2개의 내부 네트워크 및 인터넷 컨피그레이션이 포함된 ASA 8.3(x) 동적 PAT 예

목차

소개

이 문서에서는 소프트웨어 버전 8.3(1)을 실행하는 Cisco ASA(Adaptive Security Appliance)에서 동적 PAT에 대한 샘플 컨피그레이션을 제공합니다. 동적 PAT는 실제 소스 주소와 소스 포트를 매핑된 주소 및 고유한 매핑된 포트로 변환하여 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다.각 연결마다 소스 포트가 다르므로 각 연결에는 별도의 변환 세션이 필요합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 내부 네트워크에 ASA 내부에 두 개의 네트워크가 있는지 확인합니다.192.168.0.0/24—ASA에 직접 연결된 네트워크.192.168.1.0/24—ASA 내부에 있지만 다른 디바이스(예: 라우터)에 있는 네트워크.
- 내부 사용자가 다음과 같이 PAT를 받아야 합니다.192.168.1.0/24 서브넷의 호스트는 ISP(10.1.5.5)이 제공한 예비 IP 주소에 PAT를 가져옵니다.ASA 내부의 다른 호스트는 ASA의 외부 인터페이스 IP 주소(10.1.5.1)에 PAT를 가져옵니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 버전 8.3(1)
- ASDM 버전 6.3(1)

참고: ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

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.

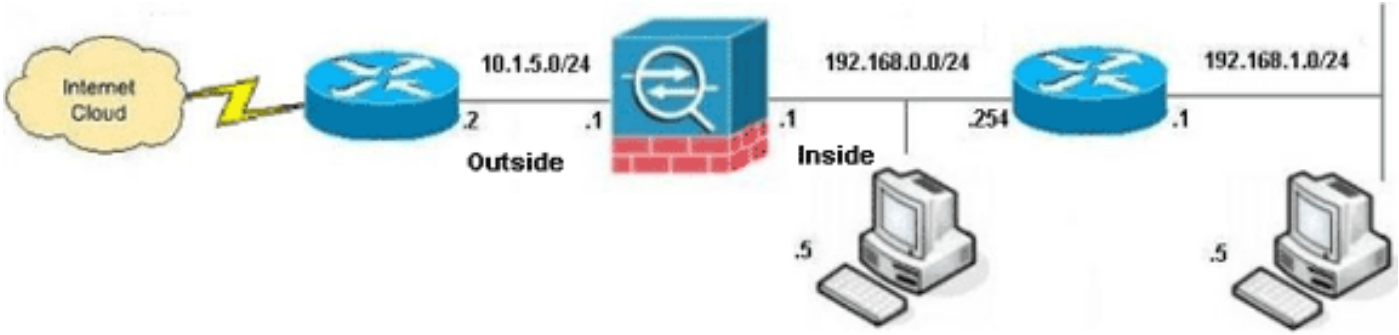
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



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

- ASA CLI 컨피그레이션
- ASDM 컨피그레이션

ASA CLI 컨피그레이션

이 문서에서는 아래 표시된 구성을 사용합니다.

ASA 동적 PAT 컨피그레이션

```
ASA#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.

!--- Creates an object called OBJ_GENERIC_ALL. !--- Any
host IP not already matching another configured !---
object will get PAT to the outside interface IP !--- on
the ASA (or 10.1.5.1), for internet bound traffic.
ASA(config)#object network OBJ_GENERIC_ALL
```

```
ASA(config-obj)#subnet 0.0.0.0 0.0.0.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface

!--- The above statements are the equivalent of the !---
nat/global combination (as shown below) in v7.0(x), !---
v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 interface


!--- Creates an object called OBJ_SPECIFIC_192-168-1-0.
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0
ASA(config-obj)#subnet 192.168.1.0 255.255.255.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5

!--- The above statements are the equivalent of the
nat/global !--- combination (as shown below) in v7.0(x),
v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA
code: nat (inside) 2 192.168.1.0 255.255.255.0
global (outside) 2 10.1.5.5
```

ASA 8.3(1) 실행 중인 컨피그레이션

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
!--- Configure the outside interface. ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip
address 10.1.5.1 255.255.255.0 !--- Configure the inside
interface. ! interface GigabitEthernet0/1 nameif inside
security-level 100 ip address 192.168.0.1 255.255.255.0
! interface GigabitEthernet0/2 shutdown no nameif no
security-level no ip address ! interface
GigabitEthernet0/3 shutdown no nameif no security-level
no ip address ! interface Management0/0 shutdown no
nameif no security-level no ip address management-only !
boot system disk0:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0
 subnet 192.168.1.0 255.255.255.0
object network OBJ_GENERIC_ALL
 subnet 0.0.0.0 0.0.0.0

pager lines 24
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400
```

```
nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface
nat (inside,outside) source dynamic OBJ_SPECIFIC_192-
168-1-0 10.1.5.5

route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 10.1.5.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
```

```
: end
```

ASDM 컨피그레이션

ASDM 인터페이스를 통해 이 컨피그레이션을 완료하려면 다음을 수행해야 합니다.

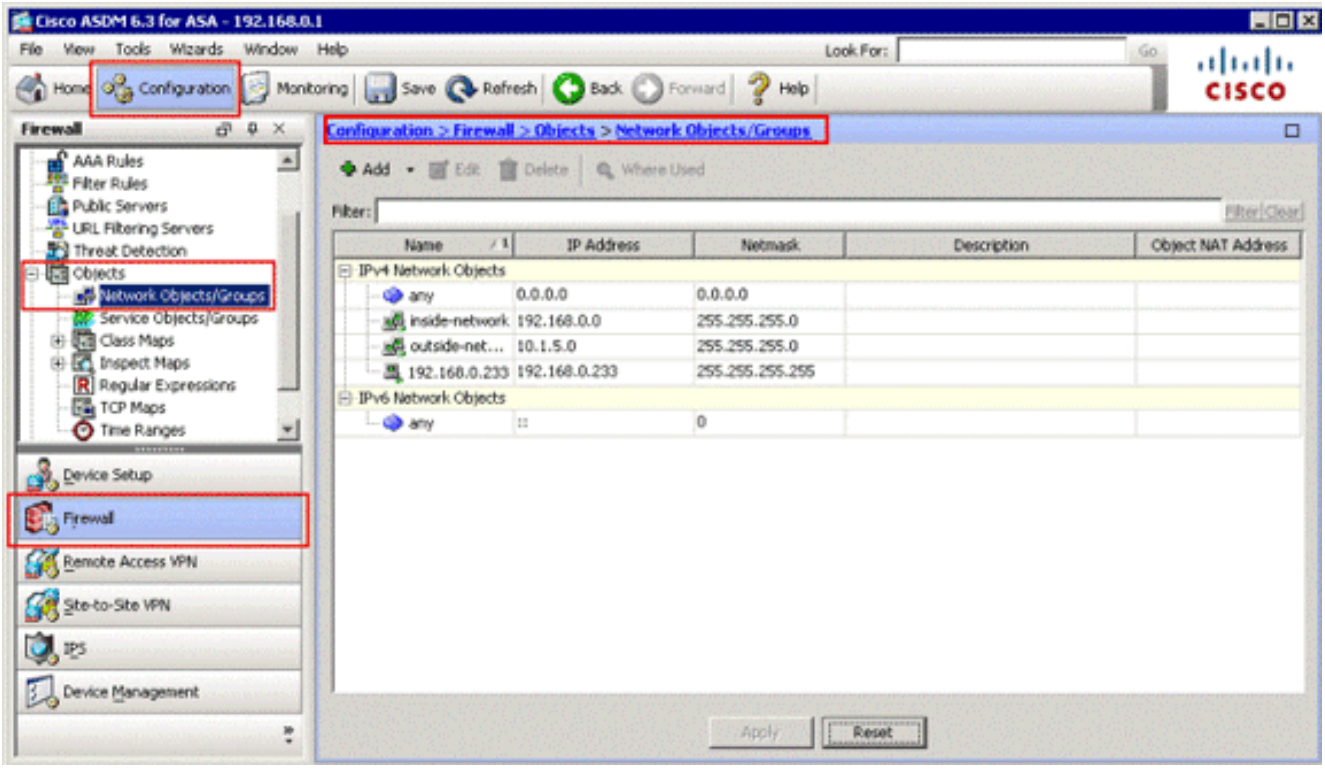
1. 3개의 네트워크 객체를 추가합니다.이 예에서는 다음 네트워크 객체를 추가합니다 .OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. 2개의 NAT/PAT 규칙을 생성합니다.다음 예에서는 이러한 네트워크 객체에 대한 NAT 규칙을 생성합니다.OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

네트워크 개체 추가

네트워크 객체를 추가하려면 다음 단계를 완료합니다.

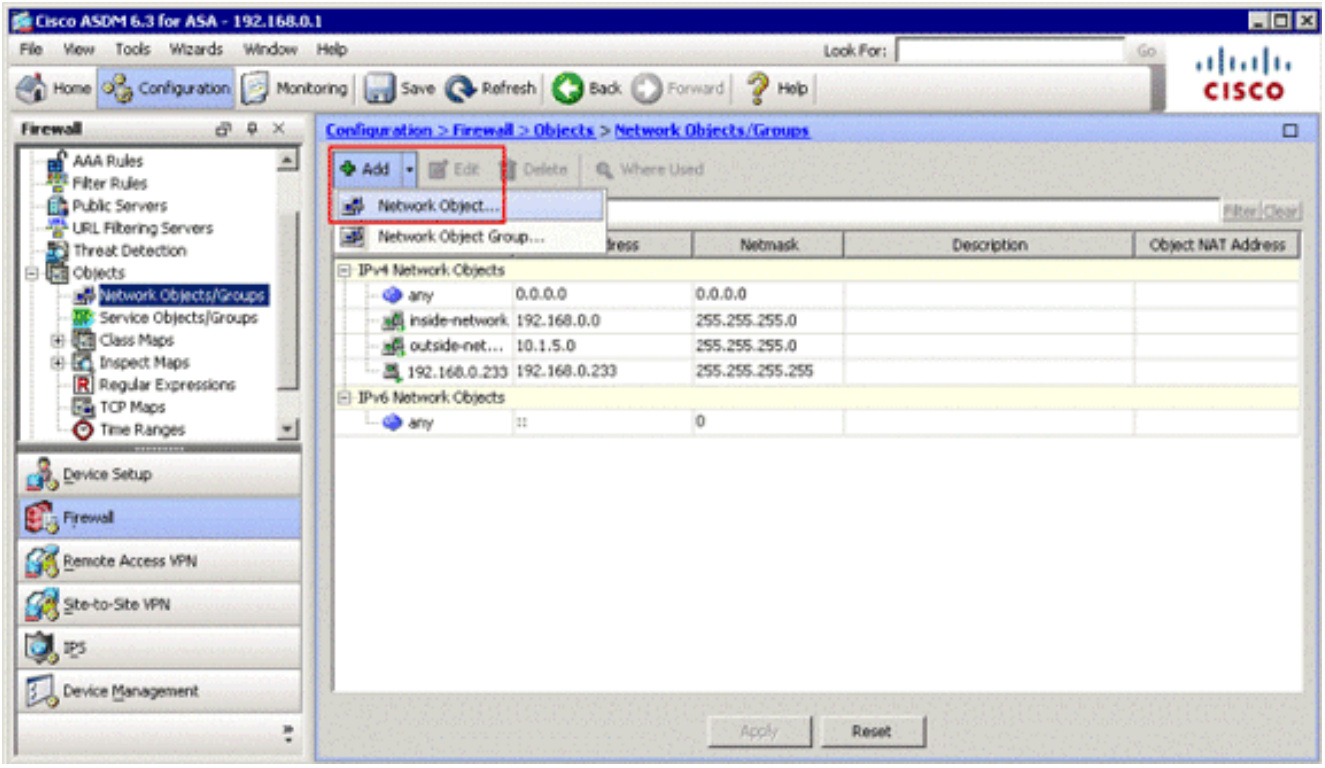
1. ASDM에 로그인하고 Configuration(컨피그레이션) **> Firewall(방화벽) > Objects(개체) > Network Objects/Groups(네트워크 개체/그룹)를** 선택합니다

.

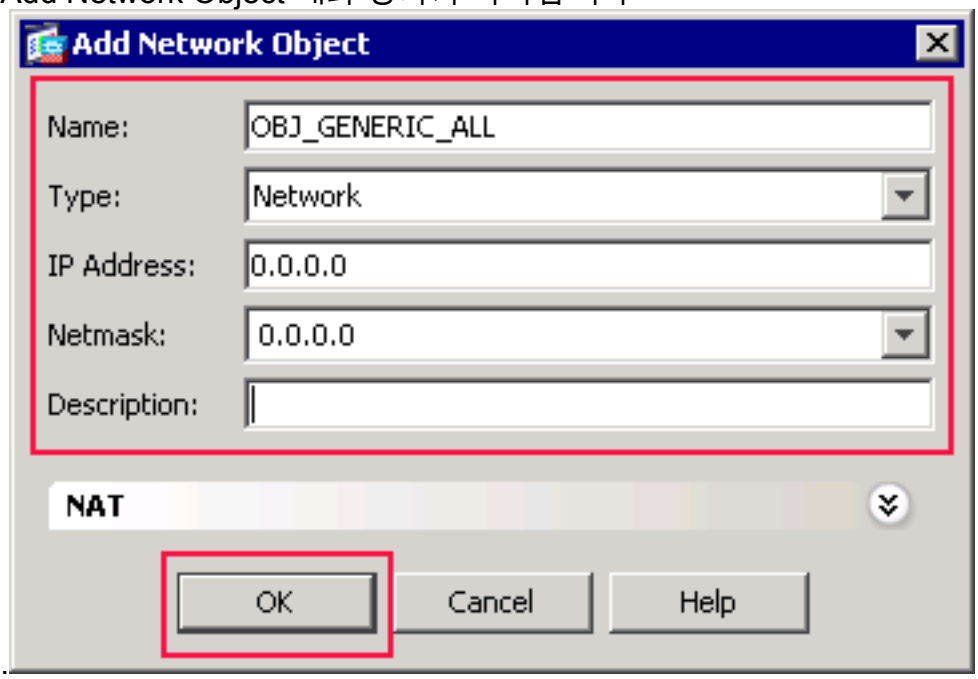


2. 네트워크 객체를 추가하려면 Add > Network Object를 선택합니다

.



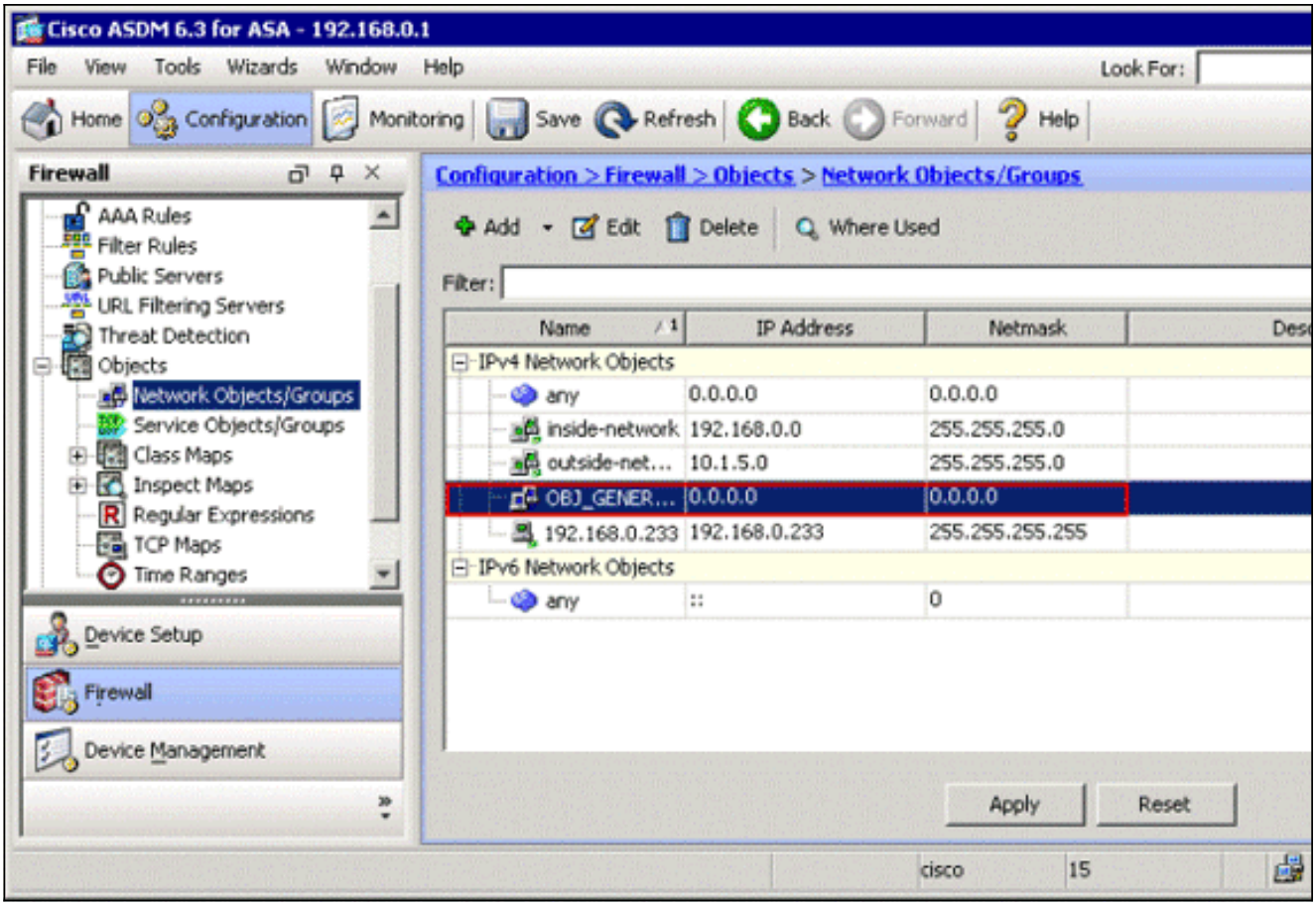
Add Network Object 대화 상자가 나타납니다



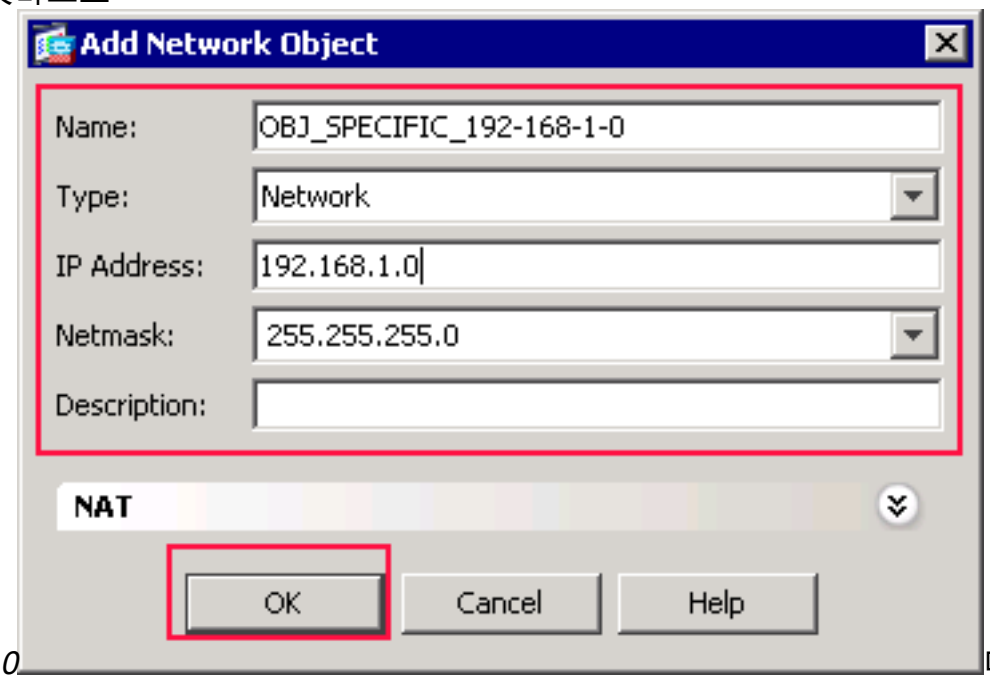
.

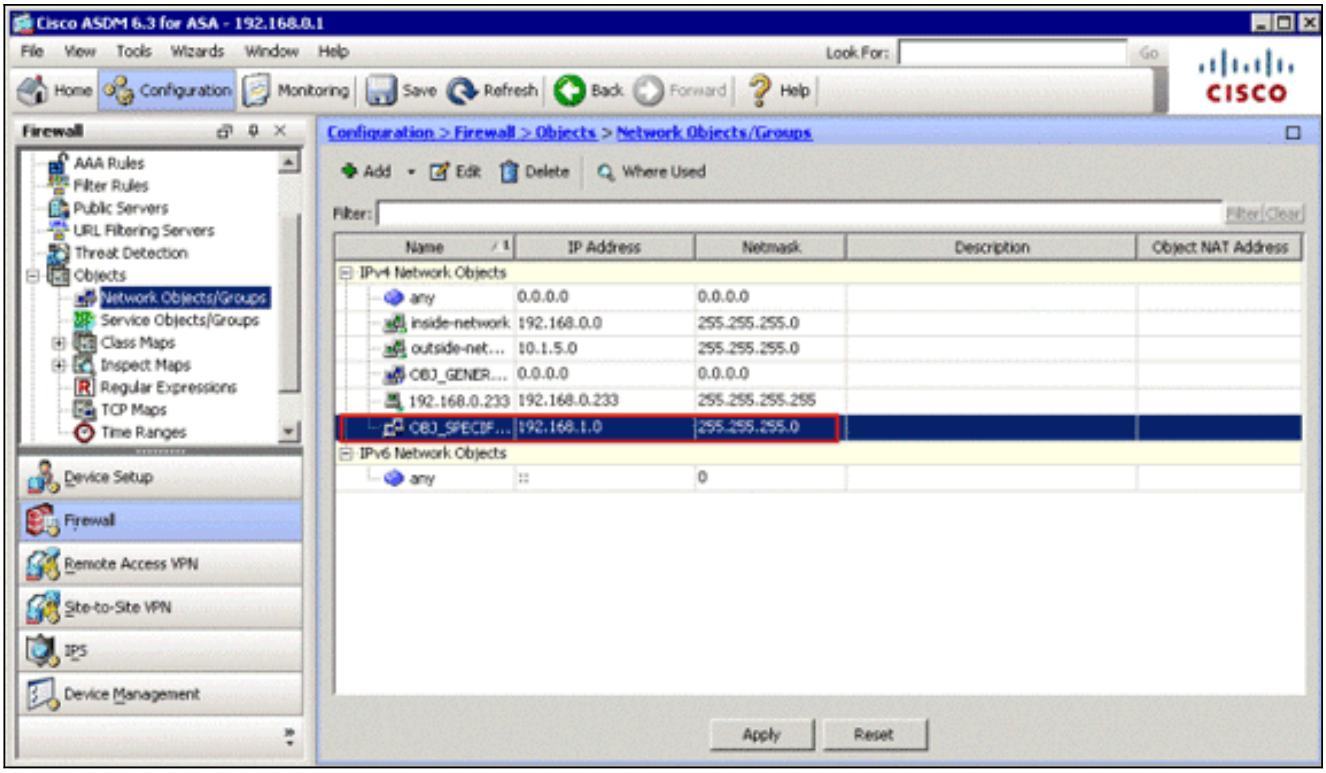
3. Add Network Object(네트워크 개체 추가) 대화 상자에 다음 정보를 입력합니다.네트워크 개체의 이름입니다.(이 예에서는 *OBJ_GENERIC_ALL을* 사용합니다.)네트워크 개체의 유형입니다.(이 예에서는 *네트워크*를 사용합니다.)네트워크 개체의 IP 주소입니다.(이 예에서는 *0.0.0.0을* 사용합니다.)네트워크 개체의 넷마스크입니다.(이 예에서는 *0.0.0.0을* 사용합니다.)
4. **확인을 클릭합니다**.네트워크 객체가 생성되어 다음 이미지에 표시된 대로 Network Objects/Groups 목록에 나타납니다

.

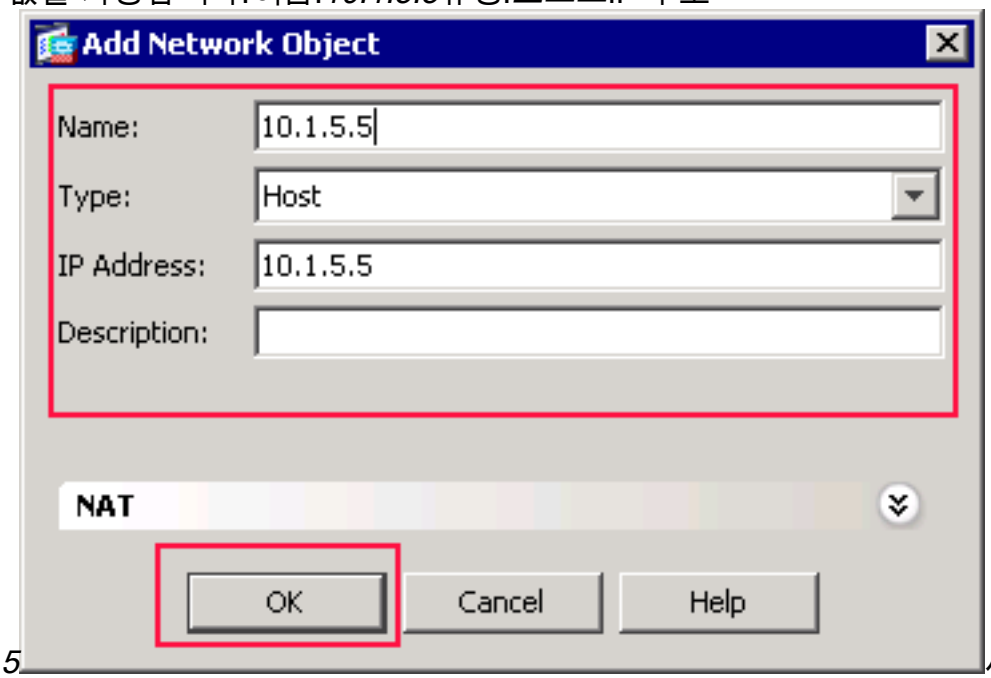


5. 두 번째 네트워크 객체를 추가하려면 이전 단계를 반복하고 **OK**(확인)를 클릭합니다.이 예에서는 다음 값을 사용합니다.이름:*OBJ_SPECIFIC_192-168-1-0*유형:*네트워크*IP 주소:*192.168.1.0*넷마스크:*255.255.255.0*다음 이미지에 표시된 대로 두 번째 객체가 생성되어 네트워크 객체/그룹 목록에 나타납니다.



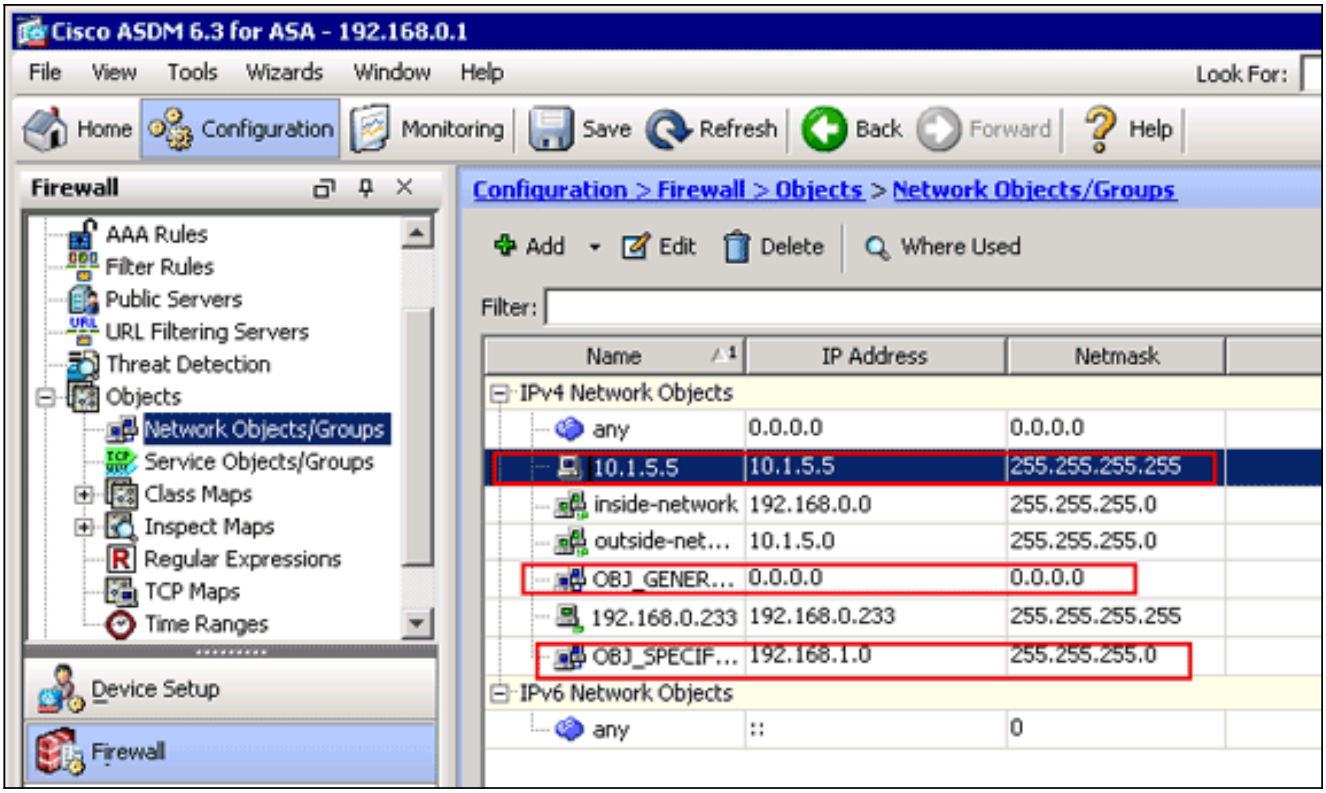


6. 세 번째 네트워크 객체를 추가하려면 이전 단계를 반복하고 **OK**(확인)를 클릭합니다.이 예에서는 다음 값을 사용합니다.이름:*10.1.5.5*유형:*호스트*IP 주소



:*10.1.5.5*세 번째 네트워크 객체가 생성되고 Network Objects/Groups(네트워크 객체/그룹) 목록에 나타납니다

.

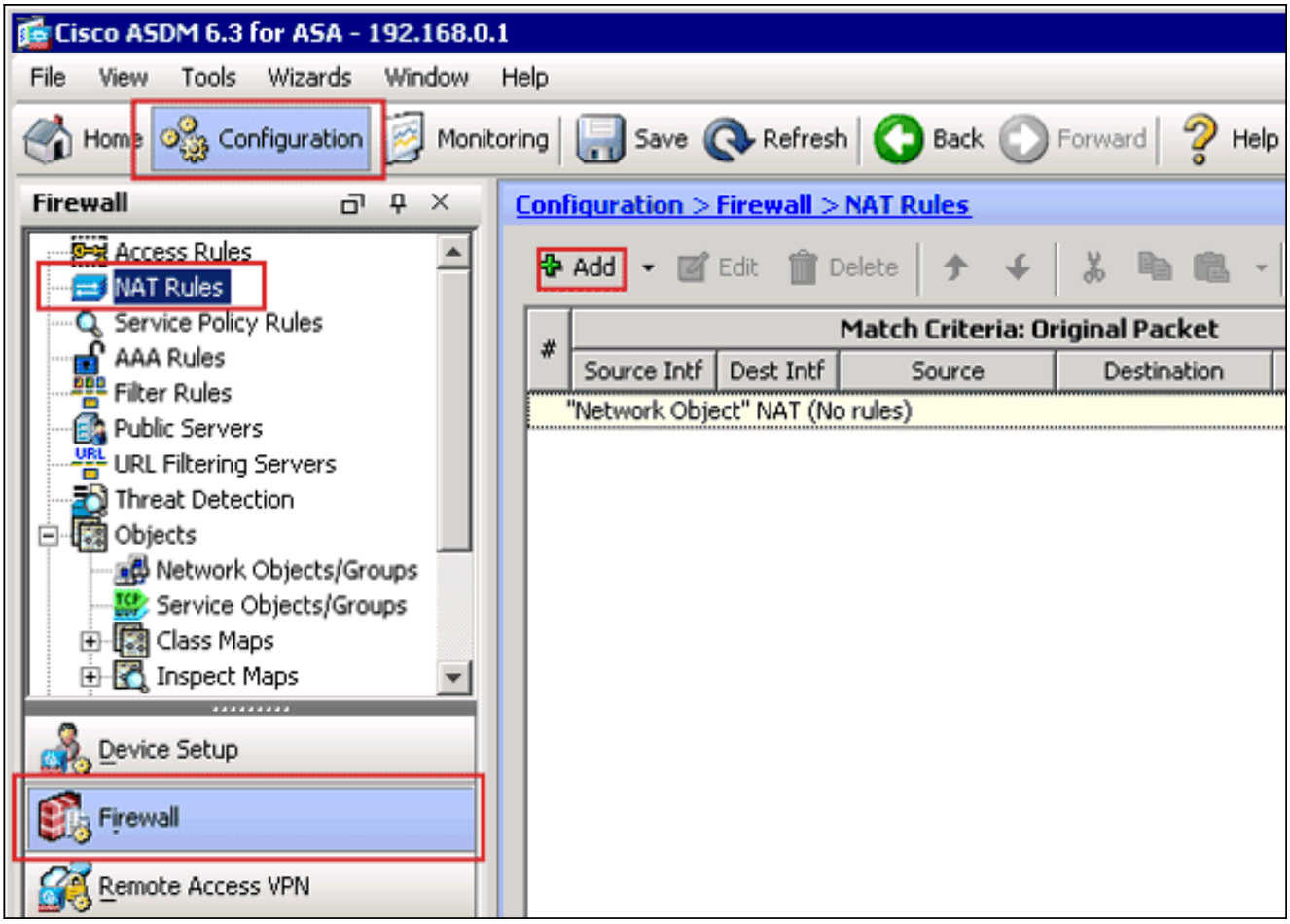


이제 Network Objects/Groups(네트워크 개체/그룹) 목록에는 NAT 규칙이 참조하는 데 필요한 3개의 필수 개체가 포함되어야 합니다.

NAT/PAT 규칙 생성

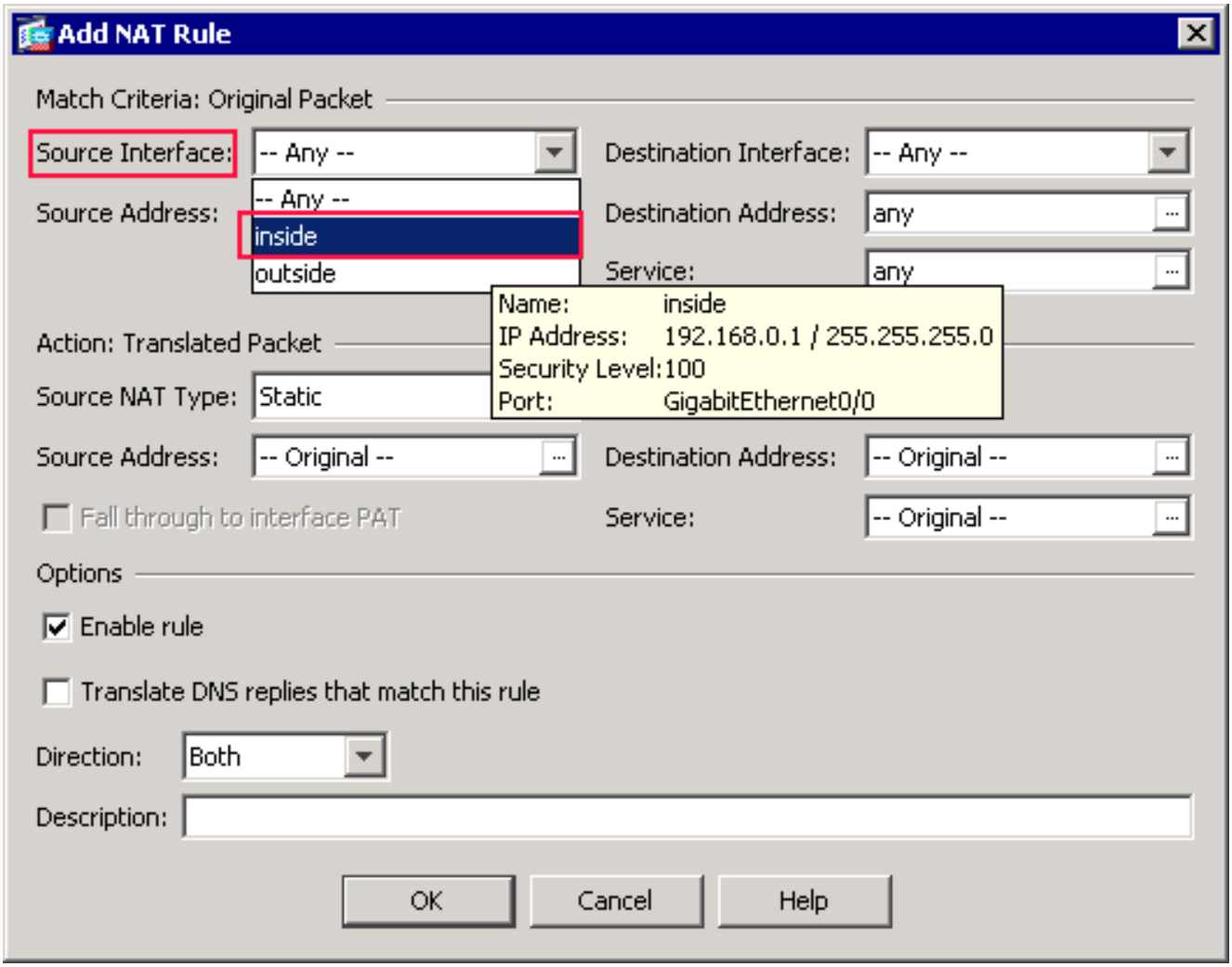
NAT/PAT 규칙을 생성하려면 다음 단계를 완료합니다.

1. 첫 번째 NAT/PAT 규칙을 생성합니다.ASDM에서 Configuration(컨피그레이션) **> Firewall(방화벽) > NAT Rules(NAT 규칙)를** 선택하고 Add(**추가**)를 클릭합니다
.



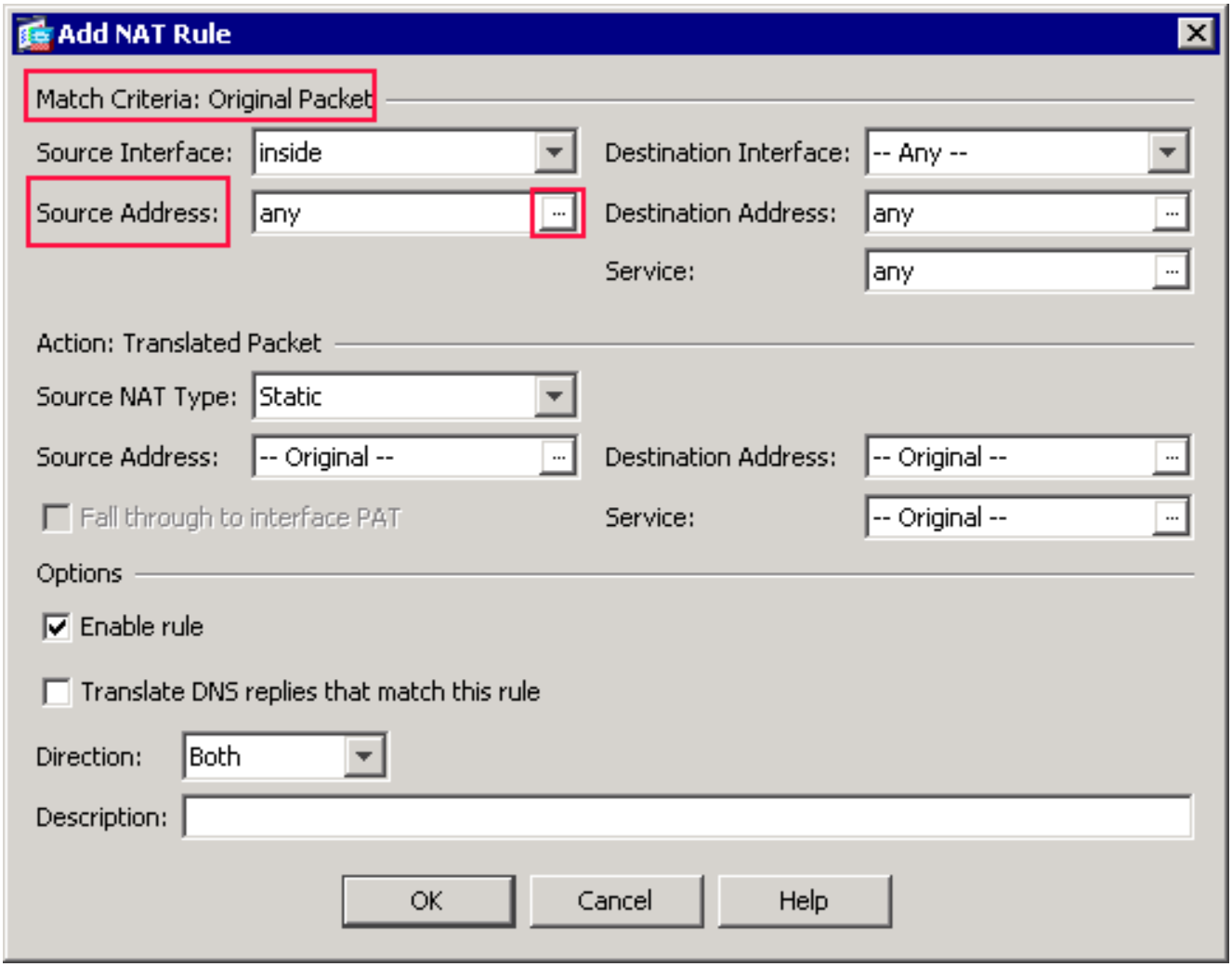
Add NAT Rule 대화 상자가 나타납니다

.



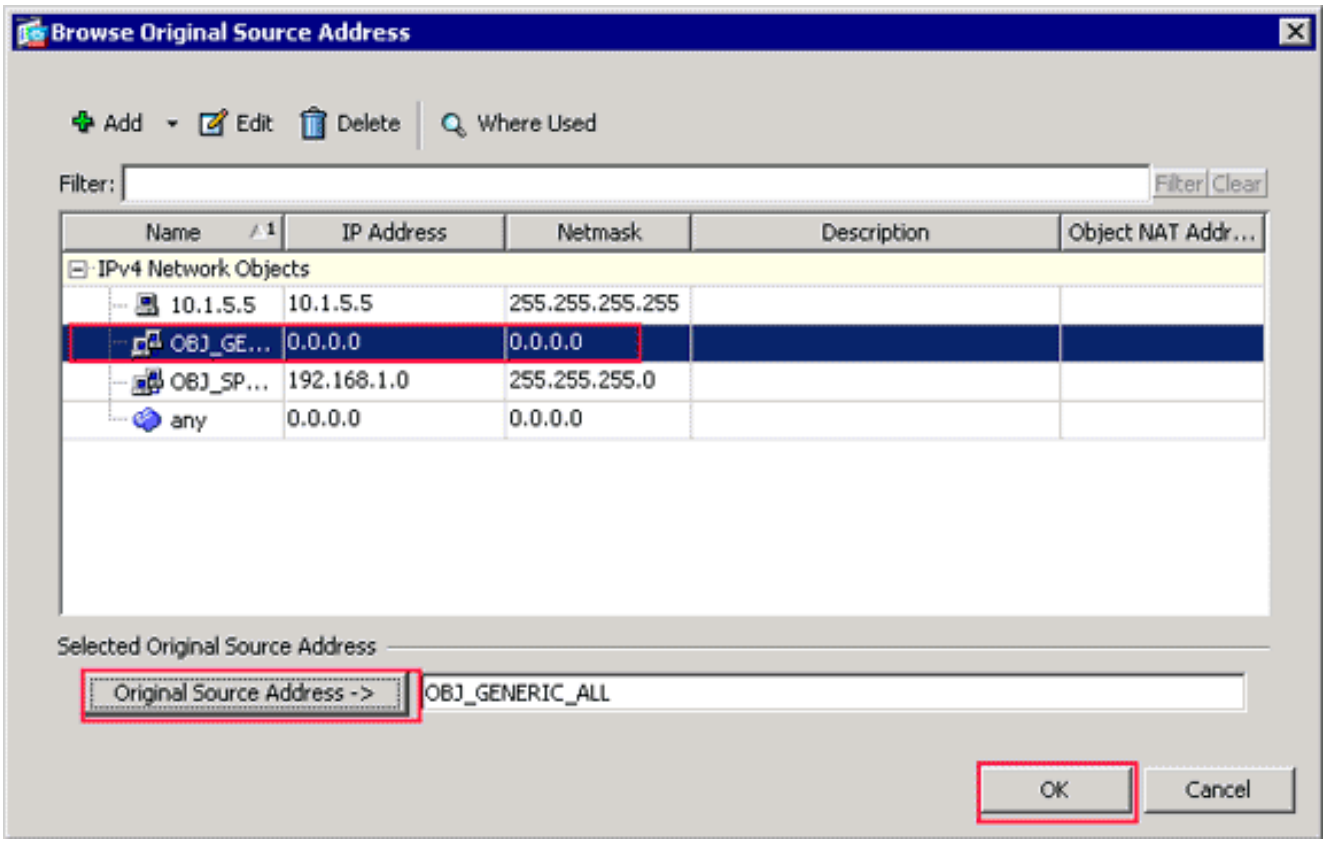
일치 기준:Add NAT Rule(NAT 규칙 추가) 대화 상자의 Original Packet(원래 패킷) 영역에서 Source Interface(소스 인터페이스) 드롭다운 목록에서 **inside(내부)**를 선택합니다

.



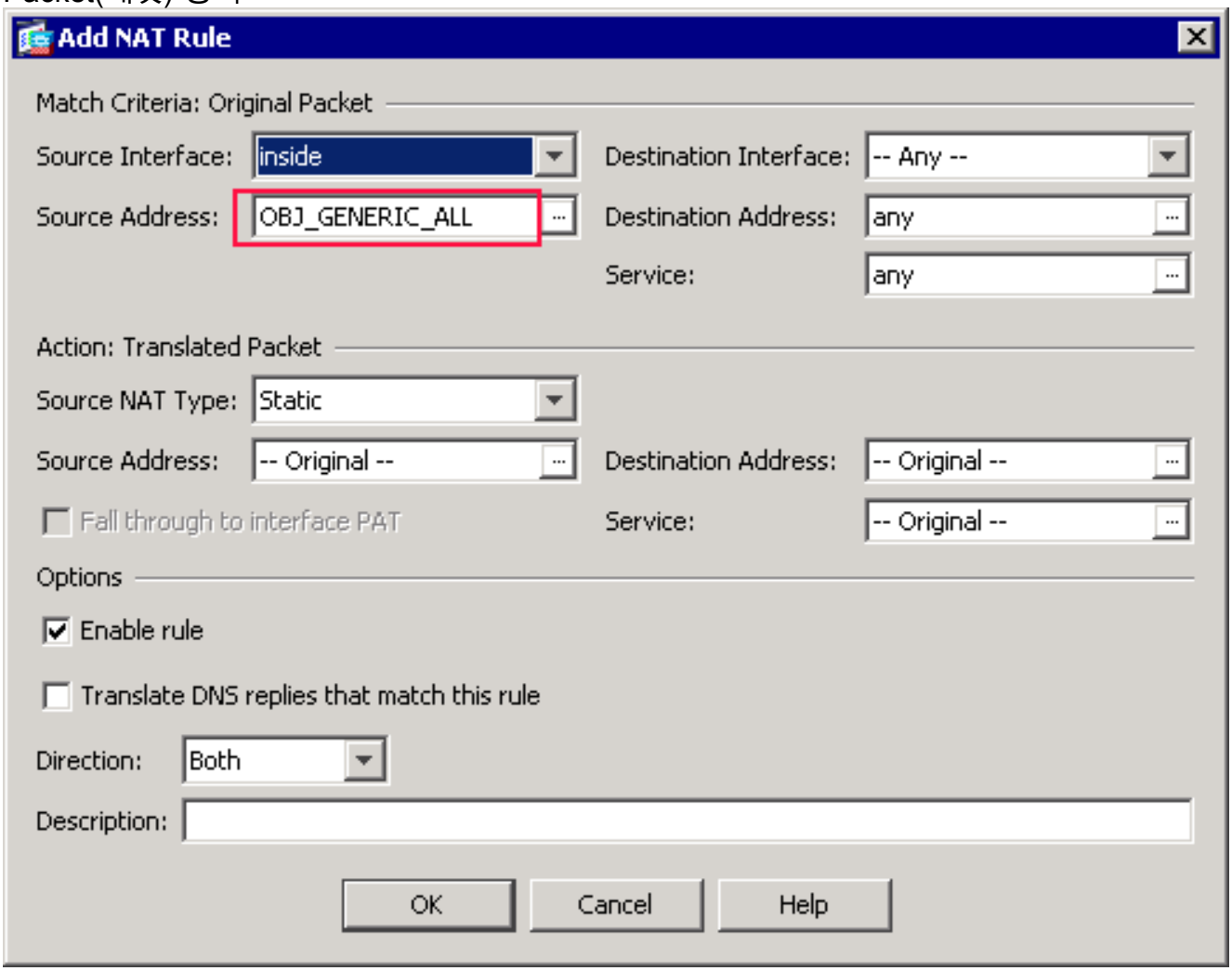
Source Address(소스 주소) 텍스트 필드 오른쪽에 있는 찾아보기(찾아보기) 버튼을 클릭합니다.Browse Original Source Address 대화 상자가 나타납니다

.



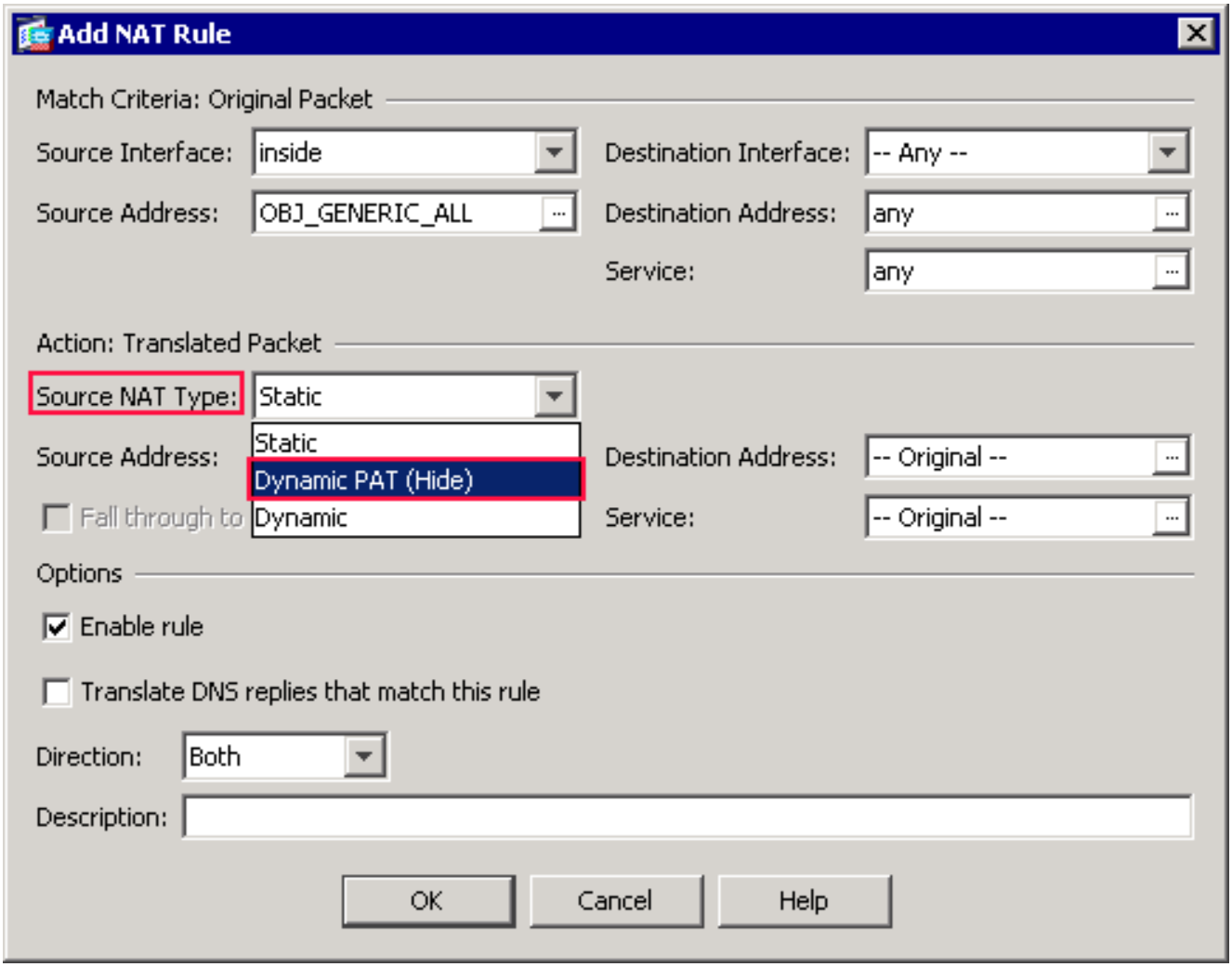
Browse Original Source Address 대화 상자에서 생성한 첫 번째 네트워크 객체를 선택합니다

.(이 예에서는 OBJ_**GENERIC_ALL을** 선택합니다.)Original **Source Address(원래 소스 주소)**를 클릭하고 **OK(확인)**를 클릭합니다.OBJ_*GENERIC_ALL* 네트워크 객체가 Match Criteria의 Source Address 필드에 나타납니다.Add NAT Rule(NAT 규칙 추가) 대화 상자의 원래 Packet(패킷) 영역



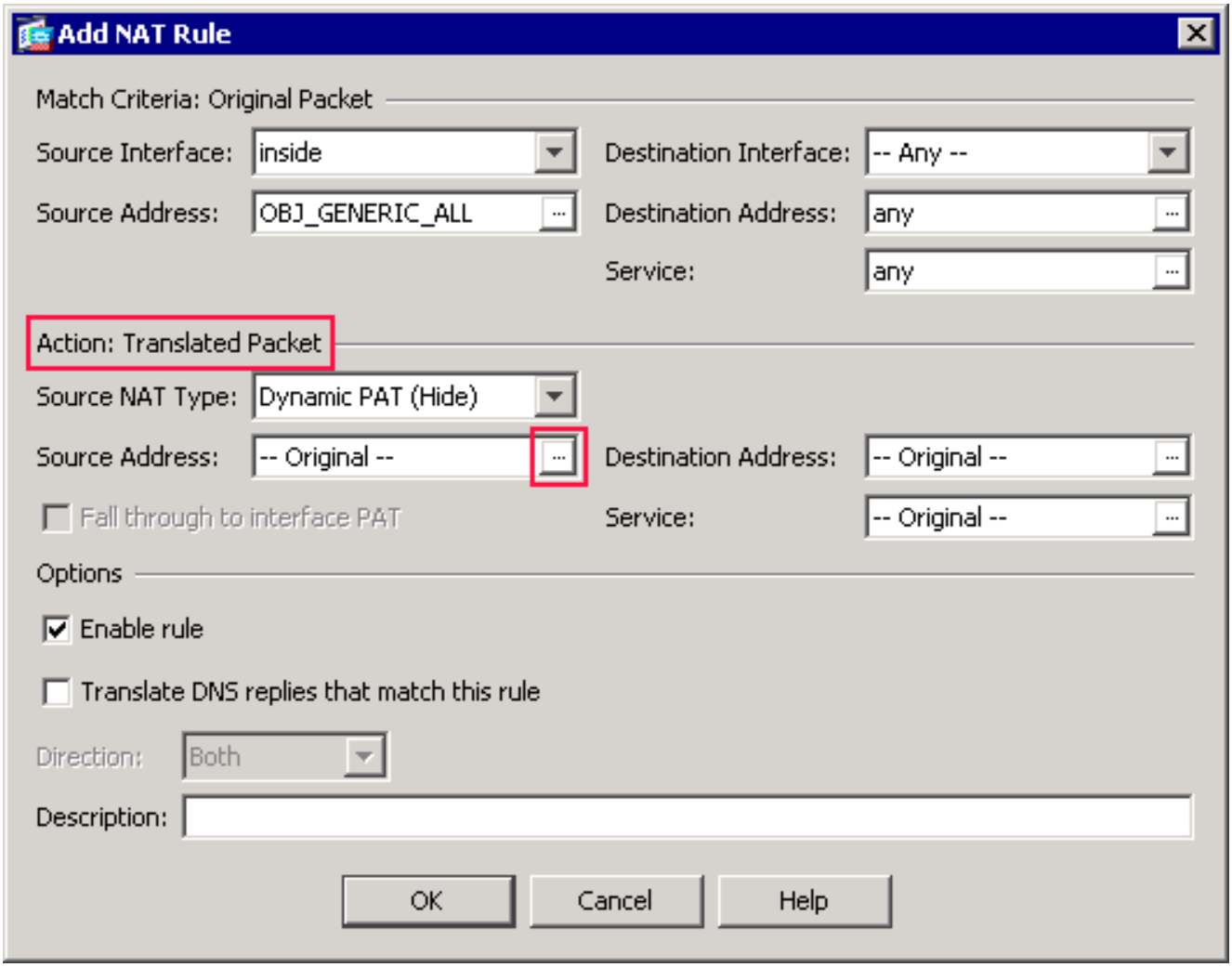
작업:Add NAT Rule(NAT 규칙 추가) 대화 상자의 Translated Packet(변환된 패킷) 영역에서 Source NAT Type(소스 NAT 유형) 대화 상자에서 **Dynamic PAT (Hide)**를 선택합니다

.



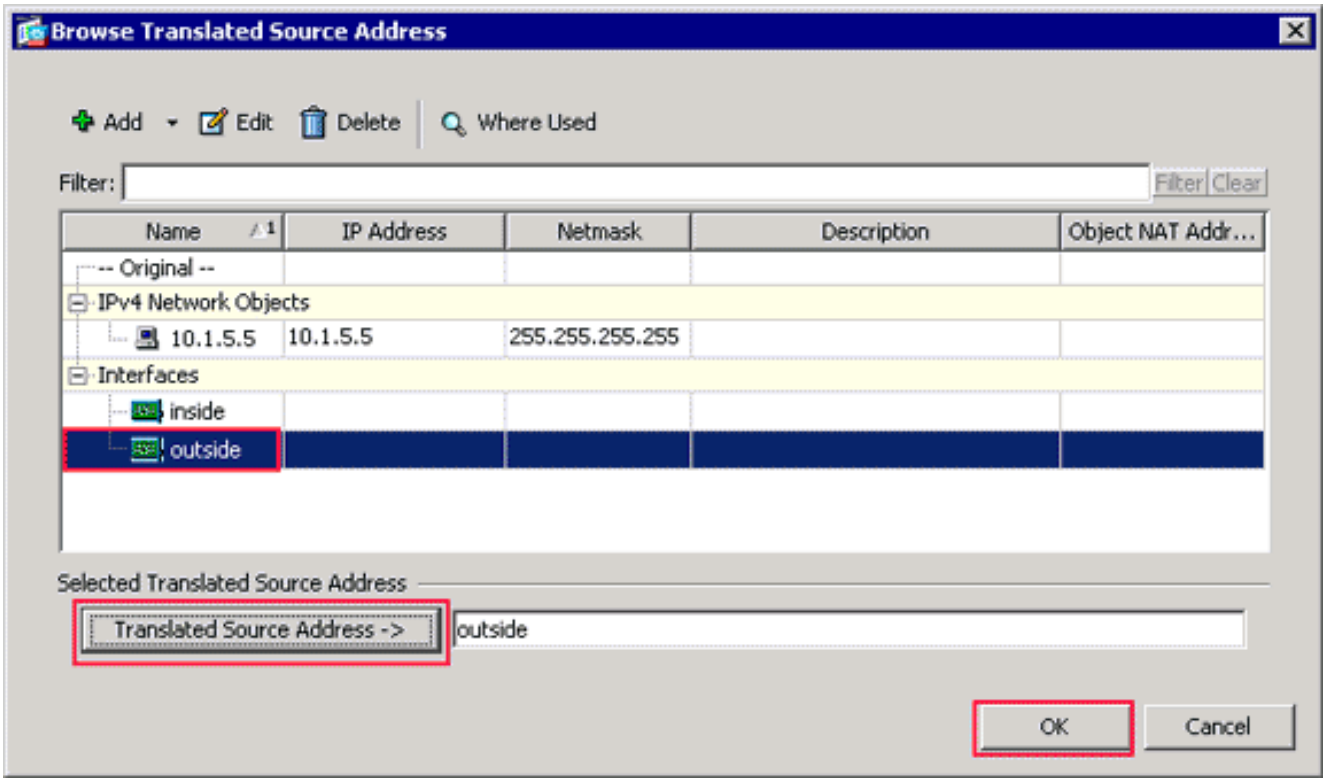
Source Address(소스 주소) 필드 오른쪽에 있는 찾아보기(..) 버튼을 클릭합니다

.



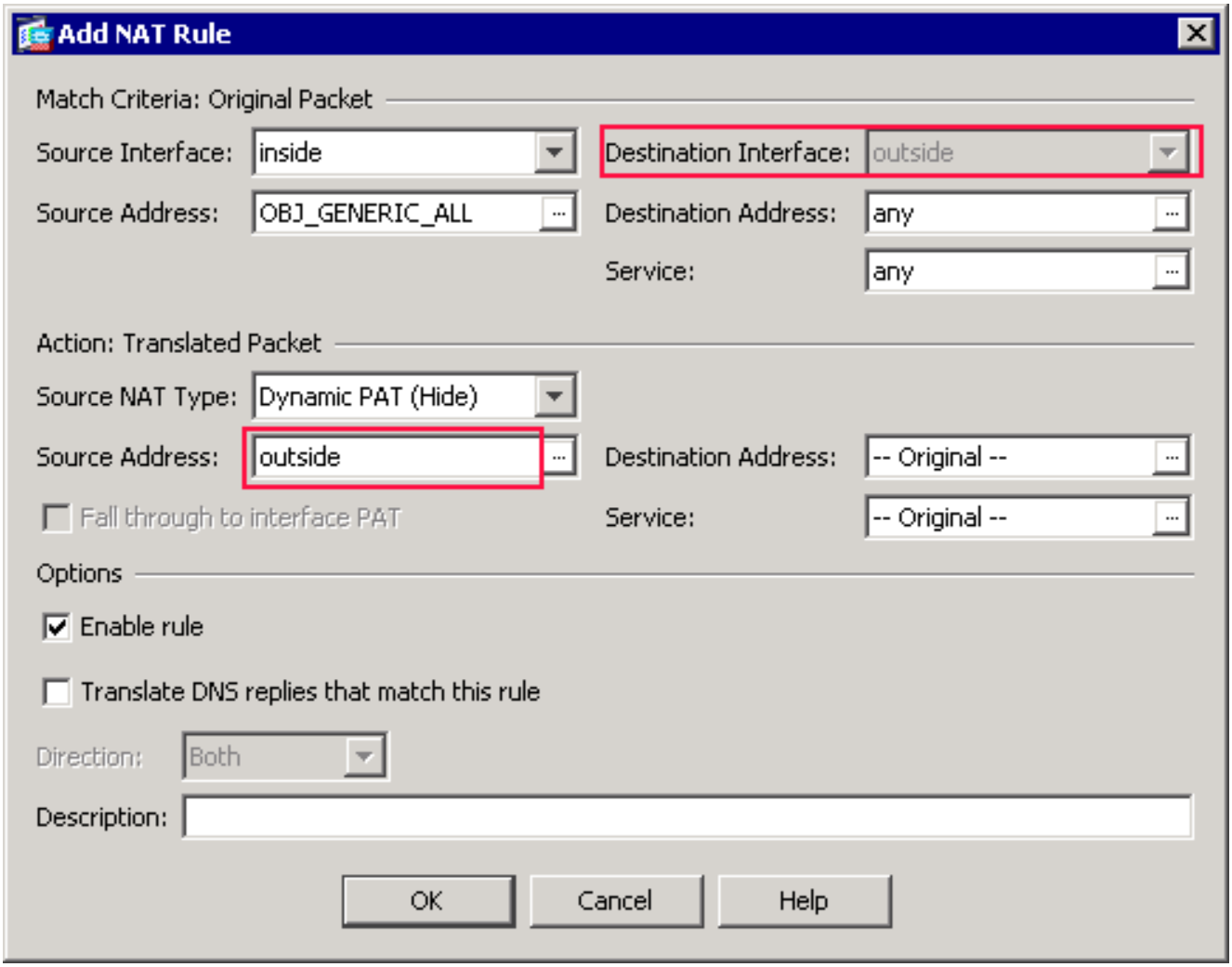
Browse Translated Source Address 대화 상자가 나타납니다

.



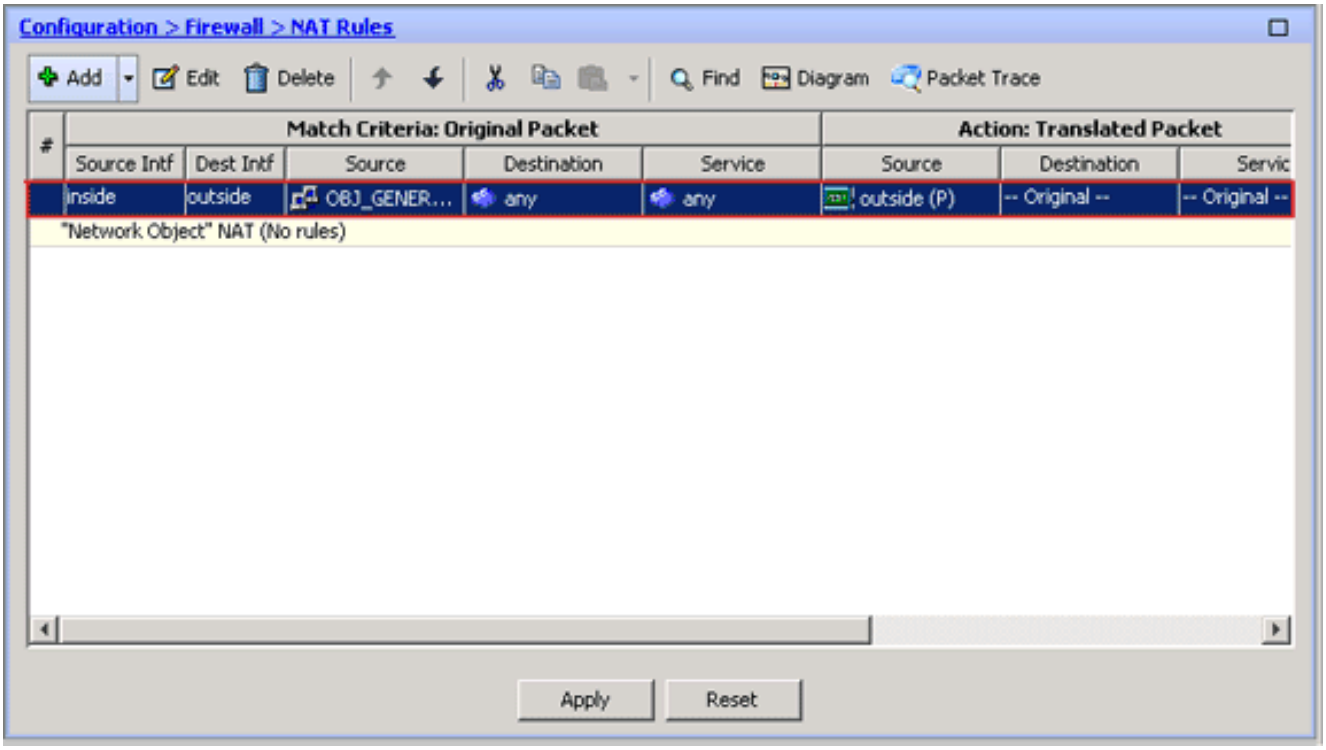
Browse Translated Source Address 대화 상자에서 **외부** 인터페이스 객체를 선택합니다.이 인터페이스는 원래 컨피그레이션의 일부이므로 이미 생성되었습니다.Translated **Source Address(변환된 소스 주소)**를 클릭하고 **OK**(확인)를 클릭합니다.이제 외부 인터페이스가

Action의 Source Address 필드에 나타납니다.Add NAT Rule 대화 상자의 Translated Packet 영역



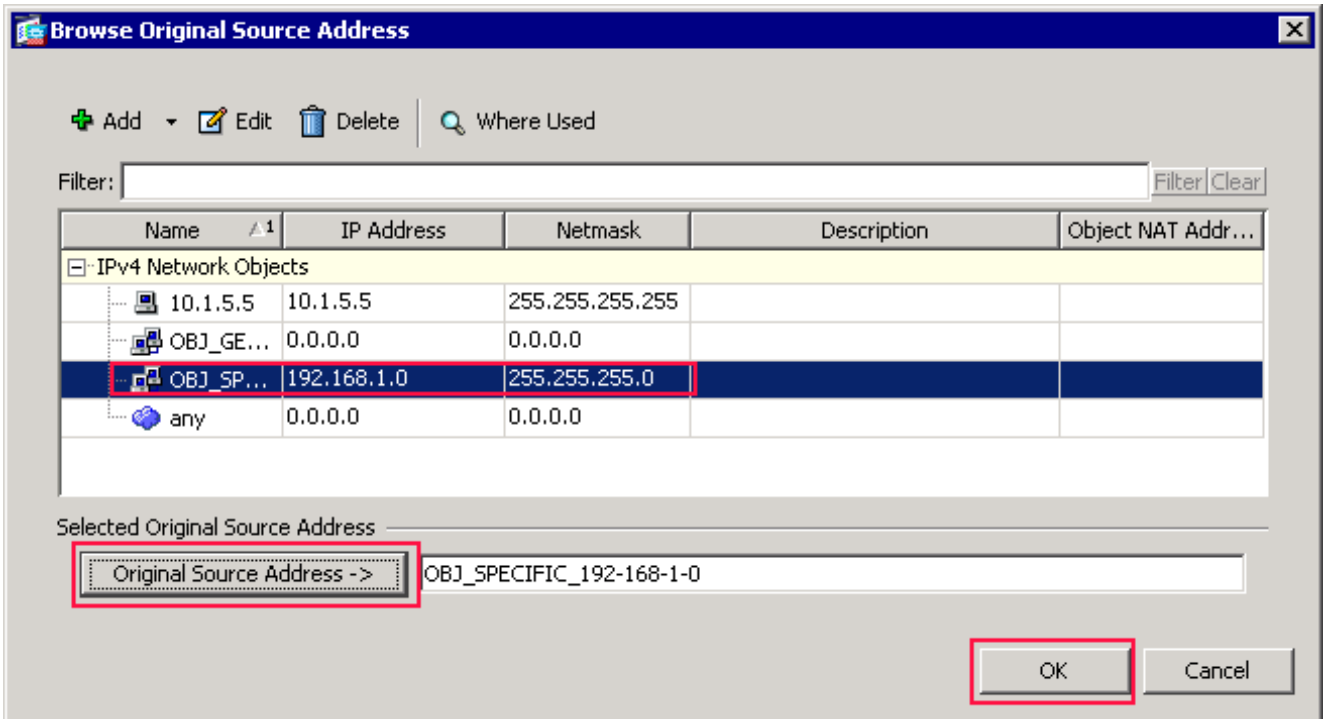
참고: Destination *Interface* 필드도 외부 인터페이스로 변경됩니다.첫 번째로 완료된 PAT 규칙이 다음과 같이 나타나는지 확인합니다.일치 기준:Original Packet(원래 패킷) 영역에서 다음 값을 확인합니다.소스 인터페이스 = 내부소스 주소 = OBJ_GENERIC_ALL대상 주소 = any서비스 = any작업:Translated Packet(변환된 패킷) 영역에서 다음 값을 확인합니다.소스 NAT 유형 = 동적 PAT(숨기기)소스 주소 = 외부대상 주소 = 원본서비스 = 원본**확인**을 **클릭합니다**.첫 번째 NAT 규칙은 다음 이미지와 같이 ASDM에 나타납니다

.



2. 두 번째 NAT/PAT 규칙을 생성합니다.ASDM에서 Configuration(컨피그레이션) **> Firewall(방화벽) > NAT Rules(NAT 규칙)를** 선택하고 Add(**추가**)를 클릭합니다.일치 기준:Add NAT Rule(NAT 규칙 추가) 대화 상자의 Original Packet(원래 패킷) 영역에서 Source Interface(소스 인터페이스) 드롭다운 목록에서 **inside(내부**)를 선택합니다.Source Address(소스 주소) 필드 오른쪽에 있는 찾아보기(**..**) 버튼을 클릭합니다.Browse Original Source Address 대화 상자가 나타납니다

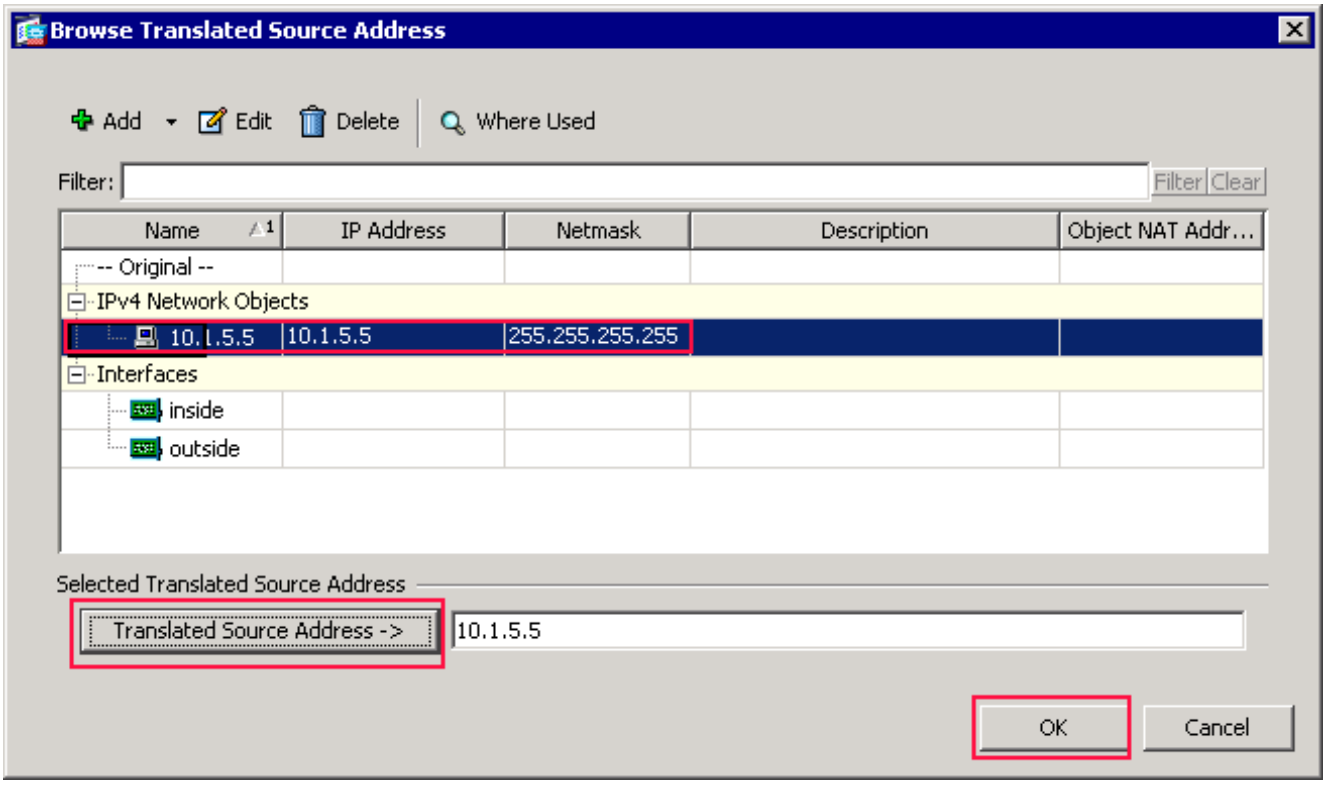
.



Browse Original Source Address 대화 상자에서 생성한 두 번째 객체를 선택합니다.(이 예에서는 **OBJ_SPECIFIC_192-168-1-0을** 선택합니다.)Original **Source Address(원래 소스 주소)**를 클릭하고 **OK(확인)**를 클릭합니다.OBJ_*SPECIFIC_192-168-1-0* 네트워크 객체는 Match Criteria의 Source Address 필드에 나타납니다.Add NAT Rule 대화 상자의 원래 Packet 영역 ..작업:Add NAT Rule(NAT 규칙 추가) 대화 상자의 Translated Packet(변환된 패킷) 영역에서 Source NAT Type(소스 NAT 유형) 대화 상자에서 **Dynamic PAT (Hide)**를 선택합니다.Source

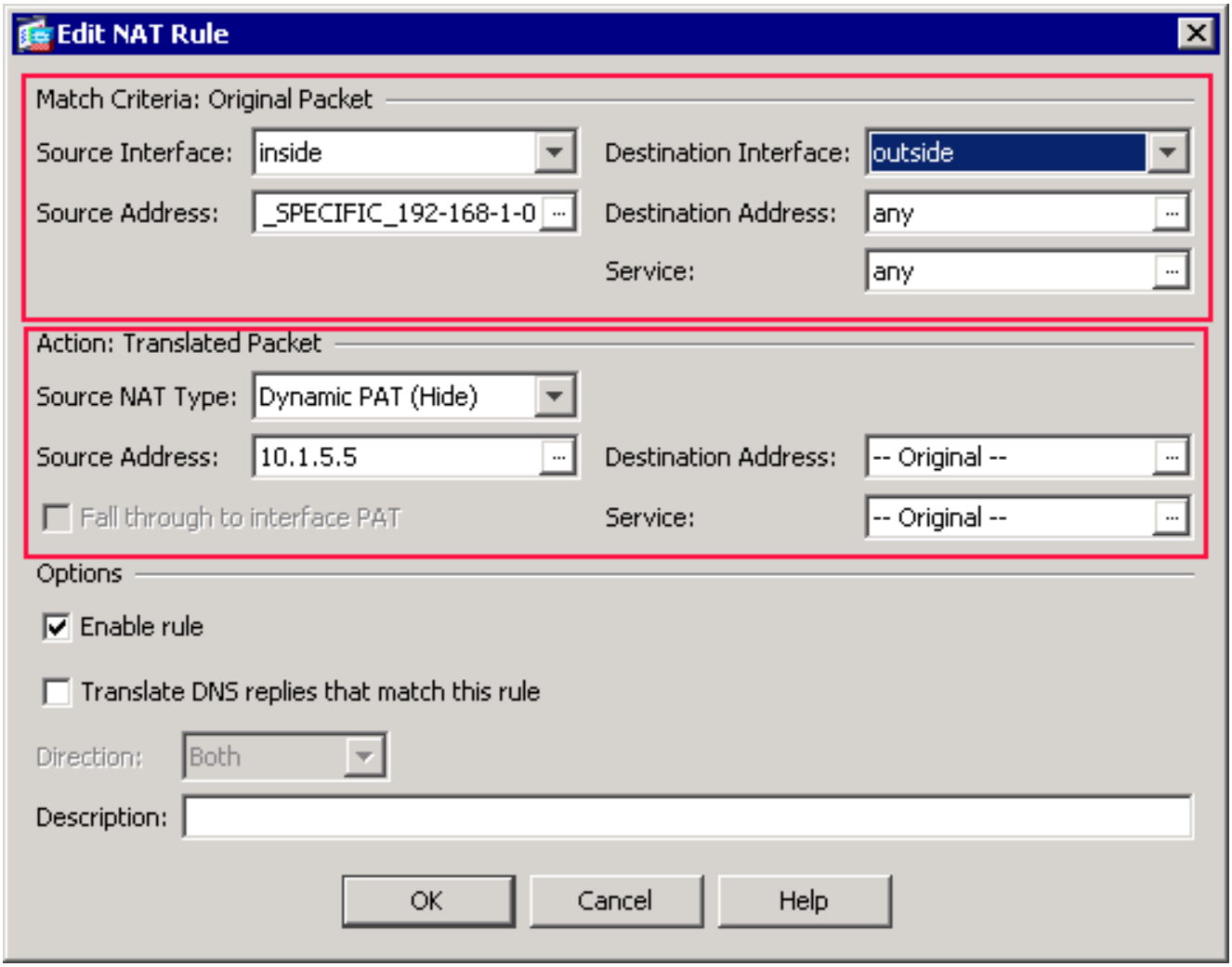
Address 필드 오른쪽에 있는 **...** 버튼을 클릭합니다.Browse Translated Source Address 대화 상자가 나타납니다

.



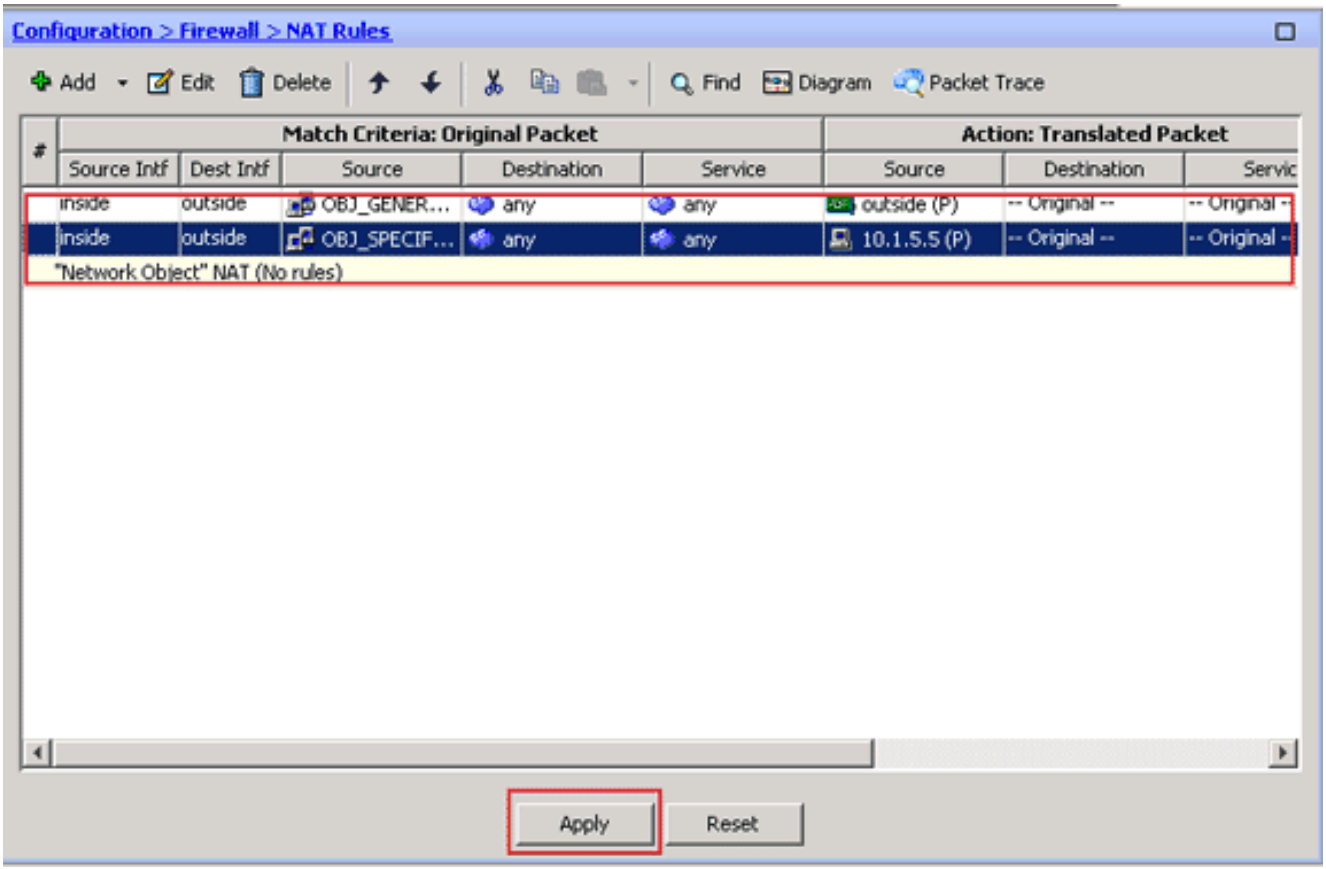
Browse Translated Source Address(변환된 소스 주소 찾아보기) 대화 상자에서 **10.1.5.5** 개체를 선택합니다.이 인터페이스는 원래 컨피그레이션의 일부이므로 이미 생성되었습니다 .Translated **Source Address(변환된 소스 주소)**를 클릭한 다음 **OK**(확인)를 클릭합니다 .**10.1.5.5** 네트워크 객체는 Action:(작업)의 Source Address(소스 주소) 필드에 나타납니다 .Add NAT Rule 대화 상자의 Translated Packet 영역..일치 기준:Original Packet(원래 패킷) 영역의 **Destination** Interface(대상 인터페이스) 드롭다운 목록에서 outside(**outside**)를 선택합니다.**참고:** 이 옵션에 대해 *외부*를 선택하지 않으면 대상 인터페이스가 Any를 *참조합니다*

.



두 번째 완료된 NAT/PAT 규칙이 다음과 같이 나타나는지 확인합니다.일치 기준:Original Packet(원래 패킷) 영역에서 다음 값을 확인합니다.소스 인터페이스 = 내부소스 주소 = OBJ_SPECIFIC_192-168-1-0대상 주소 = 외부서비스 = any작업:Translated Packet(변환된 패킷) 영역에서 다음 값을 확인합니다.소스 NAT 유형 = 동적 PAT(숨기기)소스 주소 = 10.1.5.5대상 주소 = 원본서비스 = 원본**확인**을 **클릭합니다**.완료된 NAT 컨피그레이션은 다음 이미지와 같이 ASDM에 나타납니다

.



3. 실행 중인 컨피그레이션에 변경 사항을 적용하려면 **Apply** 버튼을 클릭합니다.

이렇게 하면 Cisco ASA(Adaptive Security Appliance)에서 동적 PAT 컨피그레이션이 완료됩니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

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

일반 PAT 규칙 확인

- **show local-host**—로컬 호스트의 네트워크 상태를 표시합니다.

```
ASA#show local-host

   Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds !--- to the actual destination of
125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051,
          idle 0:00:03, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
```

```
 !--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA -
10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
```

- show conn - 지정된 연결 유형의 연결 상태를 표시합니다.

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06,
          bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01,
          bytes 13526, flags UIO
```

- show xlate - 변환 슬롯에 대한 정보를 표시합니다.

```
ASA#show xlate
4 in use, 7 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
          ri idle 0:00:23 timeout 0:00:30
```

특정 PAT 규칙 확인

- show local-host—로컬 호스트의 네트워크 상태를 표시합니다.

```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
 !--- The TCP connection outside address corresponds to !--- the actual destination of
125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067,
          idle 0:00:07, bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066,
          idle 0:00:03, bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
    TCP flow count/limit = 2/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited


 !--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.
Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:17 timeout 0:00:30
    TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
          ri idle 0:00:17 timeout 0:00:30

  Conn:
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13758, flags UIO
    TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
```

```
          bytes 11896, flags UIO
```

- show conn - 지정된 연결 유형의 연결 상태를 표시합니다.

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
          bytes 13653, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
          bytes 13349, flags UIO
```

- show xlate - 변환 슬롯에 대한 정보를 표시합니다.

```
ASA#show xlate
3 in use, 9 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
          T - twice
TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
          ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags
          ri idle 0:00:23 timeout 0:00:30
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems