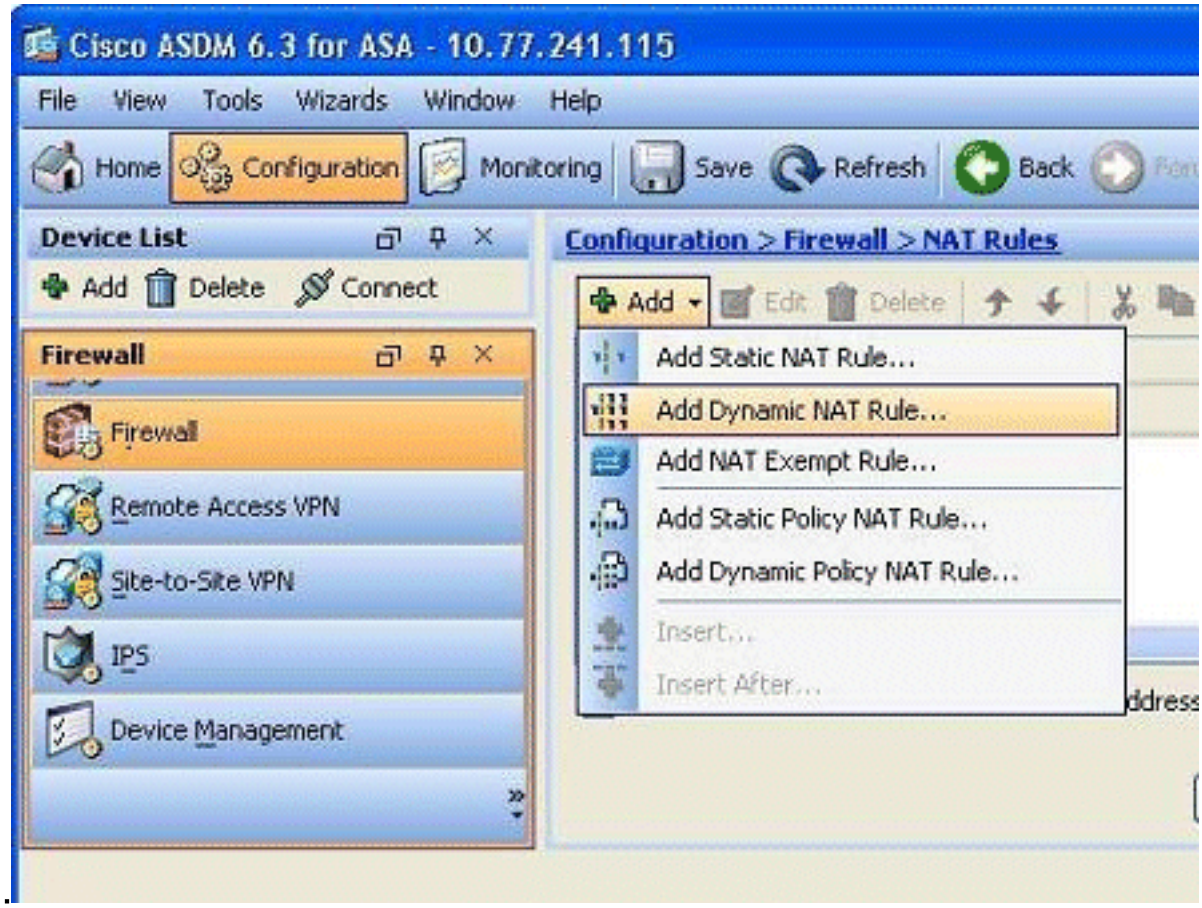


내부 호스트에서 NAT를 사용하여 외부 네트워크에 액세스 허용

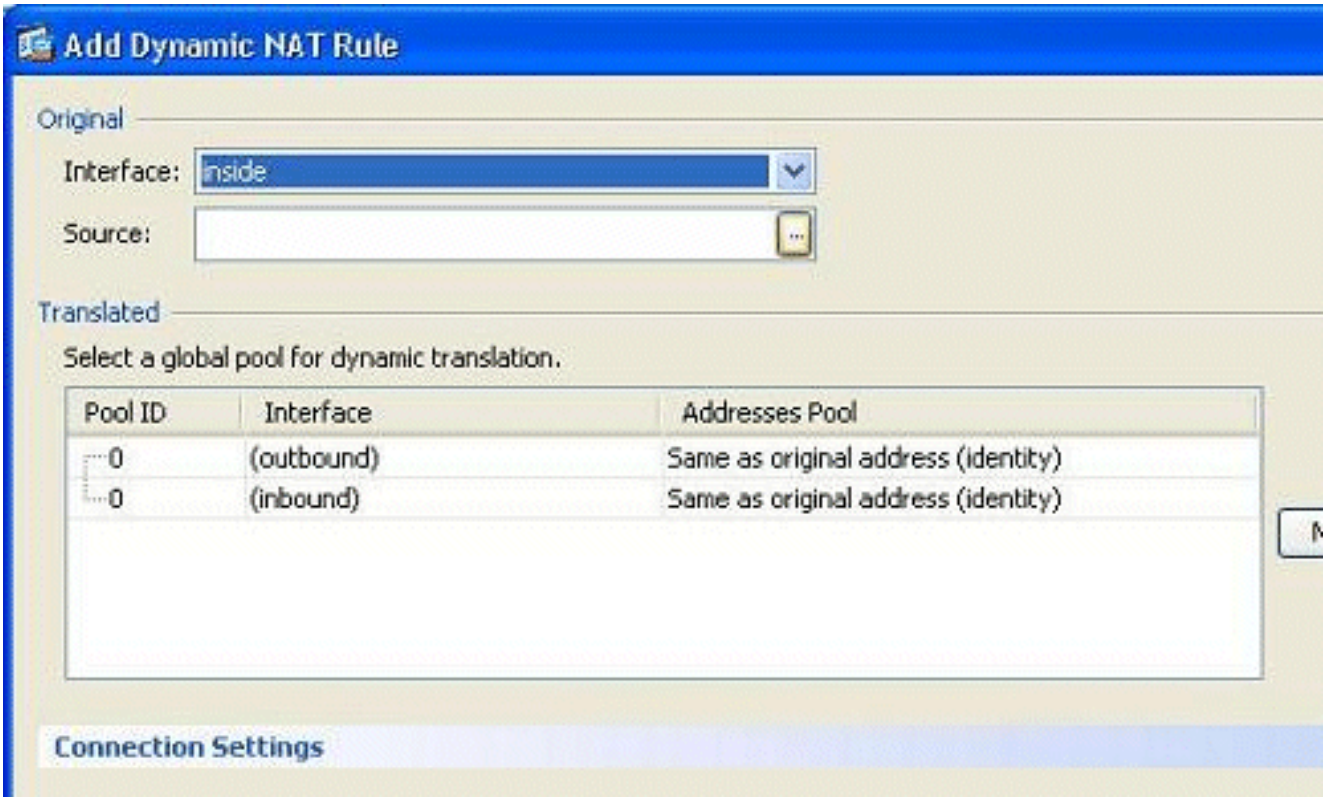
동적 NAT 규칙을 구성하여 내부 호스트/네트워크 그룹이 외부 세계에 액세스하도록 허용할 수 있습니다.이를 위해서는 액세스 권한을 부여할 호스트/네트워크의 실제 주소를 선택한 다음 변환된 IP 주소 풀에 매핑해야 합니다.

내부 호스트가 NAT를 사용하여 외부 네트워크에 액세스하도록 허용하려면 다음 단계를 완료합니다.

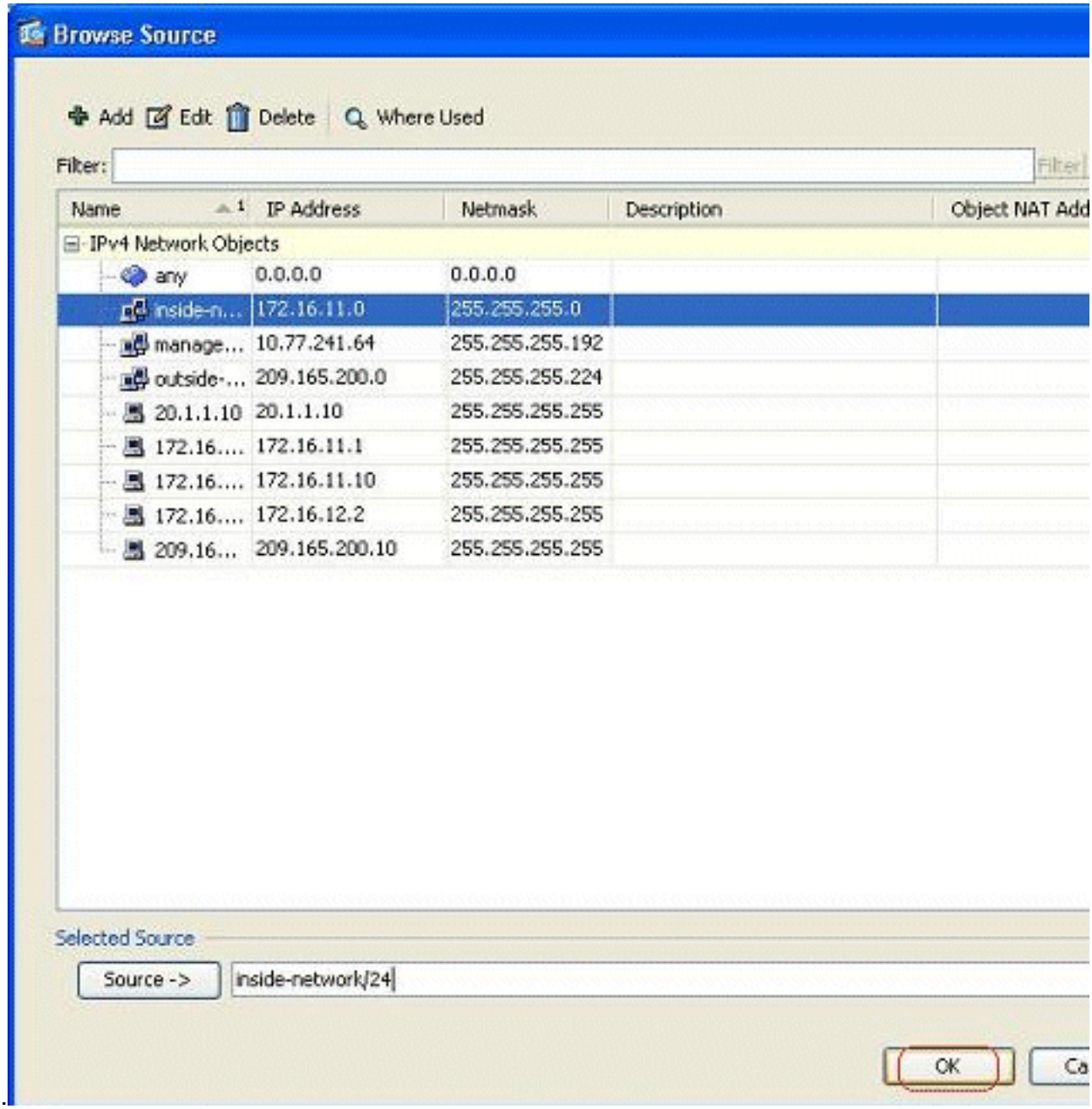
1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하여 **Add(추가)**를 클릭한 다음 **Add Dynamic NAT Rule(동적 NAT 규칙 추가) 옵션을 선택하여 동적 NAT 규칙을 구성합니다**



2. 실제 호스트가 연결된 인터페이스의 이름을 선택합니다.Source(소스) 필드의 Details(**세부사항)** 버튼을 사용하여 호스트/네트워크의 실제 IP 주소를 선택합니다

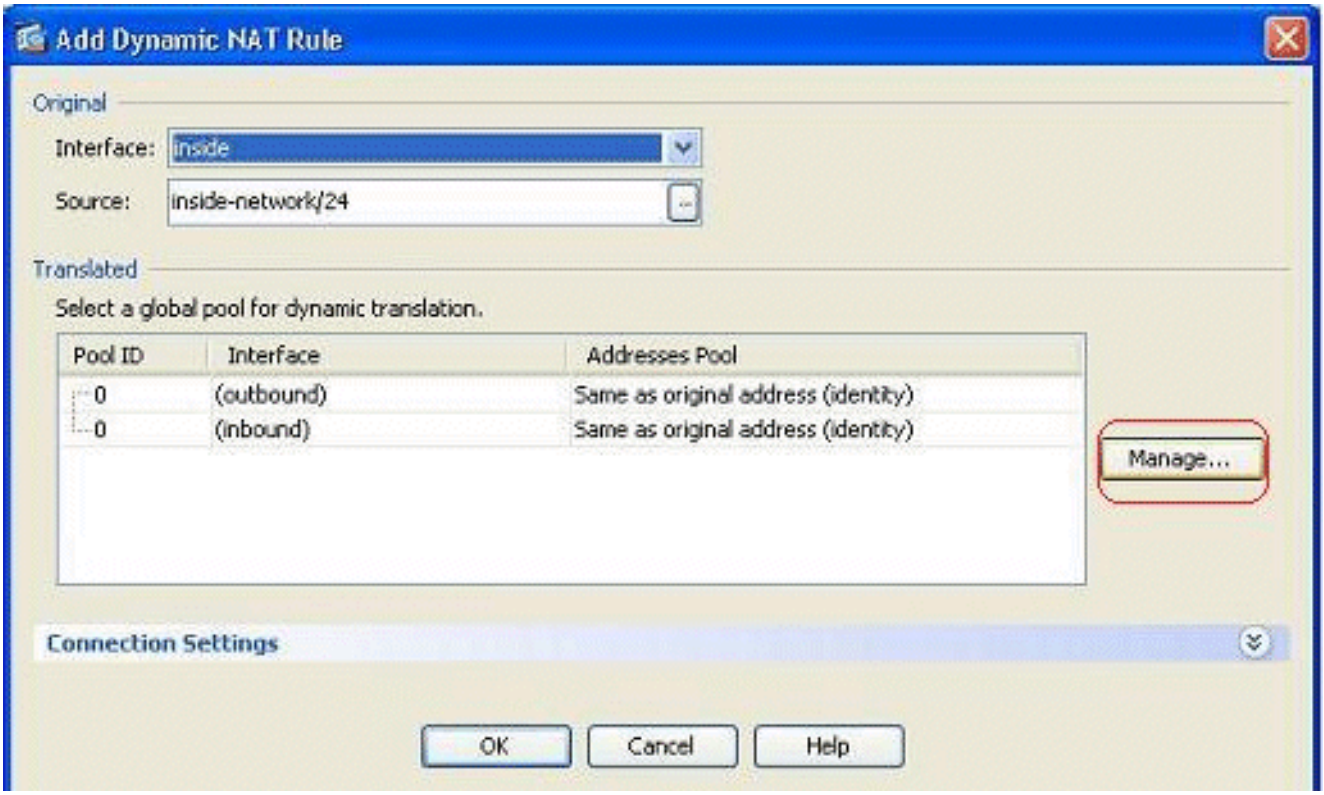


3. 이 예에서는 전체 *내부 네트워크*가 선택되었습니다.확인**을** 클릭하여 선택을 완료합니다

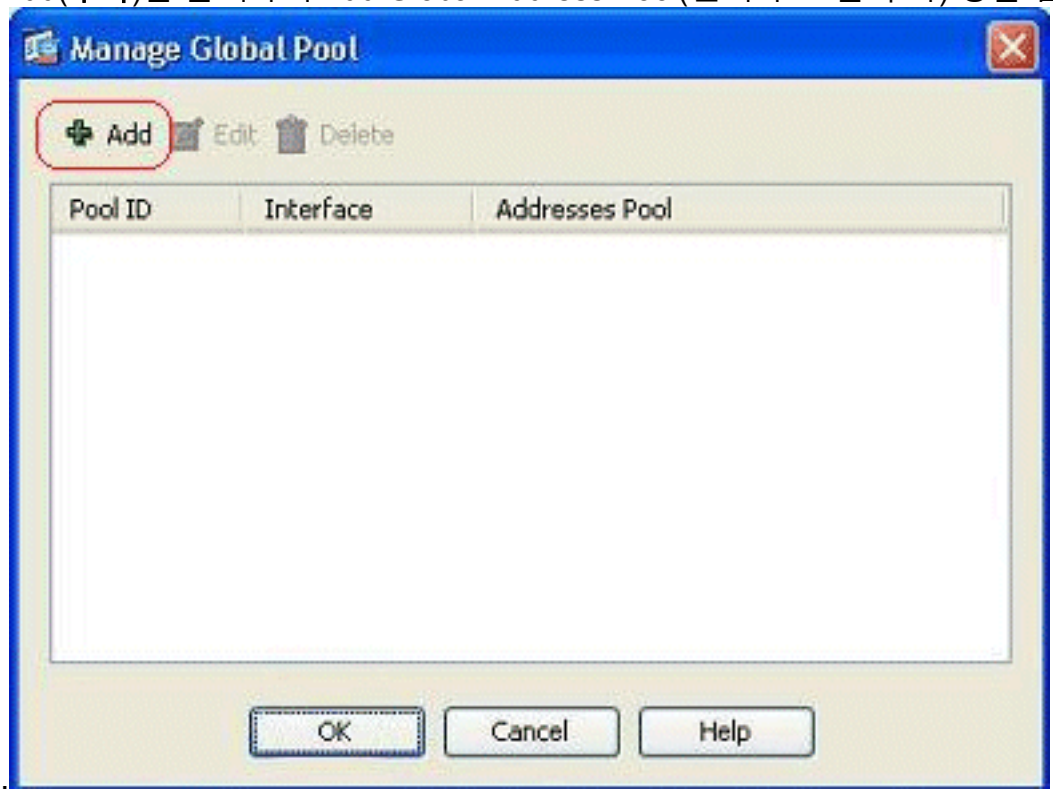


4. 실제 네트워크가 매핑될 IP 주소 풀을 선택하려면 **Manage(관리)**를 클릭합니다

.



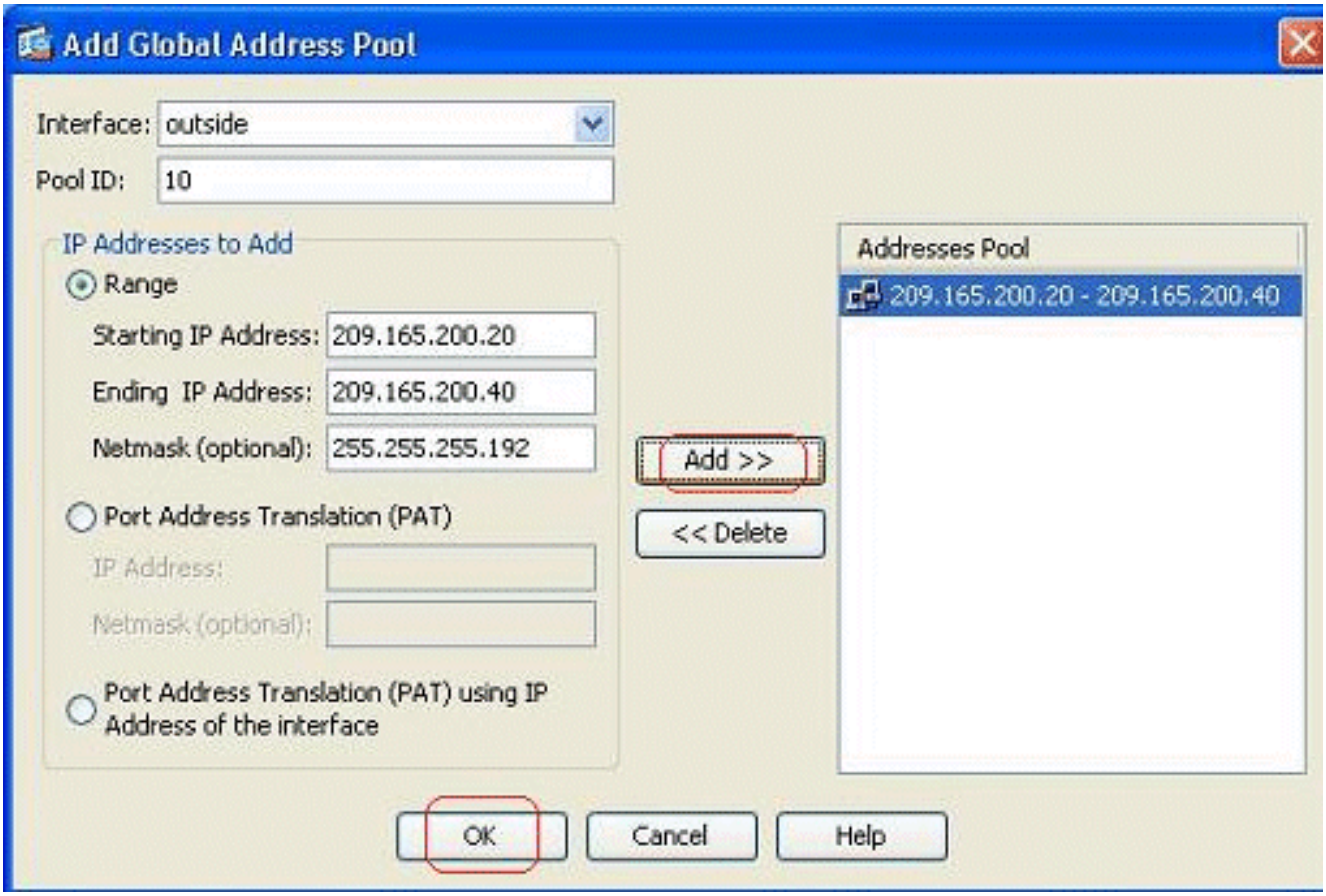
5. Add(**추가**)를 클릭하여 Add Global Address Pool(전역 주소 풀 추가) 창을 엽니다



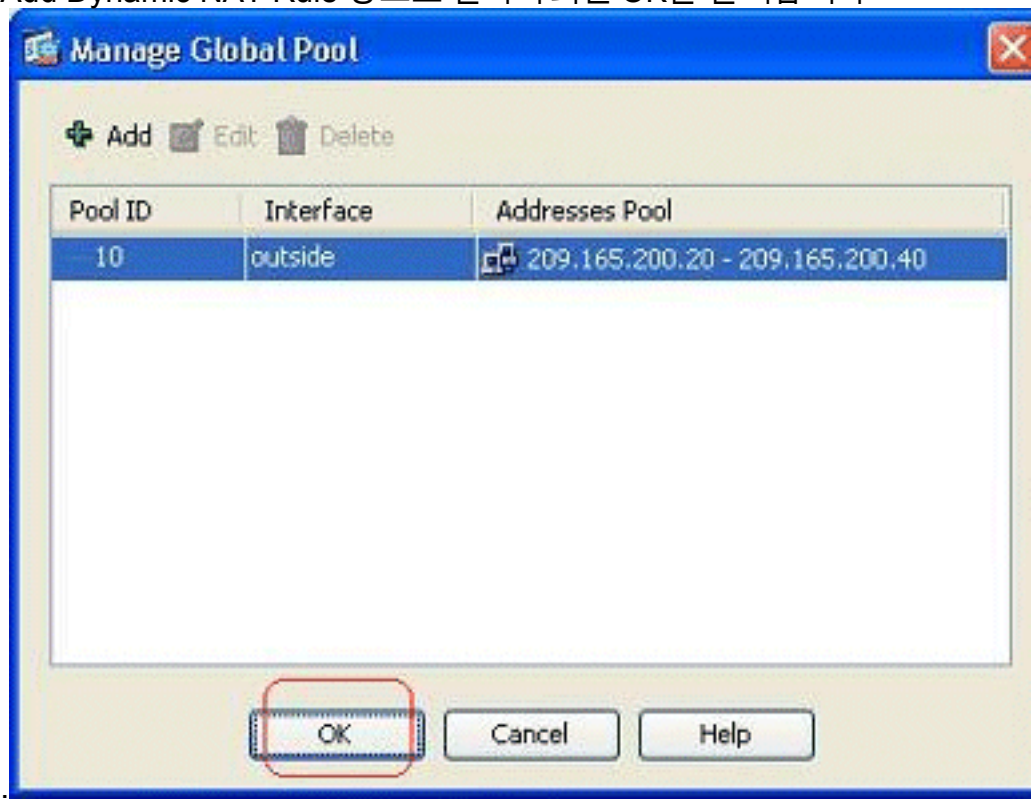
.

6. Range(**범위**) 옵션을 선택하고 이그레스 인터페이스와 함께 Starting(시작) 및 Ending IP Addresses(종료 IP 주소)를 지정합니다.또한 고유한 풀 ID를 지정하고 **Add(추가)를** 클릭하여 주소 풀에 추가합니다.Manage Global Pool(전역 풀 관리) 창으로 돌아가려면 OK(확인)를 클릭합니다

.



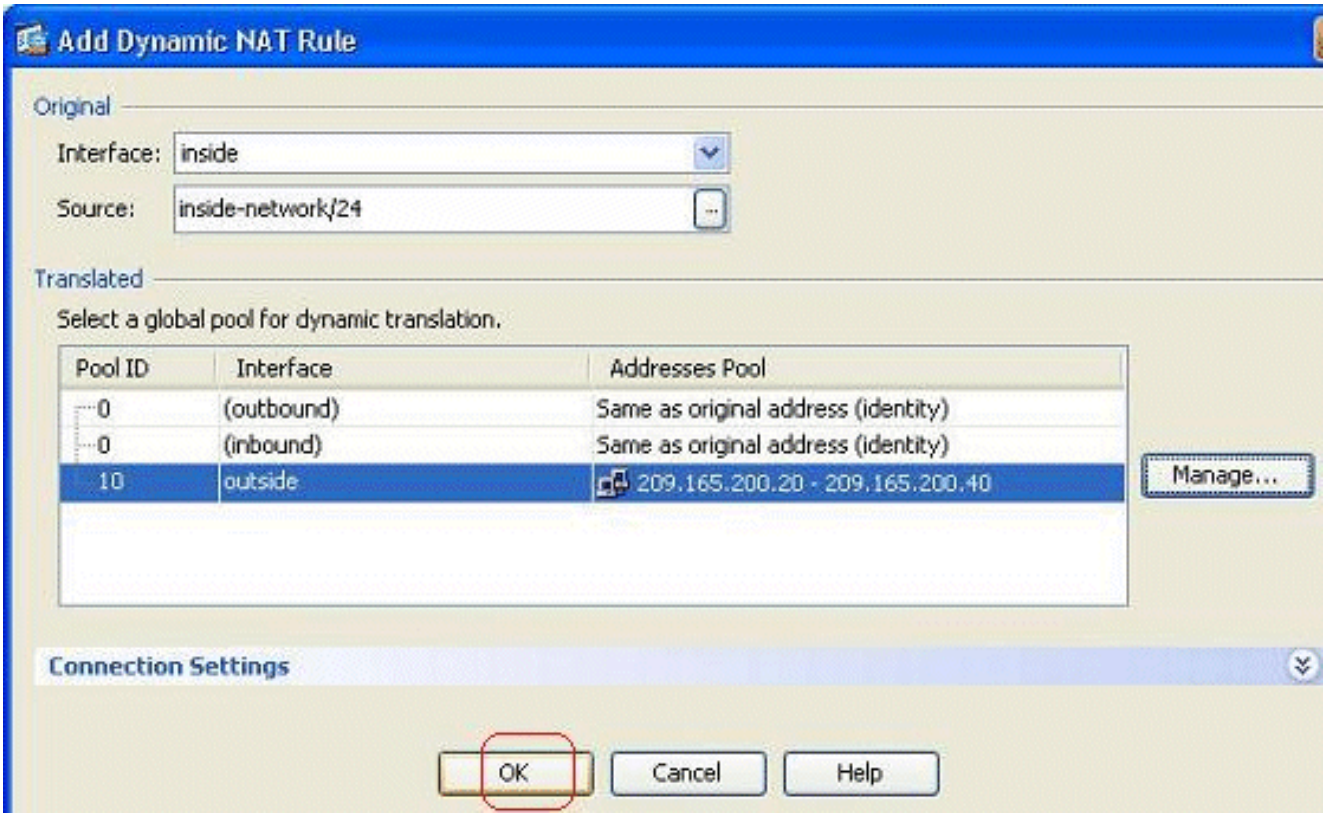
7. Add Dynamic NAT Rule 창으로 돌아가려면 OK를 클릭합니다



.

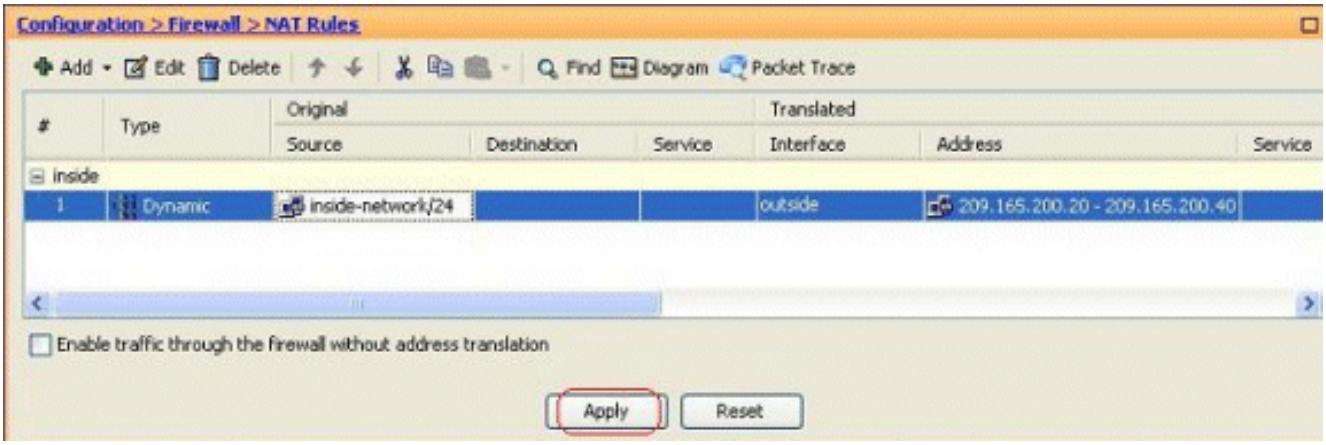
8. OK(**확인**)를 클릭하여 동적 NAT 규칙 컨피그레이션을 완료합니다

.



9. 변경 사항을 적용하려면 Apply를 클릭합니다.**참고: Enable traffic through the firewall without address translation** 옵션**은 선택** 취소되어 있습니다

.



이 ASDM 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

이 구성에 따라 172.16.11.0 네트워크의 호스트는 NAT 풀 209.165.200.20-209.165.200.40에서 모든 IP 주소로 변환됩니다. 여기에서 NAT 풀 ID는 매우 중요합니다.동일한 NAT 풀을 다른 내부/DMZ 네트워크에 할당할 수 있습니다.매핑된 풀의 주소가 실제 그룹보다 적으면 트래픽 양이 예상보다 많을 경우 주소가 부족해질 수 있습니다.따라서 PAT를 구현하거나 기존 주소 풀을 편집하여 확장할 수 있습니다.

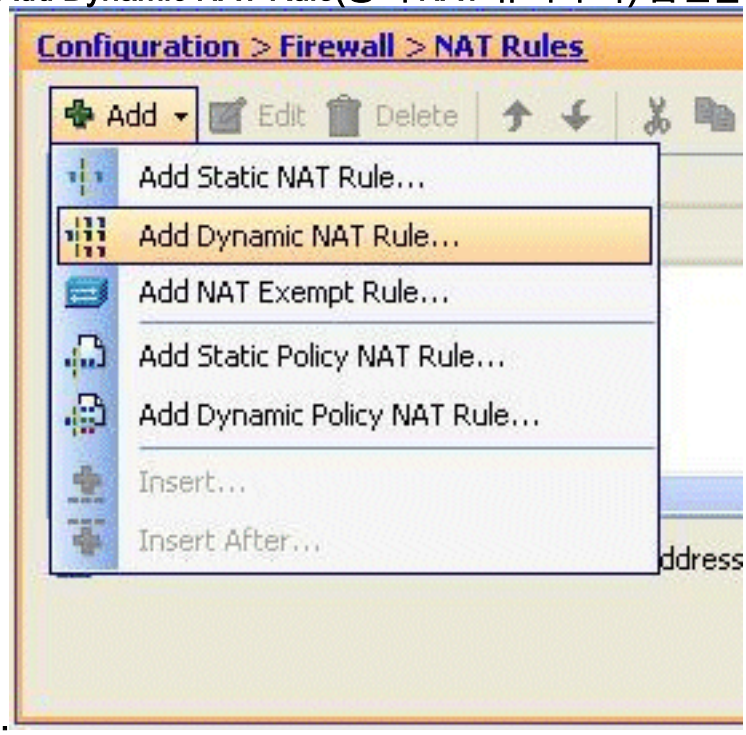
참고: 기존 변환 규칙을 수정하는 동안 clear xlate **명령**을 사용하여 수정 사항을 적용해야 합니다.그렇지 않으면 이전 기존 연결은 시간 초과될 때까지 연결 테이블에 유지됩니다.**clear xlate** 명령을 사용할 때는 기존 연결을 즉시 종료하므로 주의해야 합니다.

내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스 허용

내부 호스트에서 번역을 위해 단일 공용 주소를 공유하려면 PAT를 사용합니다.**global 문**이 하나의 주소를 지정하면 해당 주소는 포트 변환됩니다.ASA는 인터페이스당 하나의 포트 변환을 허용하며, 이 변환은 단일 전역 주소에 대해 최대 65,535개의 활성 **xlate** 객체를 지원합니다.

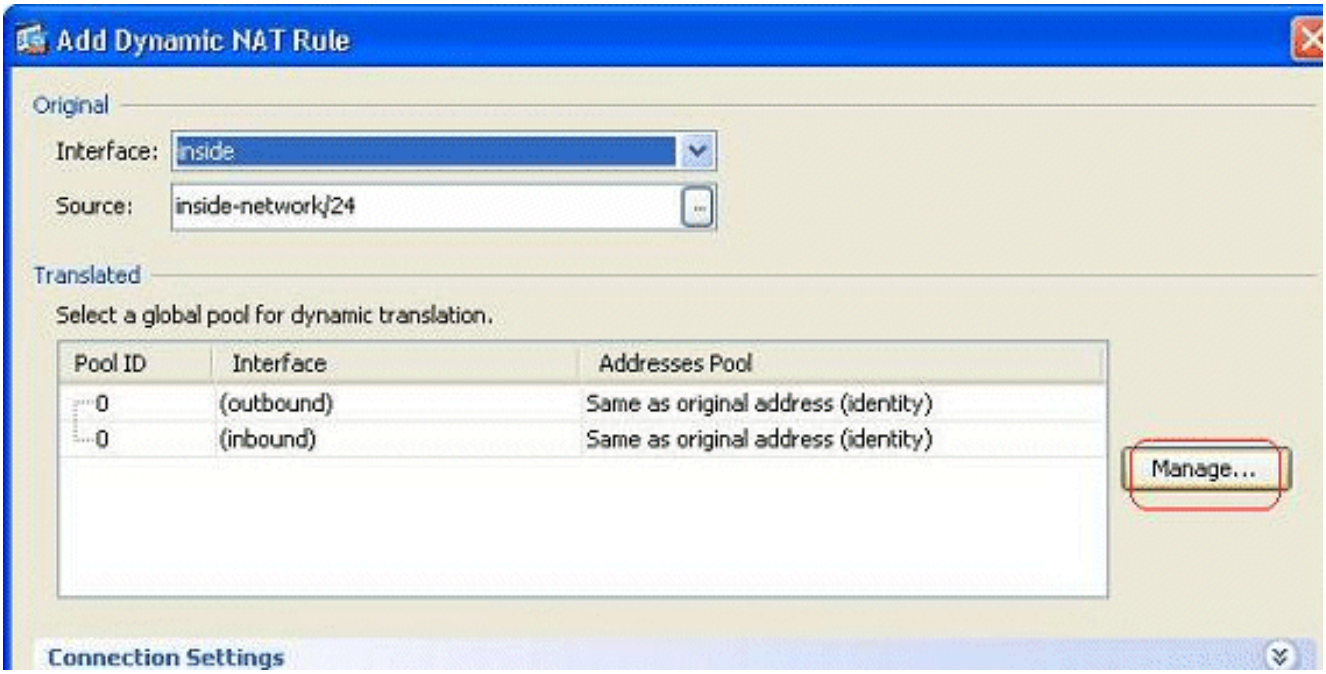
내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스하도록 허용하려면 다음 단계를 완료합니다.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하여 **Add(추가)**를 클릭한 다음 **Add Dynamic NAT Rule(동적 NAT 규칙 추가) 옵션을 선택하여 동적 NAT 규칙을 구성합니다.**

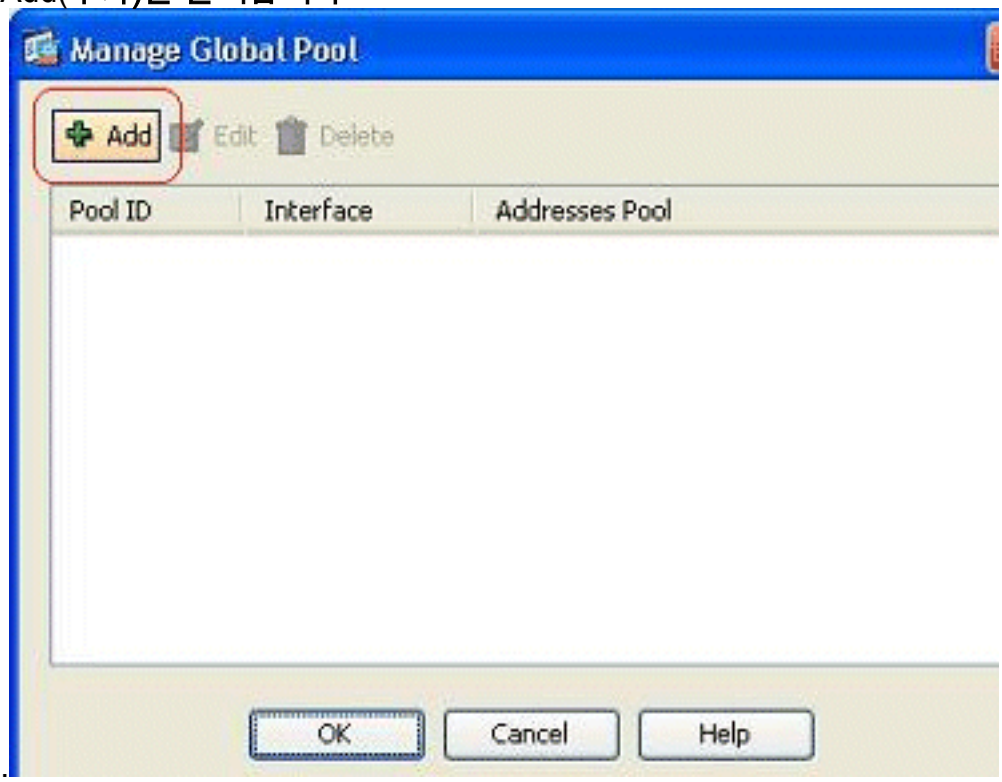


2. 실제 호스트가 연결된 인터페이스의 이름을 선택합니다.Source(소스) 필드의 Details(**세부사항)** 버튼을 사용하여 호스트/네트워크의 실제 IP 주소를 선택하고 **내부 네트워크**를 **선택합니다**.Manage(**관리**)를 클릭하여 변환된 주소 정보를 정의합니다

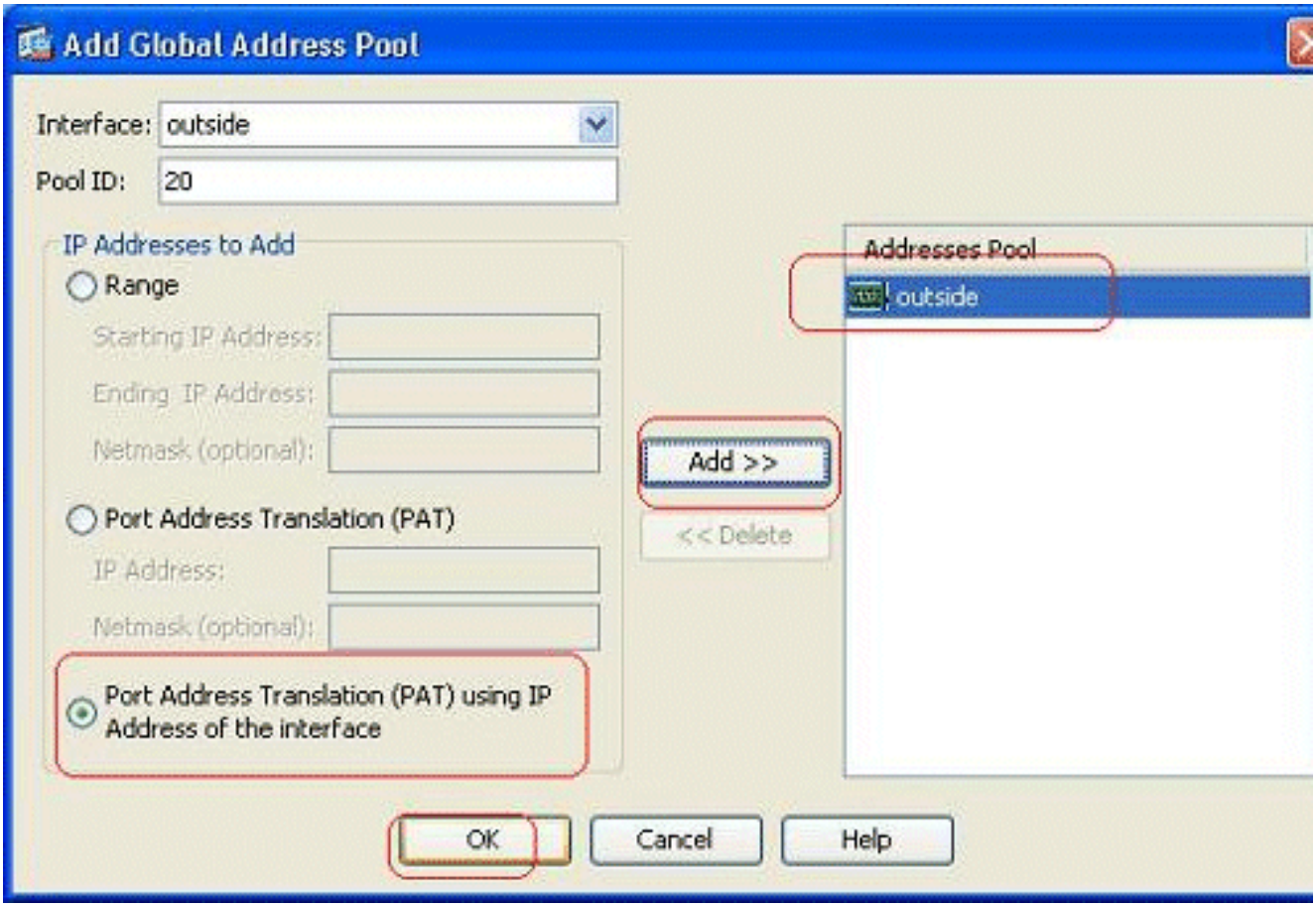
.



3. Add(**추가**)**를 클릭합니다**

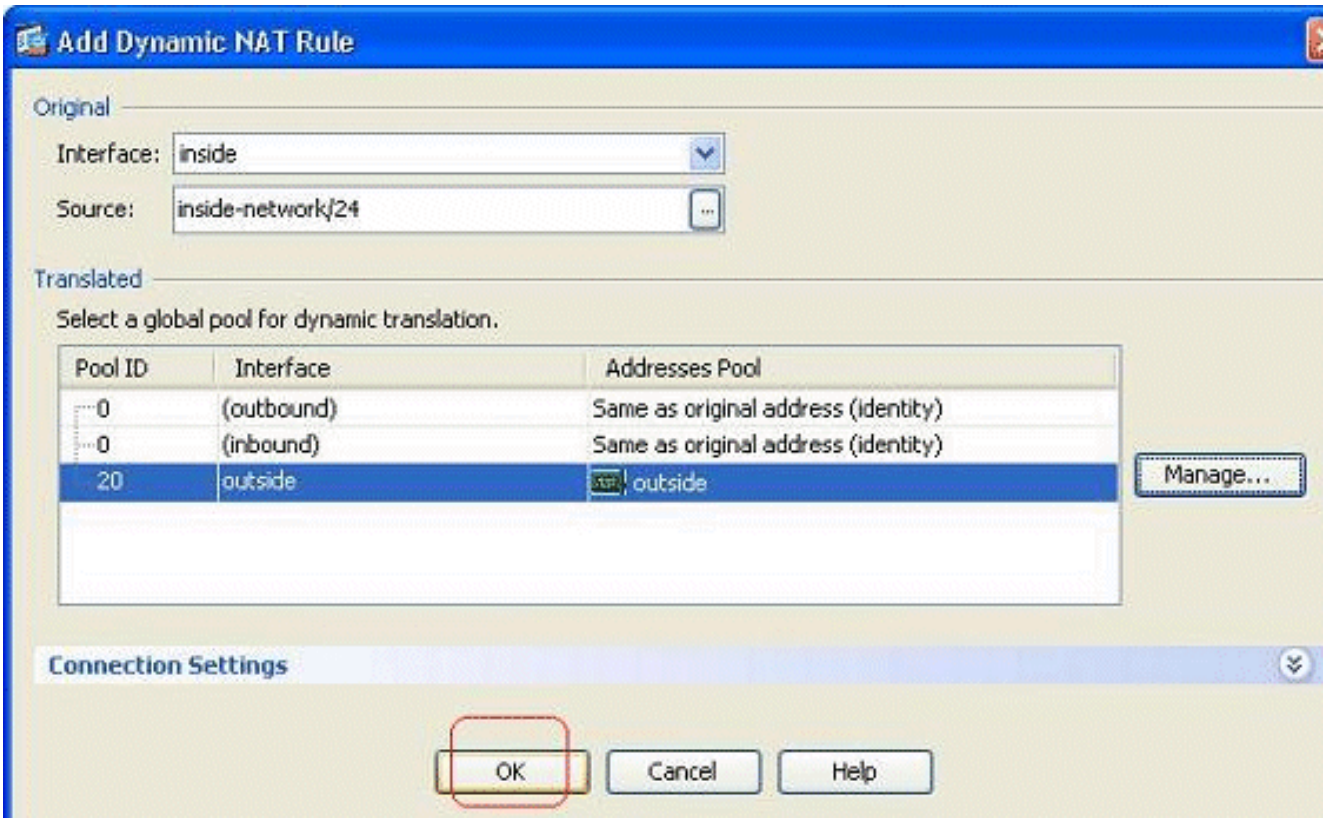


4. **인터페이스** 옵션**의 IP 주소를 사용하여 PAT(Port Address Translation)를** 선택하고 **Add를** 클릭하여 주소 풀에 추가합니다.이 NAT 주소 풀에 고유한 ID를 할당하는 것을 잊지 마십시오

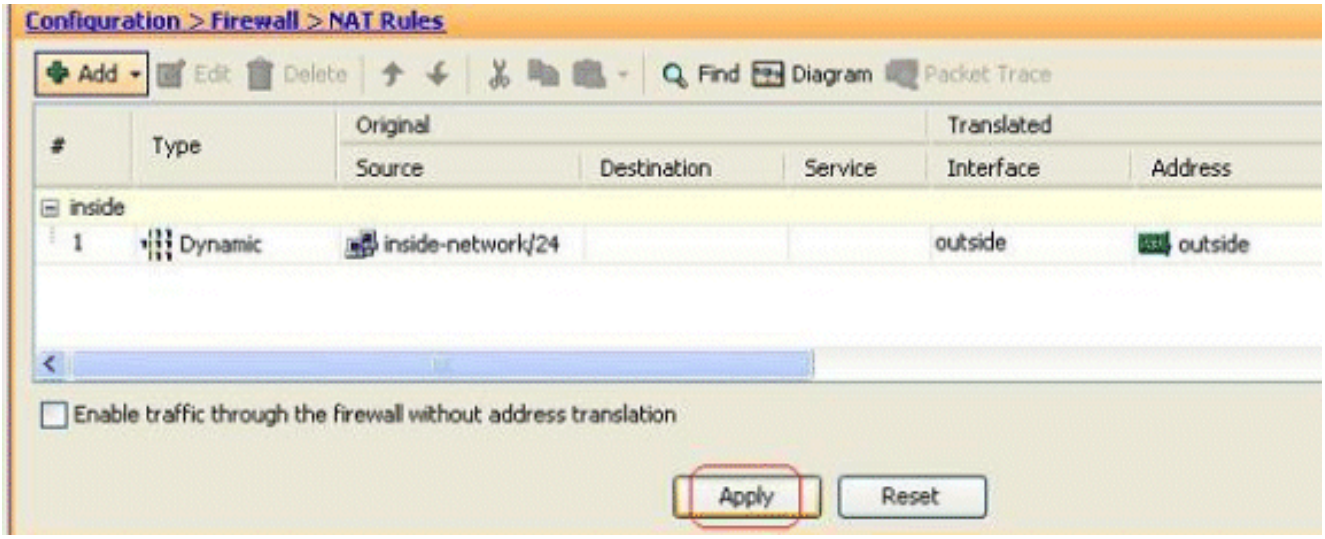


5. 여기에 표시된 것은 외부 인터페이스를 해당 풀에서 사용 가능한 유일한 주소로 구성한 주소 풀입니다.Add Dynamic NAT Rule 창으로 돌아가려면 OK를 클릭합니다

6. **확인**을 **클릭합니다**



7. 구성된 동적 NAT 규칙은 Configuration > Firewall > NAT Rules 창에 표시됩니다



이 PAT 컨피그레이션에 대한 CLI 출력입니다.

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

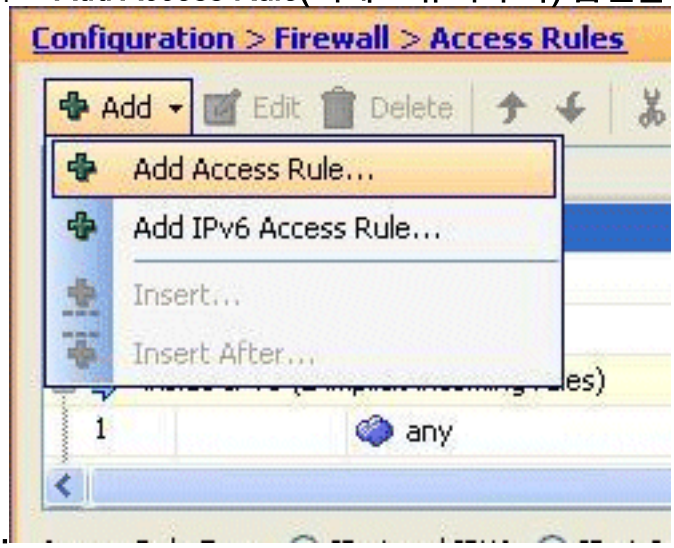
외부 네트워크에 대한 내부 호스트 액세스 제한

액세스 규칙이 정의되지 않은 경우 상위 보안 인터페이스의 사용자는 하위 보안 인터페이스와 연결된 리소스에 액세스할 수 있습니다.특정 사용자가 특정 리소스에 액세스하지 못하도록 제한하려면 ASDM에서 액세스 규칙을 사용합니다.이 예에서는 단일 사용자가 외부 리소스(FTP, SMTP, POP3, HTTPS 및 WWW 사용)에 액세스하도록 허용하고 다른 모든 사용자가 외부 리소스에 액세스하지 못하도록 제한하는 방법을 설명합니다.

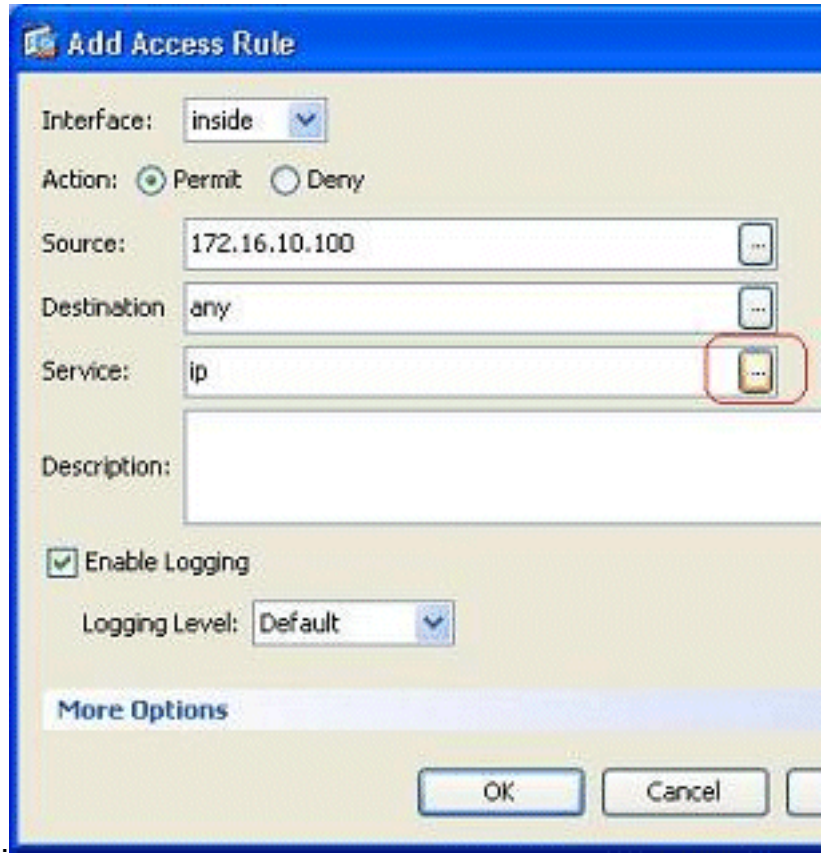
참고: 모든 액세스 목록의 끝에 "암시적 거부" 규칙이 있습니다.

다음 단계를 완료하십시오.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **Access Rules(액세스 규칙)로** 이동하여 **Add(추가)를** 클릭하고 **Add Access Rule(액세스 규칙 추가) 옵션을 선택하여 새 액세스 목록 항목을 생성합니다.**

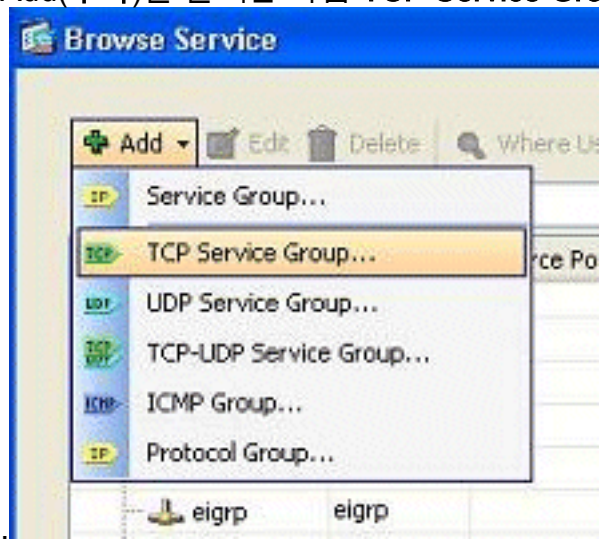


2. **Source** 필드에서 허용할 소스 IP 주소를 선택합니다.Destination(대상)으로, **내부**에서 Interface(인터페이스)로, **Permit(허용)**을 Action(작업)으로 선택합니다.마지막으로 필수 포트에 대한 TCP 서비스 그룹을 생성하려면 Service(서비스) 필드에서 Details(세부사항) 버튼을

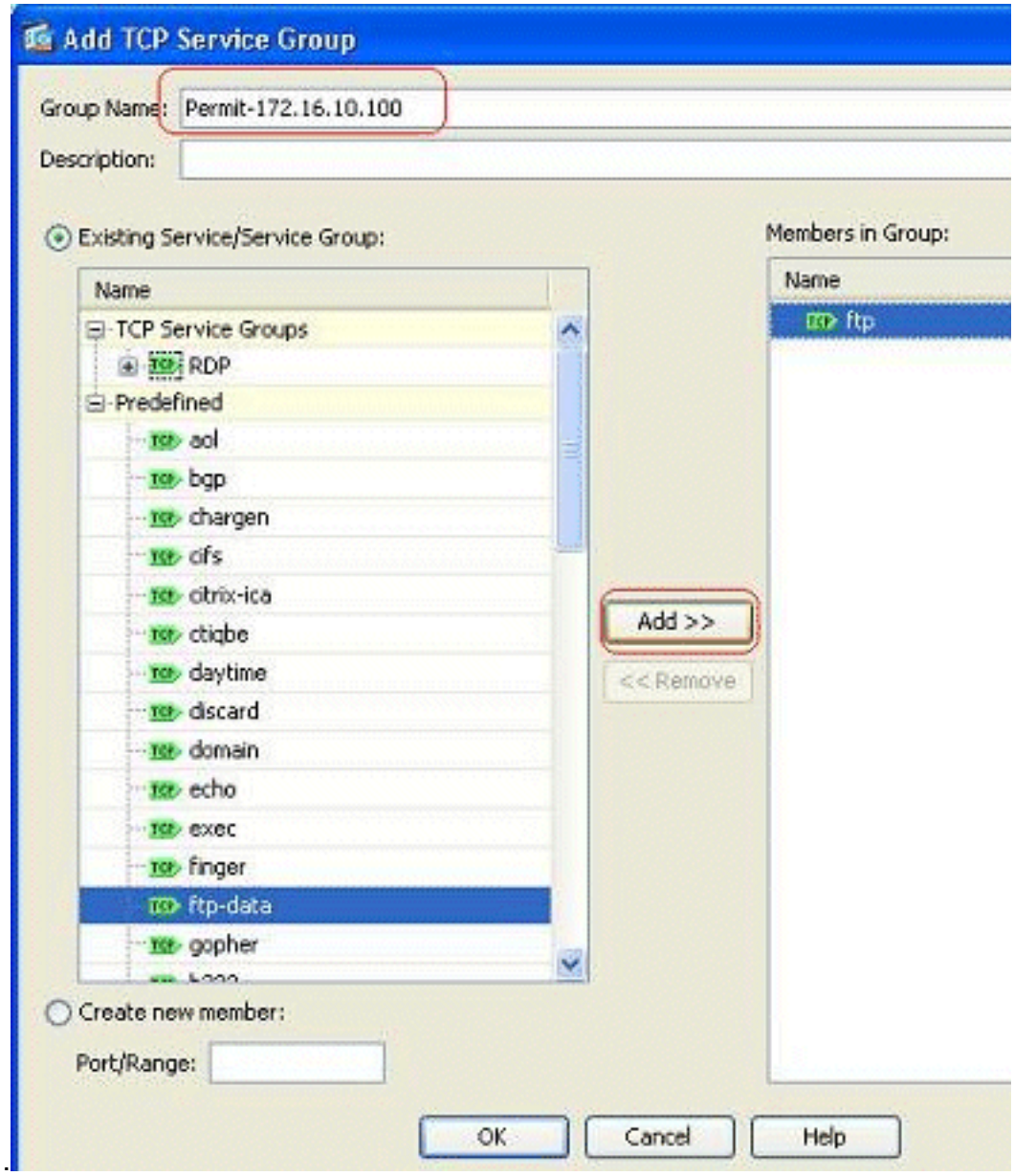


클릭합니다.

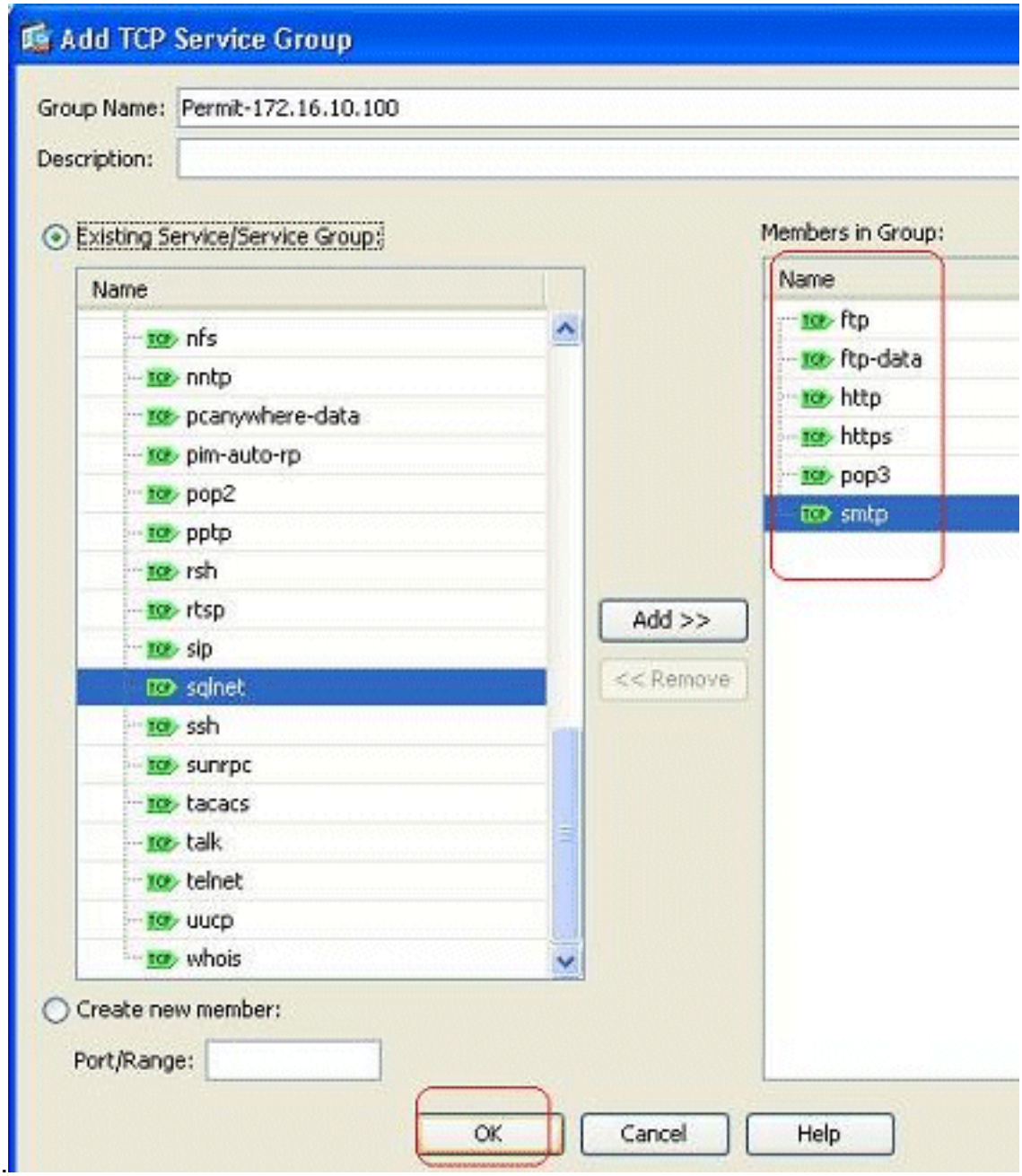
3. Add(**추가**)를 클릭한 다음 **TCP Service Group(TCP 서비스 그룹**) 옵션**을** 선택합니다



4. 이 그룹의 이름을 입력합니다.필요한 각 포트를 선택하고 Add(**추가)를** 클릭하여 Members in Group(그룹의 멤버) 필드로 이동합니다

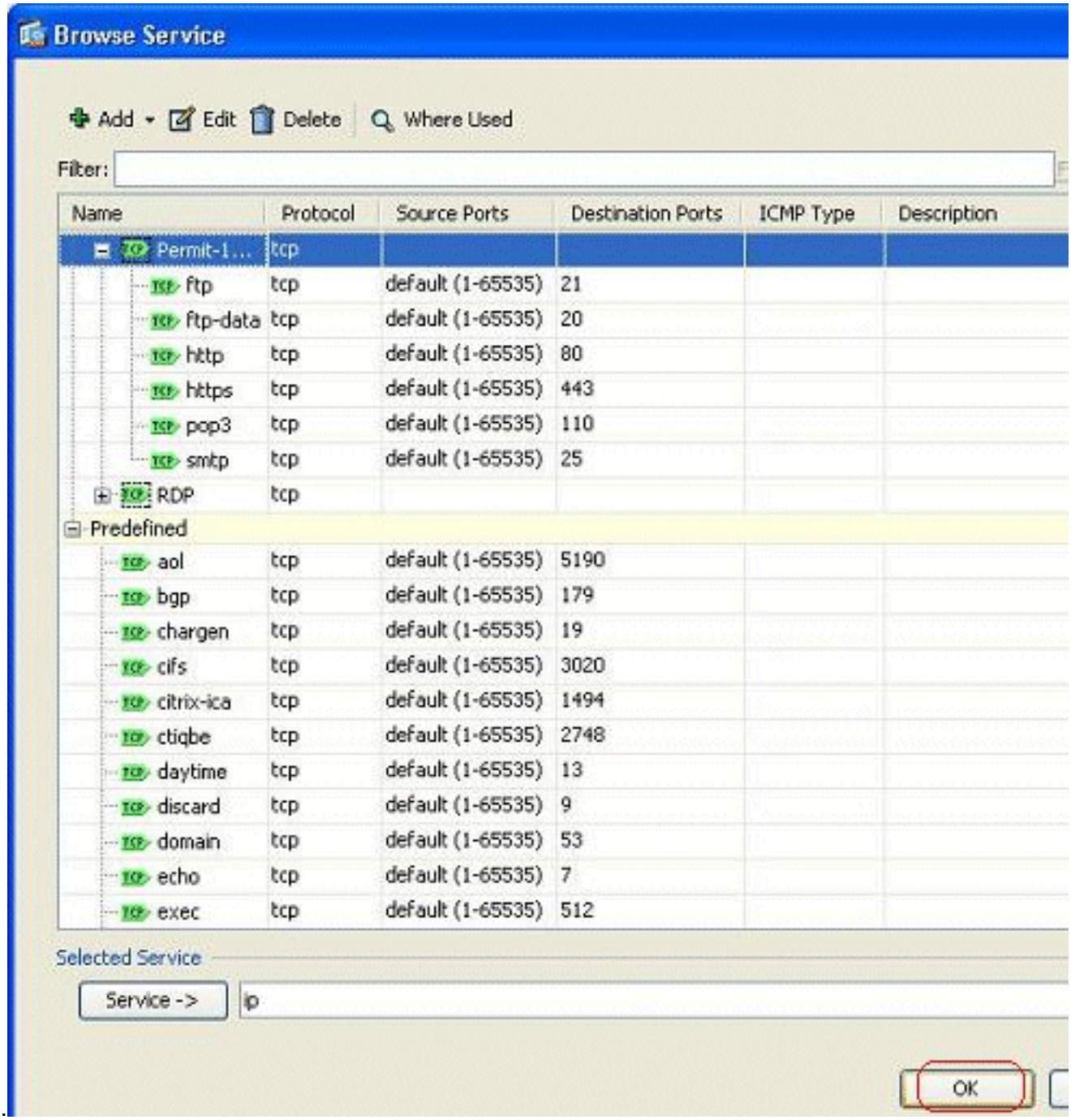


5. 오른쪽 필드에 선택한 모든 포트가 표시됩니다.확인을 클릭하여 서비스 포트 선택 프로세스를



완료합니다.

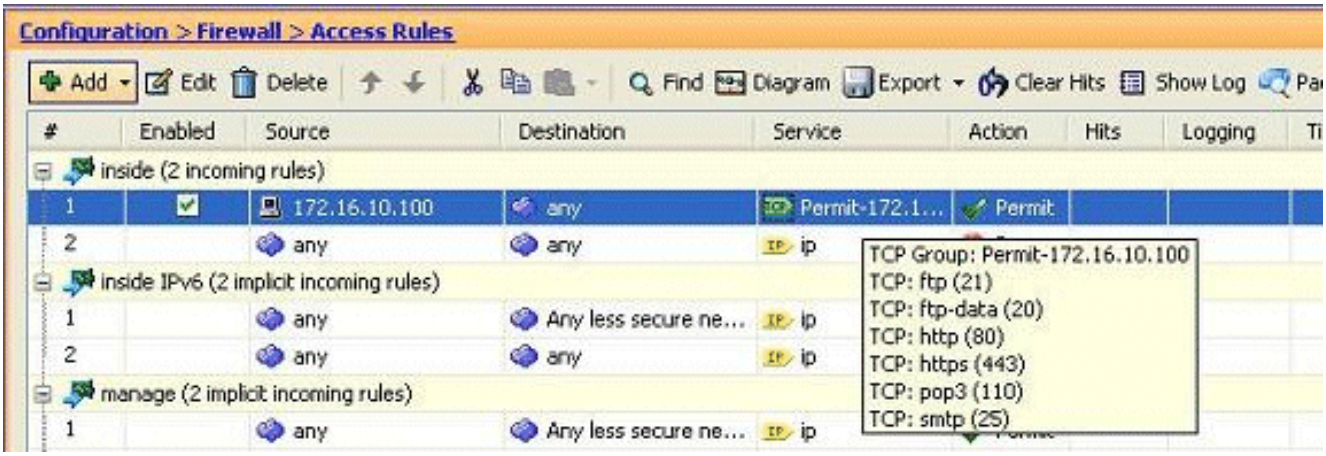
6. 여기서 구성된 TCP 서비스 그룹을 볼 수 있습니다.**확인**을 **클릭합니다**



7. OK(**확인**)를 클릭하여 컨피그레이션을 완료합니다

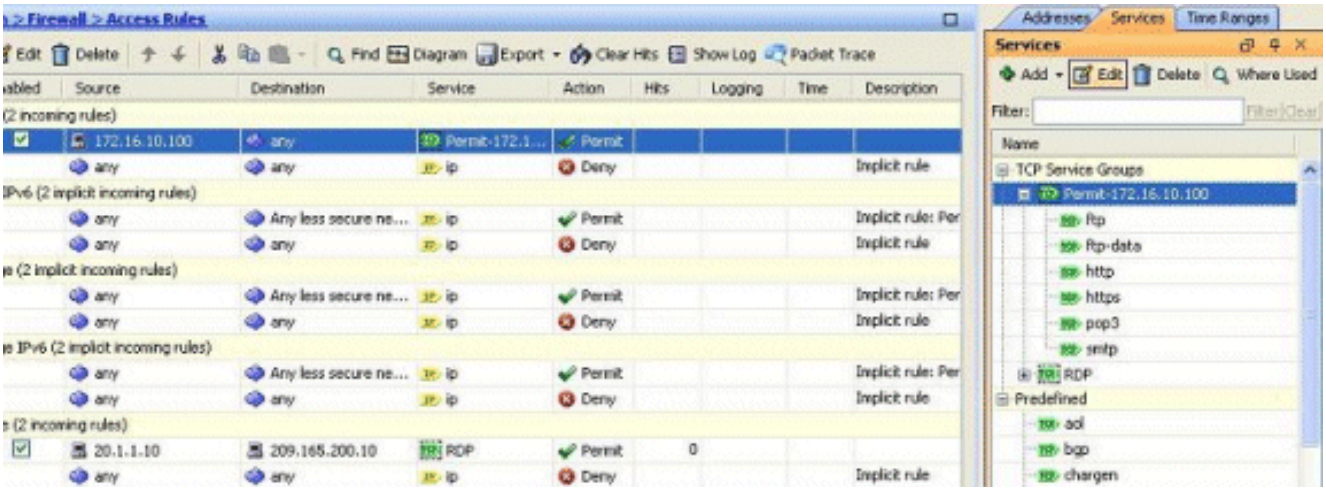
8. 구성된 액세스 규칙은 Configuration(컨피그레이션) > Firewall(방화벽) > Access Rules(액세스 규칙) 창의 **내부** 인터페이스 아래에 표시됩니다

.

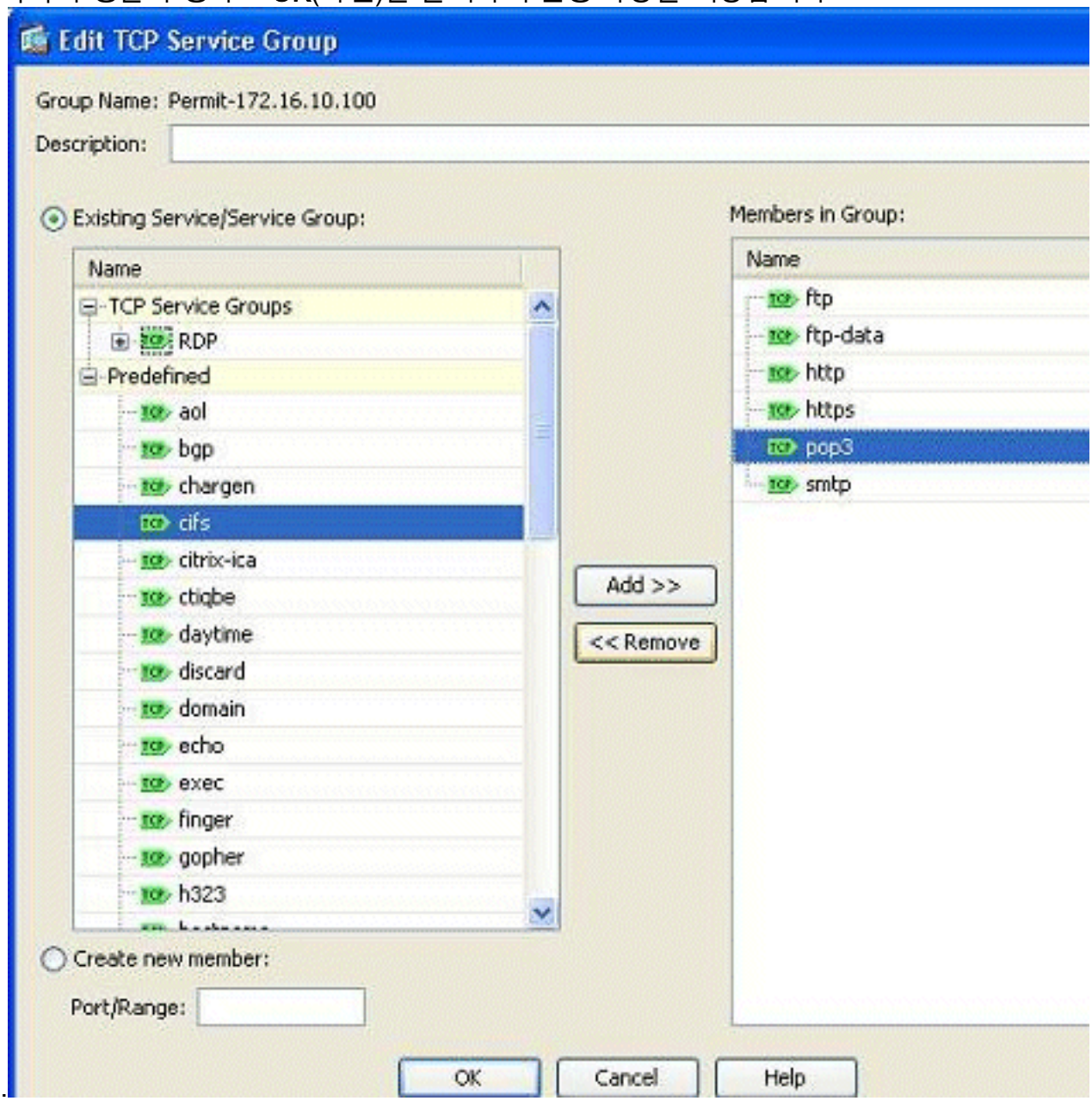


9. 사용 편의성을 위해 **Services** 탭의 오른쪽 창에 있는 TCP 서비스 그룹을 직접 편집할 수도 있습니다.이 서비스 그룹을 직접 수정하려면 Edit를 클릭합니다

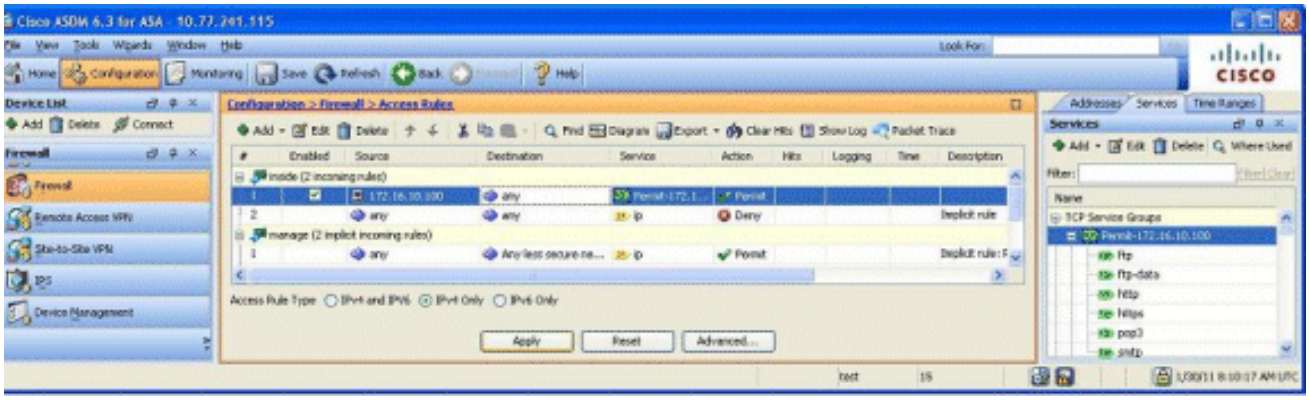
.



10. 다시 Edit TCP Service Group(TCP 서비스 그룹 수정) 창으로 리디렉션됩니다.요구 사항에 따라 수정을 수행하고 **OK**(확인)를 클릭하여 변경 사항을 저장합니다



11. 다음은 ASDM의 전체 보기입니다



이는 동일한 CLI 컨피그레이션입니다.

```
object-group service Permit-172.16.10.100 TCP
```

```
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
    object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

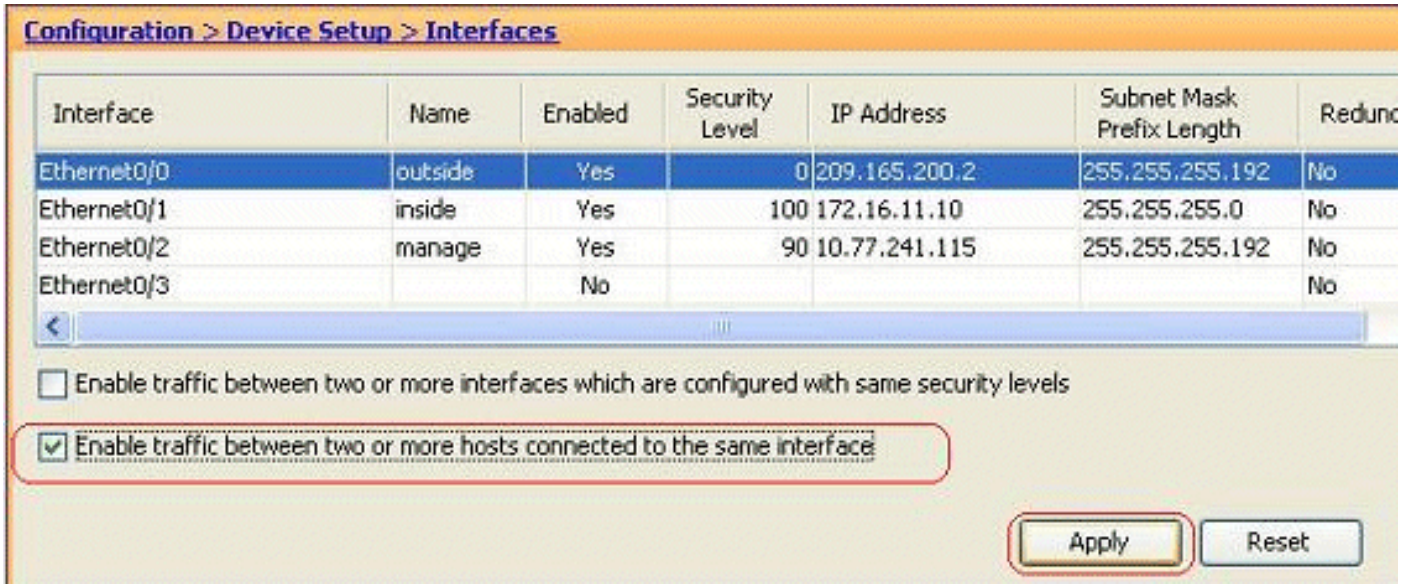
액세스 제어 구현에 대한 자세한 내용은 ASDM GUI를 통해 액세스 목록 추가 또는 수정을 참조하십시오.

보안 수준이 동일한 인터페이스 간 트래픽 허용

이 섹션에서는 보안 수준이 동일한 인터페이스 내에서 트래픽을 활성화하는 방법에 대해 설명합니다.

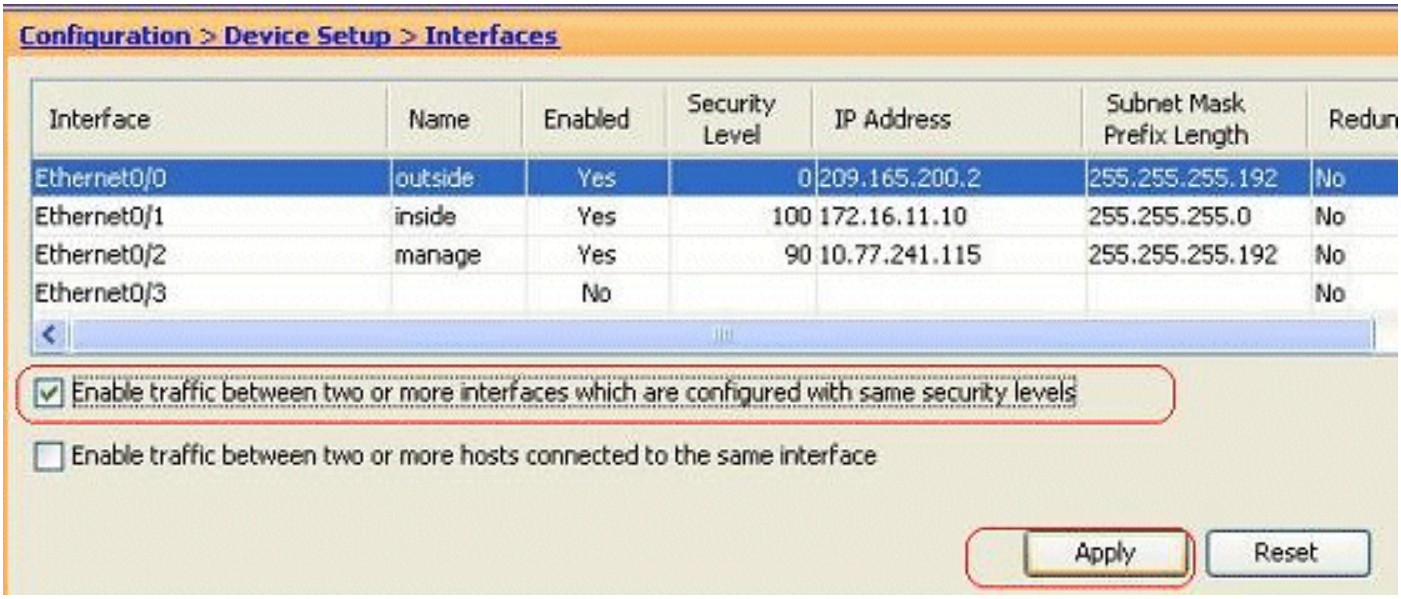
이 지침은 인터페이스 내 통신을 활성화하는 방법에 대해 설명합니다.

이는 인터페이스로 들어가지만 동일한 인터페이스로 라우팅되는 VPN 트래픽에 유용합니다.이 경우 VPN 트래픽은 암호화되지 않거나 다른 VPN 연결을 위해 다시 암호화될 수 있습니다.Configuration(컨피그레이션) > **Device Setup(디바이스 설정)** > **Interfaces(인터페이스)**로 이동하고 **Enable traffic between two or more hosts connected to the same interface** 옵션을 선택합니다.



이 지침은 인터페이스 간 통신을 활성화하는 방법에 대해 설명합니다.

이는 보안 수준이 동일한 인터페이스 간의 통신을 허용하는 데 유용합니다.Configuration(**컨피그레이션**) > **Device Setup(디바이스 설정)** > **Interfaces(인터페이스)**로 이동하고 **동일한 보안 레벨로 구성된 둘 이상의 인터페이스 간 트래픽 활성화** 옵션을 선택합니다.



이 CLI는 다음 설정 모두에 해당하는 CLI입니다.

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

신뢰할 수 없는 호스트에서 신뢰할 수 있는 네트워크의 호스트에 액세스 허용

이를 위해서는 고정 NAT 변환 및 액세스 규칙을 적용하여 해당 호스트를 허용할 수 있습니다.외부 사용자가 내부 네트워크에 있는 서버에 액세스하려는 경우 이를 구성해야 합니다.내부 네트워크의 서버에 인터넷에서 라우팅할 수 없는 전용 IP 주소가 있습니다.따라서 고정 NAT 규칙을 통해 프라이빗 IP 주소를 공용 IP 주소로 변환해야 합니다.내부 서버(172.16.11.5)이 있다고 가정합니다. 이 작업을 수행하려면 이 사설 서버 IP를 공용 IP로 변환해야 합니다.이 예에서는 172.16.11.5을 209.165.200.5으로 변환하기 위해 양방향 고정 NAT를 구현하는 방법을 설명합니다.

액세스 규칙을 구현하여 외부 사용자가 이 웹 서버에 액세스하도록 허용하는 섹션은 여기에 표시되지 않습니다.다음 내용을 이해하려면 여기에 간단한 CLI 코드 조각이 나와 있습니다.

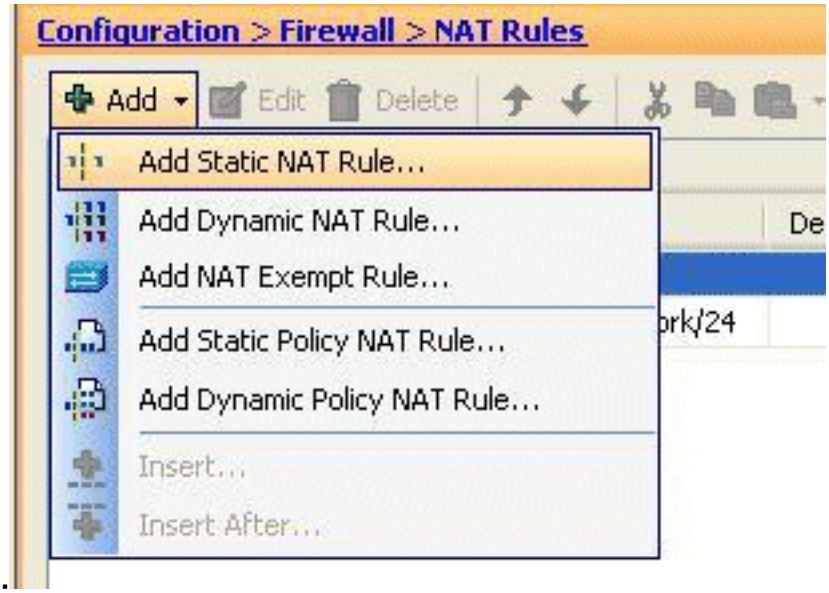
```
access-list 101 permit TCP any host 209.165.200.5
```

자세한 내용은 ASDM GUI를 통해 액세스 목록 추가 또는 수정을 참조하십시오.

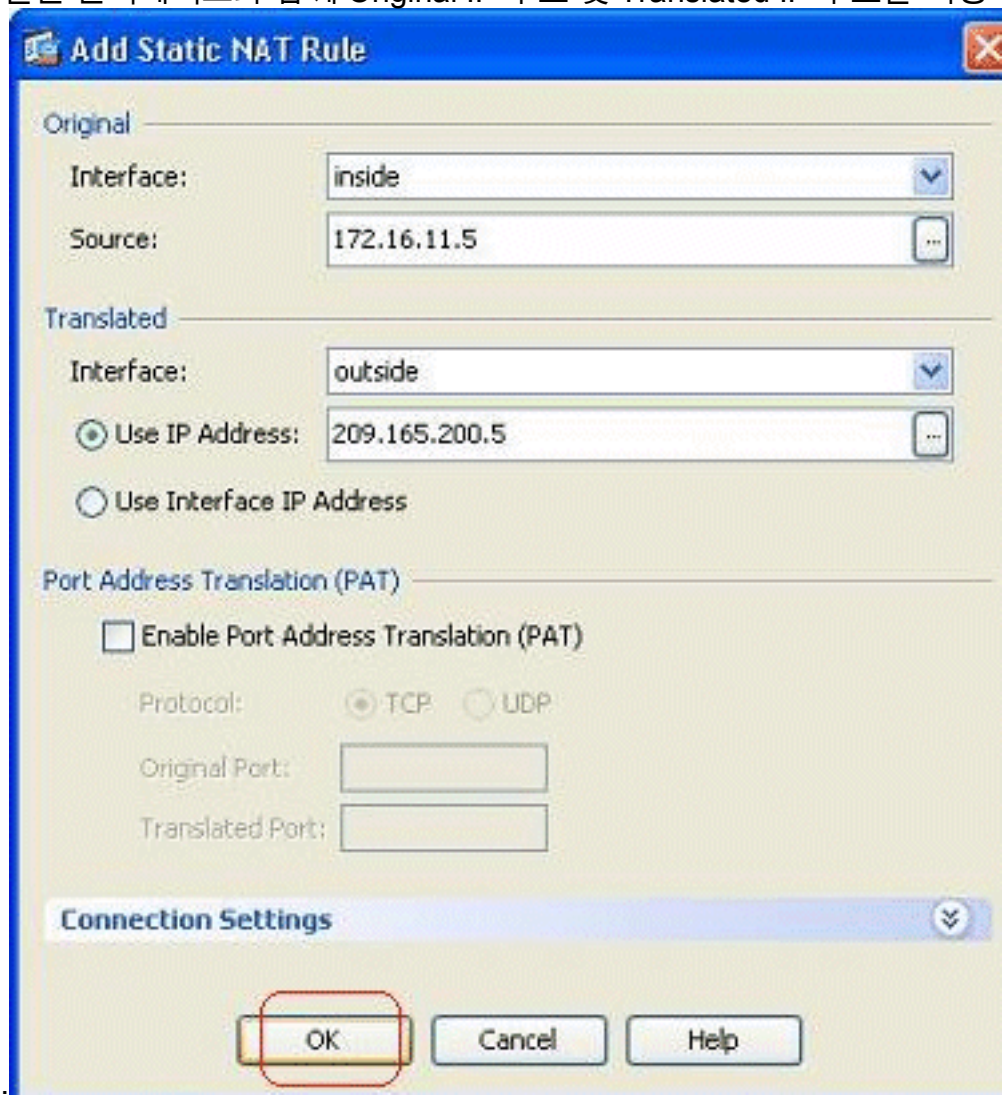
참고: "any" 키워드를 지정하면 외부 사용자가 이 서버에 액세스할 수 있습니다.또한 서비스 포트에 대해 지정되지 않은 경우 서비스 포트가 열려 있을 때 임의의 서비스 포트에서 서버에 액세스할 수 있습니다.구현할 때는 주의해야 하며, 개별 외부 사용자 및 서버의 필수 포트로 권한을 제한하는 것이 좋습니다.

고정 NAT를 구성하려면 다음 단계를 완료합니다.

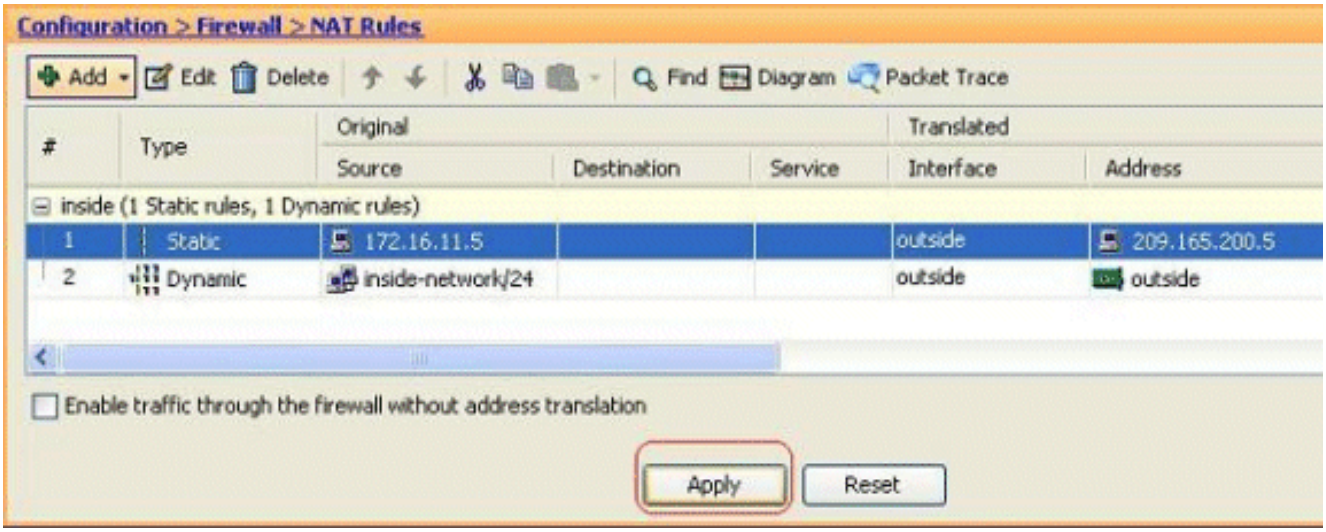
1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하고 **Add(추가)**를 클릭하고 Add Static NAT **Rule(고정 NAT 규칙 추가)을 선택합니다**



2. 연결된 인터페이스와 함께 Original IP 주소 및 Translated IP 주소를 지정하고 **OK**를 클릭합니다.



3. 여기에서 구성된 고정 NAT 항목을 볼 수 있습니다.Apply(**적용**)를 클릭하여 ASA로 전송합니다.



다음은 이 ASDM 컨피그레이션에 대한 간단한 CLI 예입니다.

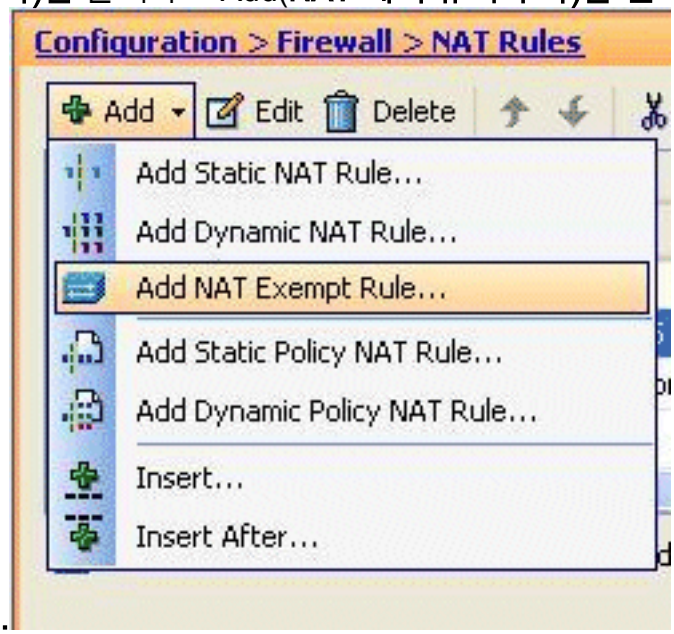
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

특정 호스트/네트워크에 대해 NAT 비활성화

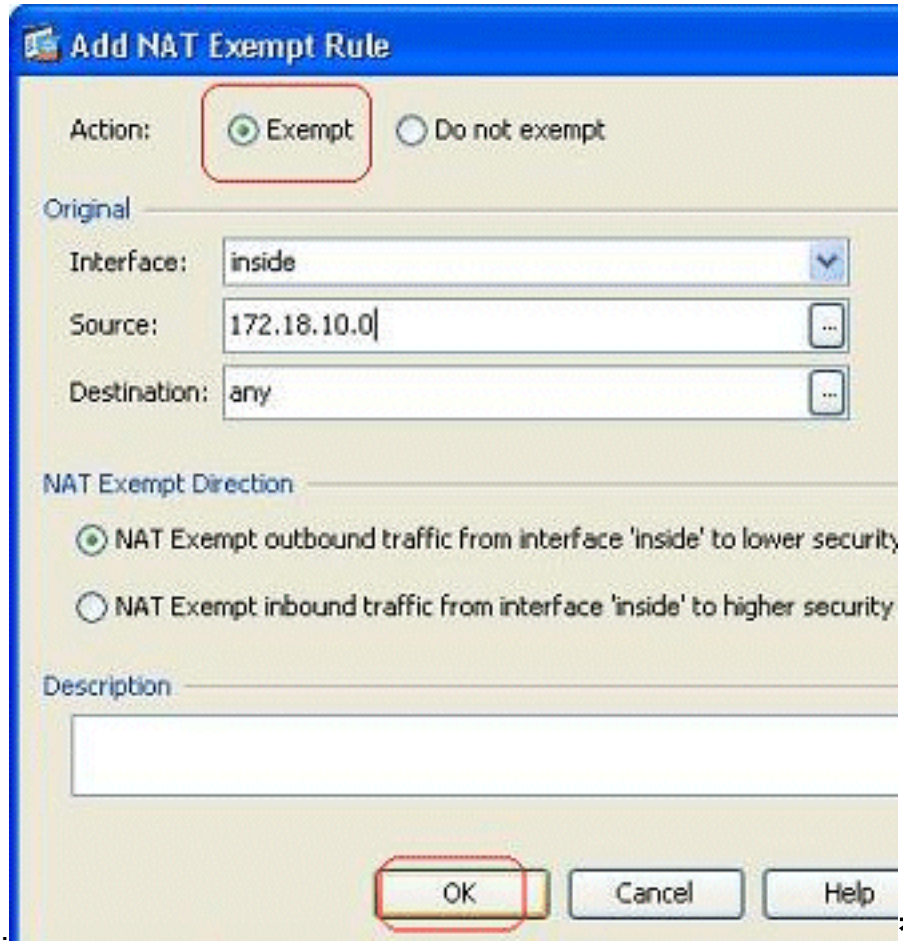
NAT에서 특정 호스트 또는 네트워크를 제외해야 하는 경우 주소 변환을 비활성화하려면 NAT Exempt Rule을 추가합니다.이렇게 하면 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

다음 단계를 완료하십시오.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하고 **Add(추가)를** 클릭하고 Add(**NAT 제외 규칙 추가)를 선택합니다**

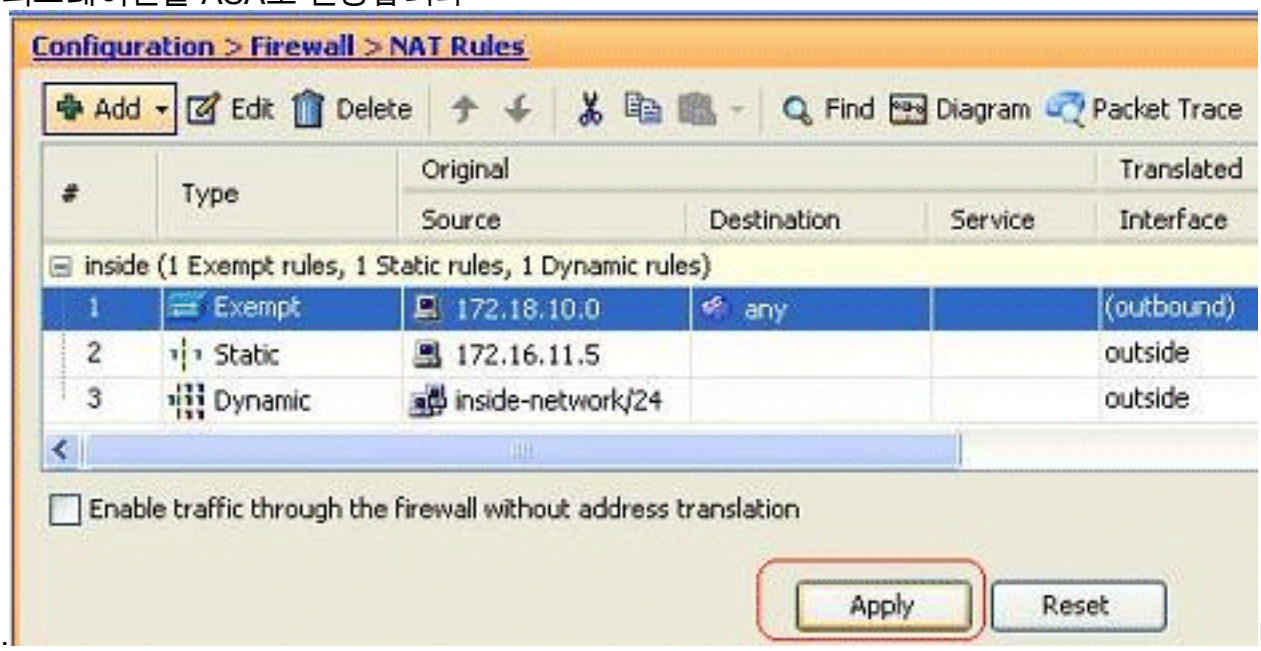


2. 여기서 내부 네트워크 172.18.10.0은 주소 변환에서 제외되었습니다.Exempt(**제외**) 옵션이 선택되었는지 확인합니다.NAT Exempt Direction에는 두 가지 옵션이 있습니다.낮은 보안 인터페이스로 향하는 아웃바운드 트래픽상위 보안 인터페이스로 향하는 인바운드 트래픽기본 옵션은 아웃바운드 트래픽에 대한 것입니다.**확인**을 클릭하여 단계를 완료합니다



참고: Do not exempt 옵션을 선택하면 해당 특정 호스트가 NAT에서 면제되지 않으며 별도의 액세스 규칙이 "deny" 키워드와 함께 추가됩니다.이는 특정 호스트가 NAT 제외에서 전체 서브넷으로 제외되는 것을 방지하는 데 도움이 되며, 이러한 호스트는 제외됩니다.

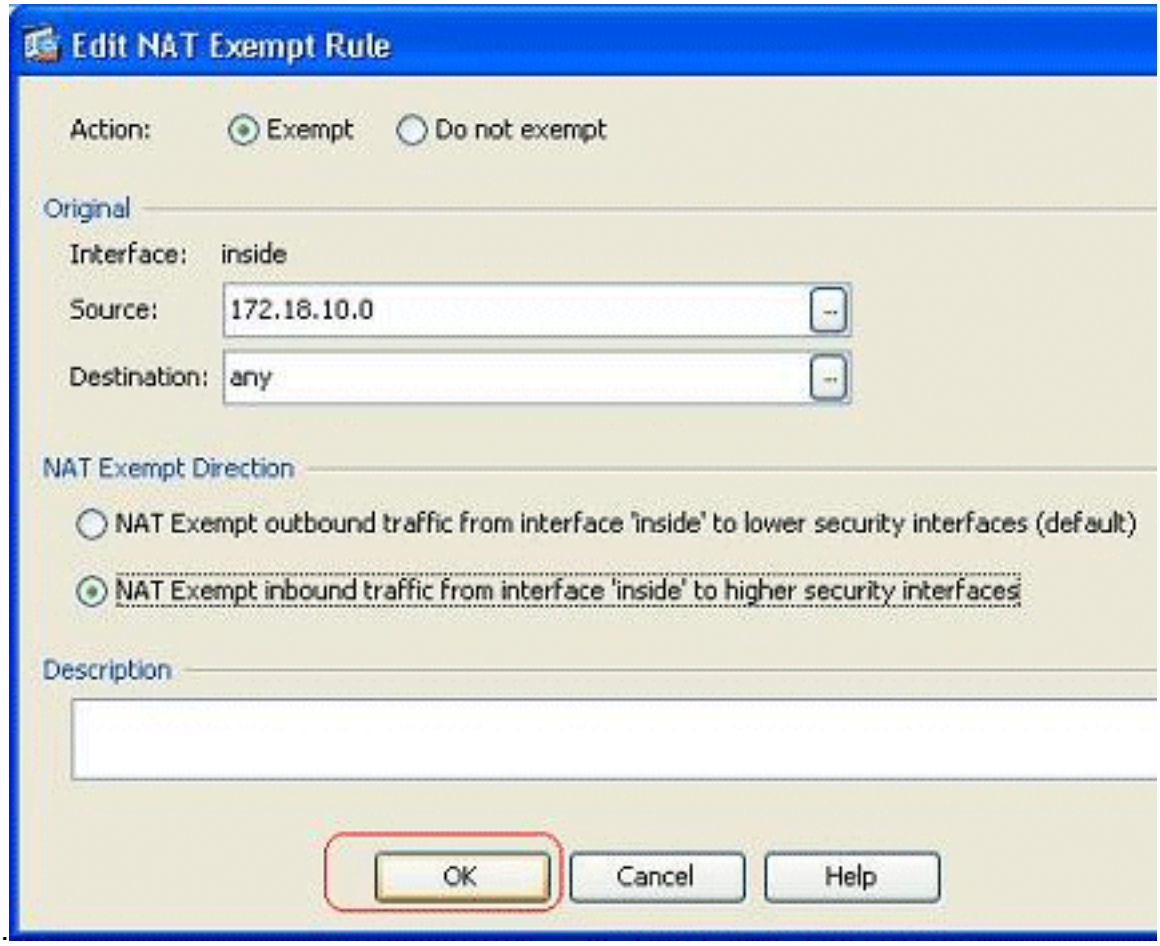
3. 여기서 아웃바운드 방향에 대한 NAT 제외 규칙을 볼 수 있습니다.Apply(**적용**)를 클릭하여 컨피그레이션을 ASA로 전송합니다



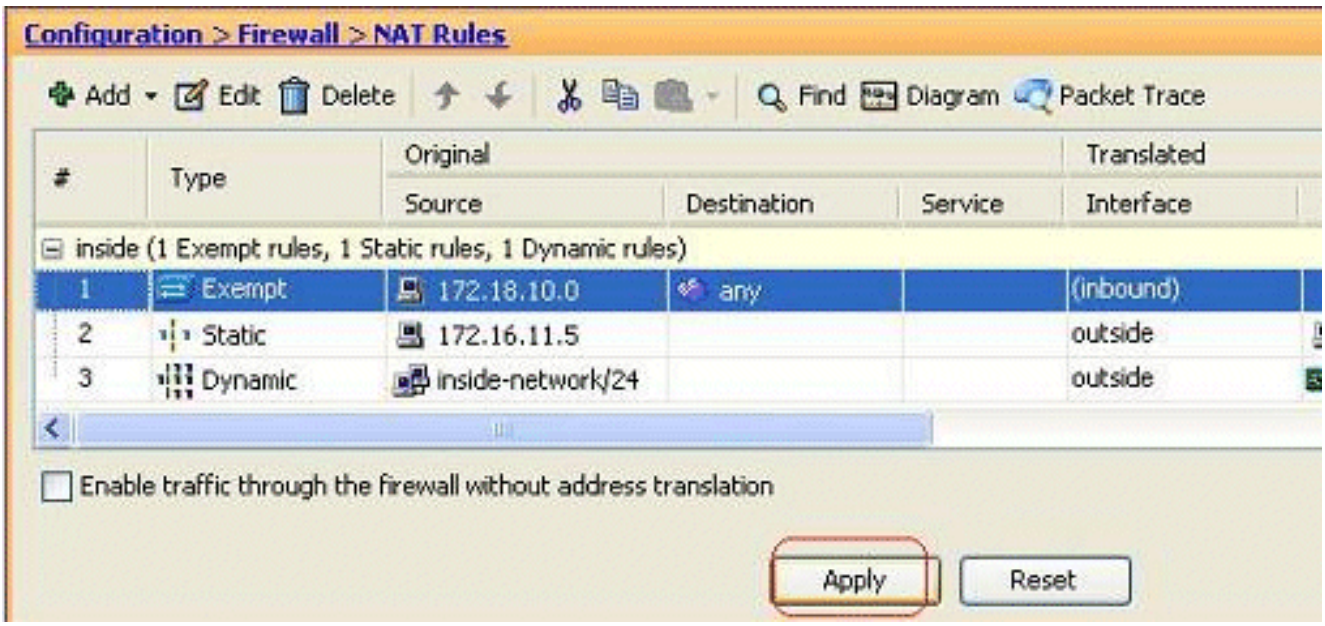
다음은 참조에 해당하는 CLI 출력입니다.

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. 여기서 방향에 대한 NAT 제외 규칙을 수정하는 방법을 확인할 수 있습니다.옵션을 적용하려면 **확인**을 클릭합니다



5. 이제 방향이 *인바운드*으로 변경되었음을 확인할 수 있습니다

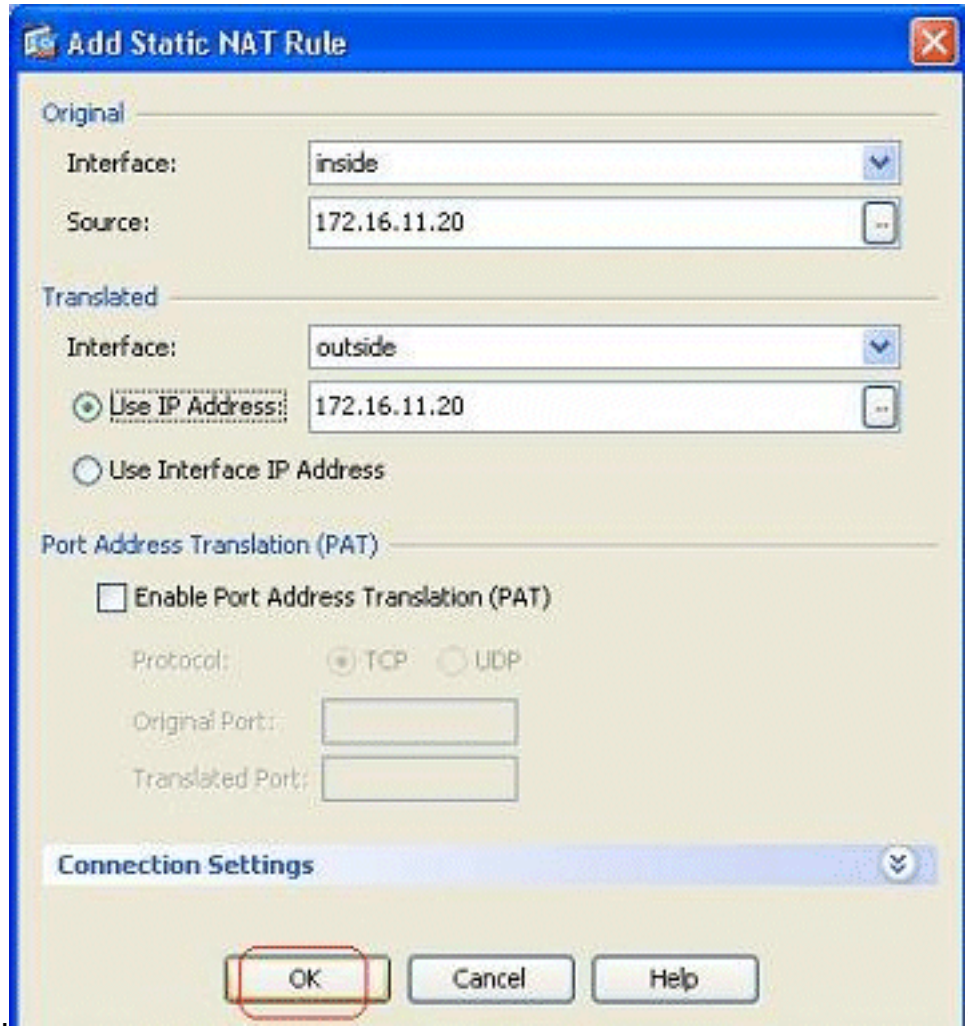


이 CLI 출력을 ASA에 전송하려면 **Apply**(적용)를 클릭합니다.

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

참고: 여기서 새 키워드(외부)가 nat **0** 명령 끝에 추가된 것을 확인할 수 있습니다.이 기능을 외부 NAT라고 **합니다**.

6. NAT를 비활성화하는 또 다른 방법은 ID NAT를 구현하는 것입니다.ID NAT는 호스트를 동일한 IP 주소로 변환합니다.다음은 외부에서 액세스할 때 호스트(172.16.11.20)이 동일한 IP 주소로 변환되는 일반 고정 ID NAT 예입니다



이는 다음과 같은 CLI 출력입니다.

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

정학을 사용한 포트 리디렉션(전달)

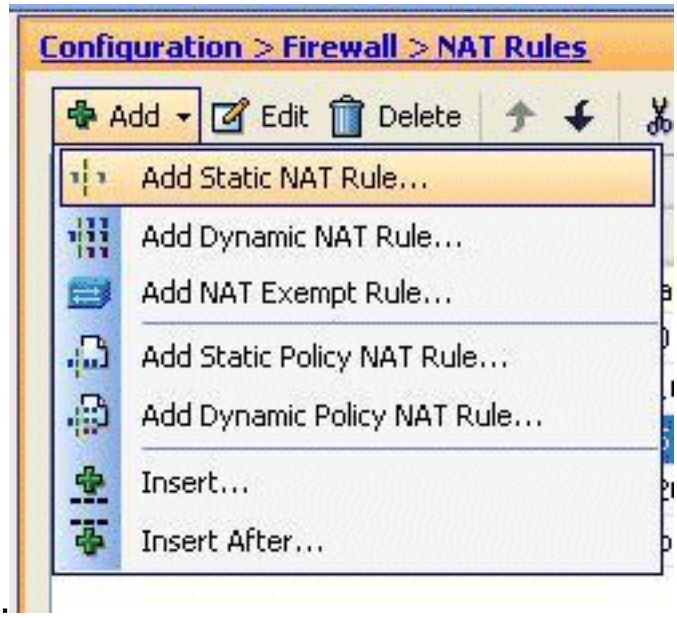
포트 전달 또는 포트 리디렉션은 외부 사용자가 특정 포트의 내부 서버에 액세스하려고 시도하는 데 유용한 기능입니다.이를 위해 사설 IP 주소가 있는 내부 서버가 공용 IP 주소로 변환되고, 이 경우 특정 포트에 대한 액세스가 허용됩니다.

이 예에서는 외부 사용자가 포트 25에서 209.165.200.15 SMTP 서버에 액세스하려고 합니다. 이 작업은 두 단계로 수행됩니다.

1. 포트 25의 172.16.11.15 내부 메일 서버를 포트 25의 공용 IP 주소 209.165.200.15으로 변환합니다.
2. 포트 25에서 209.165.200.15 공용 메일 서버에 대한 액세스를 허용합니다.

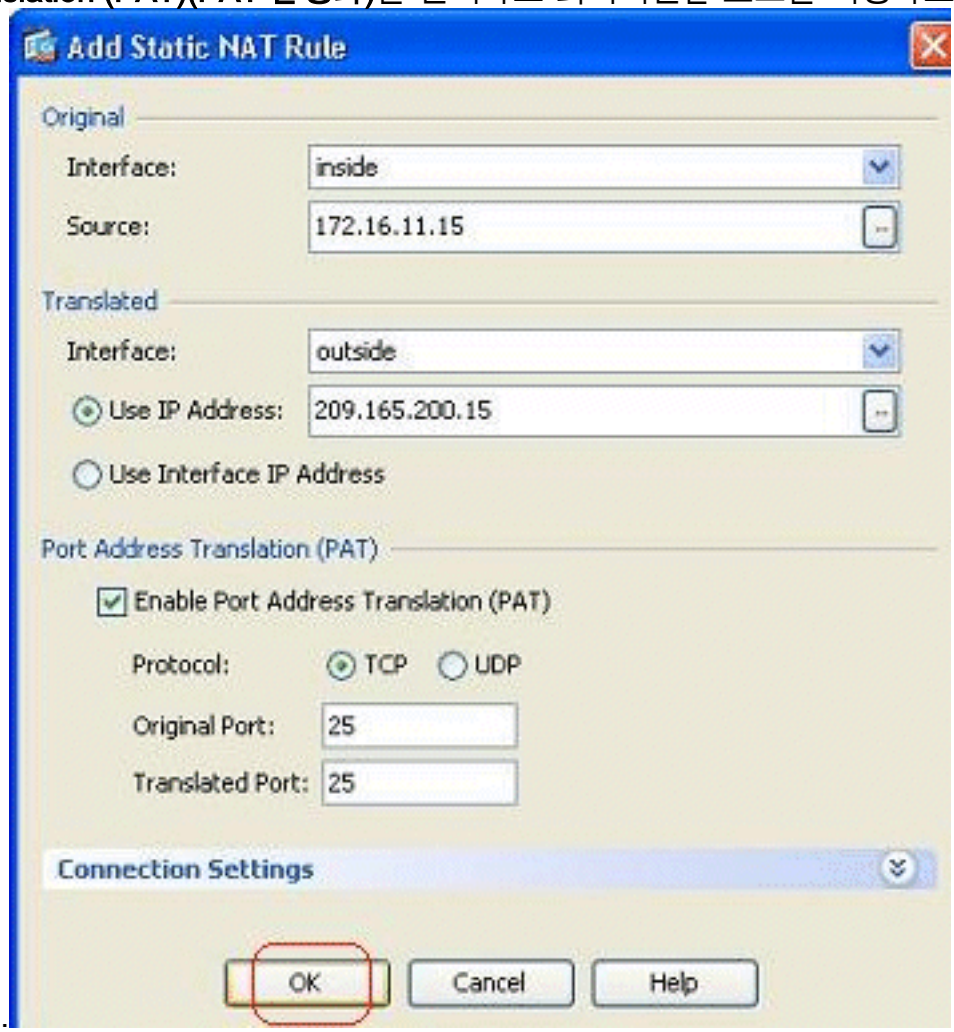
외부 사용자가 포트 25에서 서버209.165.200.15 액세스하려고 하면 이 트래픽은 내부 메일 서버, 포트 25에서 172.16.11 15로 리디렉션됩니다.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **NAT Rules(NAT 규칙)로** 이동하고 **Add(추가)**를 클릭하고 Add Static NAT **Rule(고정 NAT 규칙 추가)을 선택합니다**



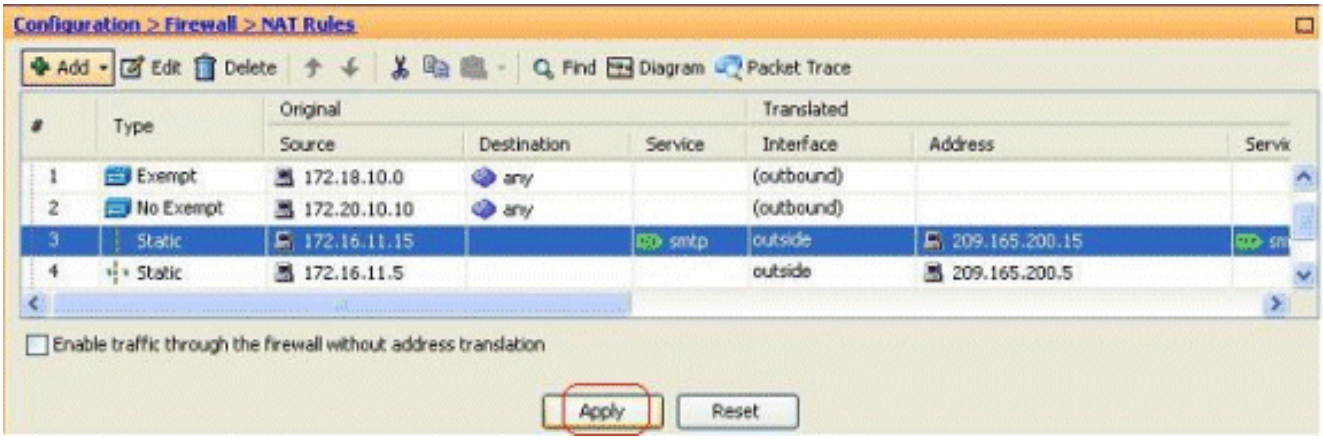
.

2. 원래 소스 및 변환된 IP 주소를 관련 인터페이스와 함께 지정합니다.Enable **Port Address Translation (PAT)(PAT 활성화)**을 선택하고 리디렉션할 포트를 지정하고 **OK(확인)**를 클릭합니다.



3. 구성된 고정 PAT 규칙은 다음과 같습니다

.



이는 다음과 같은 CLI 출력입니다.

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255
!
```

4. 외부 사용자가 다음 209.165.200.15에서 공용 smtp 서버에 액세스할 수 있도록 하는 액세스 규칙입니다

.

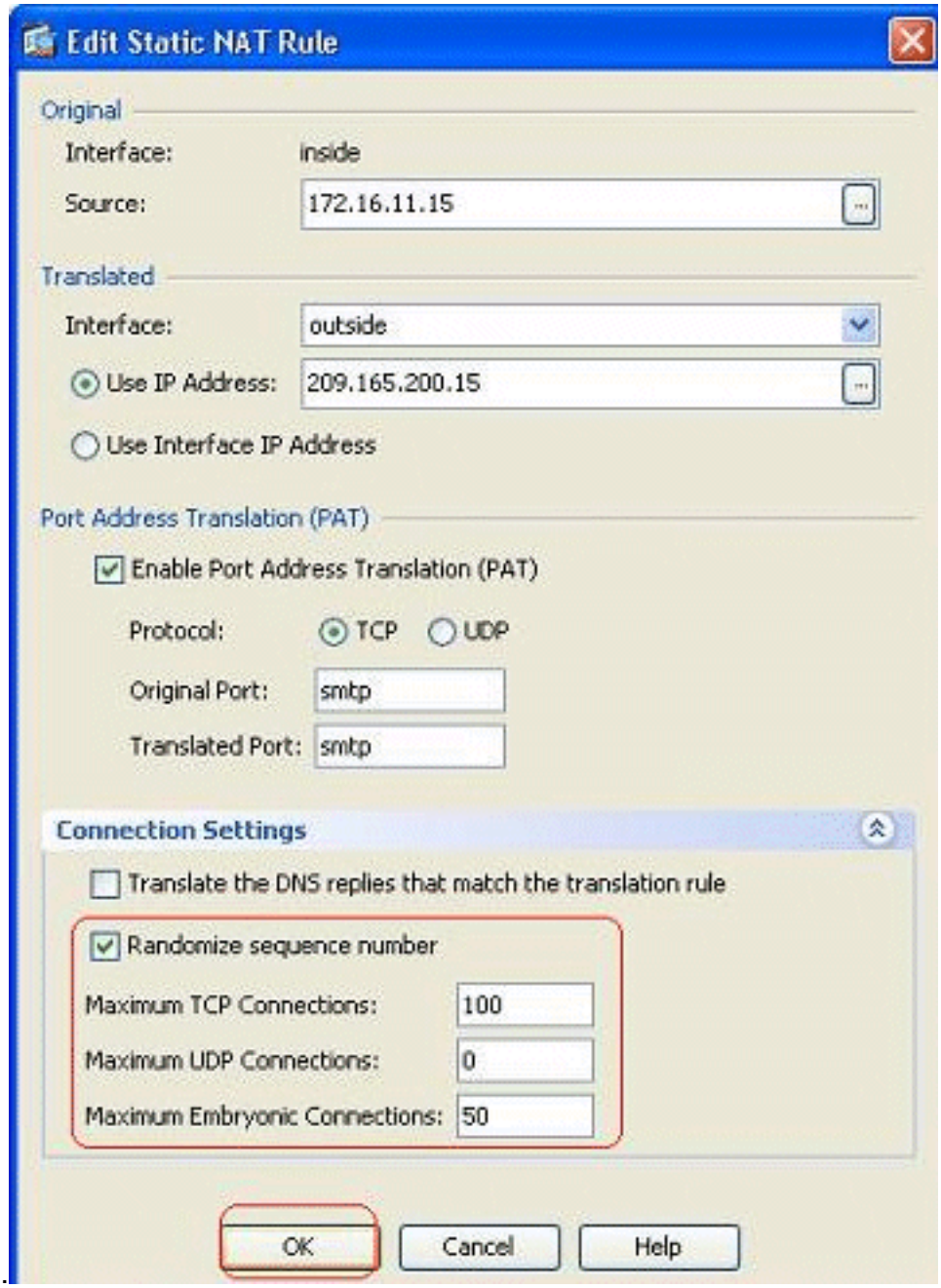
참고: 액세스 규칙 소스에서 **any** 키워드 대신 특정 호스트를 사용해야 합니다.

정적으로 TCP/UDP 세션 제한

Static Rule을 사용하여 최대 TCP/UDP 연결 수를 지정할 수 있습니다.최대 원시 연결 수를 지정할 수도 있습니다.원시 연결은 절반이 열린 상태의 연결입니다.이 중 많은 수가 ASA의 성능에 영향을 미칩니다.이러한 연결을 제한하면 DoS 및 SYN과 같은 특정 공격을 어느 정도 방지할 수 있습니다 .전체 차단을 위해 이 문서의 범위를 벗어나는 MPF 프레임워크에서 정책을 정의해야 합니다.이 항목에 대한 자세한 내용은 네트워크 공격 완화 를 참조하십시오.

다음 단계를 완료하십시오.

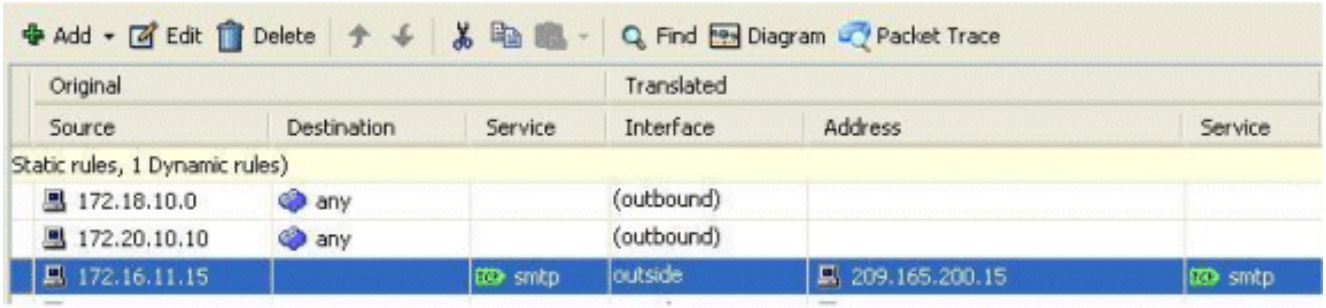
1. Connection **Settings(연결 설정)** 탭을 클릭하고 이 고정 변환에 대한 최대 연결 값을 지정합니

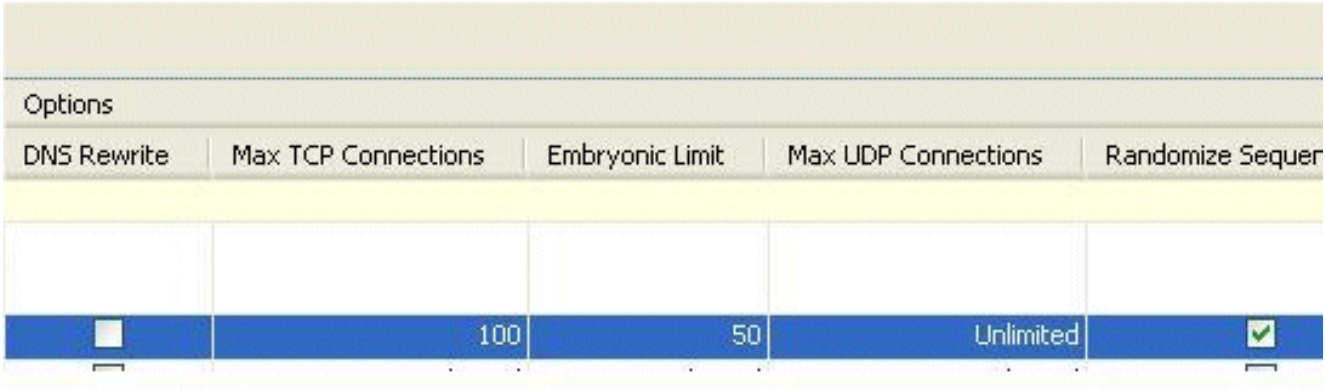


다.

2. 다음 이미지는 이 특정 정적 변환에 대한 연결 제한을 보여줍니다

.





이는 다음과 같은 CLI 출력입니다.

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
    255.255.255.255 TCP 100 50
!
```

시간 기반 액세스 목록

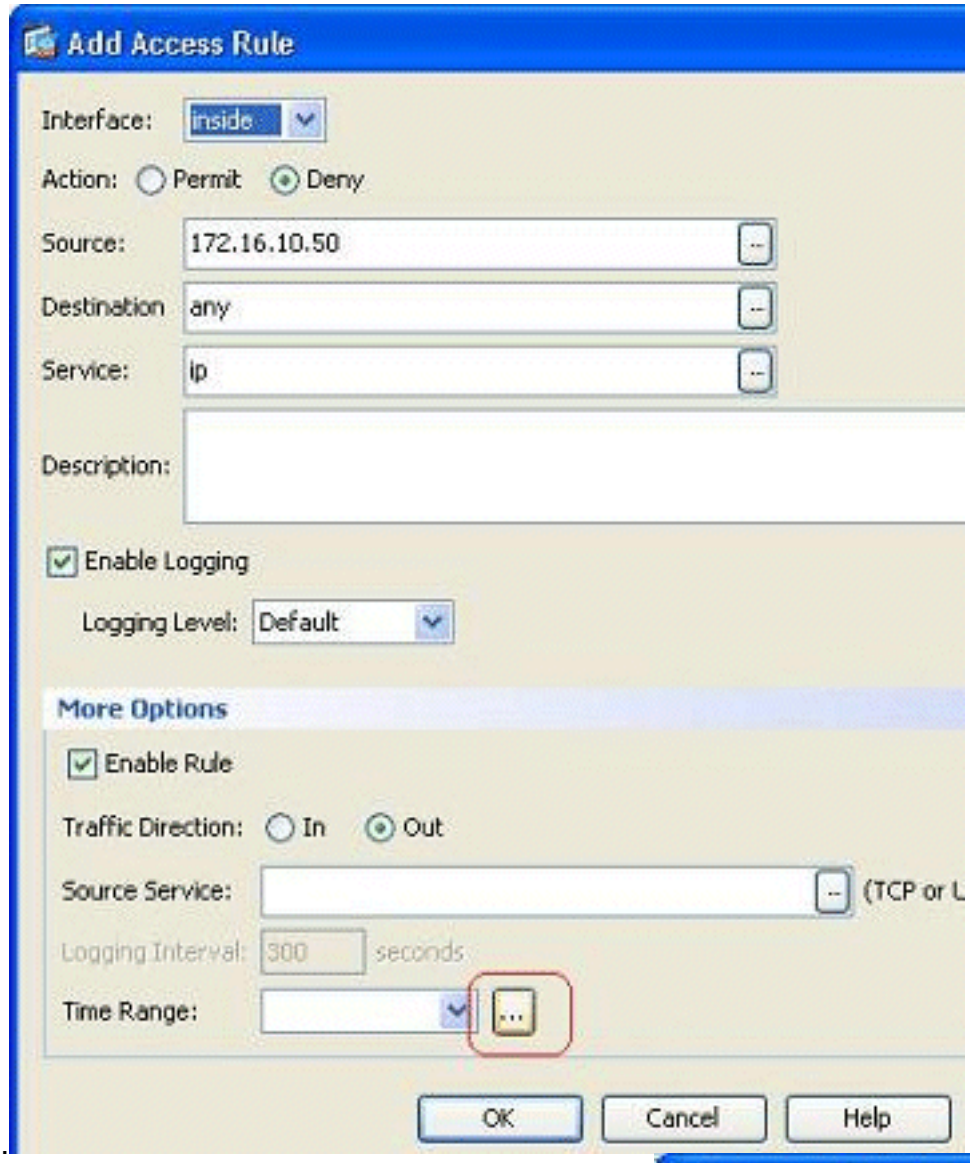
이 섹션에서는 ASDM을 사용하여 시간 기반 액세스 목록을 구현하는 방법을 다룹니다.시간에 따라 액세스 규칙을 적용할 수 있습니다.이를 구현하려면 일/주/월/년 단위로 시간을 지정하는 시간 범위를 정의해야 합니다.그런 다음 이 시간 범위를 필수 액세스 규칙에 바인딩해야 합니다.시간 범위는 두 가지 방법으로 정의할 수 있습니다.

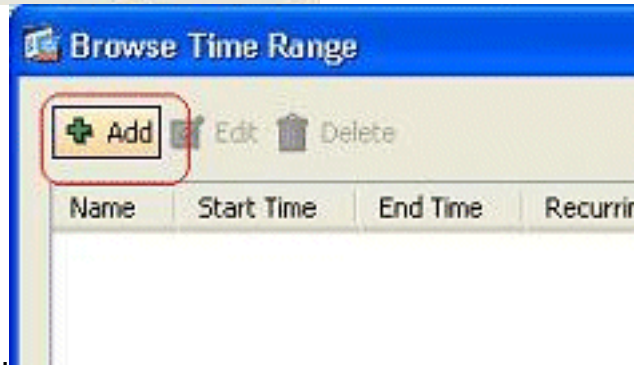
1. Absolute - 시작 시간 및 종료 시간이 포함된 기간을 정의합니다.
2. Periodic(주기적) - 반복이라고도 합니다.지정된 간격으로 발생하는 기간을 정의합니다.

참고: 시간 범위를 구성하기 전에 ASA가 시스템 클록 설정을 사용하여 구현하므로 올바른 날짜/시간 설정으로 구성되어 있는지 확인하십시오.ASA를 NTP 서버와 동기화하면 훨씬 더 나은 결과를 얻을 수 있습니다.

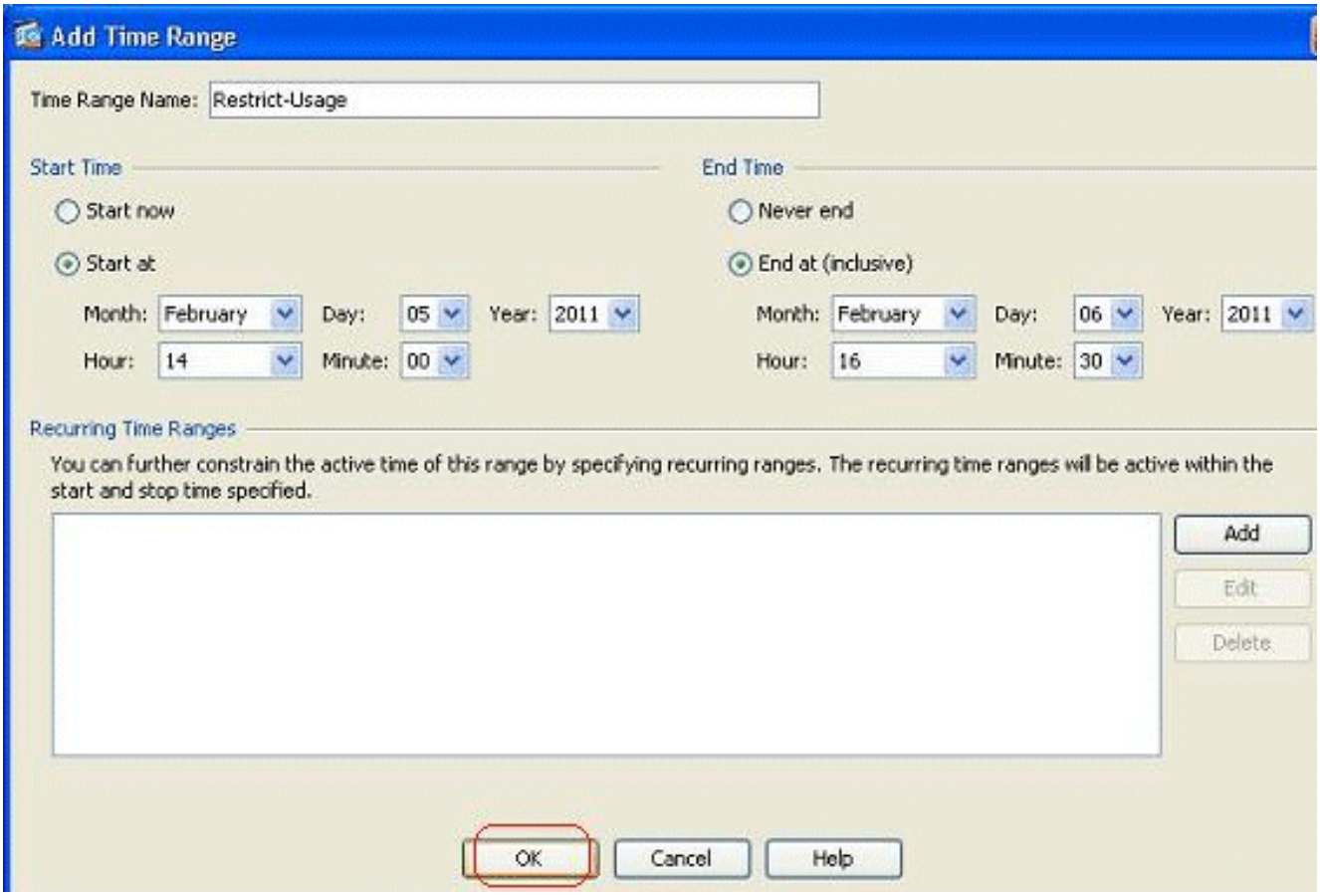
ASDM을 통해 이 기능을 구성하려면 다음 단계를 완료하십시오.

1. 액세스 규칙을 정의하는 동안 Time Range 필드에서 Details 버튼을 클릭합니다

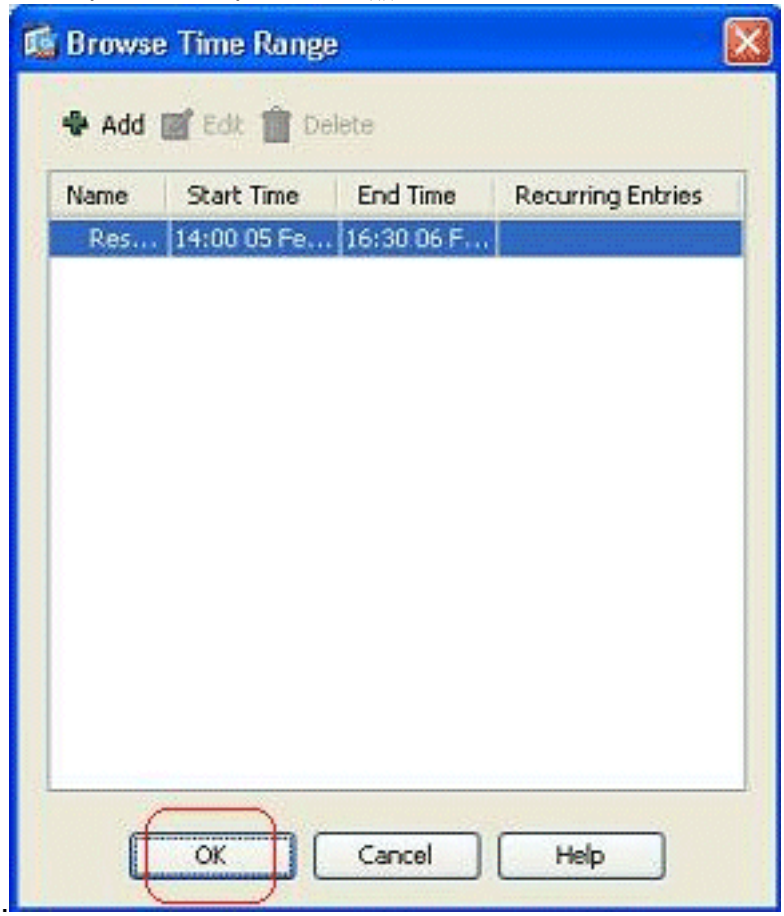




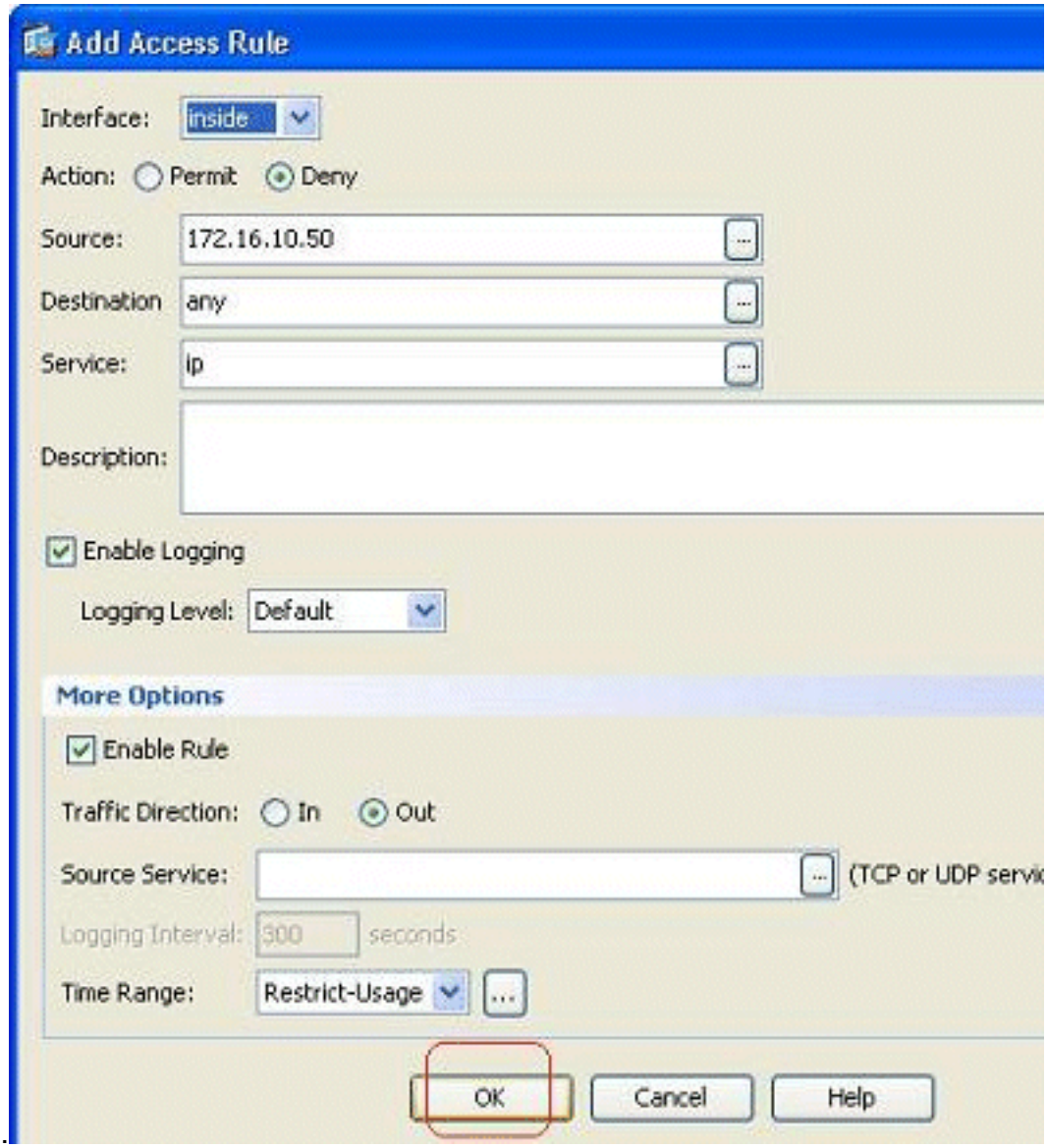
2. 새 시간 범위를 생성하려면 Add를 클릭합니다.
3. 시간 범위의 이름을 정의하고 시작 시간과 종료 시간을 지정합니다.**확인**을 **클릭합니다**
.



4. 여기서 시간 범위를 볼 수 있습니다.Add Access Rule 창으로 돌아가려면 OK를 클릭합니다



5. 이제 Restrict-Usage 시간 범위가 이 액세스 규칙에 바인딩되었음을 확인할 수 있습니다

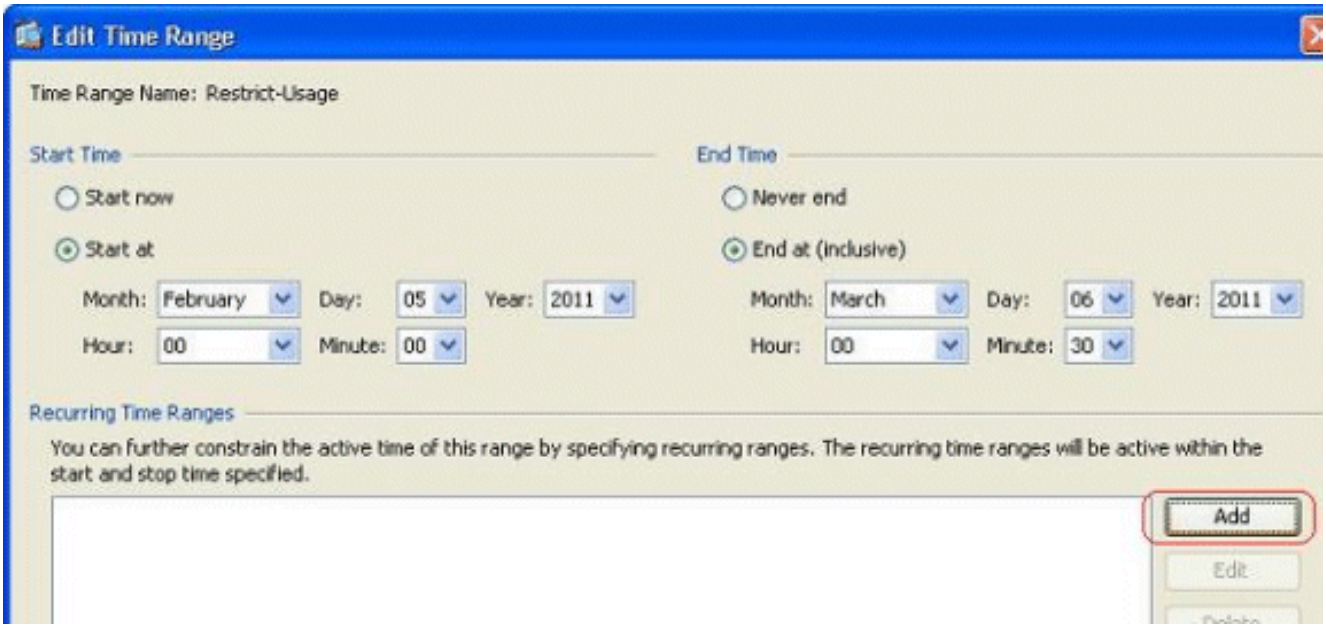


이 액세스 규칙 컨피그레이션에 따라 172.16.10.50의 사용자는 2011년 2월 5일 오후 2시(2011년 2월 5일)부터 2011년 2월 6일(오후 4시 30분)까지의 모든 리소스를 사용할 수 없습니다.이는 다음과 같은 CLI 출력입니다.

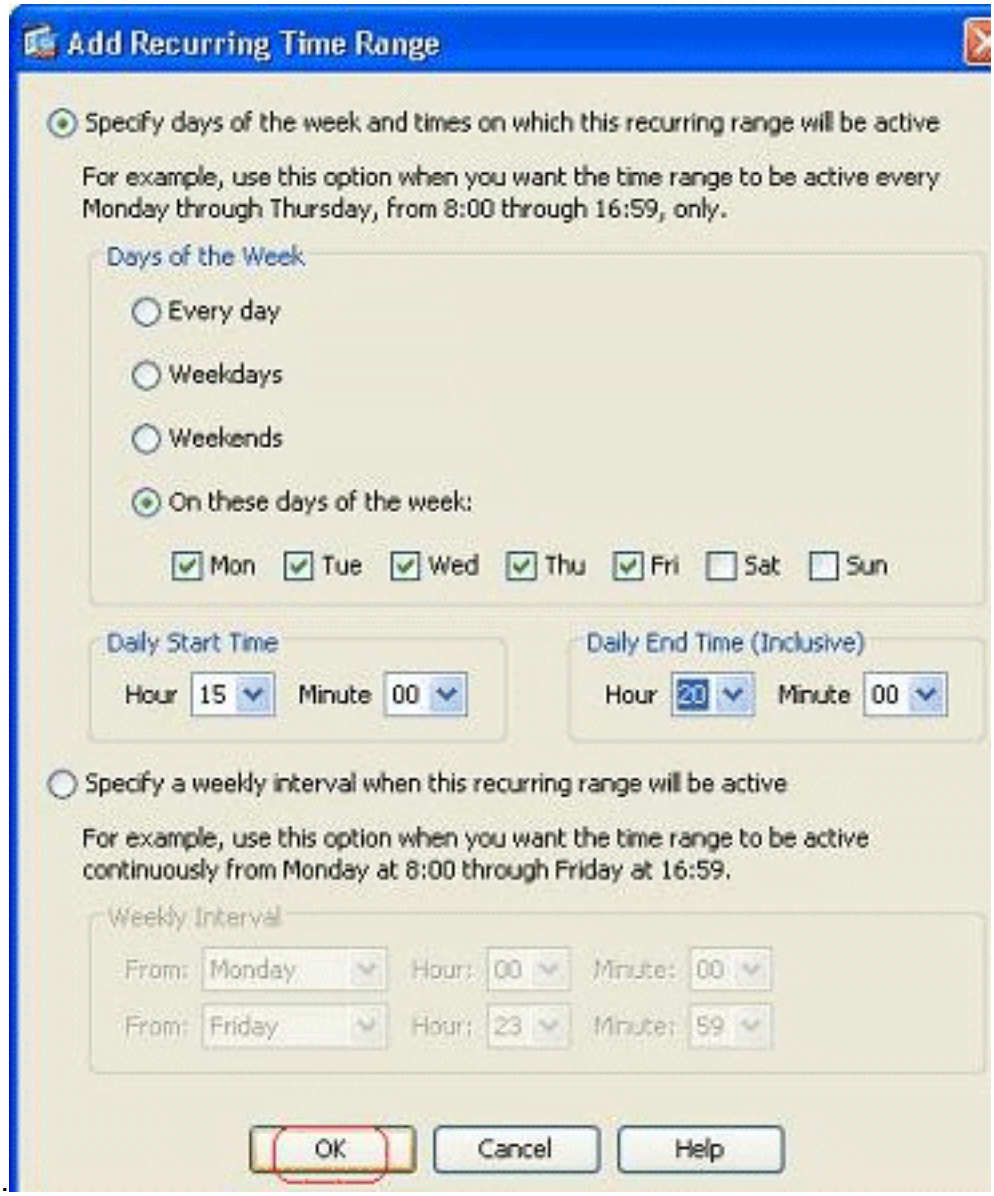
```
time-range Restrict-Usage
 absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

6. 다음은 반복 시간 범위를 지정하는 방법에 대한 예입니다.반복 시간 범위를 정의하려면 **Add**를 클릭합니다

.

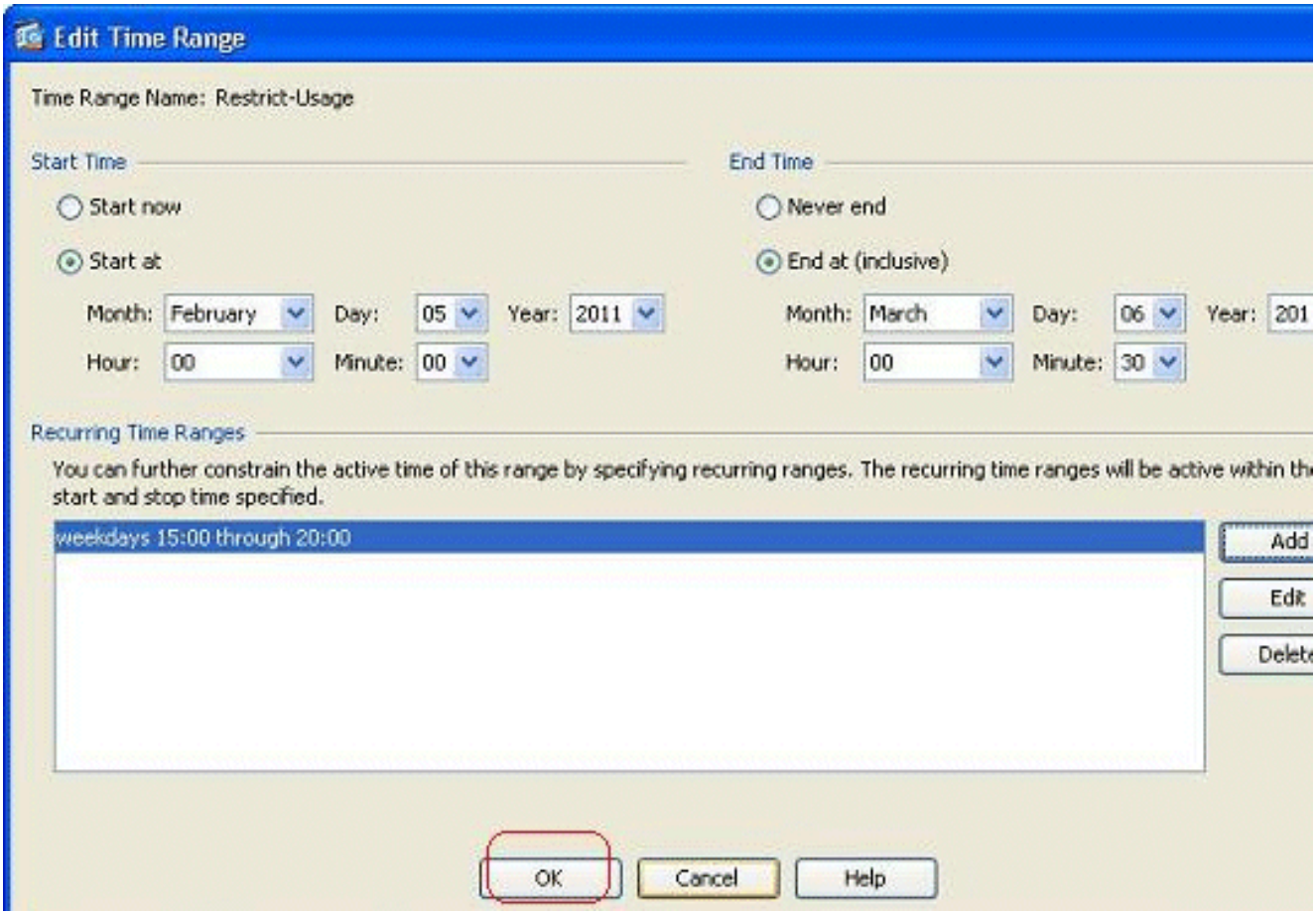


7. 요구 사항에 따라 설정을 지정하고 **확인**을 클릭하여 완료합니다



8. OK(**확인**)를 클릭하여 Time Range(시간 범위) 창으로 돌아갑니다

.



이 구성에 따라 172.16.10.50의 사용자는 토요일과 일요일을 제외한 모든 주중에 오후 3시부터 오후 8시까지 모든 리소스에 대한 액세스가 거부되었습니다.

```
!
time-range Restrict-Usage
 absolute start 00:00 05 February 2011 end 00:30 06 March 2011
 periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
    time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

참고: time-range 명령에 절대값과 주기값이 모두 지정된 경우 **주기적** 명령은 절대 시작 시간에 도달한 후에만 평가되며 절대 종료 시간에 도달한 후에는 더 평가되지 않습니다.

관련 정보

- Cisco ASA 설명서 페이지
- 기술 지원 및 문서 – Cisco Systems