# ASA 8.3 (x)与两个内部网络以及互联网动态PAT的配置示例

## Contents



# Introduction

本文为动态PAT提供一配置示例在Cisco可适应的安全工具(ASA)该运行软件版本8.3(1)。动态PAT通过转换源地址和源端口转换对单个被映射的IP地址的多个实际地址被映射的地址和唯一被映射的端口的。每个连接都需要独立的转换会话，因为每个连接都有不同的源端口。

# Prerequisites

## Requirements

尝试进行此配置之前，请确保满足以下要求：

- 确定内部网络有位于ASA的里面的两网络：192.168.0.0/24 —网络直接地被连接到ASA。192.168.1.0/24 —在ASA的里面的网络，但是在另一个设备背后(例如，路由器)。
- 保证内部用户获得PAT如下：在192.168.1.0/24子网的主机将有PAT ISP产生的一个备用的IP地址(10.1.5.5)。在ASA后的里面的其他主机将有PAT ASA (10.1.5.1)的外部接口IP地址。

## Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备 (ASA) 版本 8.3(1)
- ASDM版本6.3(1)

**Note:** 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

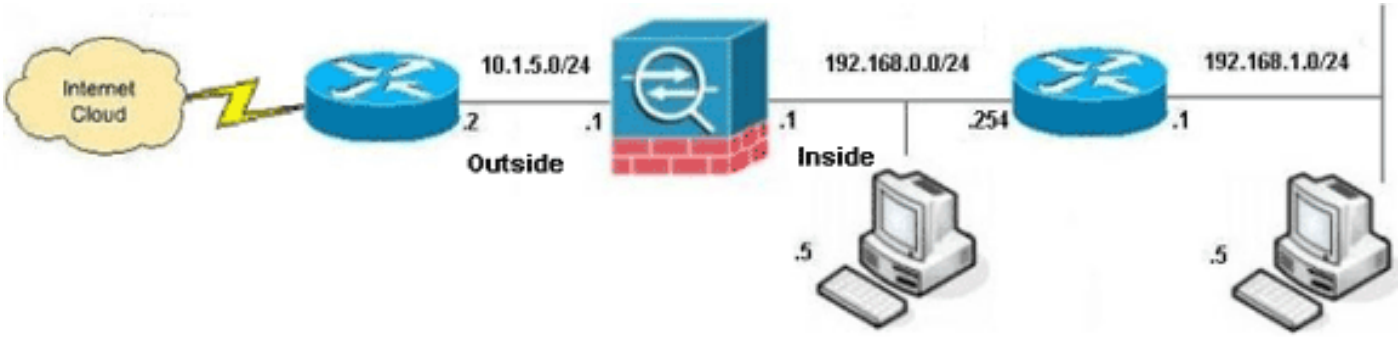
## Conventions

关于文件规则的信息，请参见Cisco技术提示规则。

# 配置

## Network Diagram

本文档使用以下网络设置：




**Note:** 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

- ASA CLI 配置
- ASDM 配置

## ASA CLI 配置

本文档使用如下所示的配置。

**ASA动态PAT配置**

```
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) 运行配置

```
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 配置

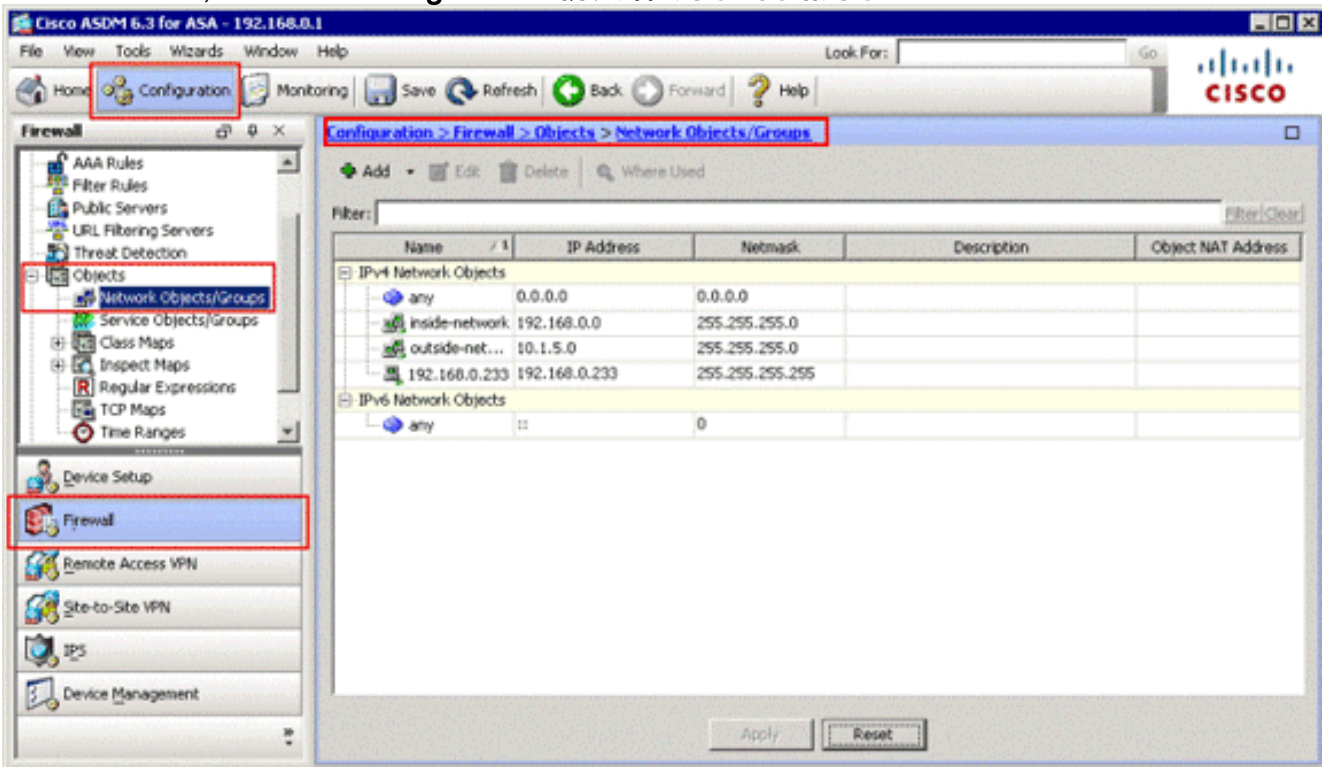
为了通过ASDM接口完成此配置，您必须：

1. 添加三个网络对象;此示例添加这些网络对象：OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. 创建两个NAT/PAT规则;此示例创建这些网络对象的NAT规则：OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

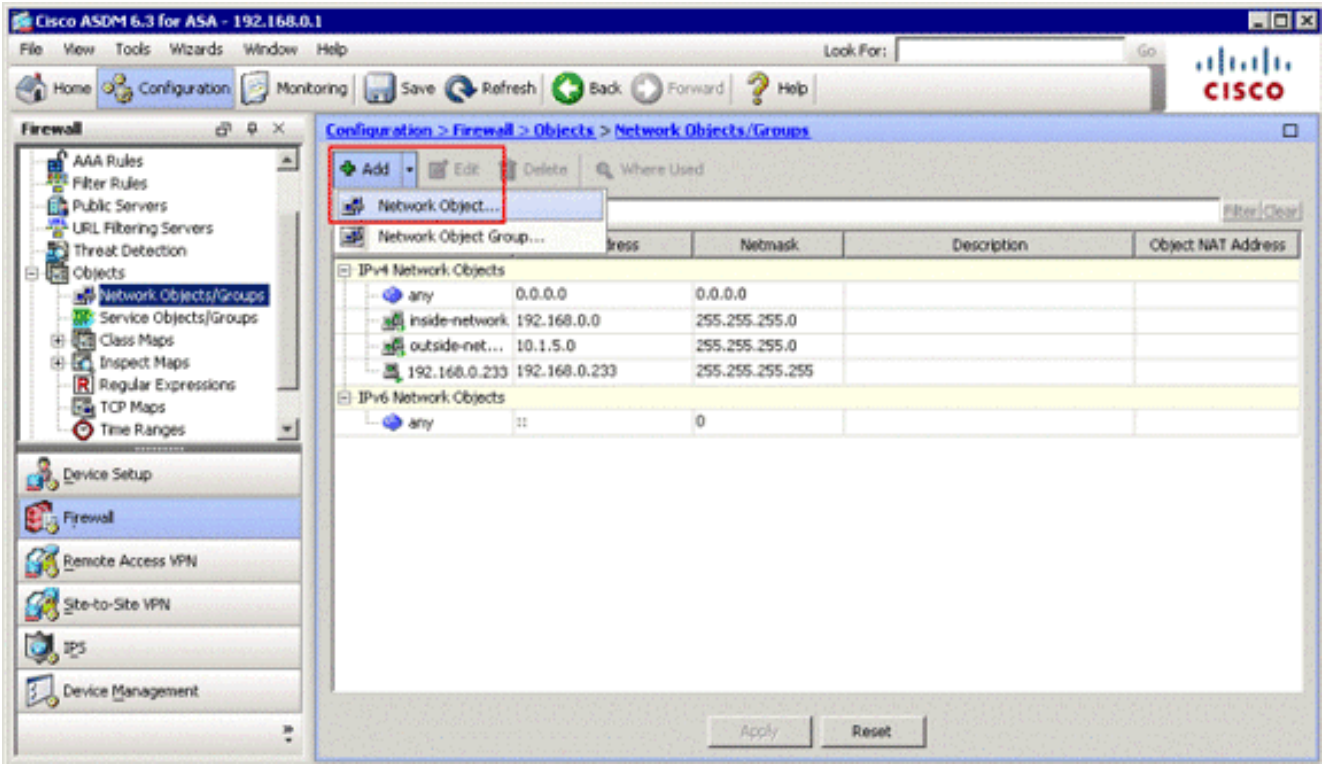
**添加网络对象**

完成这些步骤为了添加网络对象：

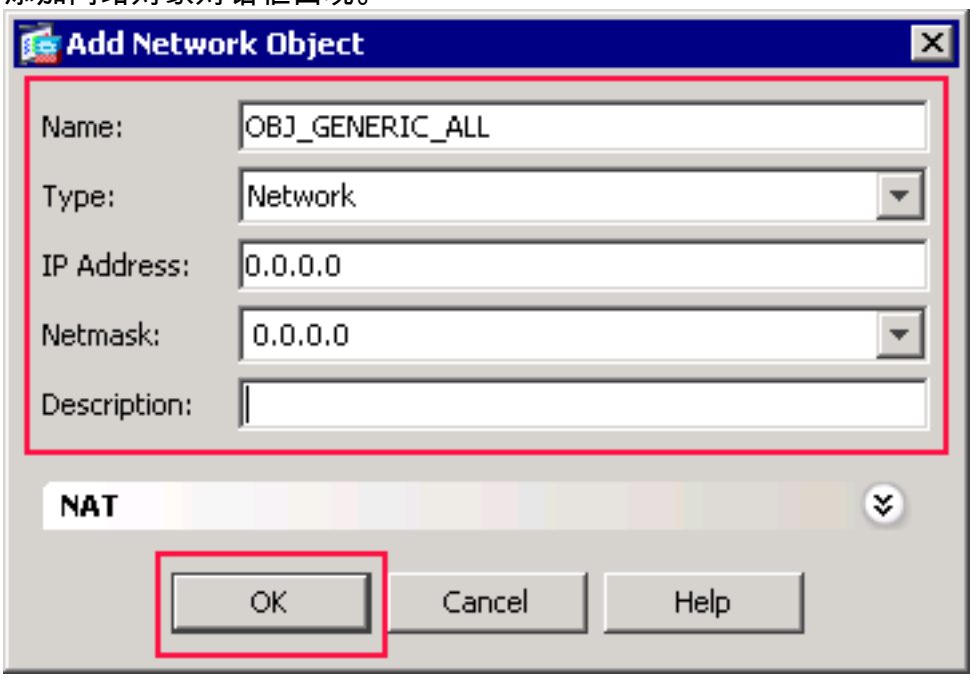
1. 登陆对ASDM，并且选择**Configuration>防火墙>对象>网络对象/组**。



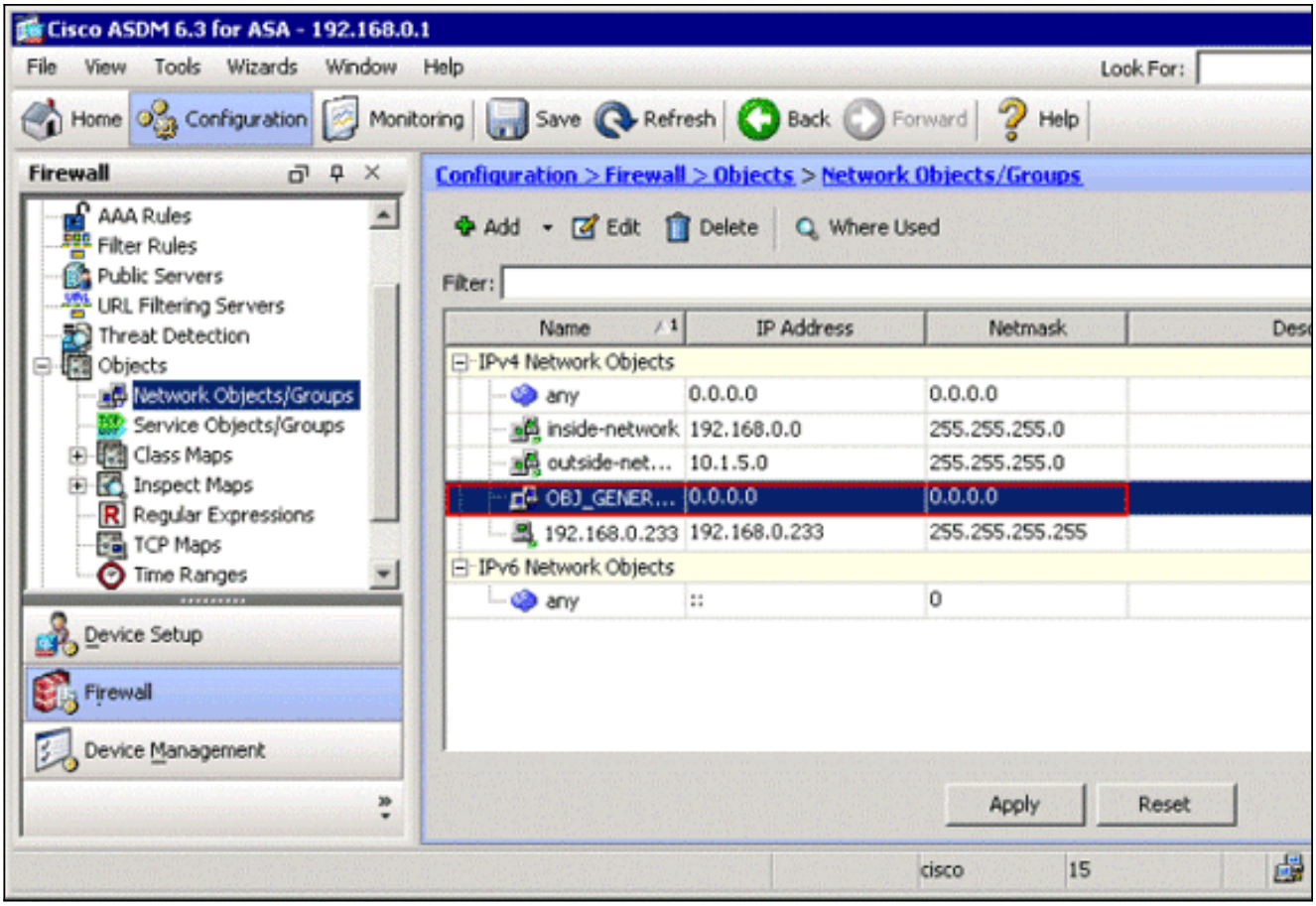

2. 选择**Add>网络对象**为了添加网络对象。



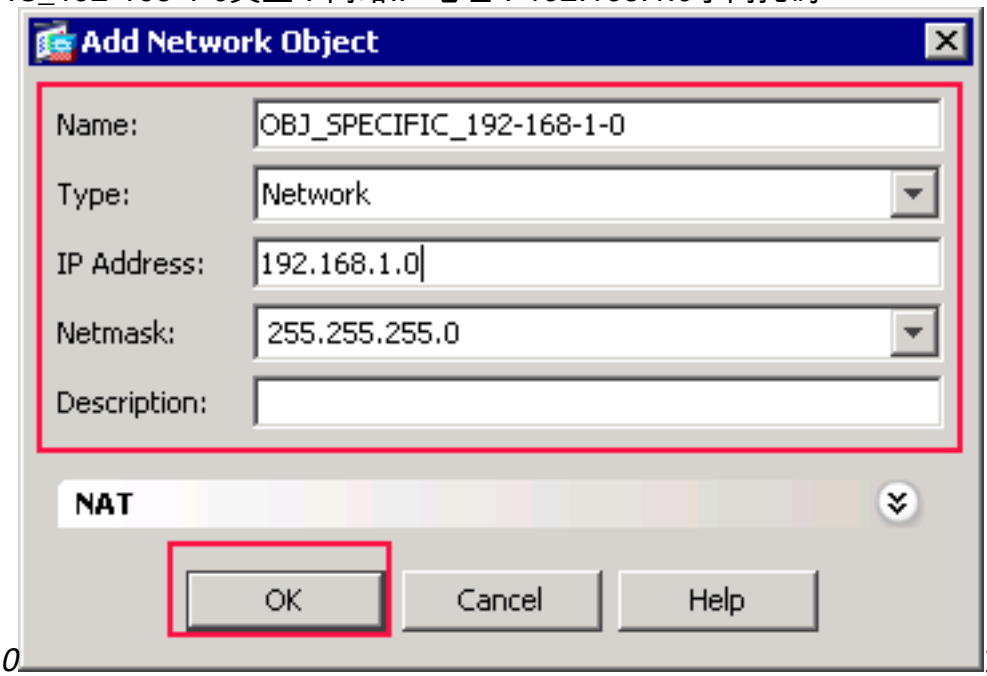

添加网络对象对话框出现。



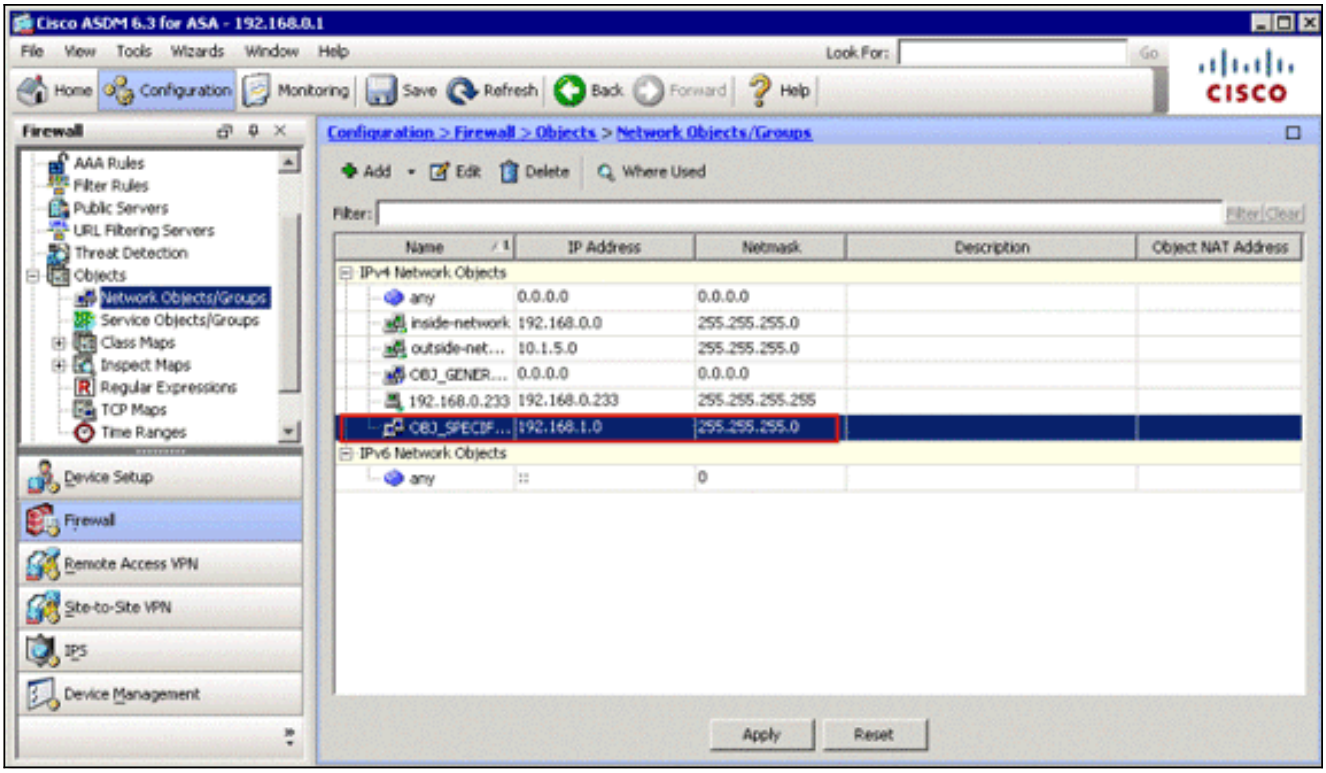

3. 输入此信息在添加网络对象对话框：网络对象的名字。(此示例使用*OBJ_GENERIC_ALL*。)网络类型对象。(此示例使用*网络*。)网络对象的IP地址。(此示例使用*0.0.0.0*。)网络对象的子网掩码。(此示例使用*0.0.0.0*。)
4. 单击 **Ok**。如此镜像所显示，网络对象被创建并且出现于网络对象/Groups列表，
：



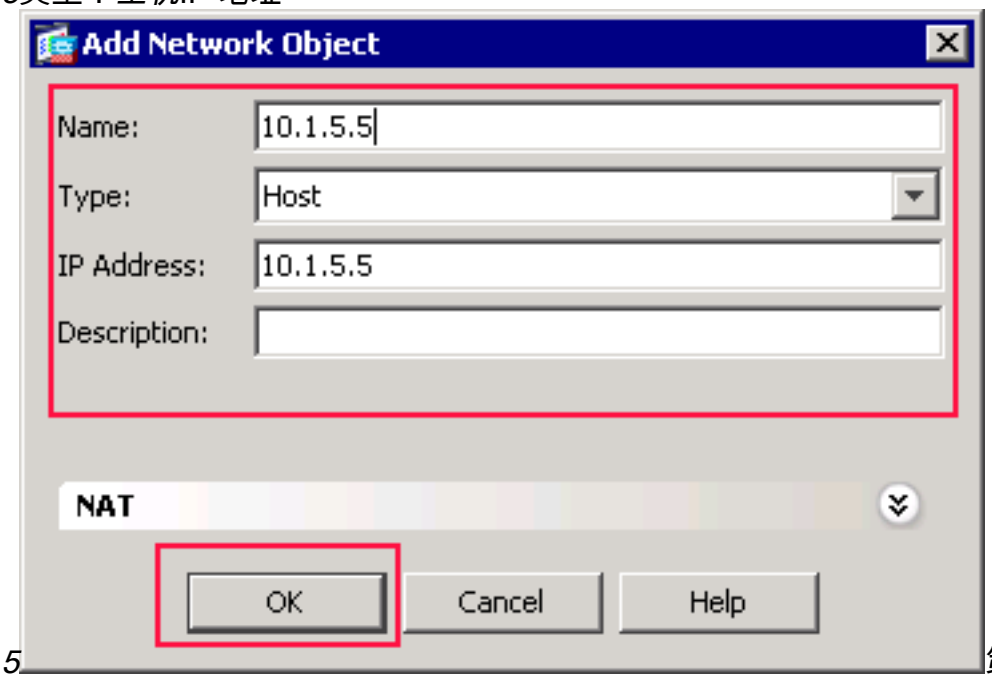

5. 重复早先步骤为了添加第二个网络对象，并且点击OK键。本示例使用这些值：名字：*OBJ_SPECIFIC_192-168-1-0*类型：网络IP 地址：*192.168.1.0*子网掩码：*255.255.255.0*



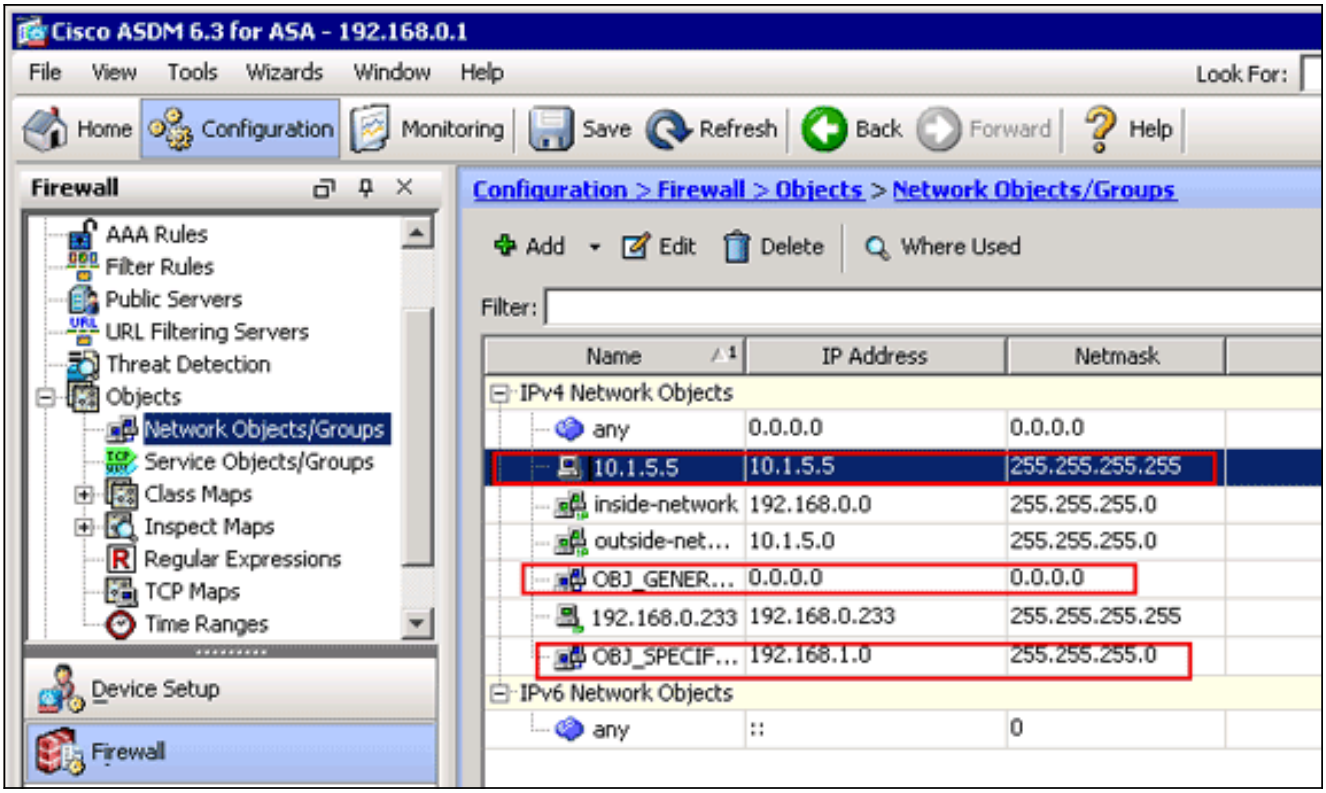

如此镜像所显示，第二个对象被创建并且出现于网络对象/Groups列表，：




6. 重复早先步骤为了添加第三个网络对象，并且点击OK键。本示例使用这些值：名字：*10.1.5.5*类型：*主机*IP 地址：*10.1.5.5*




第三个网络对象被创建并且出现于网络对象/Groups列表。

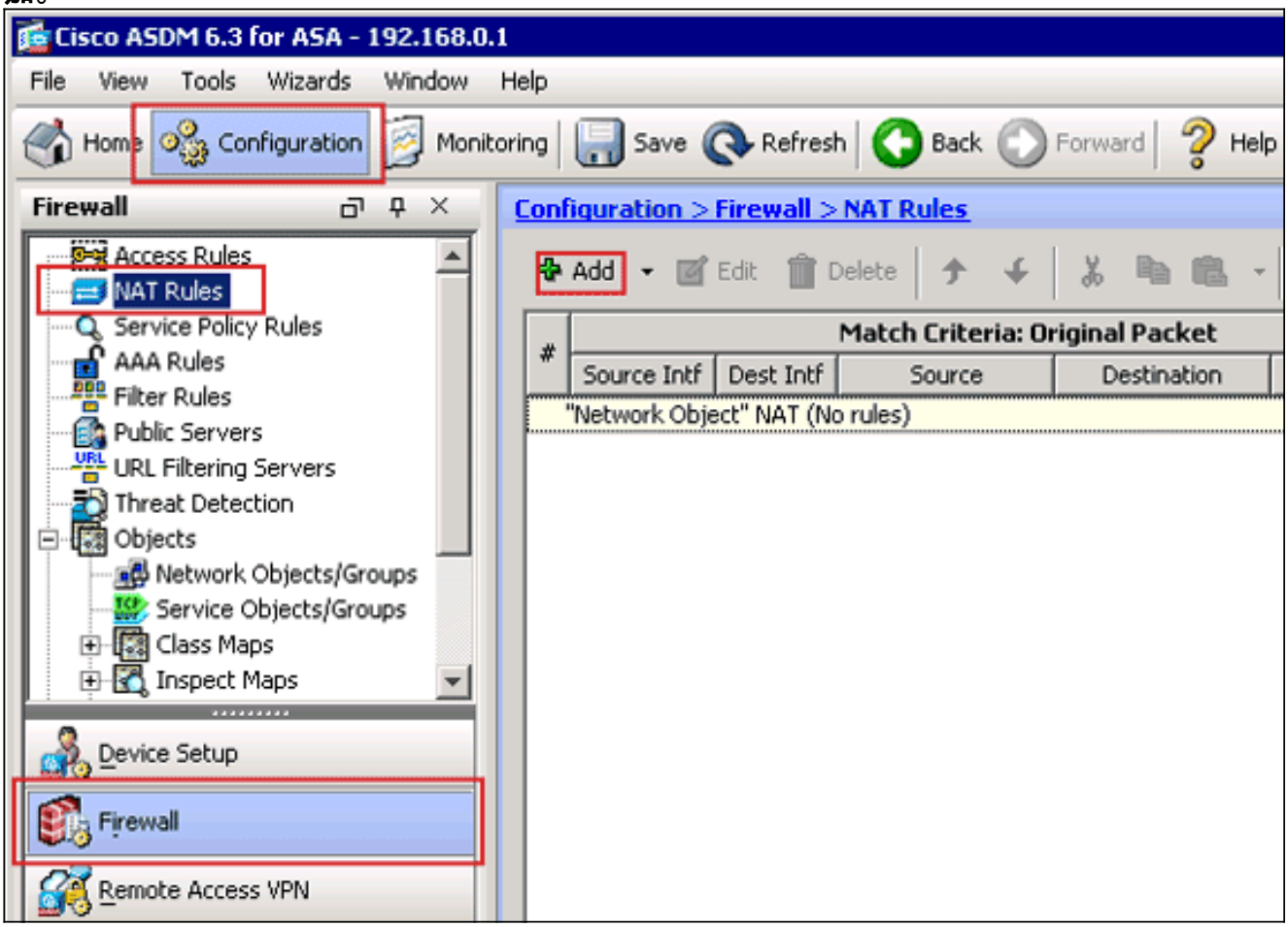



网络对象/Groups列表应该当前包括三个需要的对象必要为了NAT规则能参考。

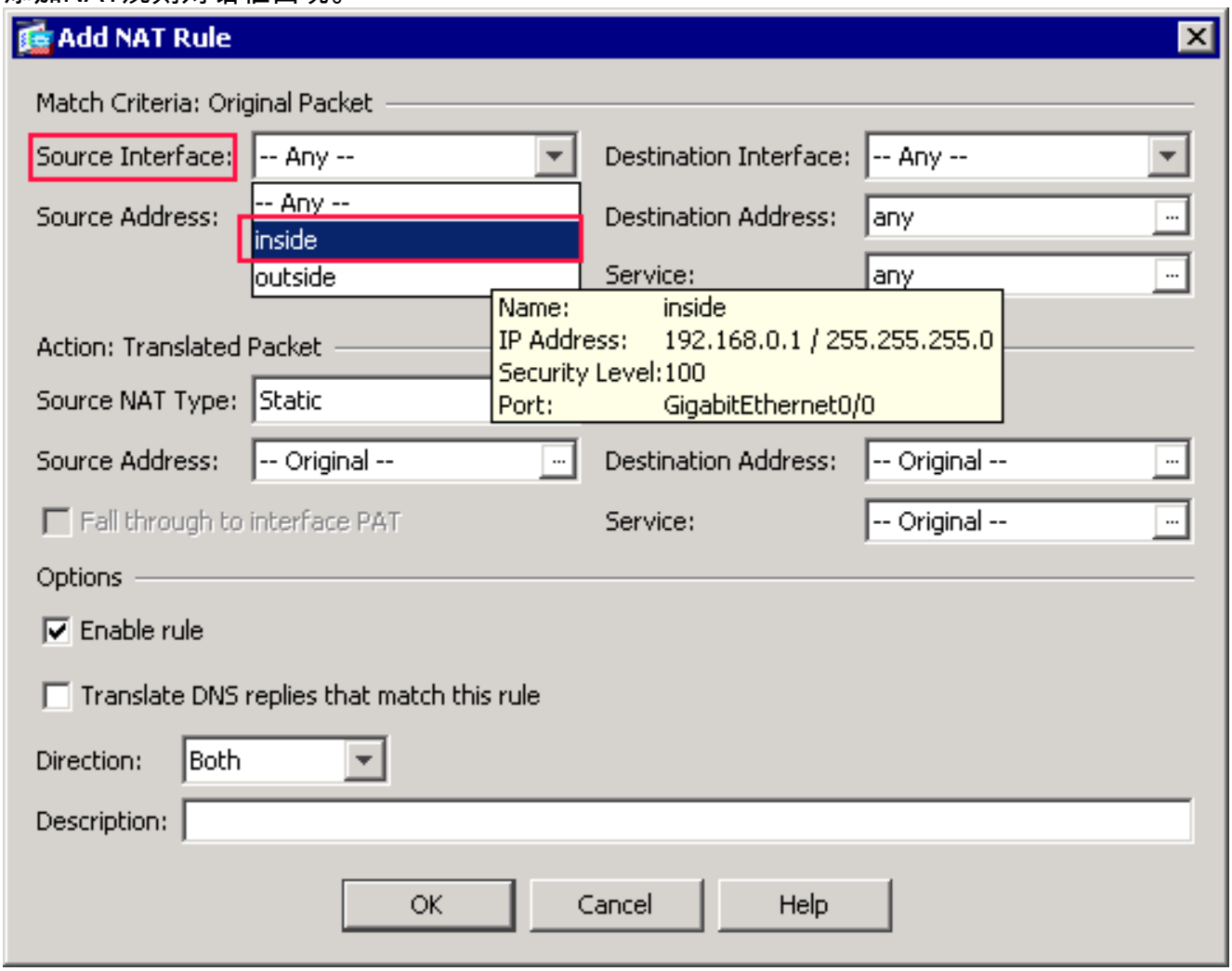
**创建NAT/PAT规则**

完成这些步骤为了创建NAT/PAT规则：

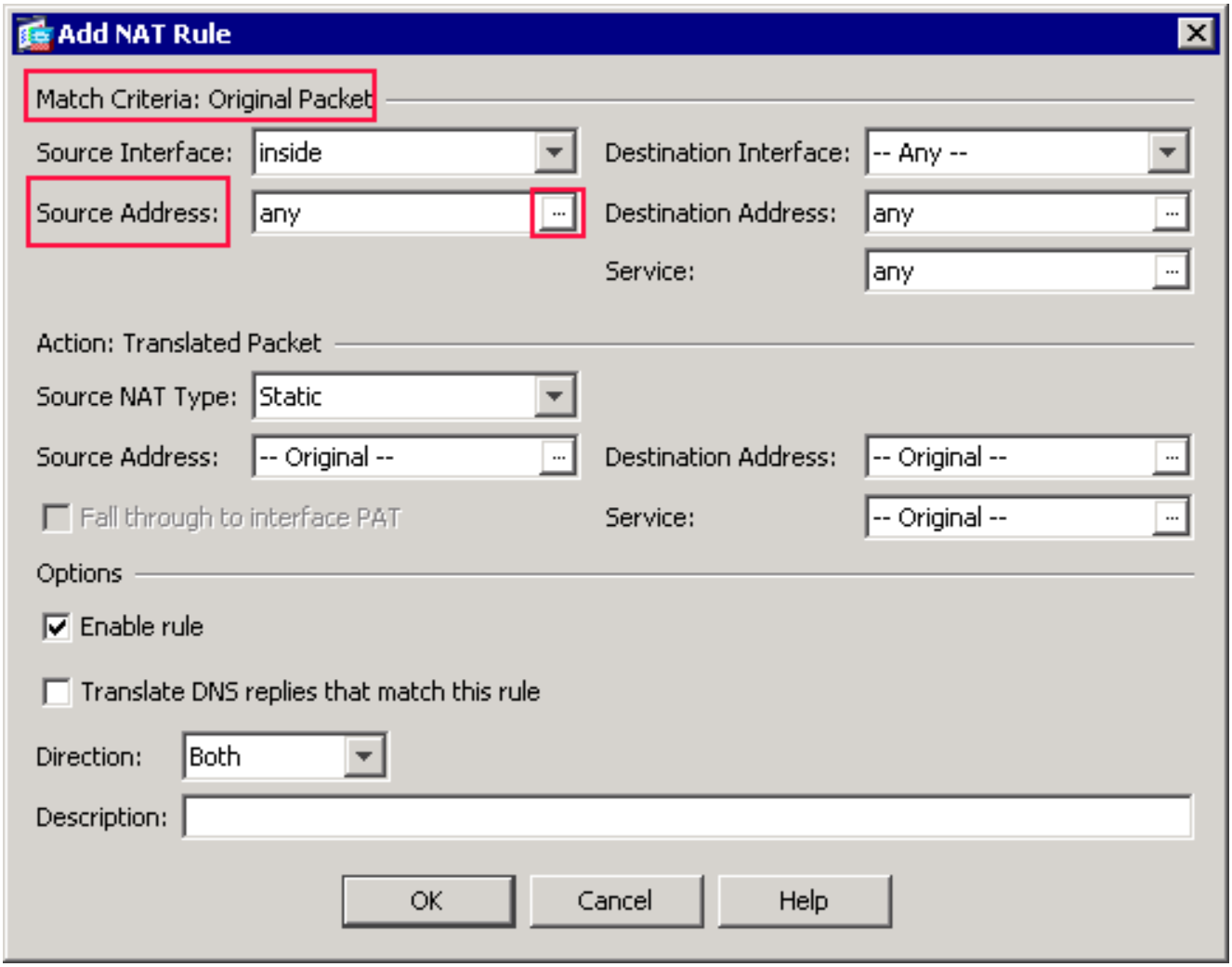
1. 创建第一个NAT/PAT规则：在ASDM，请选择**Configuration>防火墙> NAT规则**，并且点击**添加**。



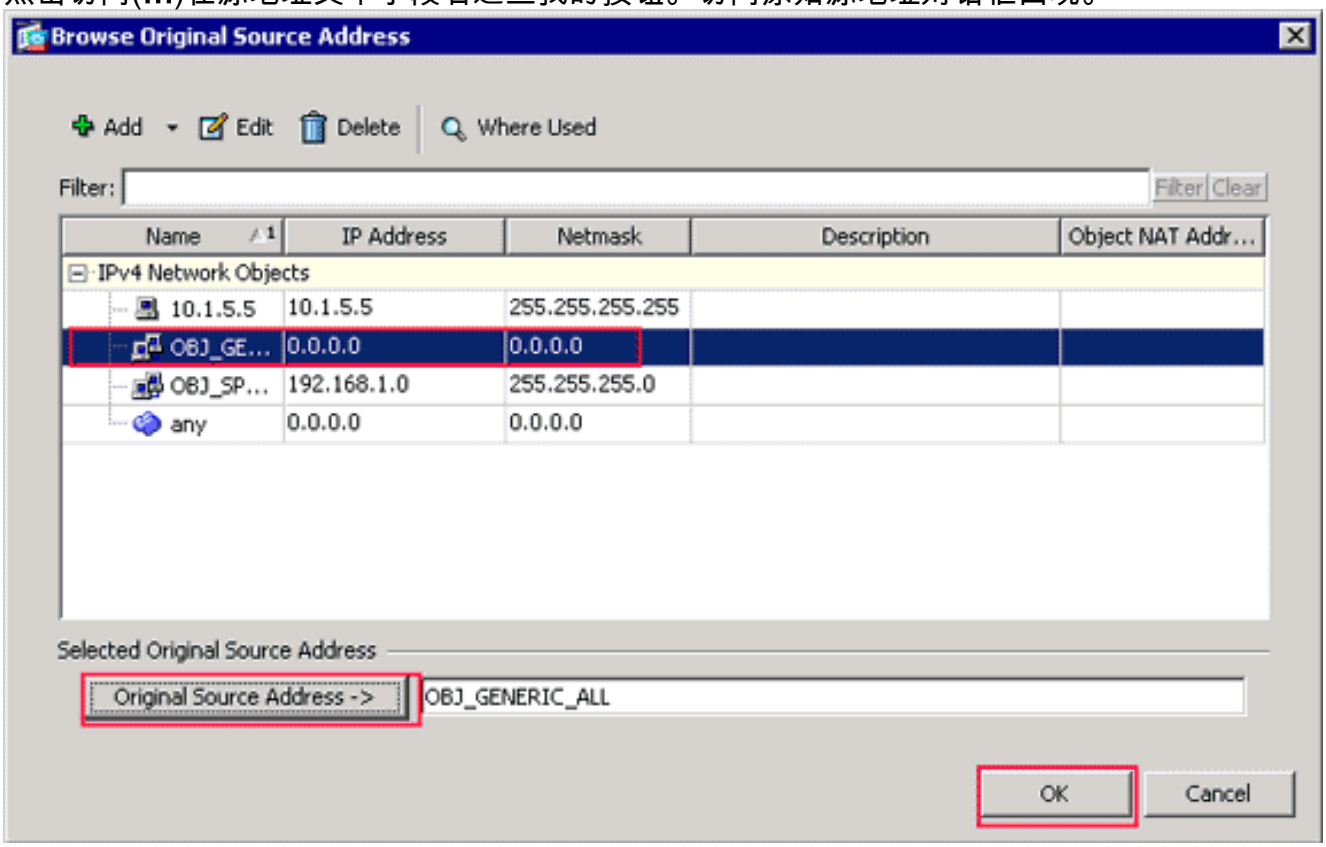
添加NAT规则对话框出现。



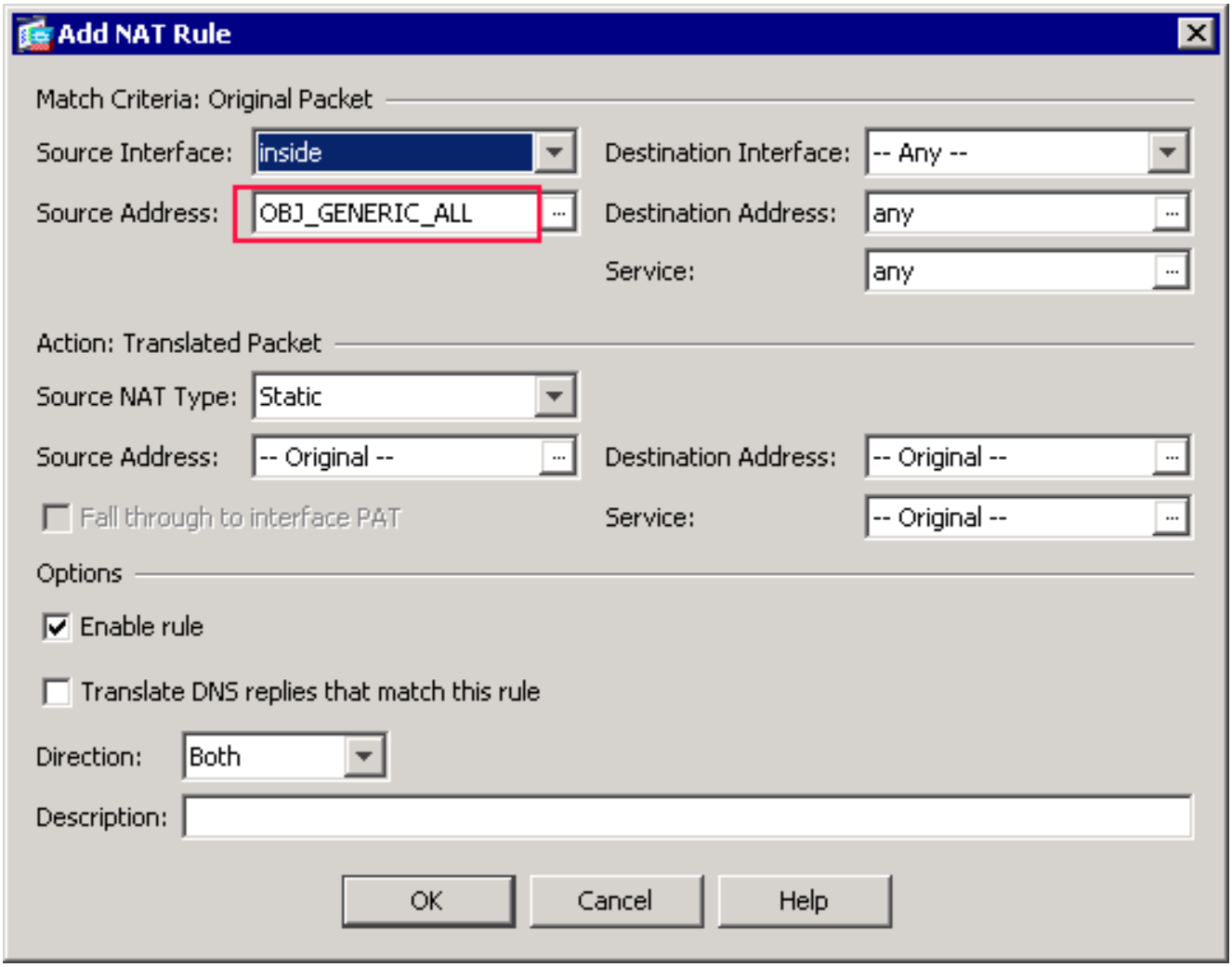

在匹配标准：添加NAT规则对话框的原始信息包地区，从源接口下拉列表选择**里面**。



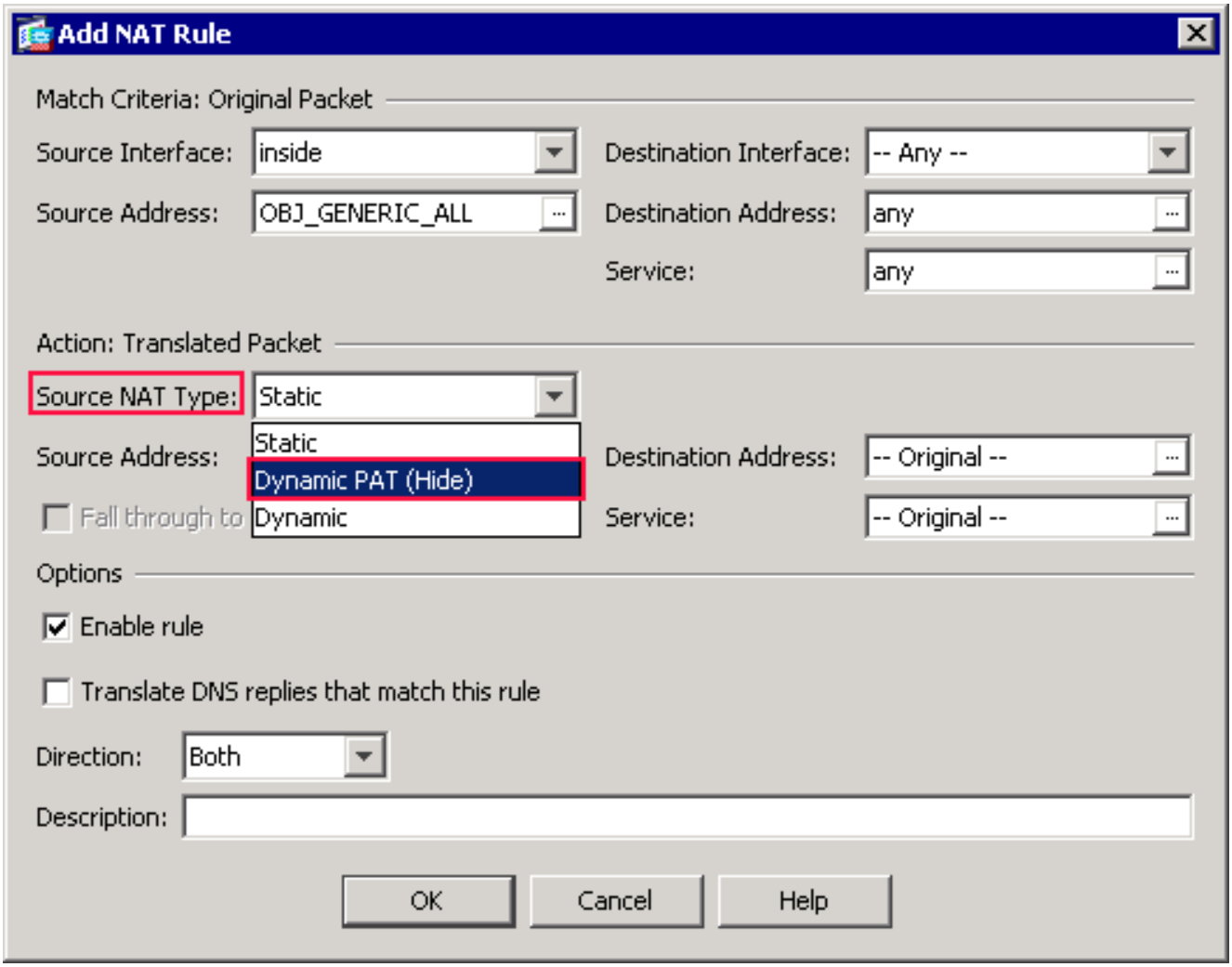

点击访问(...)在源地址文本字段右边查找的按钮。访问原始源地址对话框出现。



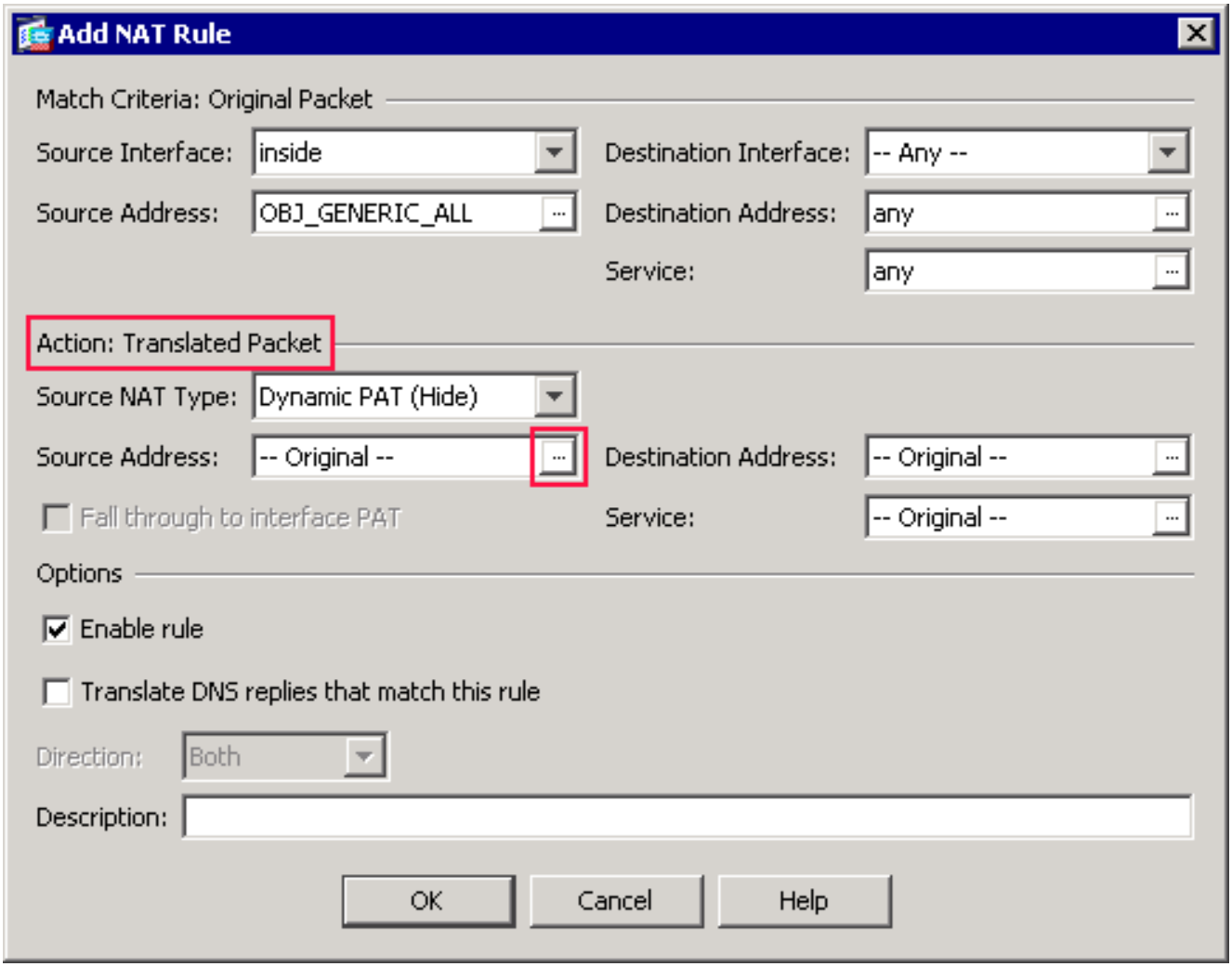

在访问原始源地址对话框中，请选择您创建的第一个网络对象。(对于此示例，请选择**OBJ_GENERIC_ALL**。)点击**原始源地址**，并且点击OK键。*OBJ_GENERIC_ALL*网络对象当前出现于在匹配标准的源地址地址字段：添加NAT规则对话框的原始信息包地区。



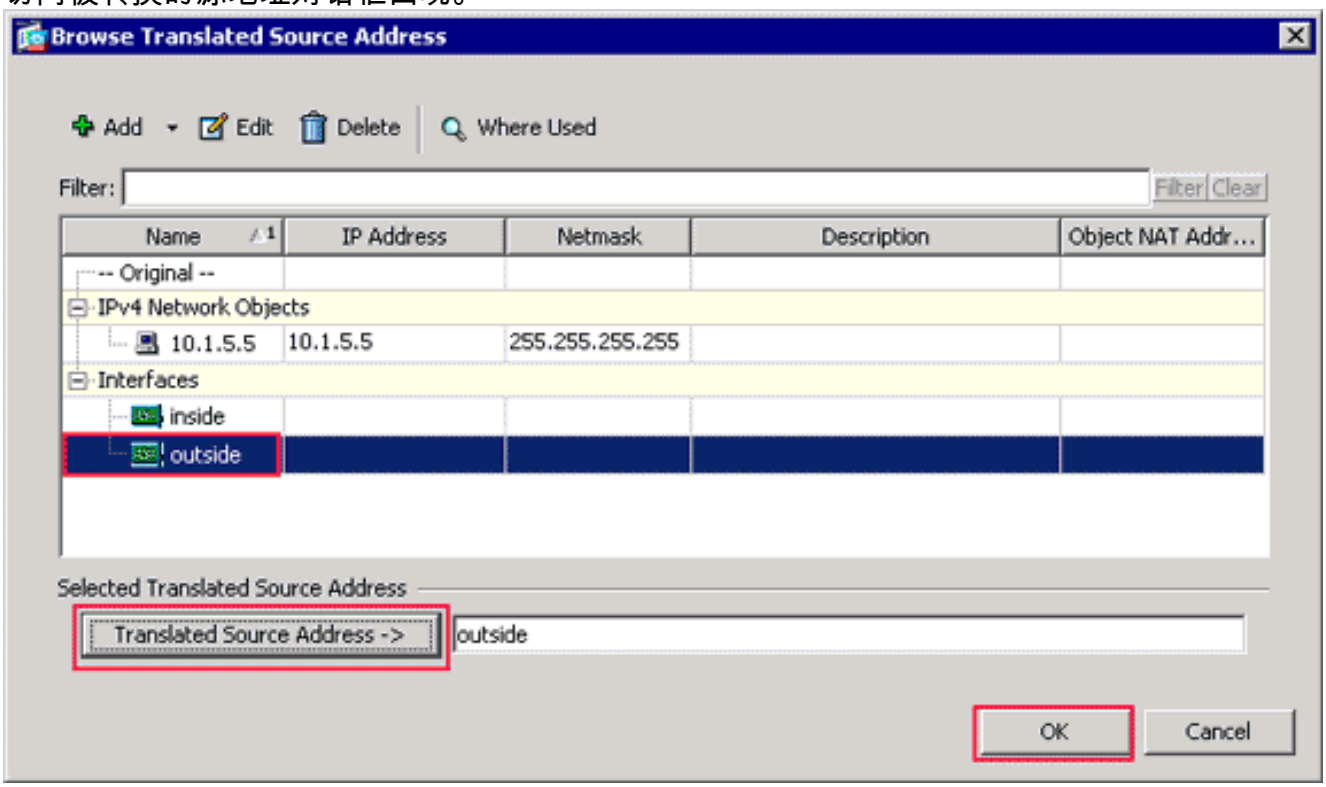

在动作：添加NAT规则对话框的被转换的信息包地区，从来源NAT类型对话框选择**动态PAT (隐藏)**。



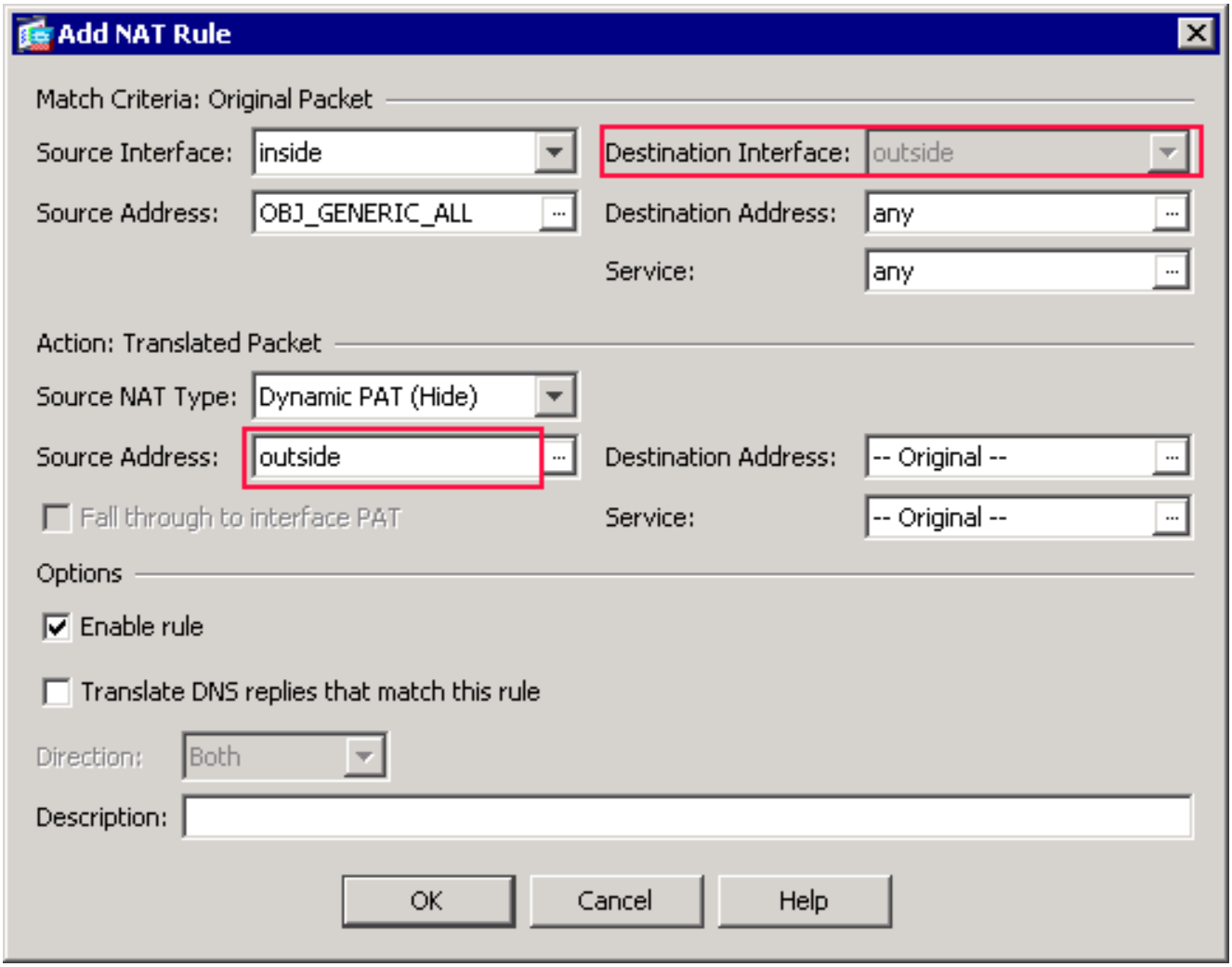

点击访问(...)在源地址地址字段右边查找的按钮。




访问被转换的源地址对话框出现。

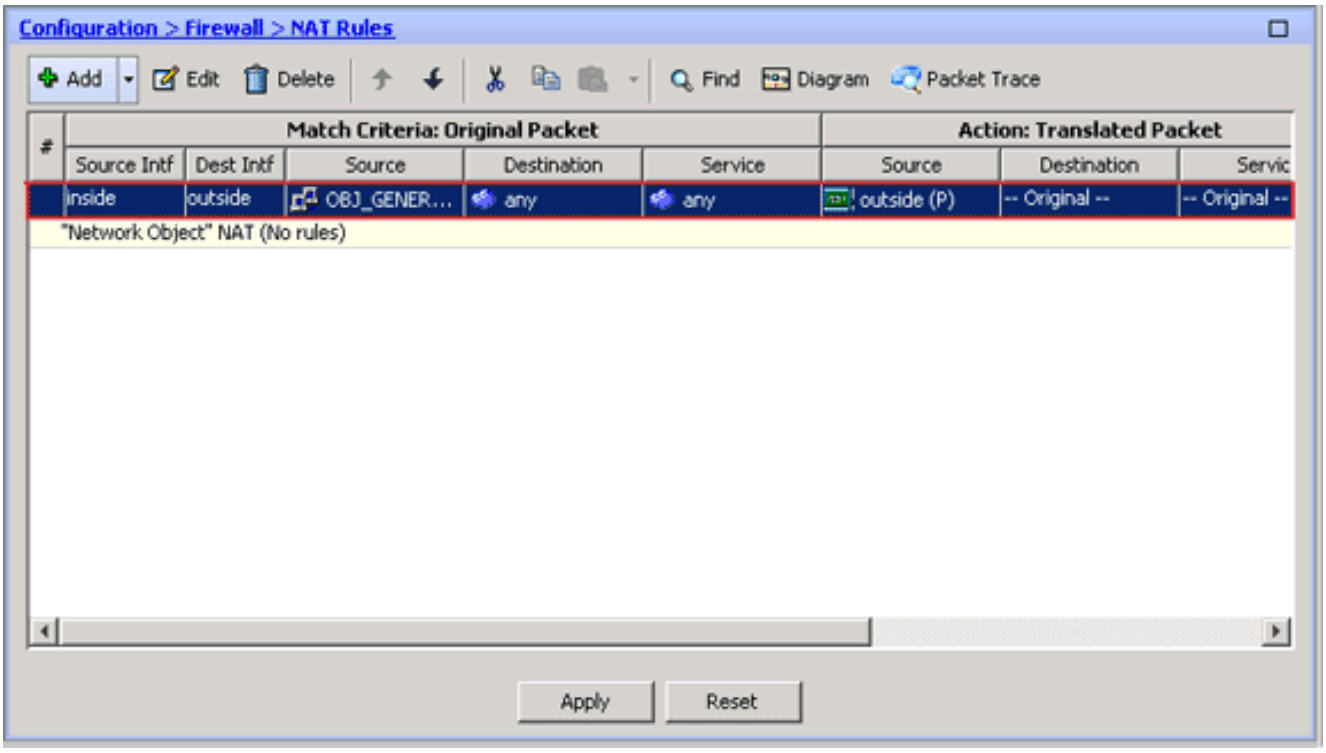



在访问被转换的源地址对话框，选择外部接口对象。(此接口已经被创建了，因为它是原始配置的一部分。)点击**被转换的源地址**，并且点击OK键。外部接口当前出现于在动作的源地址地址字段：在添加NAT规则对话框的被转换的信息包地区。

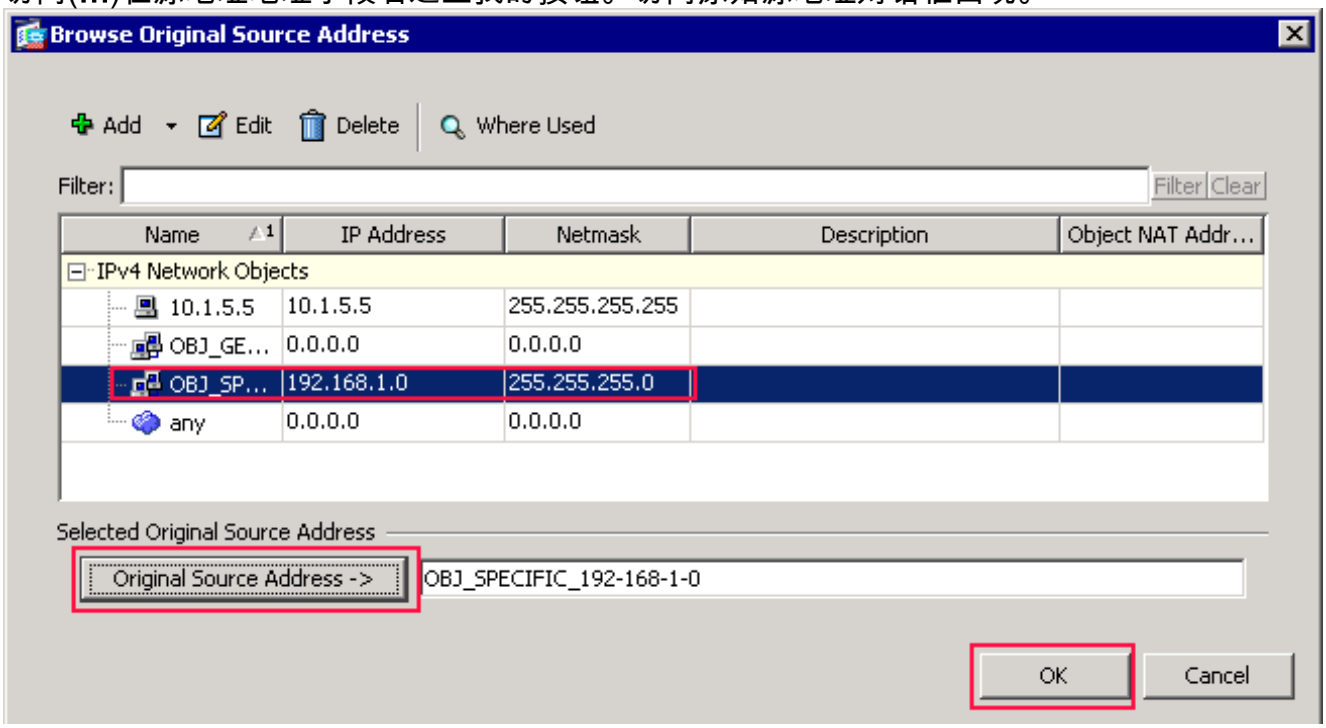



**Note:** *目的地接口*字段也变成外部接口。验证第一个完整PAT规则发表如下：在匹配标准：原始信息包地区，验证这些值：源接口=里面源地址= OBJ_GENERIC_ALL目的地地址=其中任一服务=其中任一在动作：被转换的信息包地区，验证这些值：来源NAT Type=动态PAT (隐藏)源地址=从外部目的地地址=原始服务=原始单击 **Ok**。如此镜像所显示，第一个NAT规则发表于ASDM，

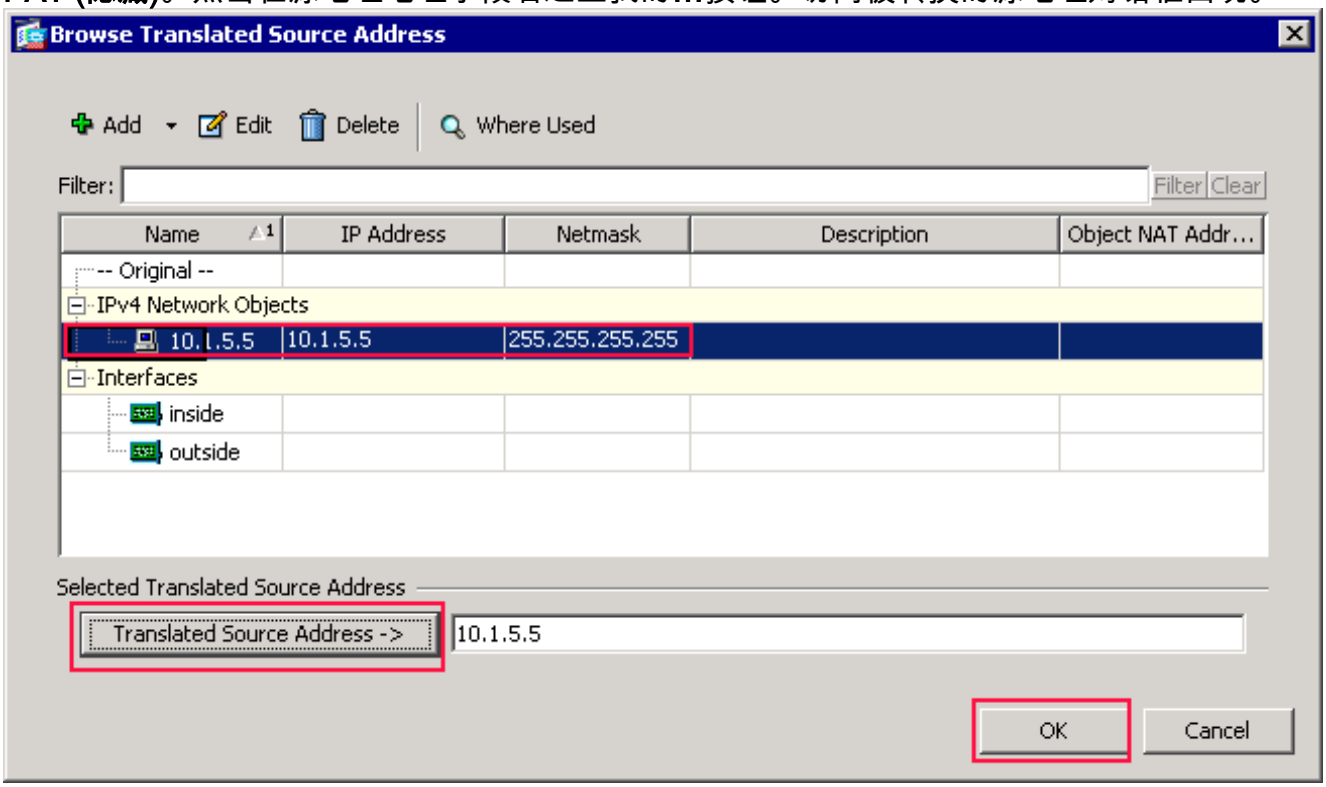
：



2. 创建第二个NAT/PAT规则：在ASDM，请选择**Configuration>防火墙> NAT规则**，并且点击**添加**。在匹配标准：添加NAT规则对话框的原始信息包地区，从源接口下拉列表选择**里面**。点击访问(...)在源地址地址字段右边查找的按钮。访问原始源地址对话框出现。

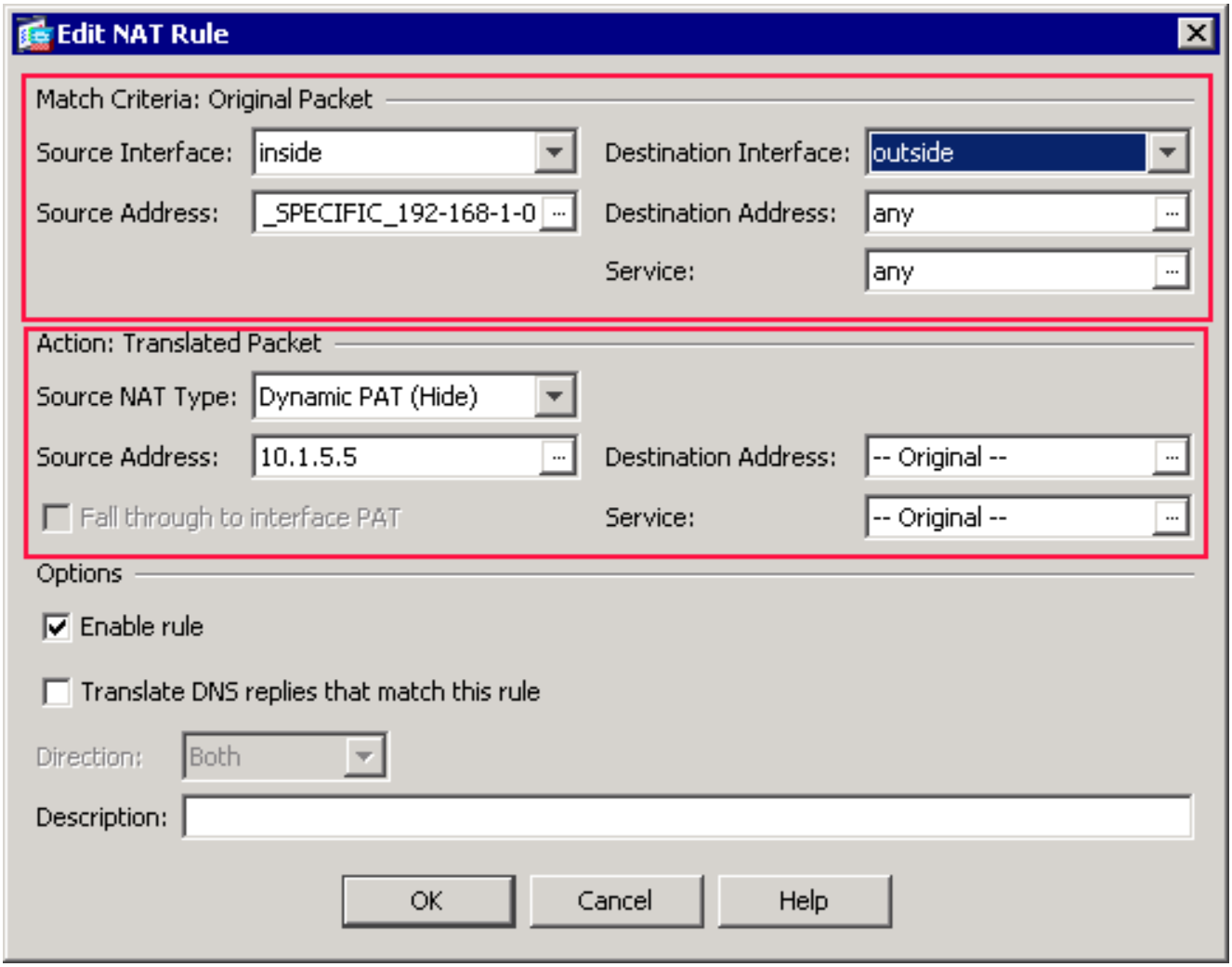



在访问原始源地址对话框中，请选择您创建的第二个对象。(对于此示例，请选择**OBJ_SPECIFIC_192-168-1-0**。)点击**原始源地址**，并且点击OK键。*OBJ_SPECIFIC_192-168-1-0*网络对象出现于在匹配标准的源地址地址字段：添加NAT规则对话框的原始信息包地区。在动作：添加NAT规则对话框的被转换的信息包地区，从来源NAT类型对话框选择**动态PAT (隐藏)**。点击在源地址地址字段右边查找的...按钮。访问被转换的源地址对话框出现。



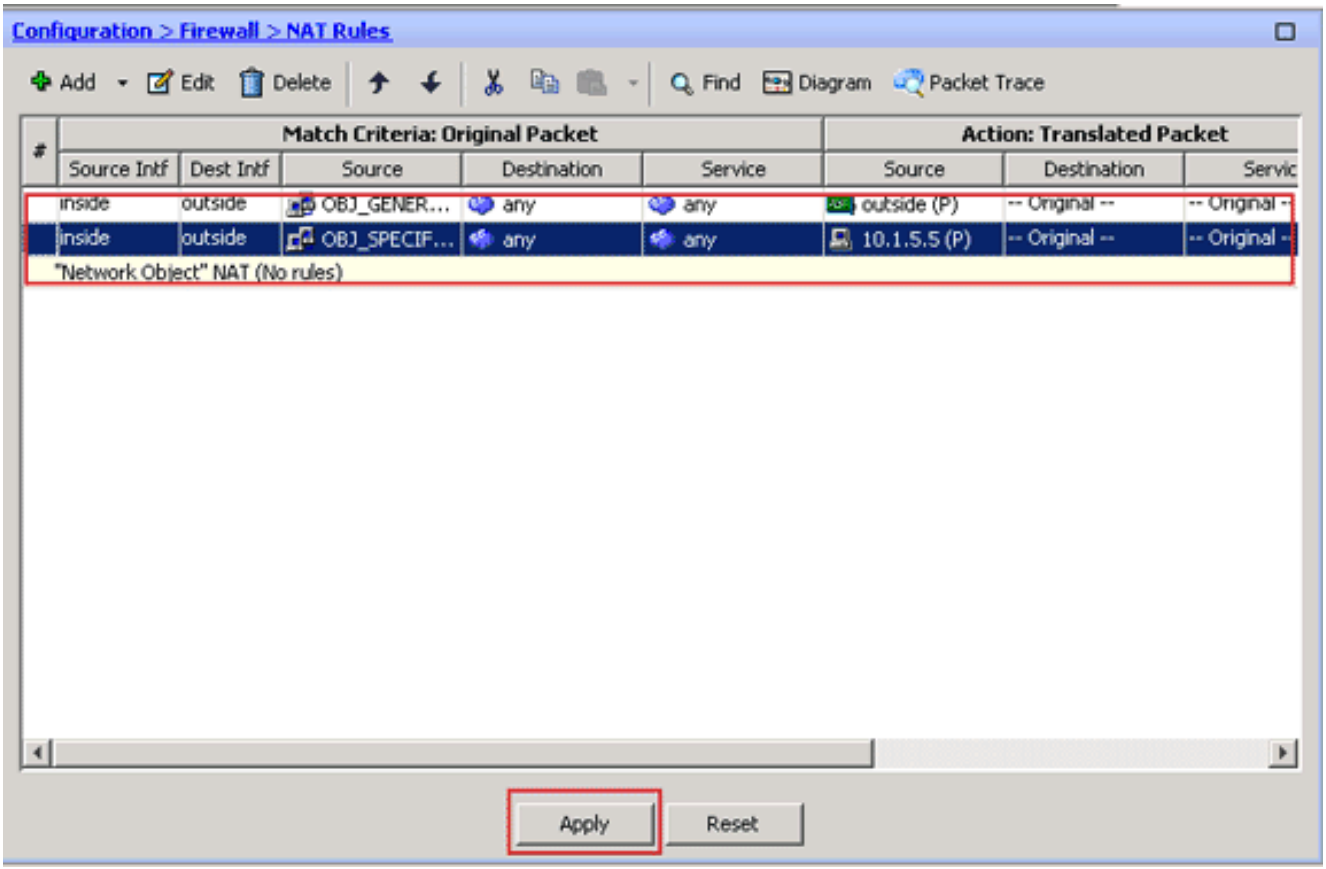

在访问被转换的源地址对话框，选择**10.1.5.5**对象。(此接口已经被创建了，因为它是原始配置的一部分)。点击**被转换的源地址**，然后点击OK键。**10.1.5.5**网络对象出现于在动作的源地址地址字段：添加NAT规则对话框的被转换的信息包地区。在匹配标准：原始信息包地区，**从外部**从目的地接口下拉列表选择。**Note:** 如果不为此选项*从外部*选择，目的地接口将参考其中*任*

一。




验证第二个完整NAT/PAT规则发表如下：在匹配标准：原始信息包地区，验证这些值：源接口=里面源地址= OBJ_SPECIFIC_192-168-1-0目的地地址=从外部服务=其中任一在动作：被转换的信息包地区，验证这些值：来源NAT Type=动态PAT (隐藏)源地址= 10.1.5.5目的地地址=原始服务=原始单击 **Ok**。如此镜像所显示，完整NAT配置出现于ASDM，

：




3. 点击**Apply按钮**为了应用对运行的配置的更改。

这完成动态PAT的配置在Cisco可适应的安全工具(ASA)上的。

# Verify

Use this section to confirm that your configuration works properly.

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

## 验证通用的PAT规则

- show local-host —显示本地主机网络状况。

```
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 —显示选定的连接类型的连接状态。

```
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 —显示关于转换插槽的信息。

```
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
```

## 验证特定PAT规则

- show local-host —显示本地主机网络状况。

```
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 —显示选定的连接类型的连接状态。

```
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 —显示关于转换插槽的信息。

```
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
```

# Troubleshoot

目前没有针对此配置的故障排除信息。

# Related Information

- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备
- 请求注解 (RFC)
- Technical Support & Documentation - Cisco Systems