

NAT를 통한 ASA 버전 9 포트 전달 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[PAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용](#)

[NAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용](#)

[신뢰할 수 있는 네트워크의 호스트에 대한 신뢰할 수 없는 호스트 액세스 허용](#)

[고정 ID NAT](#)

[정적으로 포트 리디렉션\(전달\)](#)

[다음을 확인합니다.](#)

[연결](#)

[Syslog](#)

[패킷 추적기](#)

[캡처](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 CLI 또는 ASDM(Adaptive Security Device Manager)을 사용하여 ASA(Adaptive Security Appliance) 소프트웨어 버전 9.x에서 포트 리디렉션(포워딩) 및 외부 NAT(Network Address Translation) 기능을 구성하는 방법에 대해 설명합니다.

자세한 내용은 [Cisco ASA Series Firewall ASDM 컨피그레이션](#) 가이드를 참조하십시오.

사전 요구 사항

요구 사항

ASDM에서 [디바이스](#)를 구성할 수 있도록 하려면 [관리 액세스](#) 구성을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

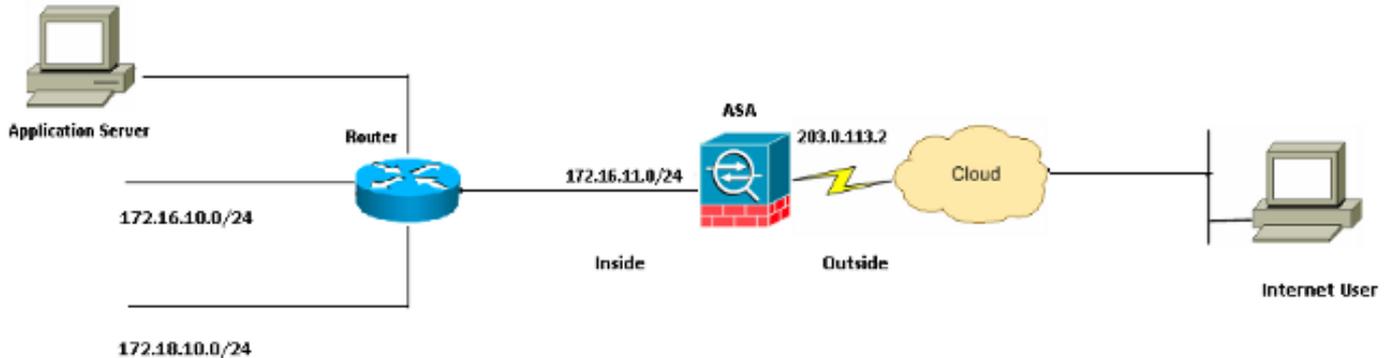
- Cisco ASA 5525 Series Security Appliance 소프트웨어 버전 9.x 이상
- ASDM 버전 7.x 이상

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다."

구성

네트워크 다이어그램



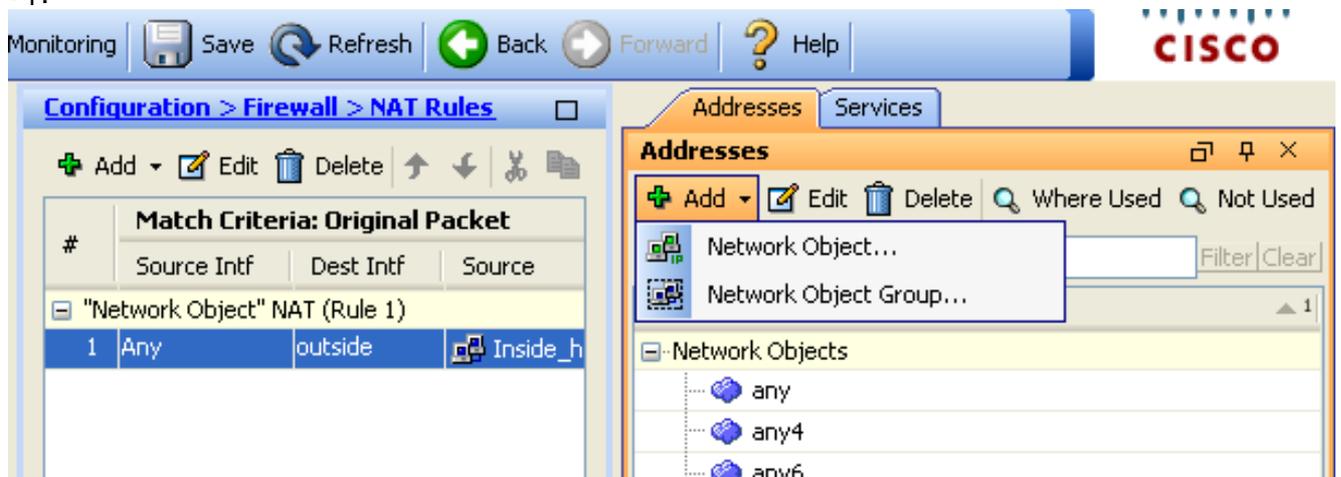
이 구성에 사용된 IP 주소 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 랩 환경에서 사용된 RFC 1918 주소입니다.

PAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용

내부 호스트에서 변환용 단일 공용 주소를 공유하려면 PAT(Port Address Translation)를 사용합니다. 가장 간단한 PAT 컨피그레이션 중 하나는 모든 내부 호스트를 외부 인터페이스 IP 주소처럼 변환하는 것입니다. 이는 ISP에서 사용할 수 있는 라우팅 가능한 IP 주소 수가 몇 개 또는 한 개로 제한될 때 사용되는 일반적인 PAT 컨피그레이션입니다.

내부 호스트가 PAT를 사용하여 외부 네트워크에 액세스할 수 있도록 허용하려면 다음 단계를 완료하십시오.

1. Configuration(컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙)를 선택합니다. 동적 NAT 규칙을 구성하려면 Add(추가)를 클릭한 다음 Network Object(네트워크 개체)를 선택합니다.



2. 동적 PAT가 필요한 네트워크/호스트/범위를 구성합니다. 이 예에서는 내부 서브넷 중 하나가 선택되었습니다. 이러한 방식으로 변환하려는 다른 서브넷에 대해 이 프로세스를 반복할 수 있습니다.

Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

OK Cancel Help

3. NAT를 확장합니다. Add **Automatic Address Translation Rules**(자동 주소 변환 규칙 추가) 확인란을 선택합니다. Type(유형) 드롭다운 목록에서 **Dynamic PAT (Hide)**를 선택합니다. Translated Addr 필드에서 외부 인터페이스를 반영하는 옵션을 선택합니다. **Advanced**(고급)를 클릭합니다.

Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

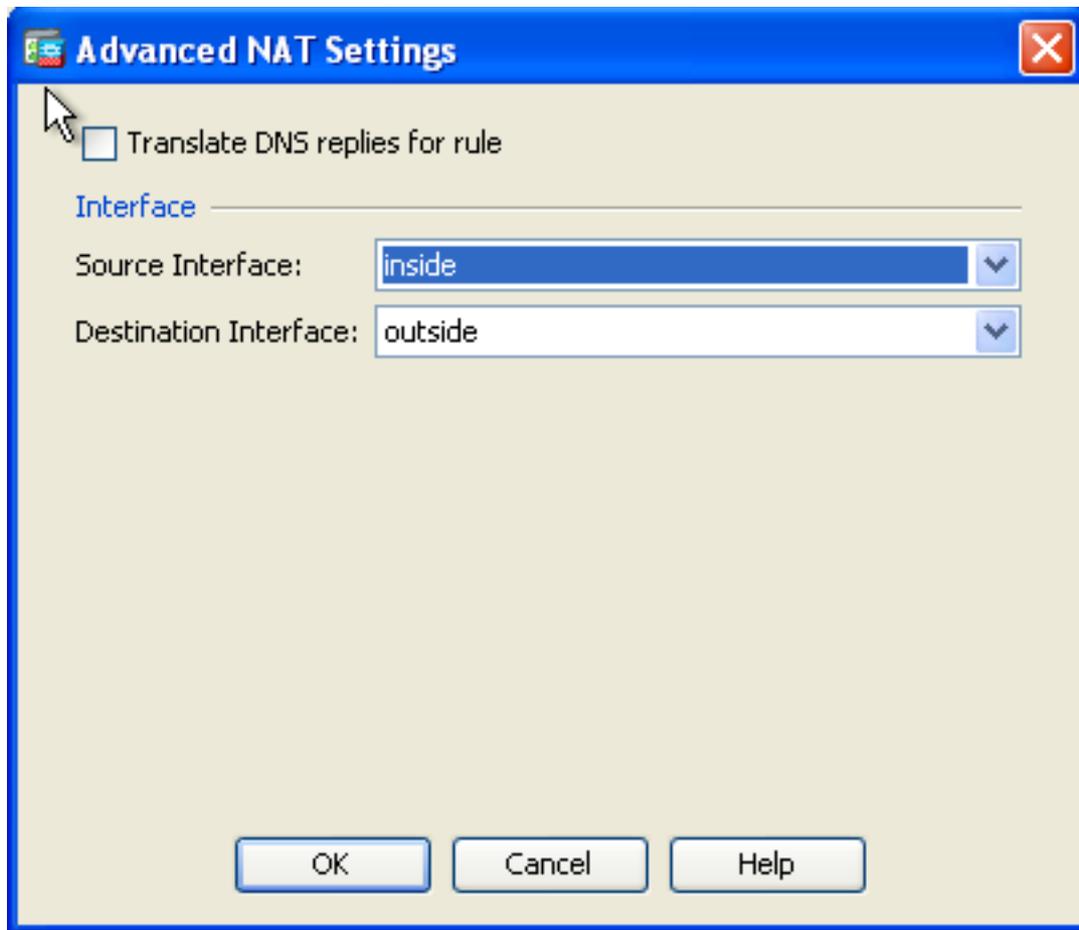
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. 변경 사항을 적용하려면 **OK(확인)**를 클릭하고 **Apply(적용)**를 클릭합니다.



이 PAT 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

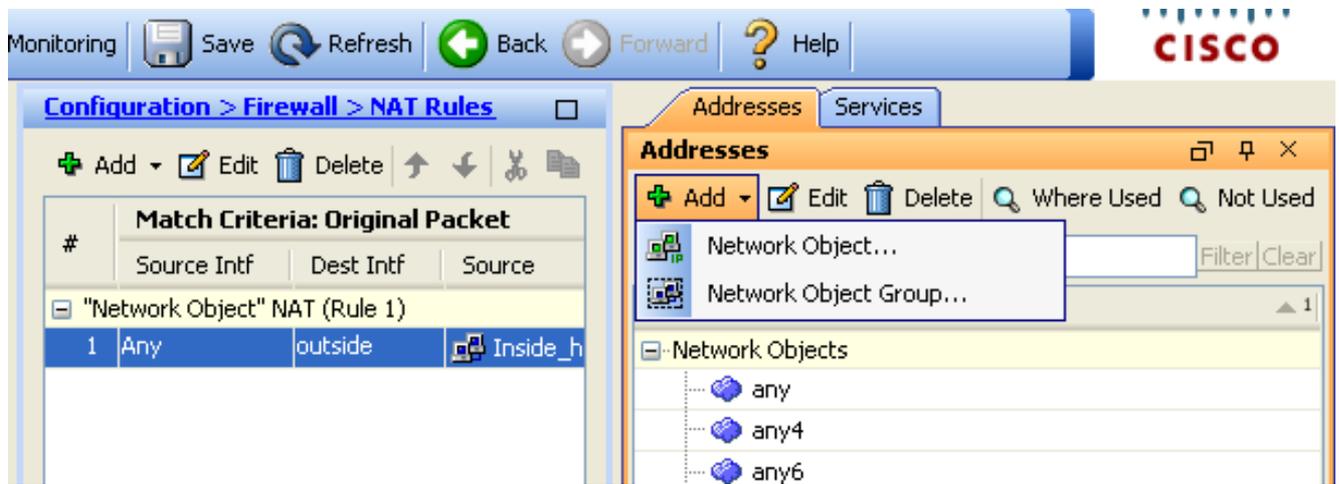
NAT를 사용하여 내부 호스트가 외부 네트워크에 액세스하도록 허용

동적 NAT 규칙의 컨피그레이션으로 내부 호스트/네트워크의 그룹이 외부 세계에 액세스하도록 허용할 수 있습니다. PAT와 달리 동적 NAT는 주소 풀에서 변환된 주소를 할당합니다. 그 결과, 호스트는 자체 변환된 IP 주소에 매핑되며 두 호스트는 동일한 변환된 IP 주소를 공유할 수 없습니다.

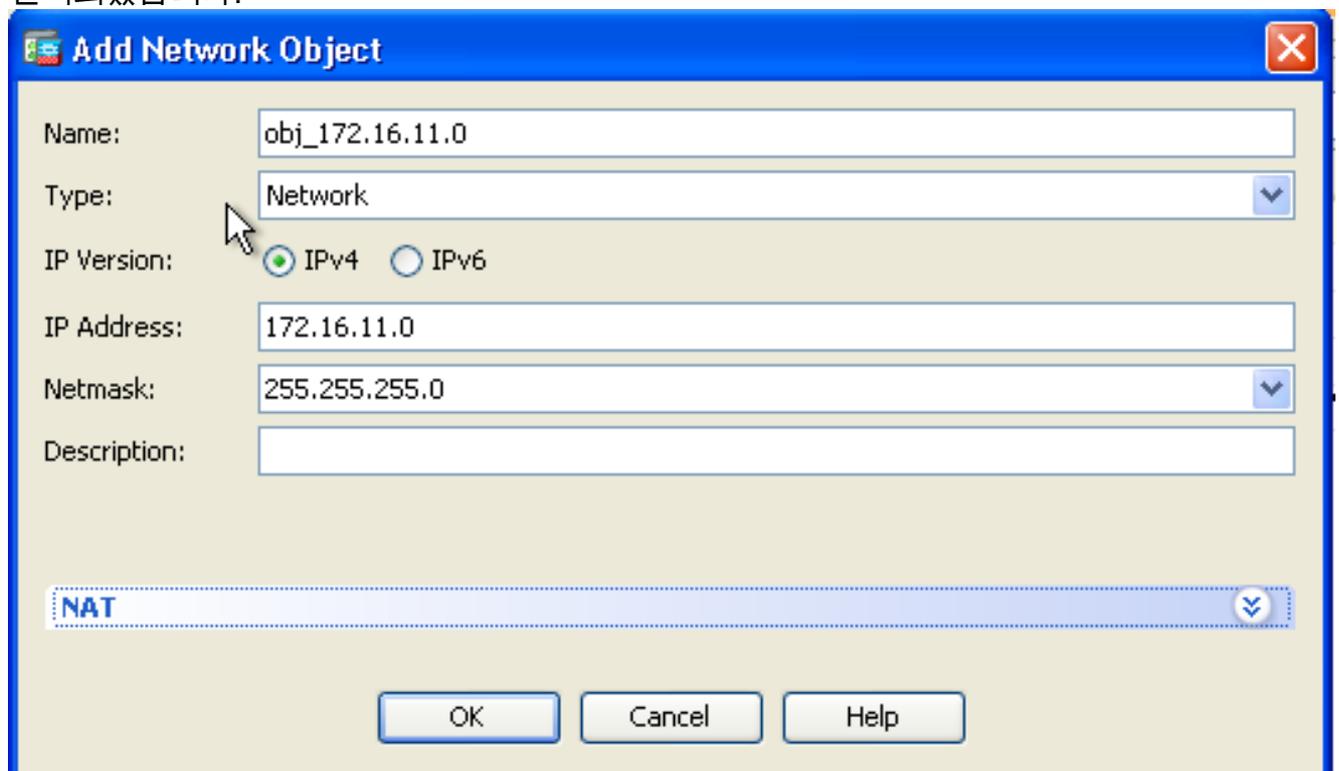
이렇게 하려면 액세스 권한을 부여할 호스트/네트워크의 실제 주소를 선택한 다음 변환된 IP 주소 풀에 매핑해야 합니다.

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

1. Configuration(컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙)를 선택합니다. 동적 NAT 규칙을 구성하려면 Add(추가)를 클릭한 다음 Network Object(네트워크 개체)를 선택합니다.



2. 동적 PAT가 필요한 네트워크/호스트/범위를 구성합니다. 이 예에서는 전체 내부 네트워크가 선택되었습니다.



3. NAT를 확장합니다. Add Automatic Address Translation Rules(자동 주소 변환 규칙 추가) 확인란을 선택합니다. Type 드롭다운 목록에서 Dynamic을 선택합니다. 변환된 주소 필드에서 적절한 항목을 선택합니다. Advanced(고급)를 클릭합니다.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: ...

Use one-to-one address translation

PAT Pool Translated Address: ...

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. 네트워크 객체를 추가하려면 Add를 클릭합니다. Type 드롭다운 목록에서 Range를 선택합니다. Start Address 및 End Address 필드에 시작 및 종료 PAT IP 주소를 입력합니다. OK(확인)를 클릭합니다.

Add Network Object

Name: obj-my-range

Type: Range

IP Version: IPv4 IPv6

Start Address: 203.0.113.10

End Address: 203.0.113.20

Description:

NAT

OK Cancel Help

5. Translated Addr 필드에서 주소 객체를 선택합니다. 소스 인터페이스와 대상 인터페이스를 선택하려면 Advanced를 클릭합니다.

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

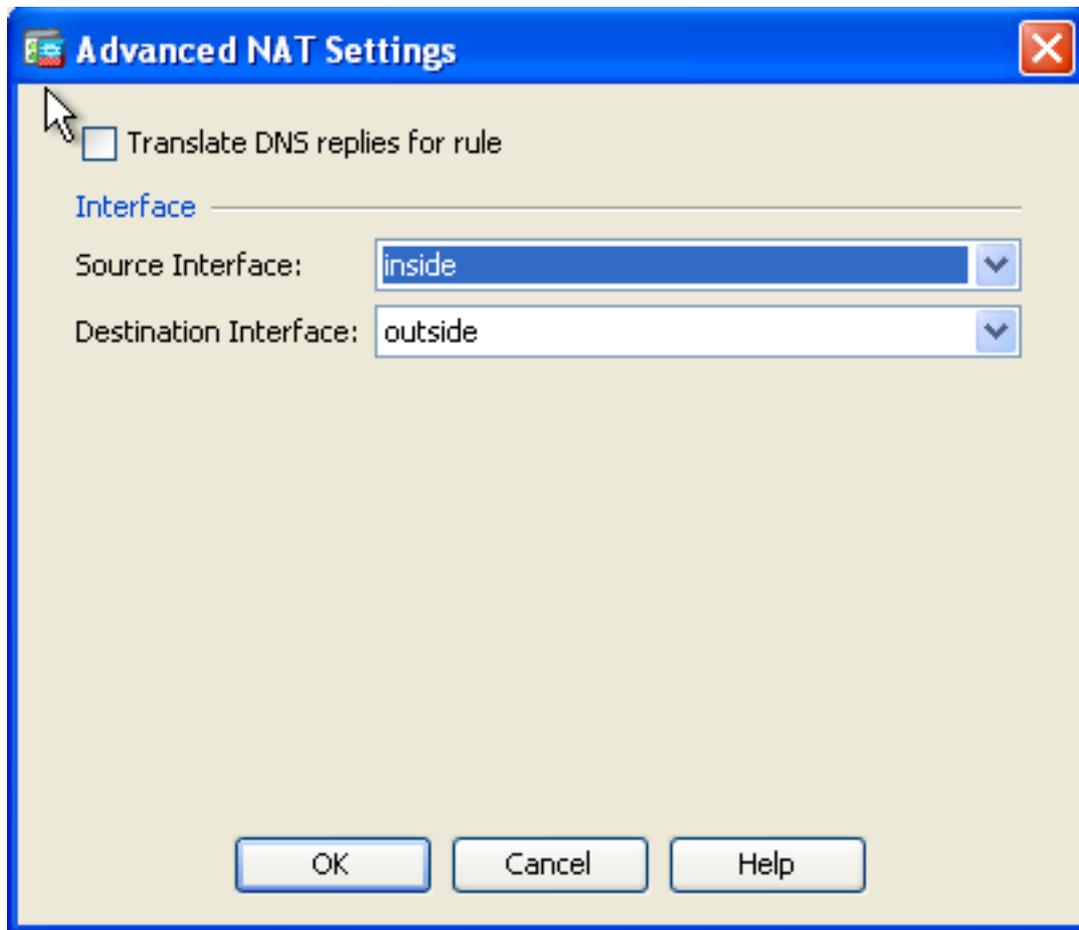
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

6. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. 변경 사항을 적용하려면 **OK(확인)**를 클릭하고 **Apply(적용)**를 클릭합니다.



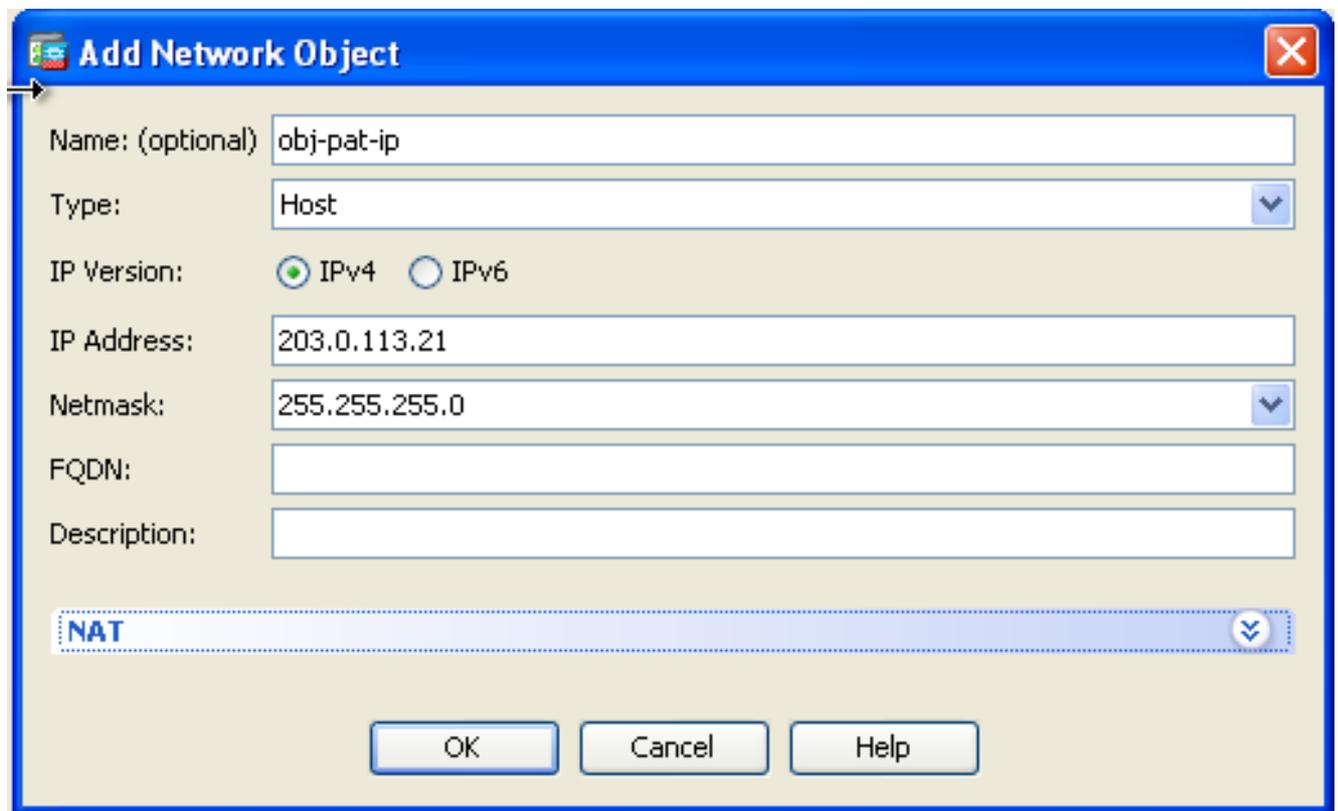
이 ASDM 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj-my-range  
range 203.0.113.10 203.0.113.20
```

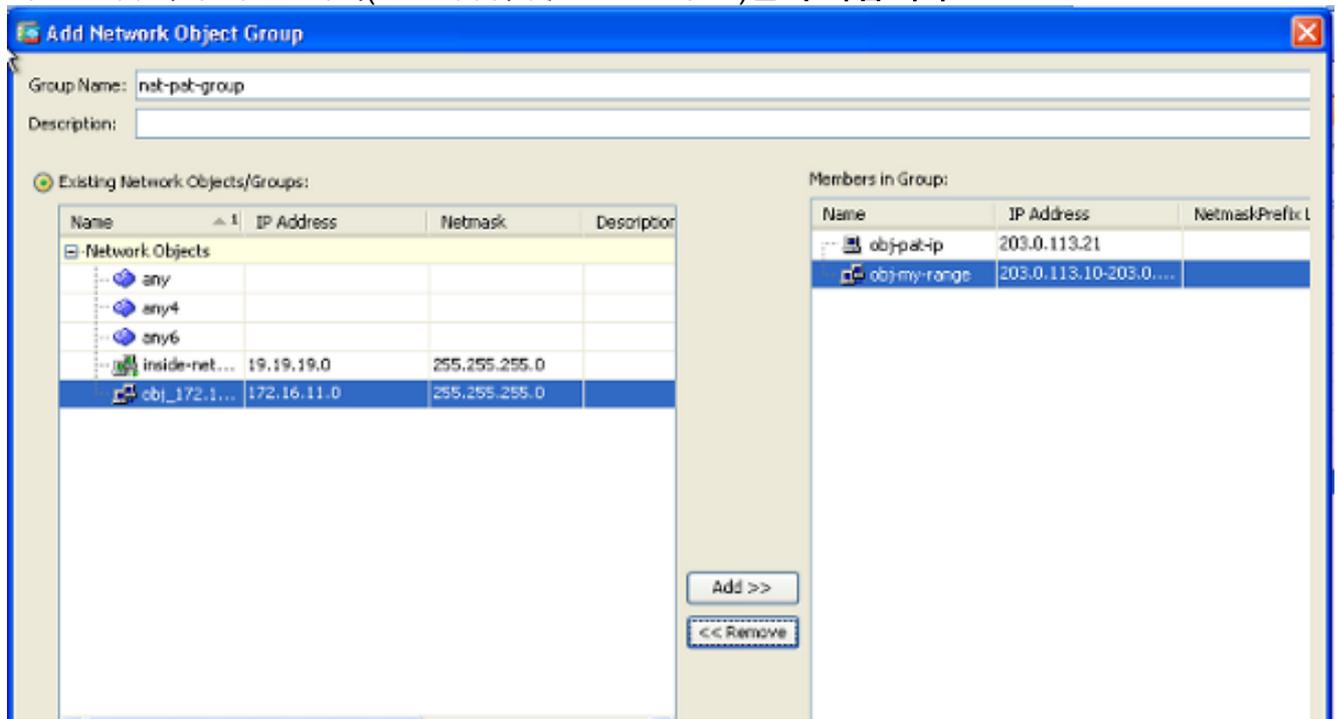
```
object network obj_172.16.11.0  
subnet 172.16.11.0 255.255.255.0  
nat(inside,outside) dynamic obj-my-range
```

이 컨피그레이션에 따라 172.16.11.0 네트워크의 호스트는 NAT 풀 203.0.113.10 - 203.0.113.20의 모든 IP 주소로 변환됩니다. 매핑된 풀의 주소 수가 실제 그룹보다 적을 경우 주소가 부족해질 수 있습니다. 따라서 동적 PAT 백업으로 동적 NAT를 구현하거나 현재 풀을 확장할 수 있습니다.

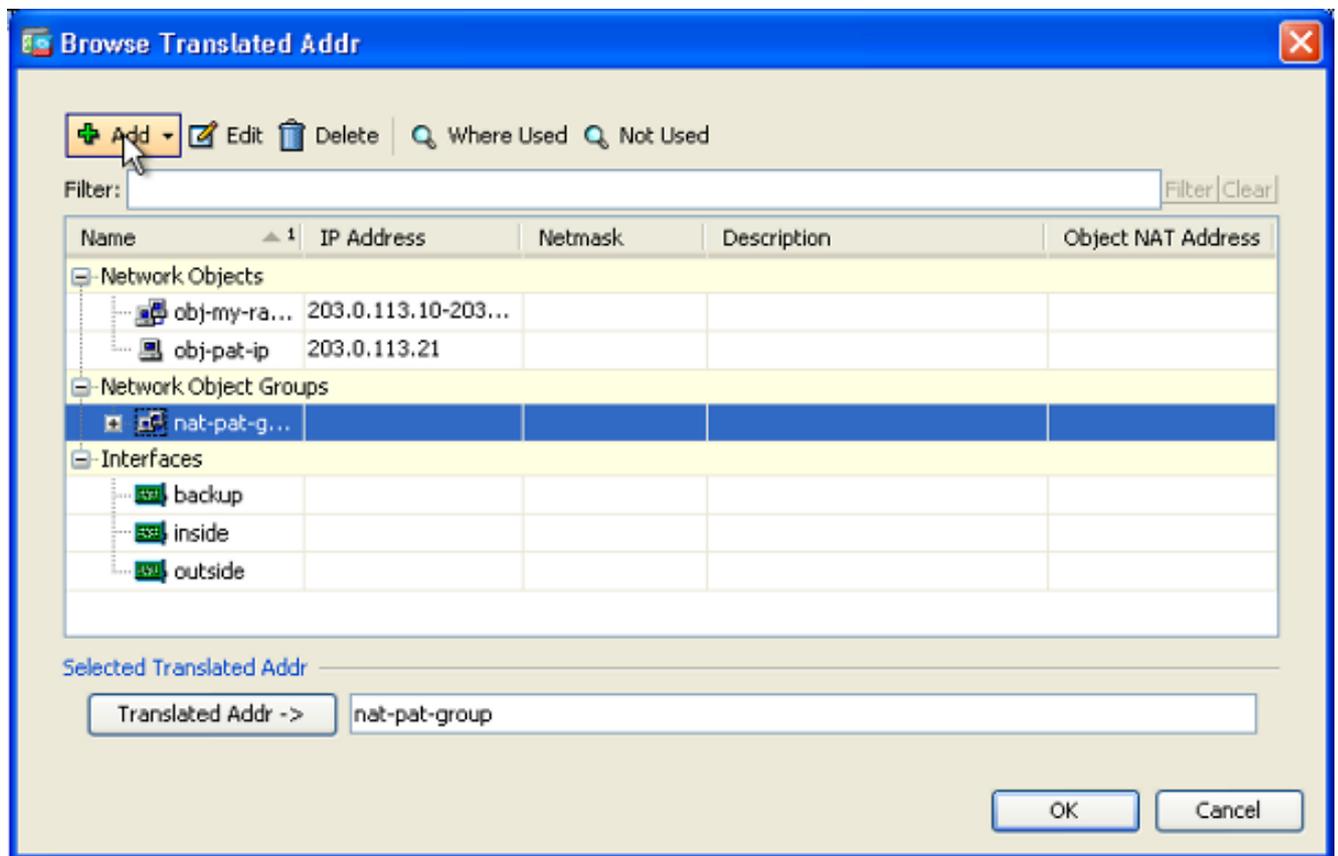
1. 네트워크 객체를 추가하려면 이전 컨피그레이션에서 1~3단계를 반복하고 **Add(추가)**를 다시 한 번 클릭합니다. Type 드롭다운 목록에서 Host를 **선택**합니다. IP Address 필드에 PAT 백업 IP 주소를 입력합니다. **OK(확인)**를 클릭합니다.



2. 네트워크 객체 **그룹**을 추가하려면 Add를 클릭합니다. Group Name 필드에 그룹 이름을 입력하고 그룹에 두 주소 객체(NAT 범위 및 PAT IP 주소)를 **추가**합니다.



3. 구성된 NAT 규칙을 선택하고 변환된 주소를 새로 구성된 그룹 'nat-pat-group'(이전의 'obj-my-range')으로 변경합니다. **OK(확인)**를 클릭합니다.



4. NAT 규칙을 추가하려면 OK를 클릭합니다. 소스 인터페이스와 대상 인터페이스를 선택하려면 Advanced를 클릭합니다.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: nat-pat-group

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

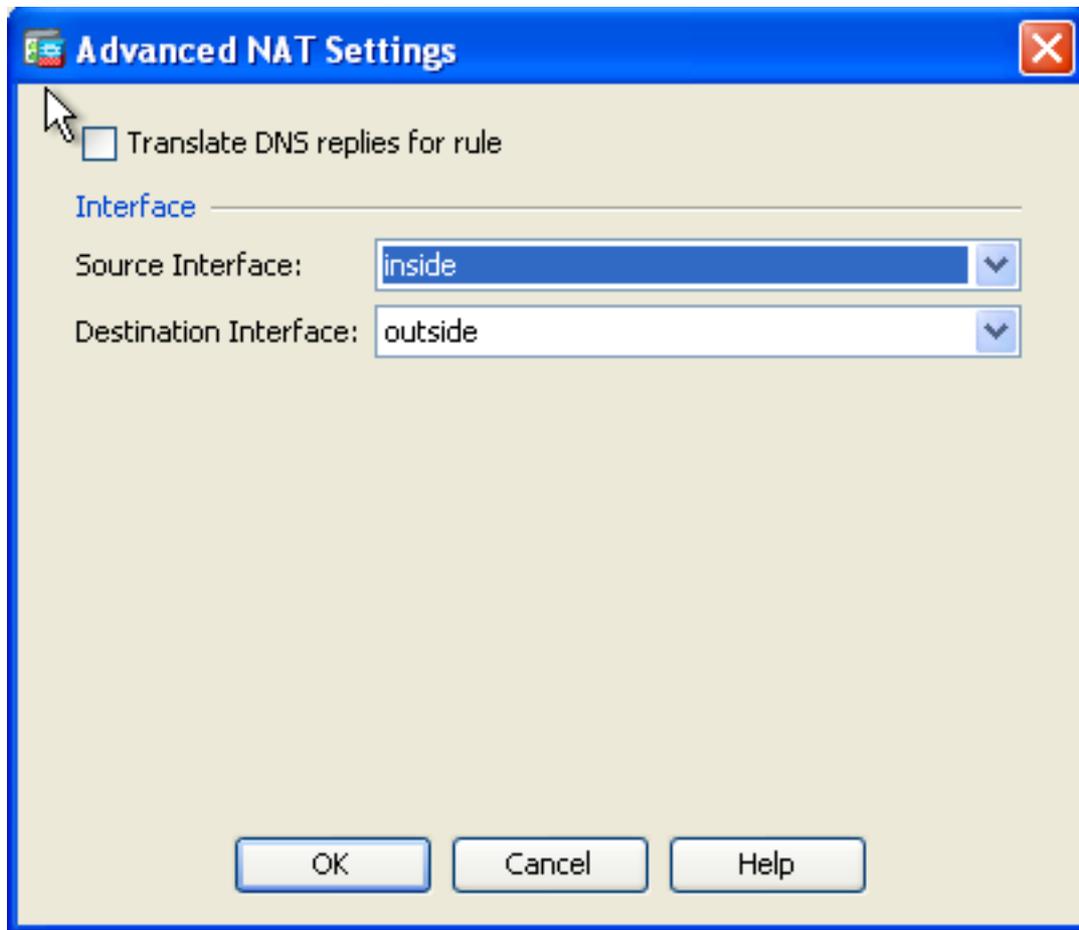
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

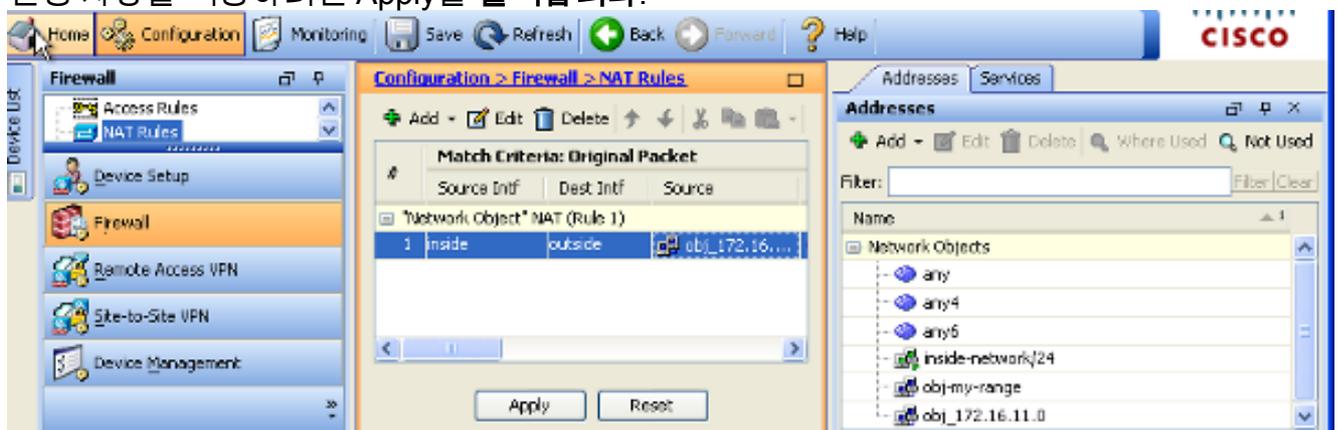
Advanced...

OK Cancel Help

5. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. **OK(확인)**를 클릭합니다.



6. 변경 사항을 적용하려면 Apply를 클릭합니다.



이 ASDM 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj-my-range
range 203.0.113.10 203.0.113.20
```

```
object network obj-pat-ip
host 203.0.113.21
```

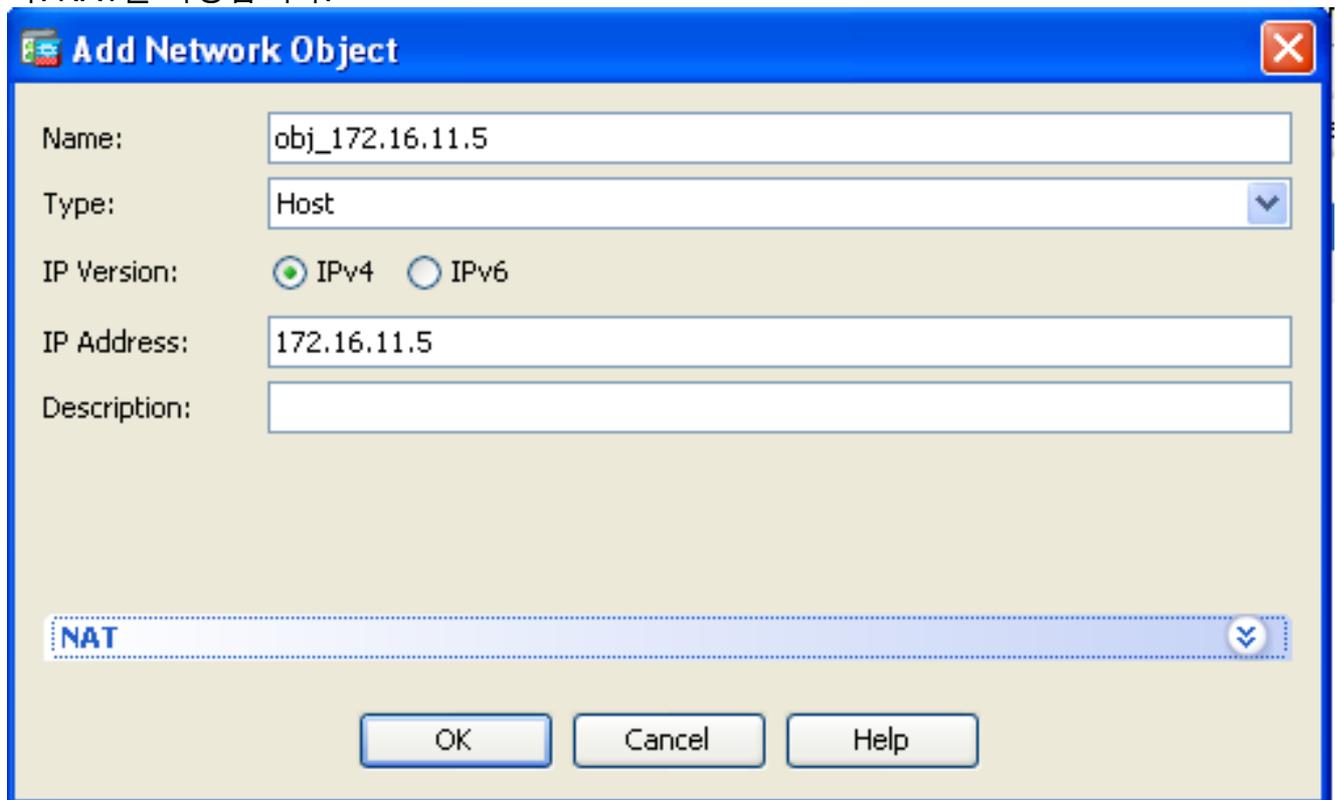
```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

신뢰할 수 있는 네트워크의 호스트에 대한 신뢰할 수 없는 호스트 액세스 허용

이는 고정 NAT 변환 및 이러한 호스트를 허용하는 액세스 규칙의 적용을 통해 달성할 수 있습니다. 외부 사용자가 내부 네트워크에 있는 서버에 액세스하려는 경우 항상 이를 구성해야 합니다. 내부 네트워크의 서버는 인터넷에서 라우팅할 수 없는 사설 IP 주소를 가질 수 있습니다. 따라서 고정 NAT 규칙을 통해 해당 사설 IP 주소를 공용 IP 주소로 변환해야 합니다. 내부 서버(172.16.11.5)가 있다고 가정합니다. 이 작업을 수행하려면 이 개인 서버 IP 주소를 공용 IP 주소로 변환해야 합니다. 이 예에서는 172.16.11.5를 203.0.113.5로 변환하기 위해 양방향 고정 NAT를 구현하는 방법에 대해 설명합니다.

1. Configuration(컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙)를 선택합니다. 고정 NAT 규칙을 구성하려면 Add(추가)를 클릭한 다음 Network Object(네트워크 개체)를 선택합니다. NAT를 확장합니다.



2. Add Automatic Address Translation Rules(자동 주소 변환 규칙 추가) 확인란을 선택합니다. Type 드롭다운 목록에서 Static을 선택합니다. Translated Addr 필드에 IP 주소를 입력합니다. 소스 인터페이스와 대상 인터페이스를 선택하려면 Advanced를 클릭합니다.

Add Network Object

Name: obj_172.16.11.5

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.16.11.5

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.113.5

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

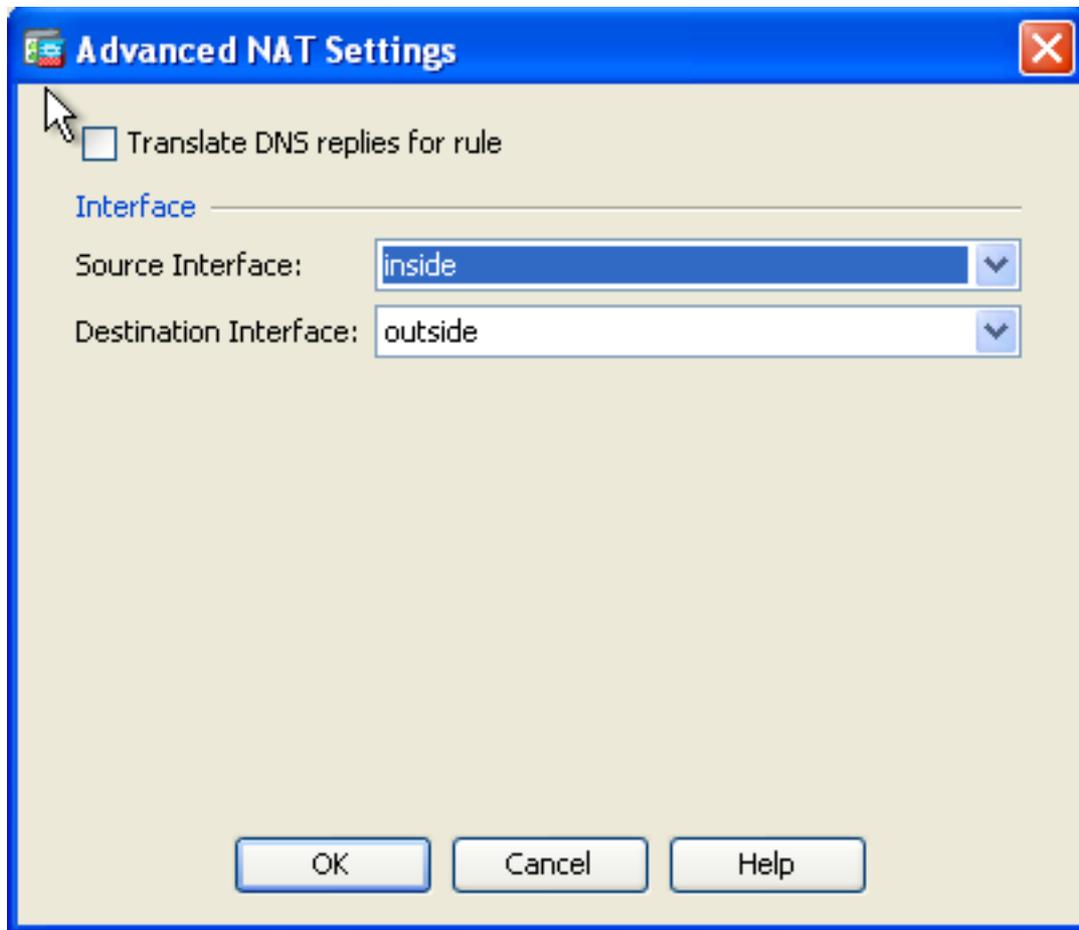
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

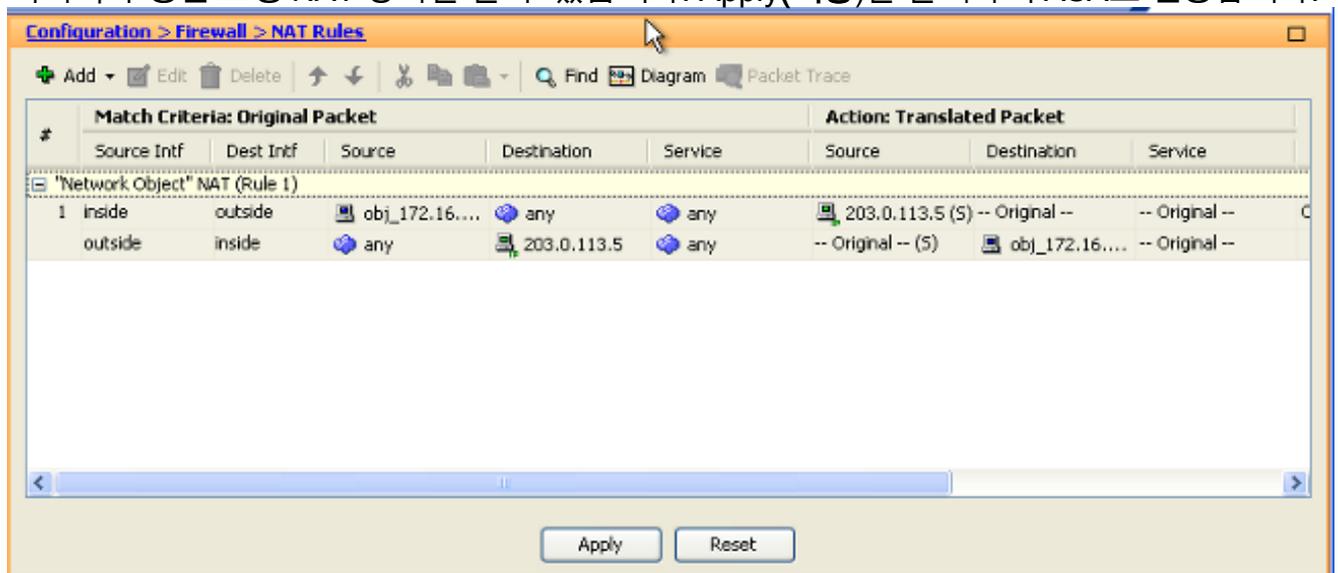
Advanced...

OK Cancel Help

3. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. **OK(확인)**를 클릭합니다.



4. 여기서 구성된 고정 NAT 항목을 볼 수 있습니다. Apply(적용)를 클릭하여 ASA로 전송합니다.



이 NAT 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

고정 ID NAT

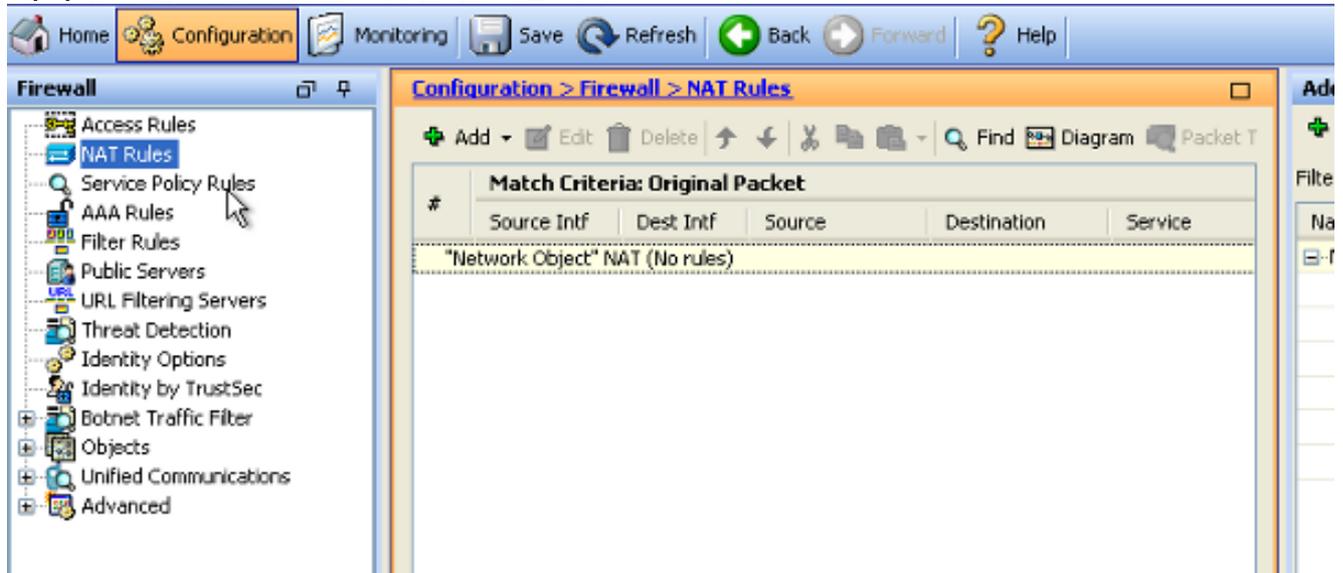
NAT 제외는 내부 사용자가 NAT를 완료하지 않고 ASA의 다른 인터페이스 뒤에서 호스팅되는 원격 VPN 호스트/서버 또는 일부 호스트/서버에 액세스하려고 시도하는 유용한 기능입니다. 이를 위해 사설 IP 주소가 있는 내부 서버를 자체 ID로 변환하여 NAT를 수행하는 목적지에 액세스할 수 있습

니다.

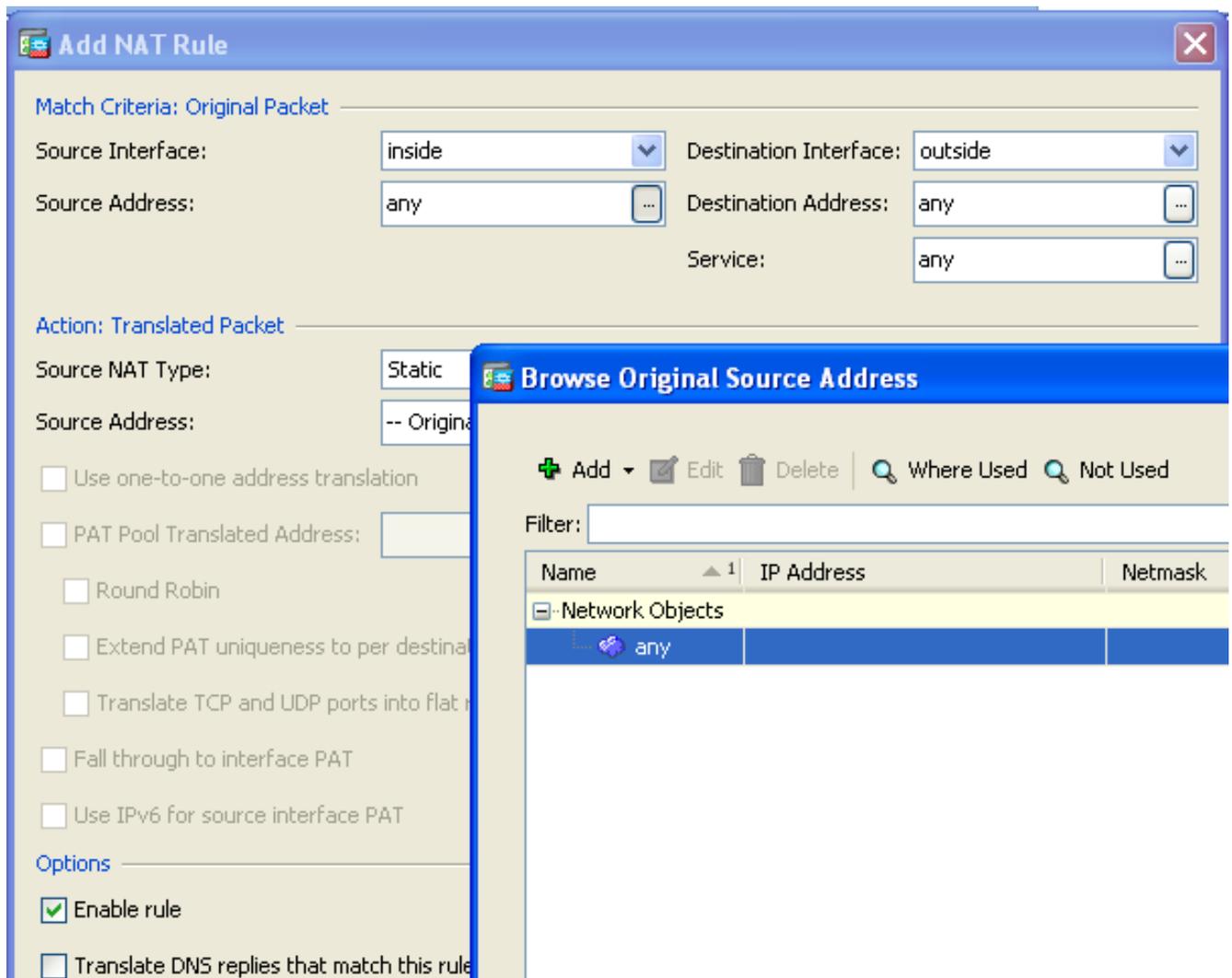
이 예에서 내부 호스트 172.16.11.15는 원격 VPN 서버 172.20.21.15에 액세스해야 합니다.

NAT를 완료하여 내부 호스트가 원격 VPN 네트워크에 액세스하도록 허용하려면 다음 단계를 완료하십시오.

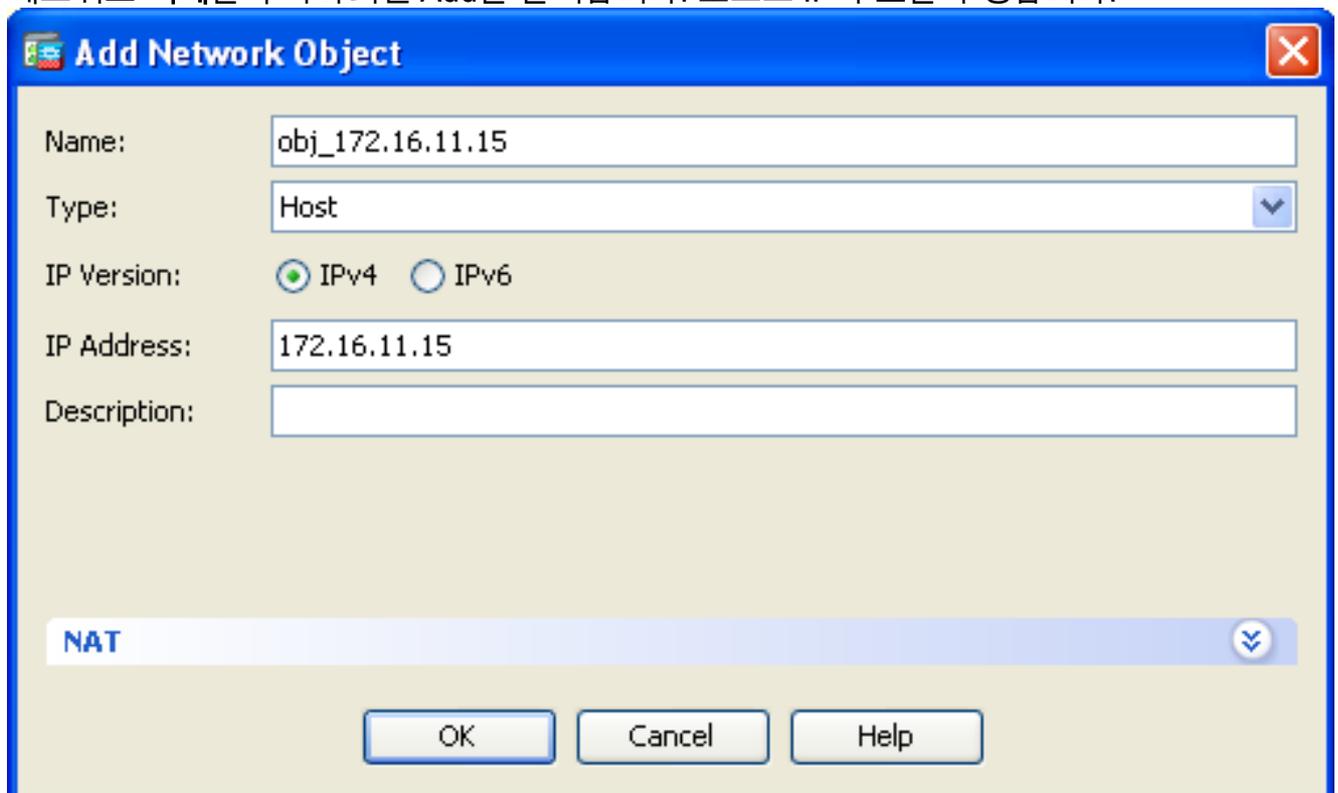
1. Configuration(컨피그레이션) > Firewall(방화벽) > NAT Rules(NAT 규칙)를 선택합니다. NAT 제외 규칙을 구성하려면 Add를 클릭합니다.



2. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. Source Address 필드에서 적절한 항목을 선택합니다.



3. 네트워크 객체를 추가하려면 Add를 클릭합니다. 호스트 IP 주소를 구성합니다.



4. 마찬가지로, Destination Address(대상 주소)를 찾습니다. 네트워크 객체를 추가하려면 Add를

클릭합니다. 호스트 IP 주소를 구성합니다.

Add Network Object

Name: obj_172.20.21.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.20.21.15

Description:

NAT

OK Cancel Help

5. 구성된 Source Address 및 Destination Address 객체를 선택합니다. Disable Proxy ARP on egress interface and Lookup route table(이그레스 인터페이스에서 프록시 ARP 비활성화) 확인란을 선택하여 이그레스 인터페이스를 찾습니다. OK(확인)를 클릭합니다.

Add NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address: Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

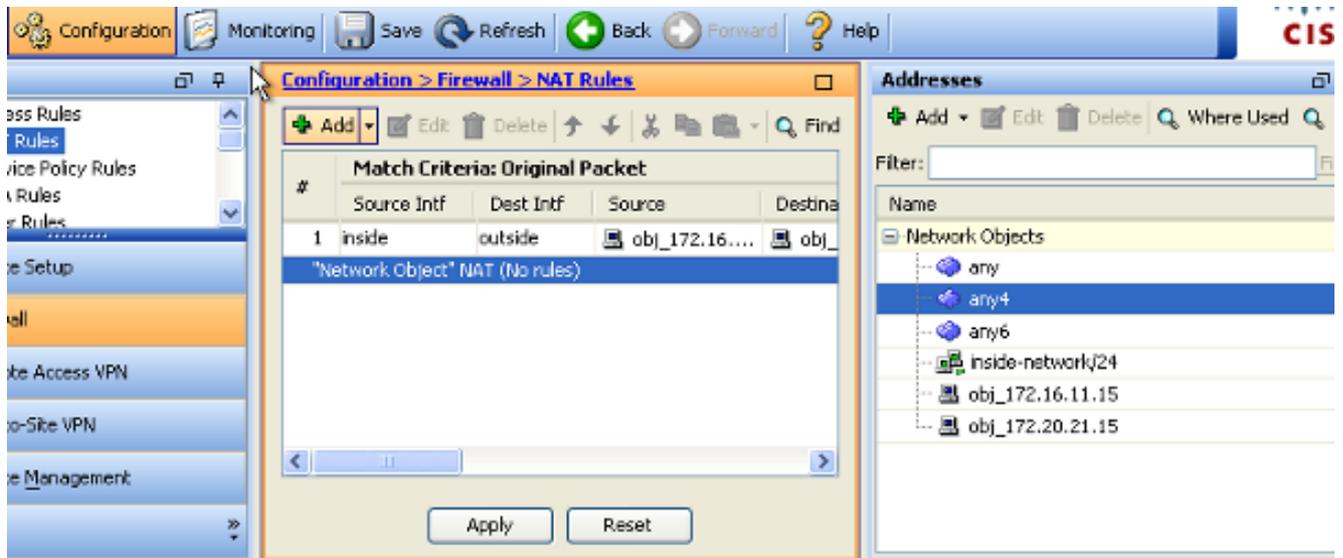
Lookup route table to locate egress interface

Direction:

Description:

OK Cancel Help

6. 변경 사항을 적용하려면 Apply를 클릭합니다.



NAT Exempt 또는 Identity NAT 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15
```

```
nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

정적으로 포트 리디렉션(전달)

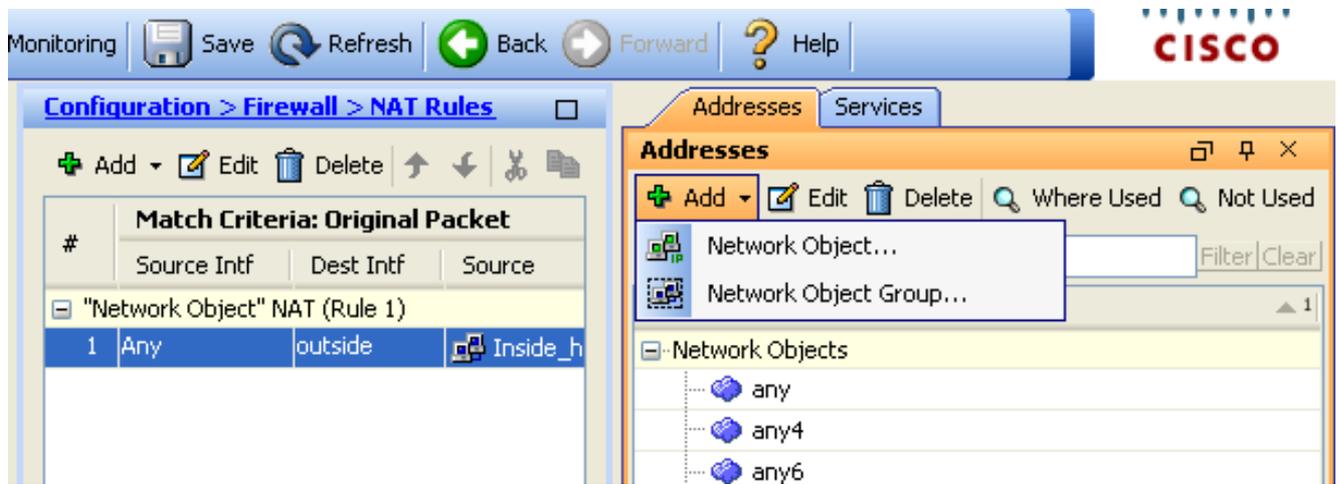
포트 전달 또는 포트 리디렉션은 외부 사용자가 특정 포트의 내부 서버에 액세스하려고 시도하는 유용한 기능입니다. 이를 위해 사설 IP 주소가 있는 내부 서버를 공용 IP 주소로 변환하면 특정 포트에 대한 액세스가 허용됩니다.

이 예에서 외부 사용자는 포트 25의 SMTP 서버 203.0.113.15에 액세스하려고 합니다. 이 작업은 두 단계로 수행됩니다.

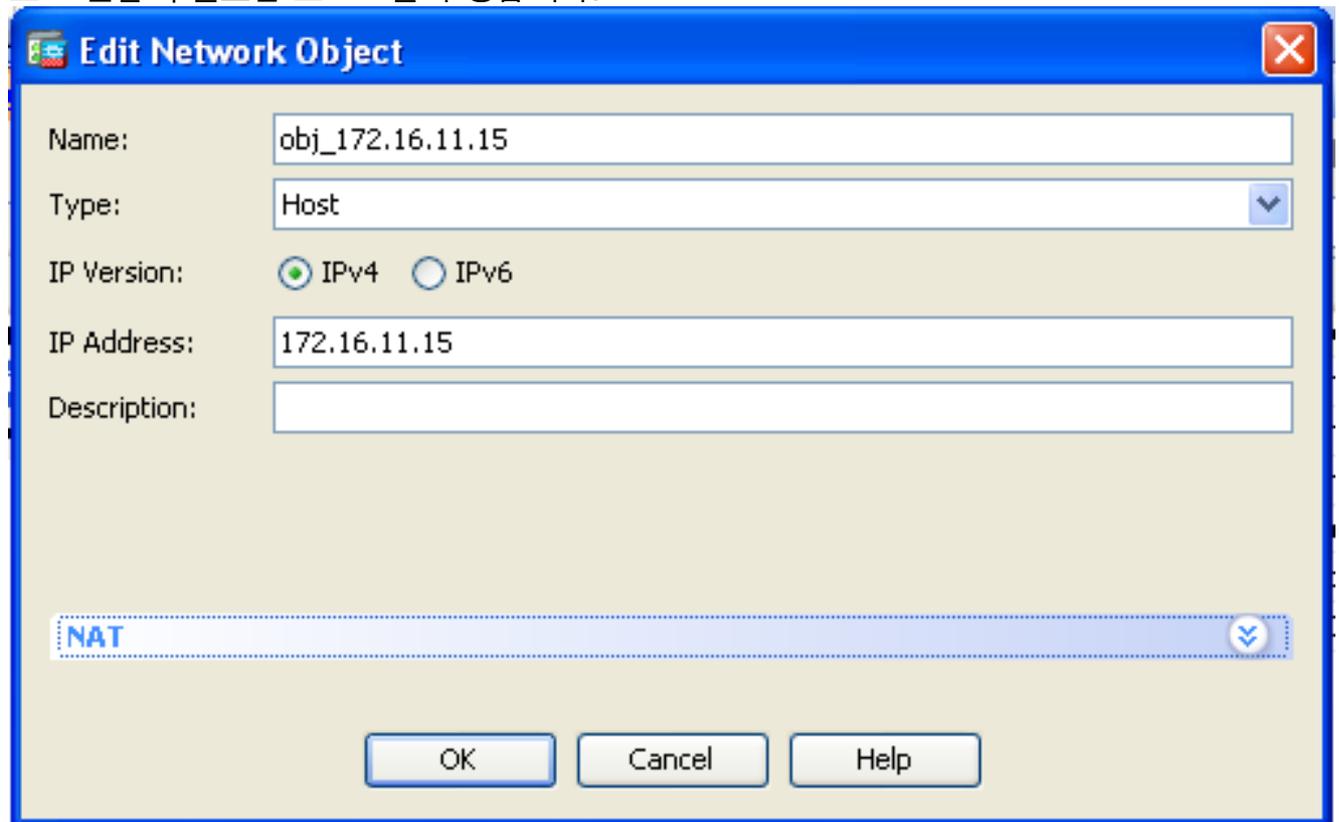
1. 포트 25의 내부 메일 서버 172.16.11.15를 포트 25의 공용 IP 주소 203.0.113.15로 변환합니다.
2. 포트 25에서 공용 메일 서버 203.0.113.15에 대한 액세스를 허용합니다.

외부 사용자가 포트 25에서 서버 203.0.113.15에 액세스하려고 하면 이 트래픽은 포트 25에서 내부 메일 서버 172.16.11.15로 리디렉션됩니다.

1. Configuration > Firewall > NAT Rules를 선택합니다. 고정 NAT 규칙을 구성하려면 Add(추가)를 클릭한 다음 Network Object(네트워크 개체)를 선택합니다.



2. 포트 전달이 필요한 호스트를 구성합니다.



3. NAT를 확장합니다. Add Automatic Address Translation Rules(자동 주소 변환 규칙 추가) 확인란을 선택합니다. Type 드롭다운 목록에서 Static을 선택합니다. Translated Addr 필드에 IP 주소를 입력합니다. 서비스와 소스 및 대상 인터페이스를 선택하려면 **Advanced**(고급)를 클릭합니다.

Edit Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

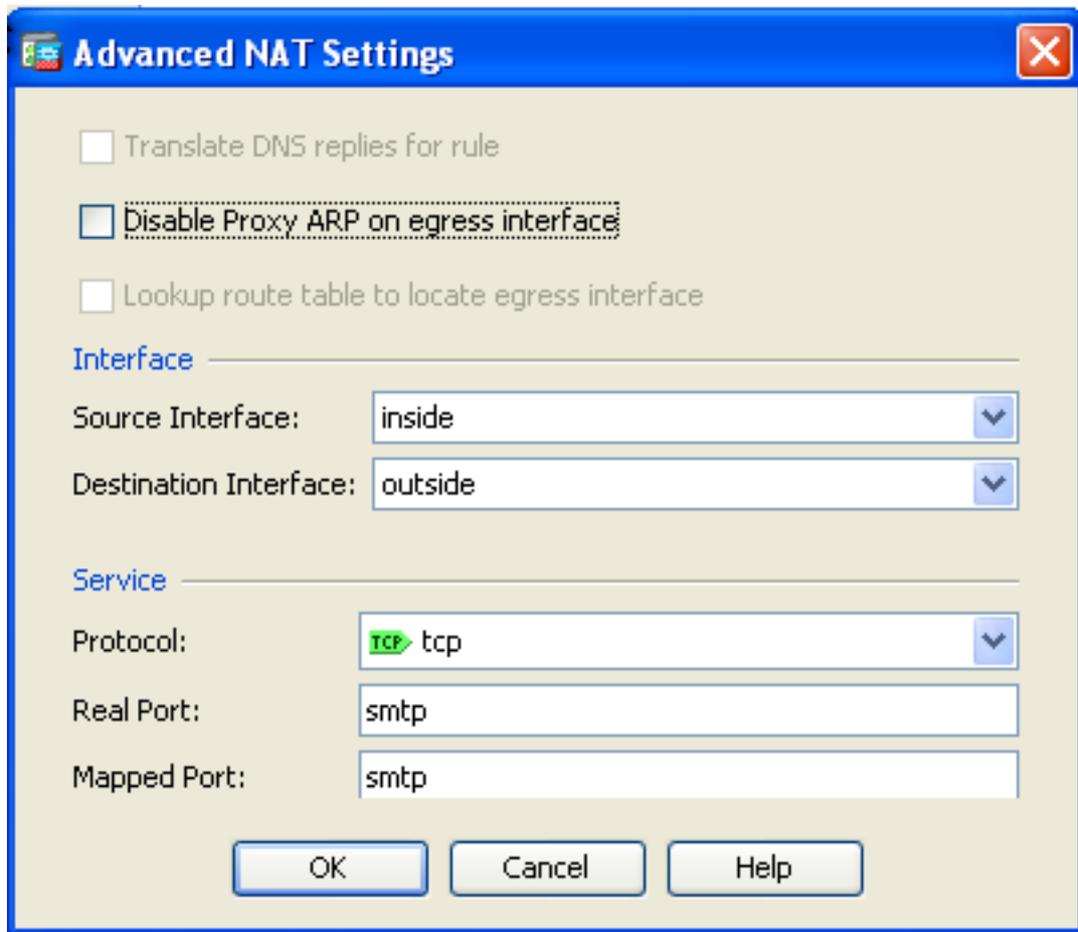
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

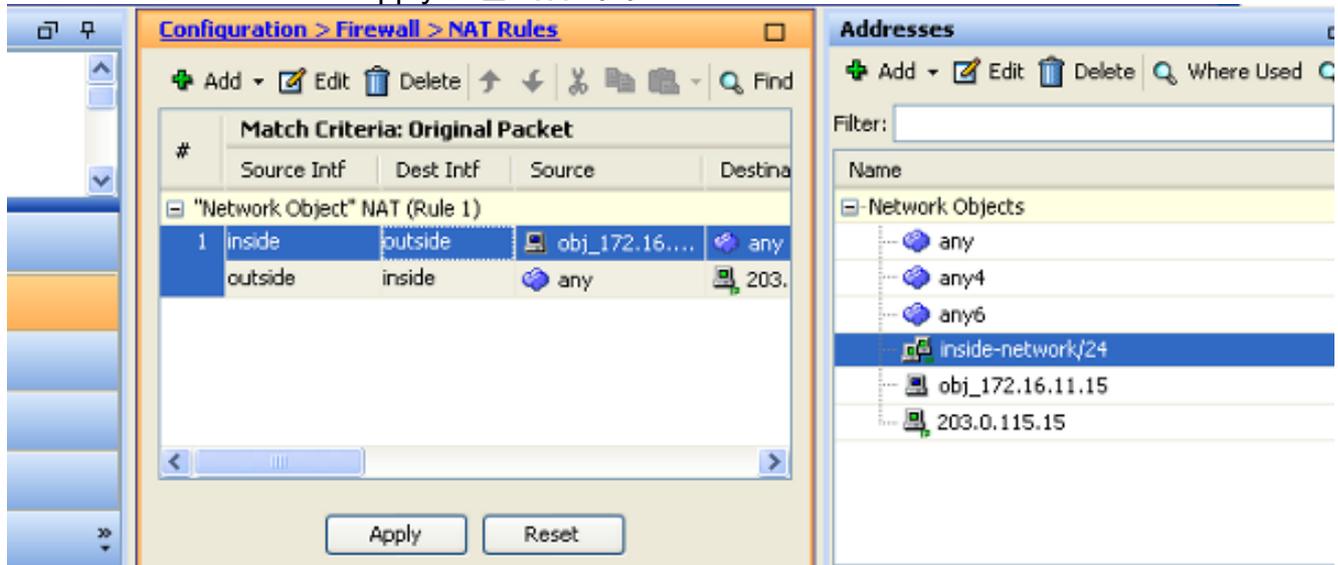
Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. Source Interface and Destination Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다. 서비스를 구성합니다. **OK(확인)**를 클릭합니다.



5. 변경 사항을 적용하려면 Apply를 클릭합니다.



이 NAT 컨피그레이션에 대한 동등한 CLI 출력입니다.

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Cisco CLI Analyzer(등록 고객만 해당)는 특정 show 명령을 지원합니다. Cisco CLI Analyzer를 사용

하여 **show** 명령 출력의 분석을 봅니다.

웹 브라우저에서 HTTP를 통해 웹 사이트에 액세스합니다. 이 예에서는 198.51.100.100에서 호스팅되는 사이트를 사용합니다. 연결에 성공하면 ASA CLI에서 이 출력을 볼 수 있습니다.

연결

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA는 스테이트풀 방화벽이며, 웹 서버의 반환 트래픽은 방화벽 연결 테이블의 연결과 일치하므로 방화벽을 다시 통과할 수 있습니다. 존재하는 연결과 일치하는 트래픽은 인터페이스 ACL에 의해 차단되지 않고 방화벽을 통과할 수 있습니다.

이전 출력에서 내부 인터페이스의 클라이언트는 외부 인터페이스의 198.51.100.100 호스트에 대한 연결을 설정했습니다. 이 연결은 TCP 프로토콜로 이루어지며 6초 동안 유휴 상태입니다. 연결 플래그는 이 연결의 현재 상태를 나타냅니다. 연결 플래그에 대한 자세한 내용은 [ASA TCP 연결 플래그](#)에서 확인할 수 있습니다.

Syslog

```
ASA(config)# show log | in 172.16.11.5
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

ASA 방화벽은 정상 작동 중에 syslog를 생성합니다. syslogs는 로깅 컨피그레이션을 기준으로 자세한 정보를 제공합니다. 출력은 레벨 6 또는 '정보' 레벨에서 보이는 두 개의 syslog를 보여줍니다.

이 예에서는 2개의 syslog가 생성됩니다. 첫 번째는 방화벽이 변환, 특히 PAT(Dynamic TCP Translation)를 작성했음을 나타내는 로그 메시지입니다. 이는 트래픽이 내부에서 외부 인터페이스로 이동할 때 소스 IP 주소 및 포트, 변환된 IP 주소 및 포트를 나타냅니다.

두 번째 syslog는 방화벽이 클라이언트와 서버 간의 이 특정 트래픽에 대한 연결을 연결 테이블에 구축했음을 나타냅니다. 이 연결 시도를 차단하기 위해 방화벽을 구성했거나 다른 요인으로 인해 이 연결의 생성이 금지된 경우(리소스 제약 또는 잘못된 구성 가능성), 방화벽은 연결이 구축되었음을 나타내는 로그를 생성하지 않습니다. 대신 연결이 거부되는 이유나 어떤 요인으로 인해 연결이 생성되지 못했는지 알려주는 메시지가 기록됩니다.

패킷 추적기

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80
```

--Omitted--

Result:

input-interface: inside

```
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ASA의 패킷 추적기 기능을 사용하면 *시뮬레이션된 패킷*을 지정하고 방화벽이 트래픽을 처리할 때 거치는 다양한 단계, 검사 및 기능을 모두 볼 수 있습니다. 이 도구를 사용하면 방화벽을 통과할 수 있다고 생각되는 트래픽의 예를 식별하고, 트래픽을 시뮬레이션하기 위해 이 5튜플을 사용하는 것이 좋습니다. 이전 예에서는 패킷 추적기를 사용하여 다음 조건을 충족하는 연결 시도를 시뮬레이션했습니다.

- 시뮬레이션된 패킷이 내부에 도착합니다.
- 사용되는 프로토콜은 TCP입니다.
- 시뮬레이션된 클라이언트 IP 주소는 172.16.11.5입니다.
- 클라이언트는 포트 1234에서 소싱된 트래픽을 전송합니다.
- 트래픽은 IP 주소 198.51.100.100의 서버로 전달됩니다.
- 트래픽은 포트 80으로 전달됩니다.

명령에 인터페이스 외부에 대한 언급이 없습니다. 이것은 패킷 추적기 설계에 의한 것입니다. 이 틀은 방화벽이 어떤 인터페이스에서 어떤 유형의 연결 시도를 라우팅하는지, 즉 어떤 방식으로 연결을 시도하는지 알려줍니다. 패킷 추적기에 대한 자세한 내용은 [Tracing Packets with Packet Tracer](#)를 참조하십시오.

캡처

캡처 적용

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA#show capture capin
```

```
3 packets captured
```

```
1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA#show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA 방화벽은 인터페이스로 들어오거나 나가는 트래픽을 캡처할 수 있습니다. 이러한 캡처 기능은 트래픽이 방화벽에 도착하는지 또는 방화벽에서 출발하는지 여부를 확실히 입증할 수 있으므로 매우 유용합니다. 앞의 예에서는 내부 및 외부 인터페이스에서 각각 capin 및 capout이라는 두 개의 캡처를 구성하는 것을 보여 줍니다. capture 명령에서는 캡처할 트래픽에 대해 구체적으로 지정할 수

있는 match 키워드를 사용했습니다.

캡처 캡틴의 경우 TCP 호스트 172.16.11.5 호스트 198.51.100.100과 일치하는 내부 인터페이스(인그레스 또는 이그레스)에 표시되는 트래픽과 일치시키려고 한다고 표시했습니다. 즉, 호스트 172.16.11.5에서 호스트 198.51.100.100으로 또는 그 반대로 전송되는 모든 TCP 트래픽을 캡처하려고 합니다. match 키워드를 사용하면 방화벽에서 양방향으로 트래픽을 캡처할 수 있습니다. 외부 인터페이스에 대해 정의된 capture 명령은 내부 클라이언트 IP 주소를 참조하지 않습니다. 방화벽이 해당 클라이언트 IP 주소에서 PAT를 수행하기 때문입니다. 따라서 해당 클라이언트 IP 주소와 일치할 수 없습니다. 대신 이 예에서는 any를 사용하여 가능한 모든 IP 주소가 해당 조건과 일치함을 나타냅니다.

캡처를 구성한 후 다시 연결을 설정하고 show capture <capture_name> 명령을 사용하여 캡처를 **확인합니다**. 이 예에서는 클라이언트가 캡처에 표시된 TCP 3-Way 핸드셰이크에 의해 확인된 것처럼 서버에 연결할 수 있음을 확인할 수 있습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [ASA Syslog 컨피그레이션 예](#)
- [CLI 및 ASDM 컨피그레이션을 사용한 ASA 패킷 캡처 예](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.