配置ASA版本9.x与NAT的端口转发

目录

简介

本文解释如何配置端口重定向(转发)和在可适应安全工具(ASA)软件版本9.x的外部网络地址地址转换(NAT)功能，与使用CLI或可适应安全设备管理器(ASDM)。

参考思科ASA系列防火墙ASDM配置指南其他信息。

先决条件

要求

参考配置管理访问为了允许ASDM将配置的设备。

使用的组件

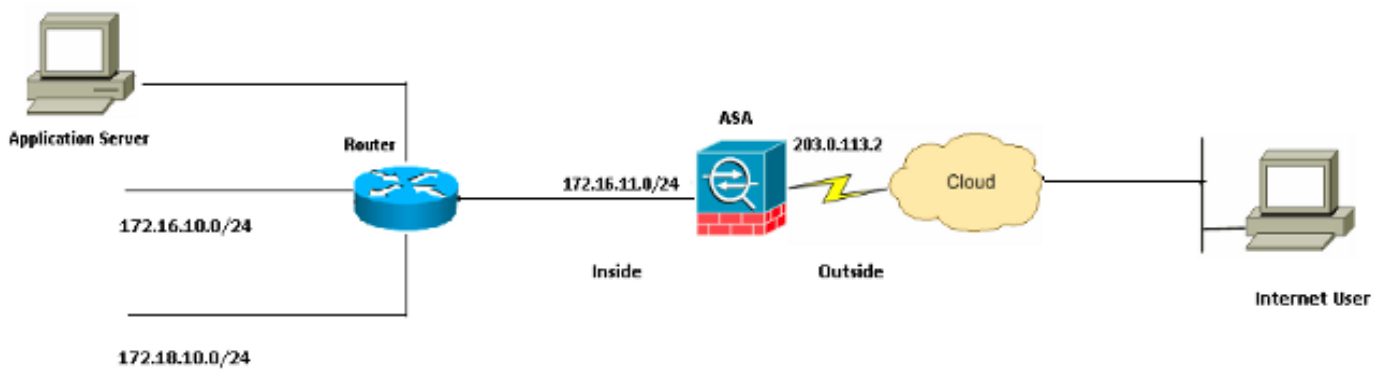
本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 5525系列安全工具软件版本9.x和以上
- ASDM版本7.x和以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



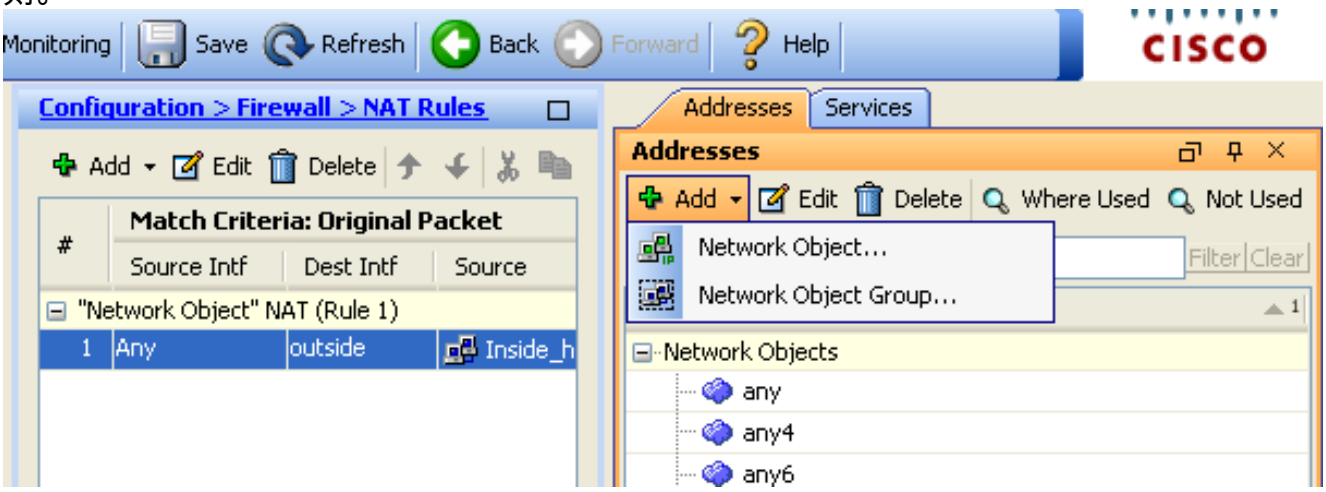
此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

允许内部主机对外部网络的访问与PAT

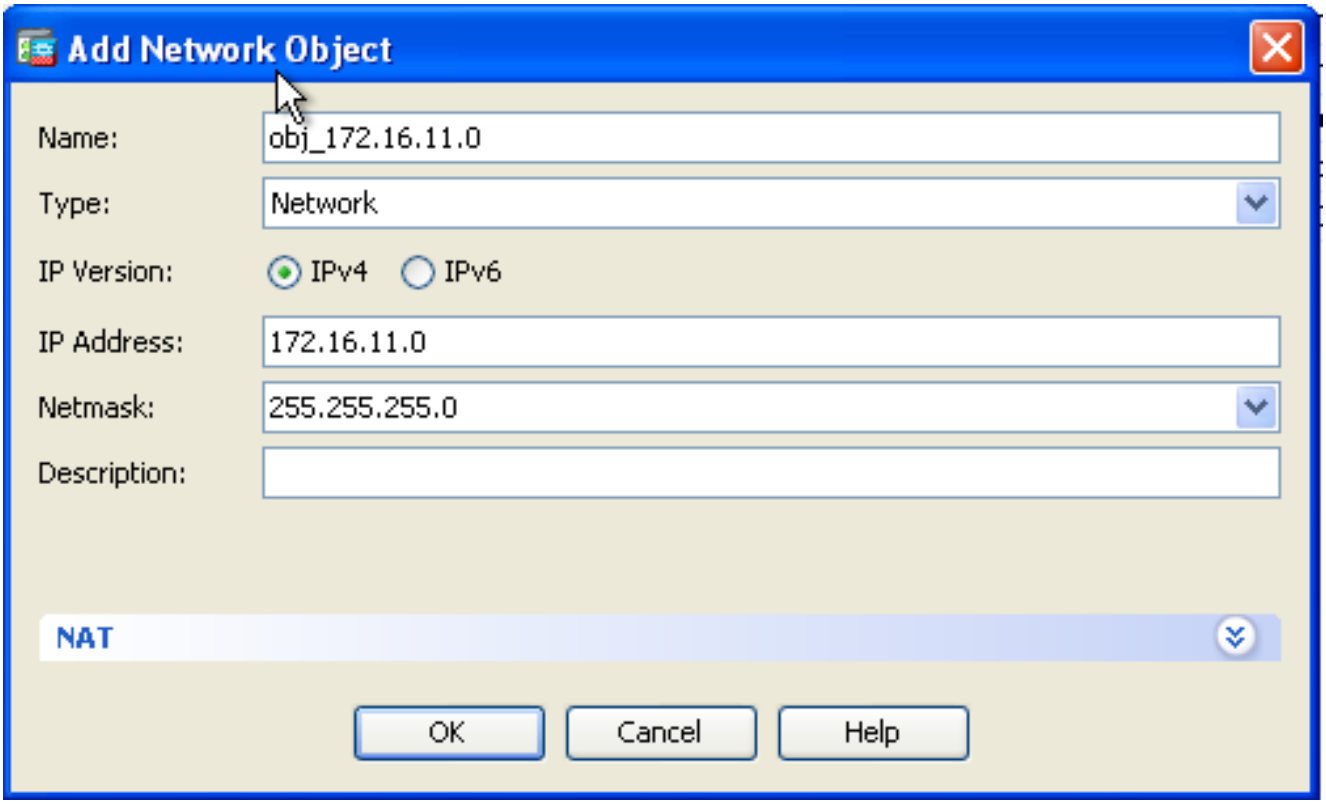
如果希望内部主机共享转换的单个公共地址，请使用端口地址转换(PAT)。其中一最简单的PAT配置介入所有内部主机的转换看起来象外部接口IP地址。这是使用的典型PAT配置，当可路由IP地址数量可得到从ISP对仅一些时被限制，或许或者一个。

完成这些步骤为了允许内部主机对外部网络的访问与PAT ：

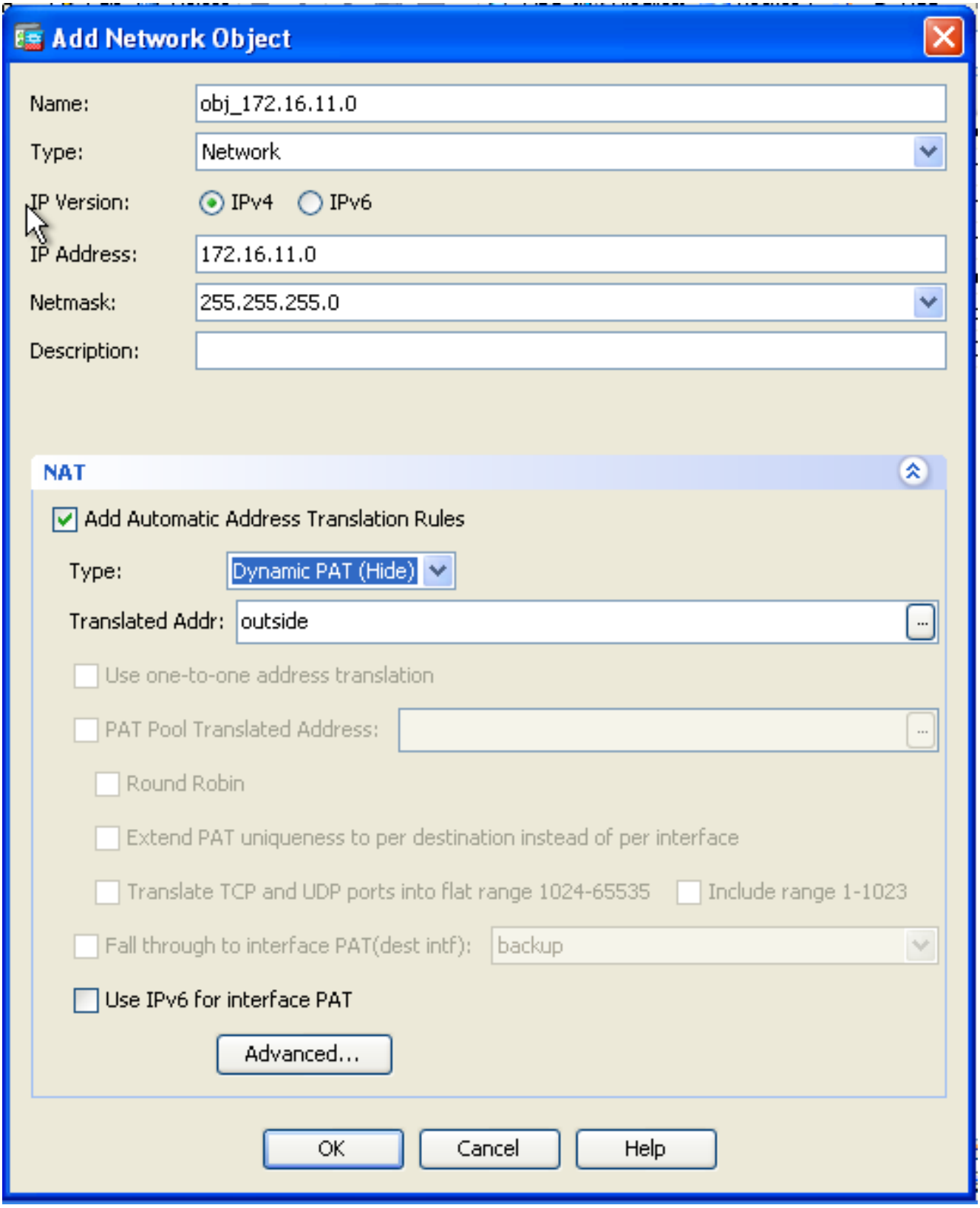
1. 选择**Configuration>防火墙> NAT规则**。单击**添加**然后选择**网络对象**为了配置一个动态NAT规则。



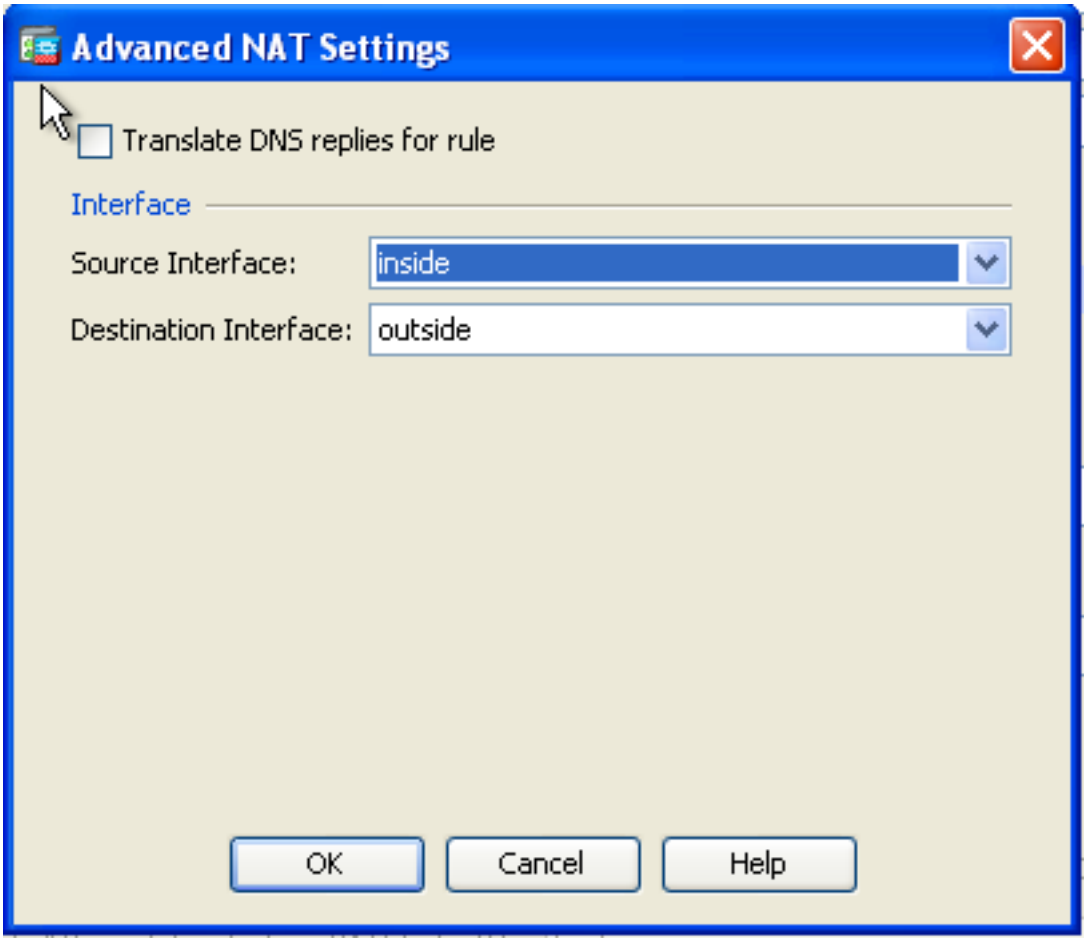
2. 配置网络/host/**动态PAT**要求的范围。在本例中，其中一内部的子网选择。此进程可以为您希望如此翻译的其他子网被重复。



3. 展开NAT。检查**添加自动地址转换规则**复选框。在类型下拉列表中，请选择**动态PAT (隐藏)**。在**翻译的地址**字段，请选择选项反射外部接口。单击 Advanced。



4. 在源接口和目的地接口下拉列表中，请选择适当的接口。点击OK键并且单击**运用**使更改生效。



这是为此PAT配置输出的等同CLI ：

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

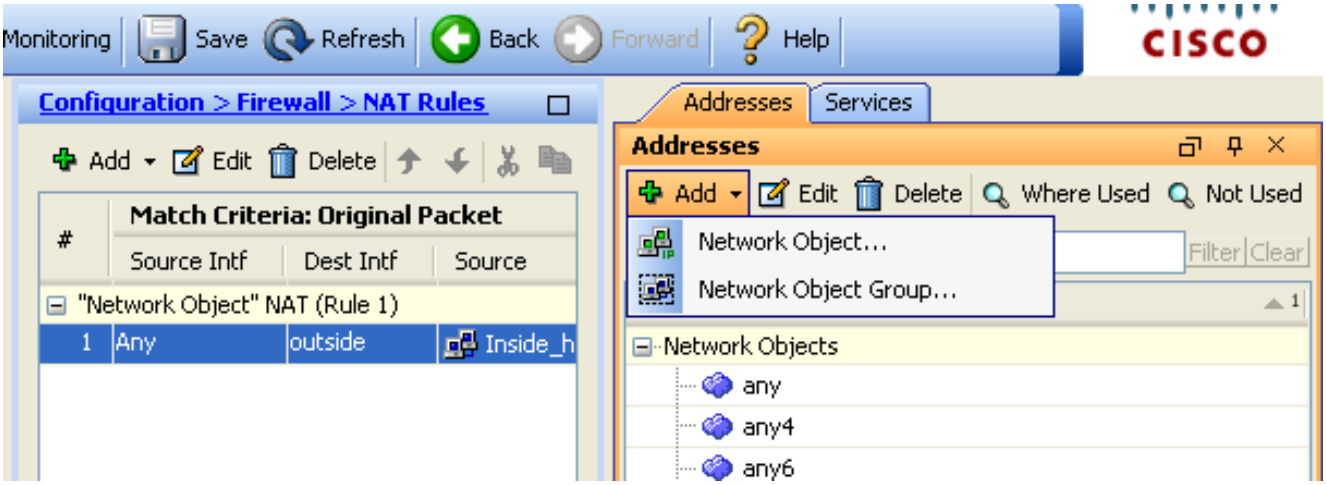
允许内部主机使用 NAT 访问外部网络

您可能允许内部主机/网络的一组访问与动态NAT规则的配置的外界。不同于PAT，动态NAT从地址池分配转换地址。结果，主机被映射对其自己的转换后的IP地址，并且两台主机不能共享同样转换后的IP地址。

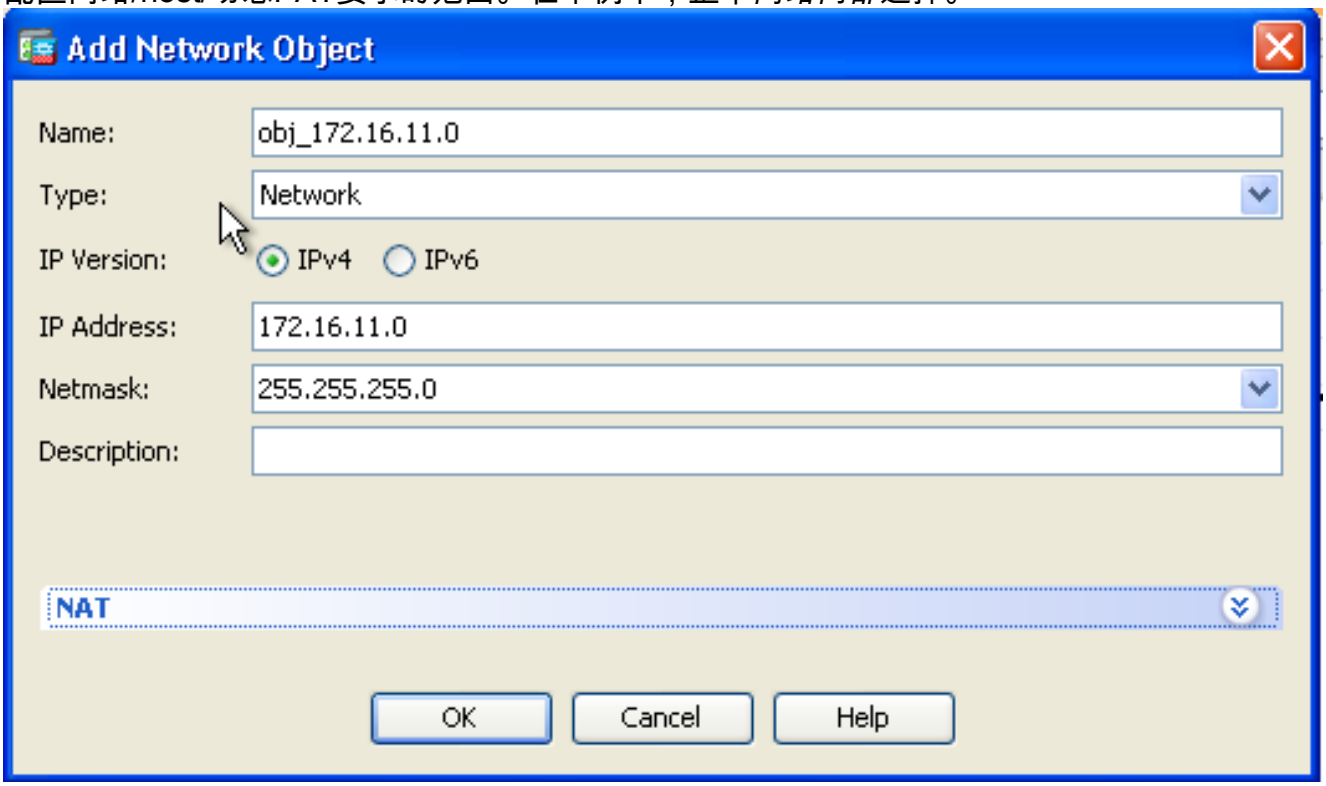
为了完成此，您需要选择将给的主机/网络的实际地址访问，并且他们必须然后被映射对翻译的IP地址的池。

完成这些步骤为了允许内部主机对外部网络的访问与NAT:

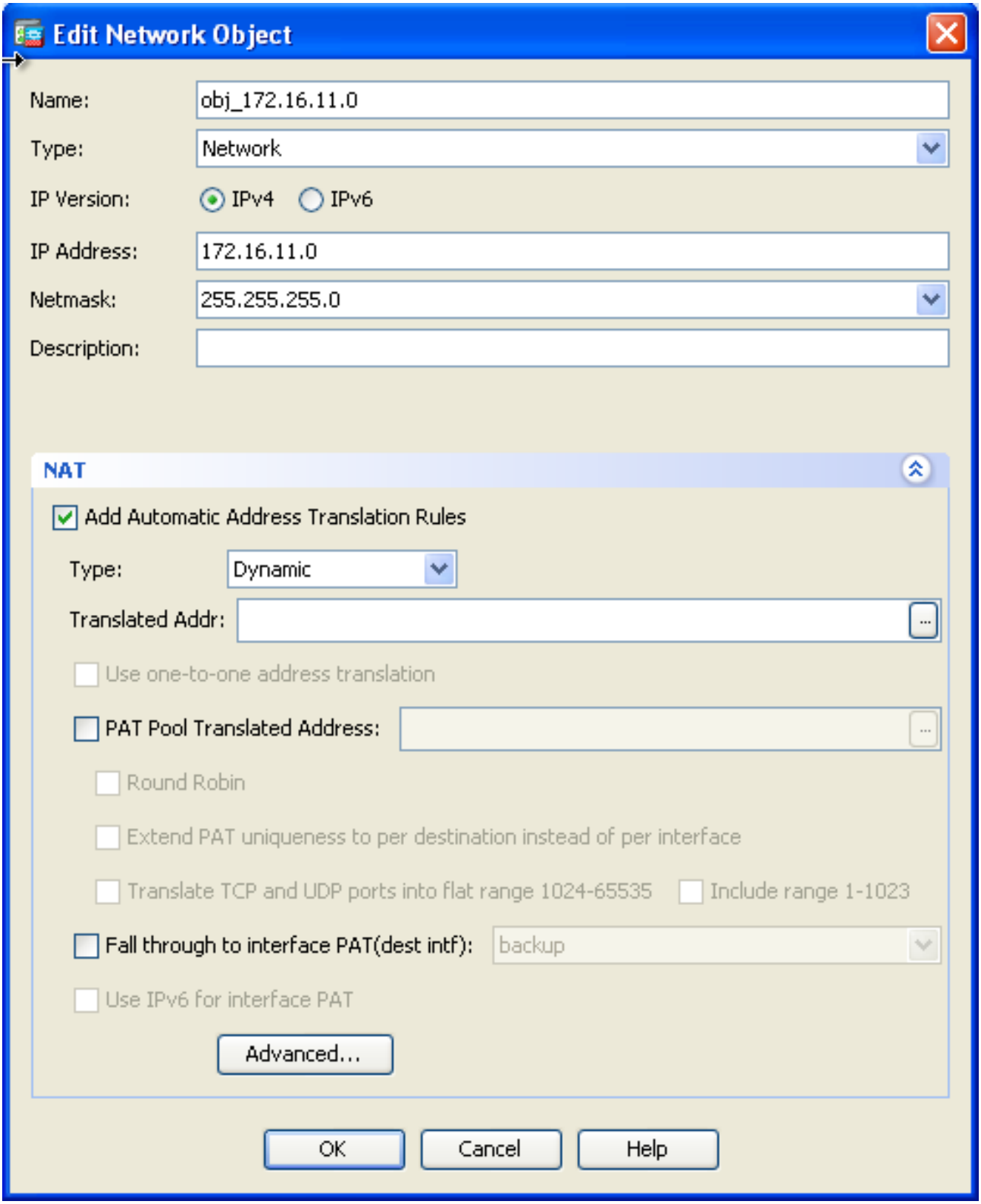
1. 选择**Configuration>防火墙> NAT规则**。单击**添加**然后选择**网络对象**为了配置一个动态NAT规则。



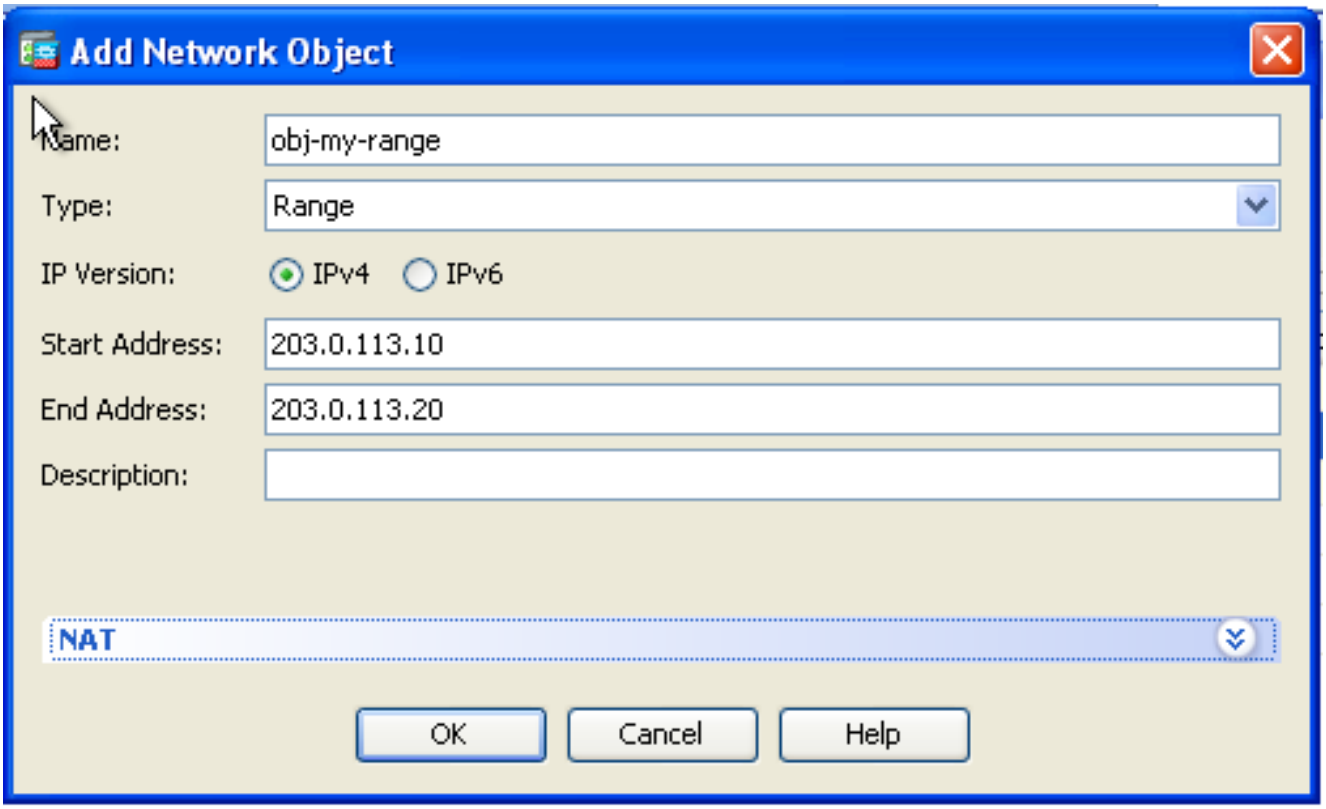
2. 配置网络/host/动态PAT要求的范围。在本例中，整个*网络内部*选择。



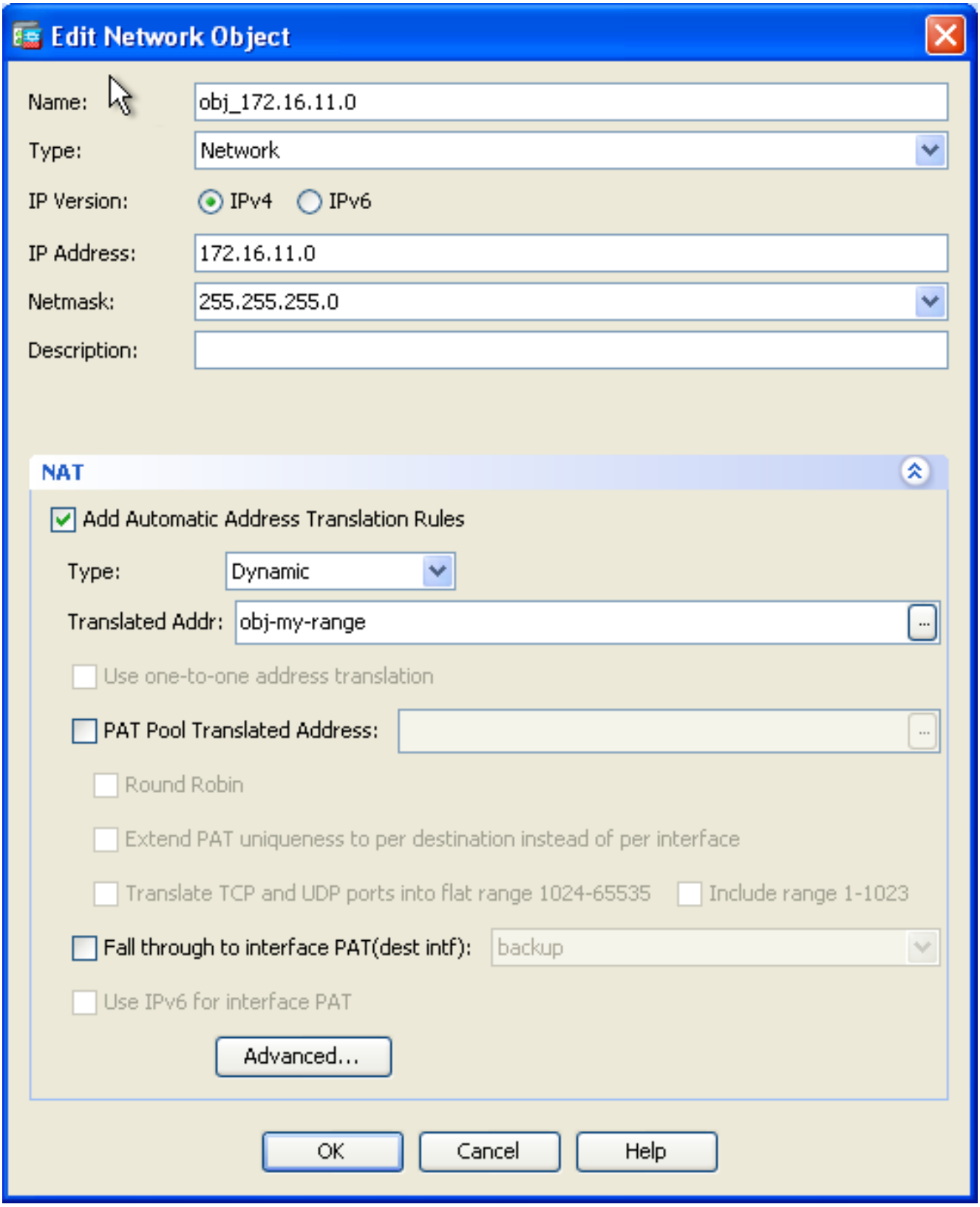
3. 展开NAT。检查**添加自动地址转换规则**复选框。在类型下拉列表中，请选择**动态**。在翻译的地址字段，请选择适当的选择。单击 **Advanced**。



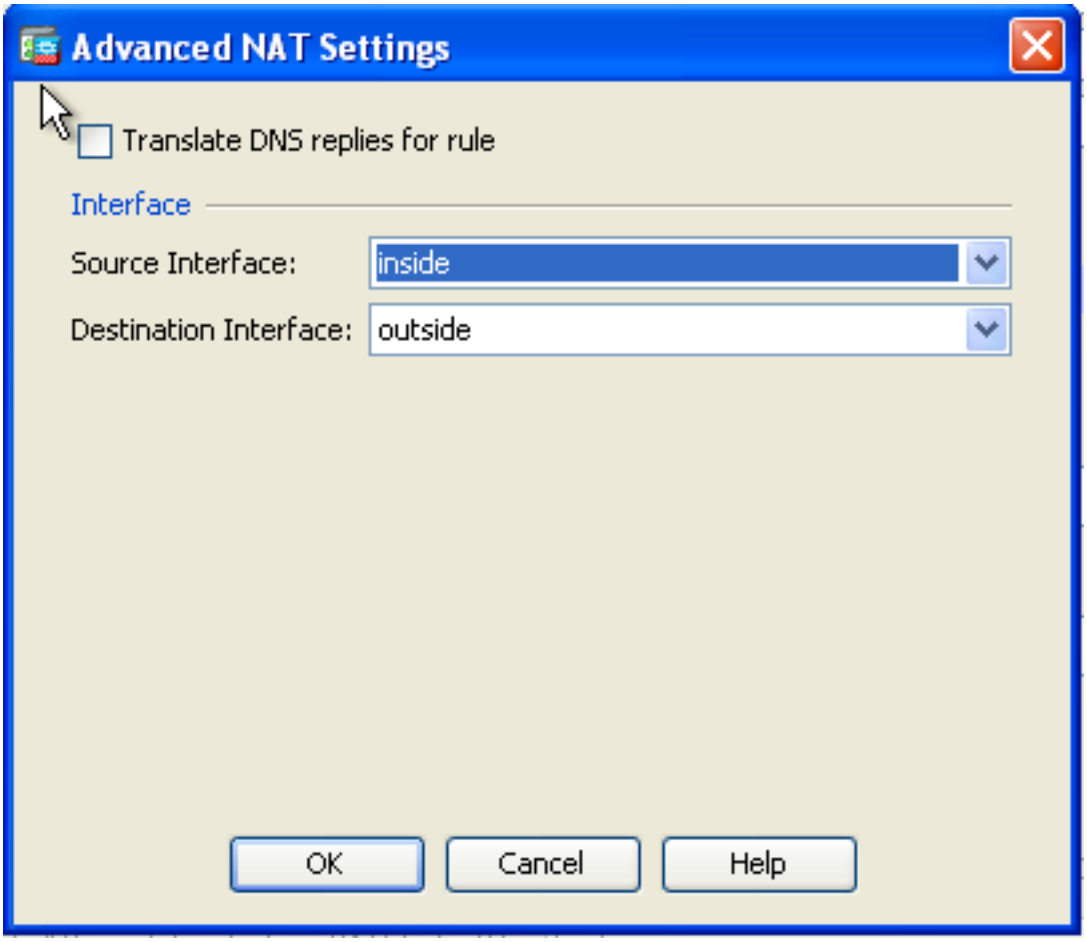
4. 单击**添加**添加网络对象。在类型下拉列表中，请选择**范围**。在起始地址和末端地址字段，请输入开始的和结束的PAT IP地址。单击 **Ok**。



5. 在翻译的地址字段，请选择地址对象。单击**先进**为了选择源和目的接口。



6. 在源接口和目的地接口下拉列表中，请选择适当的接口。点击OK键并且单击**运用**使更改生效。

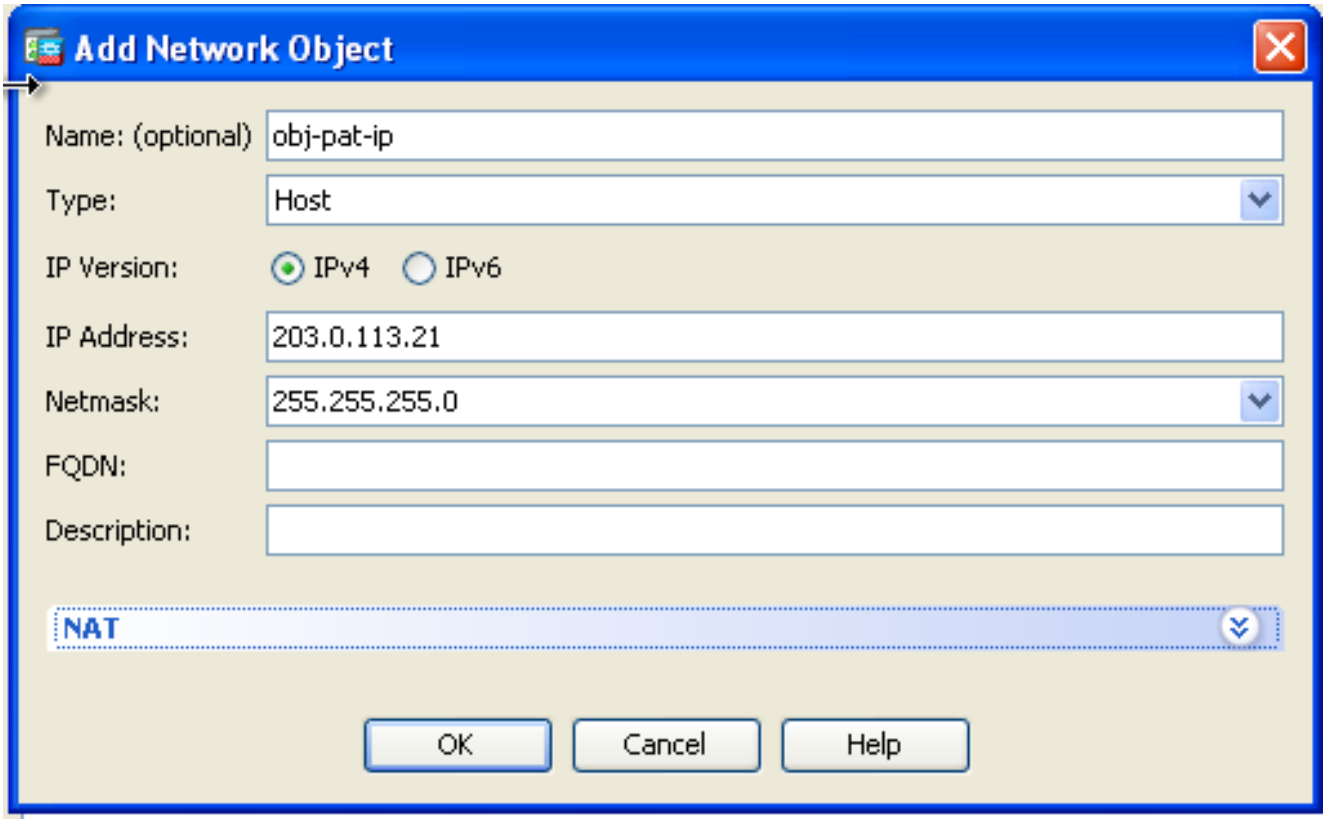


这是为此ASDM配置输出的等同CLI ：

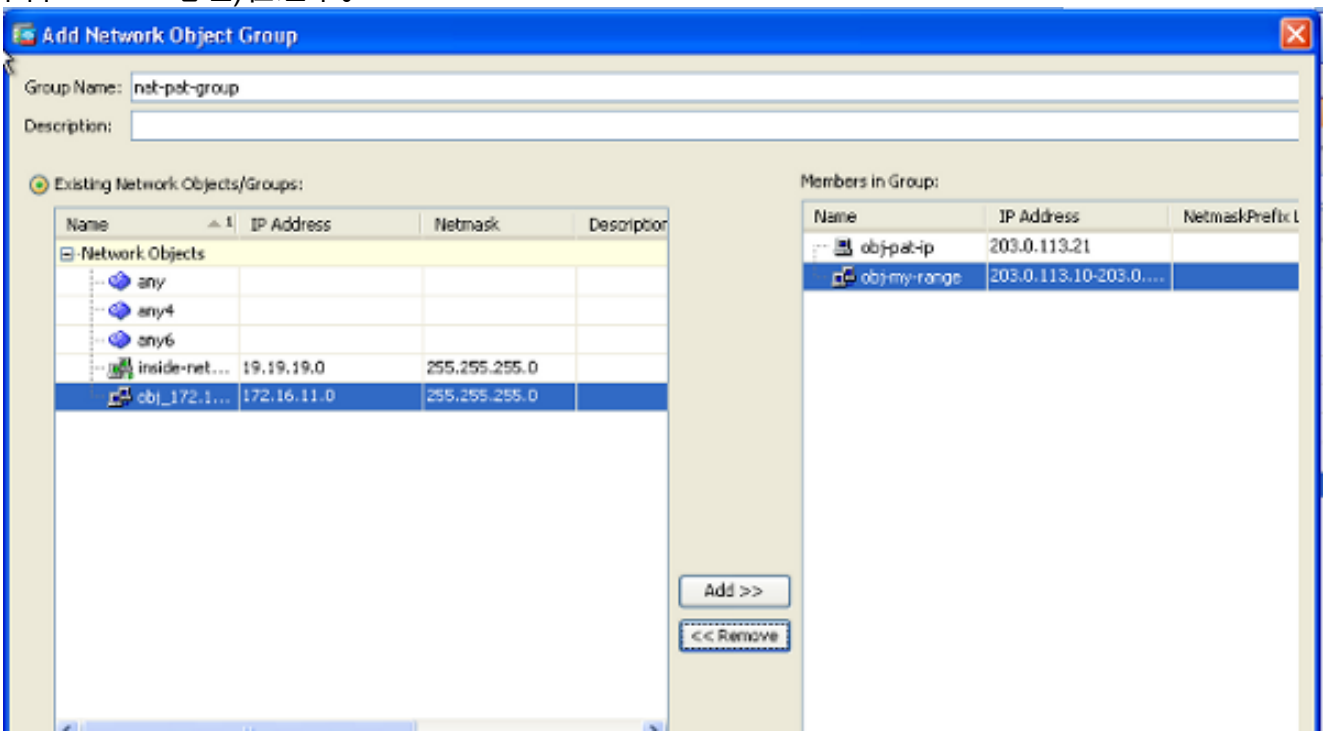
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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

根据此配置，在172.16.11.0网络的主机将被转换对从NAT池的所有IP地址， 203.0.113.10 - 203.0.113.20。如果被映射的池比实时组有少量地址，您可能用尽地址。结果，您可能设法实现与动态PAT备份的动态NAT或您可能设法展开现有池。

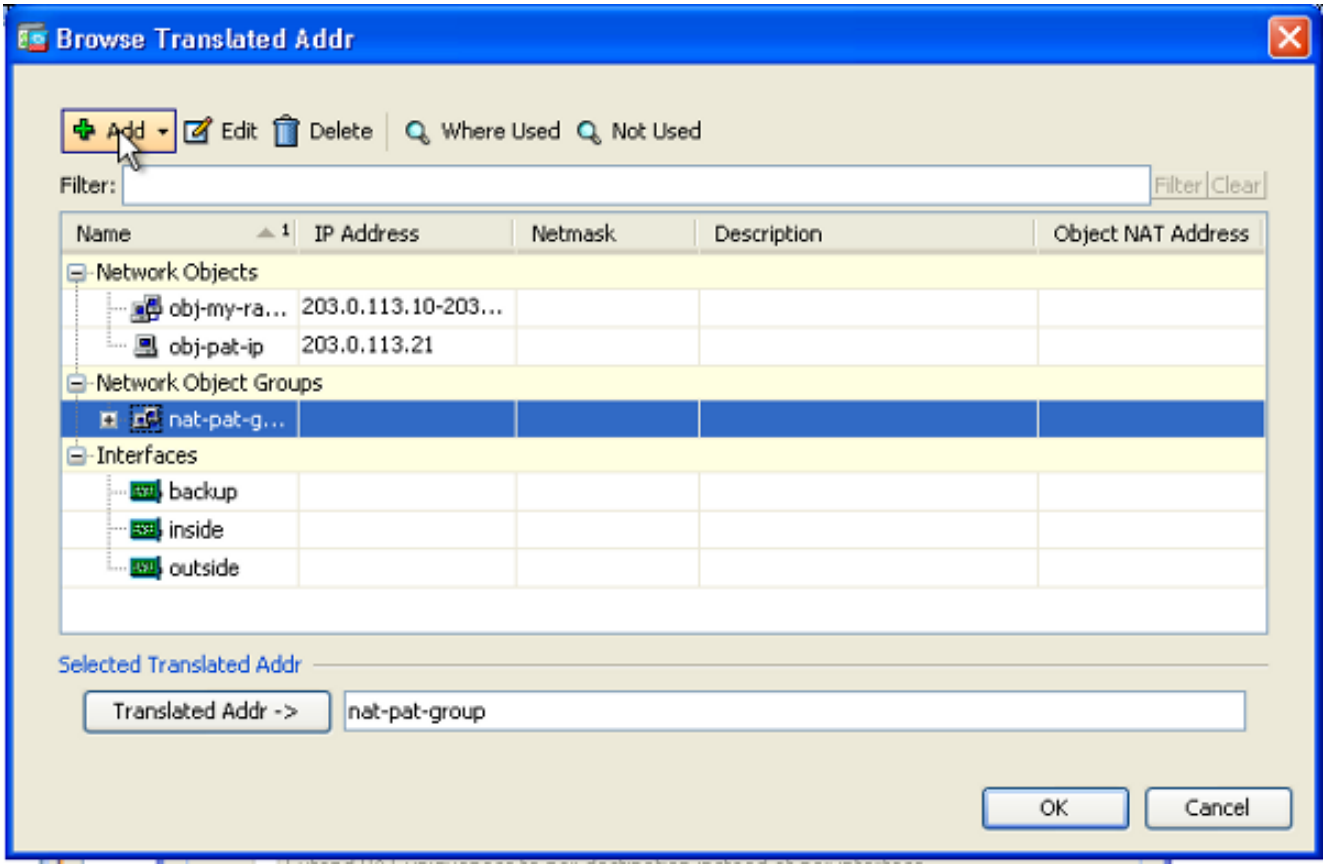
1. 重复步骤1到3在先前配置里并且单击再次**添加**为了添加网络对象。在类型下拉列表中，请选择**主机**。在IP地址字段，请输入PAT备份IP地址。单击 **Ok**。



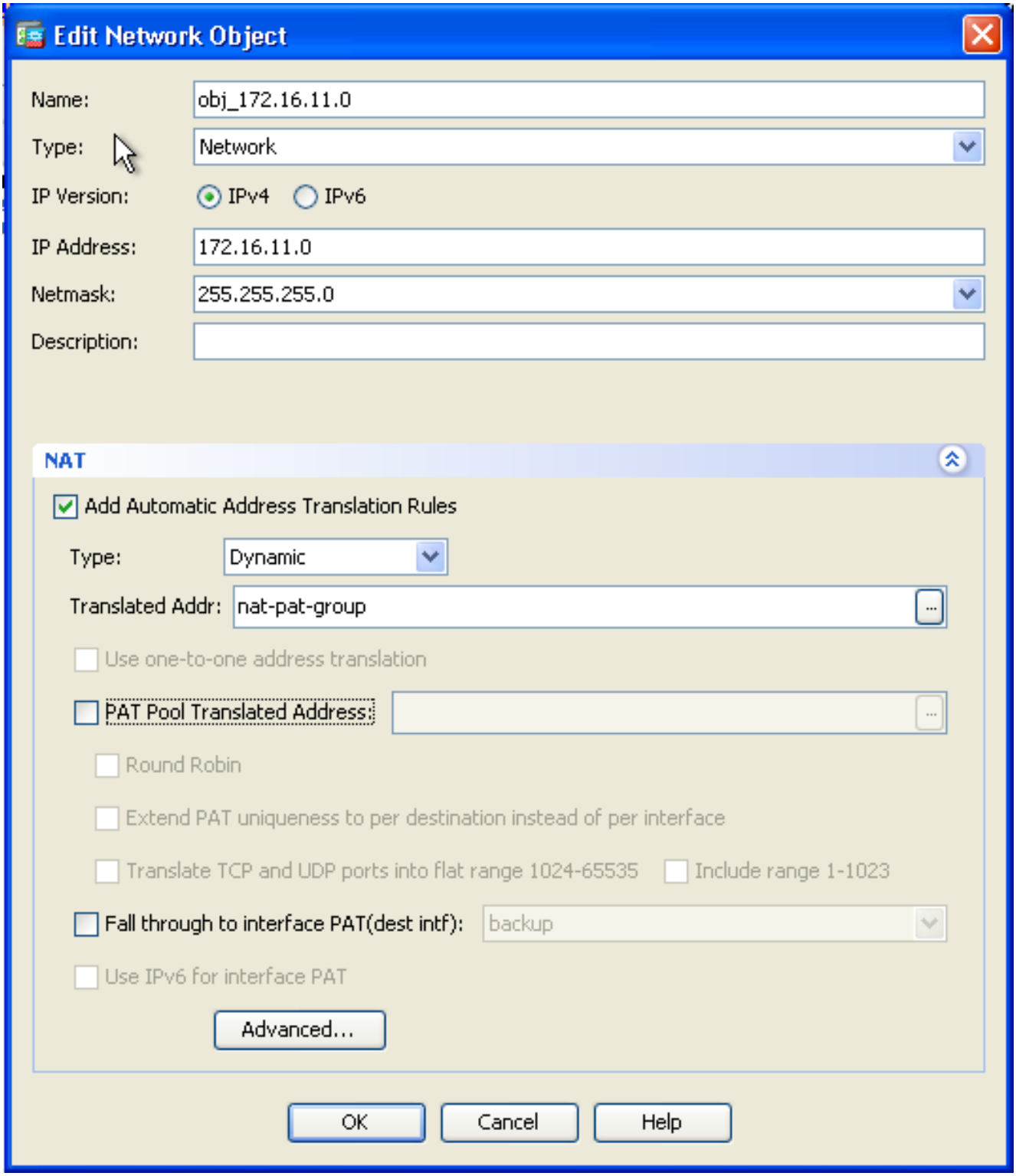
2. 单击**添加**添加每网络对象组。在Group Name字段，请输入组名并且**添加**两个地址对象(NAT范围和PAT IP地址)在组中。



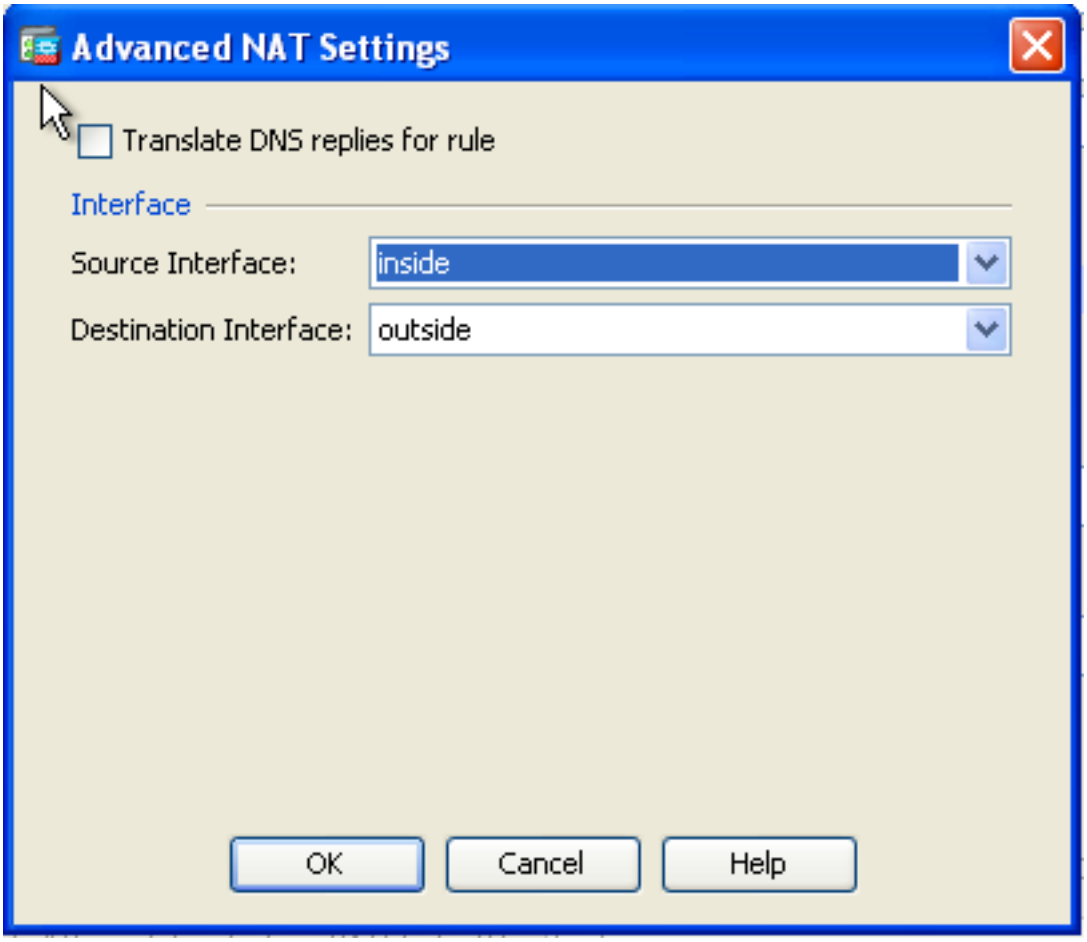
3. 选择已配置的NAT规则并且最近更改翻译的地址是已配置组'nat PAT组' (以前是'OBJ我范围')。单击 **Ok**。



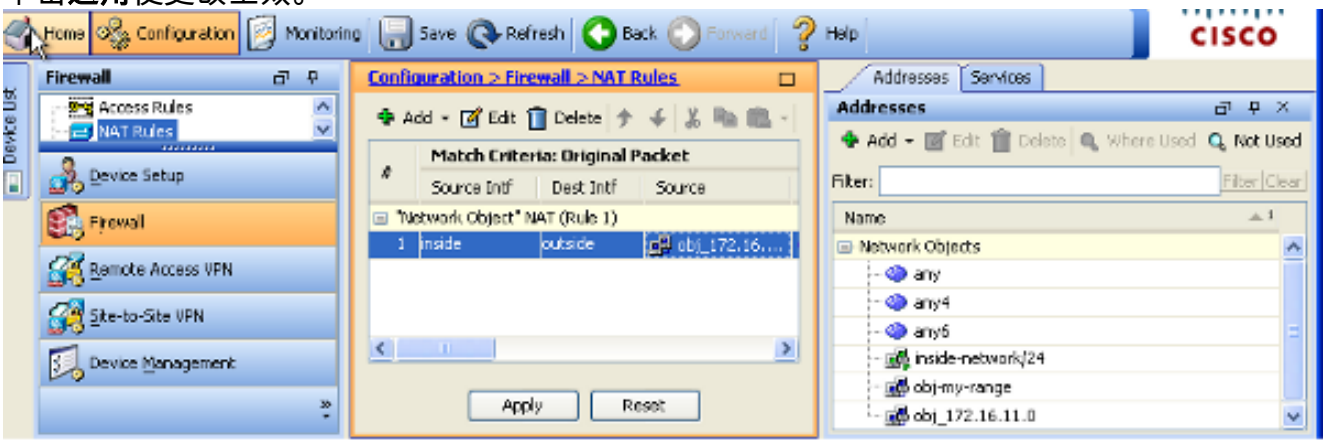
4. 点击OK键为了增加NAT规则。单击**先进**为了选择源和目的接口。



5. 在源接口和目的地接口下拉列表中，请选择适当的接口。单击 **Ok**。



6. 单击**运用**使更改生效。



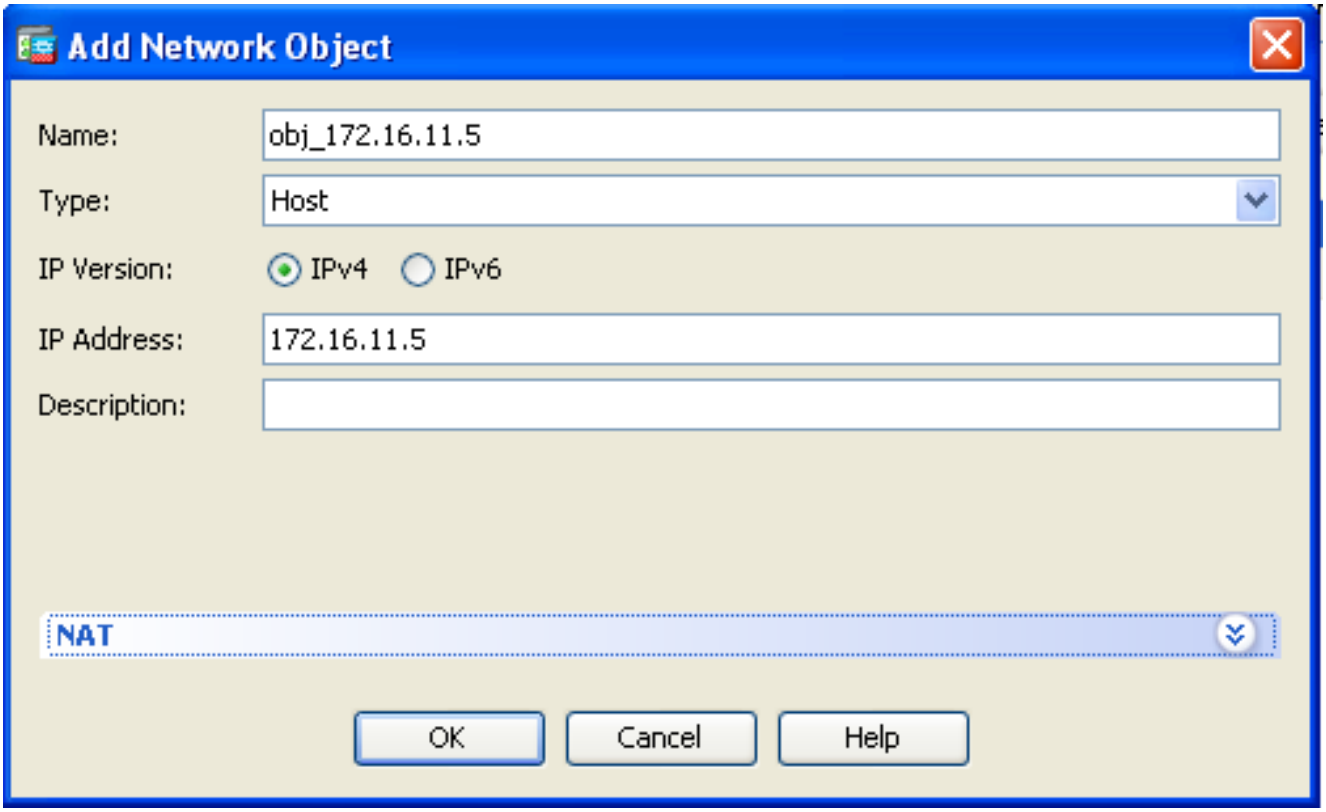
这是为此ASDM配置输出的等同CLI ：

```
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
nat (inside,outside) dynamic nat-pat-group
```

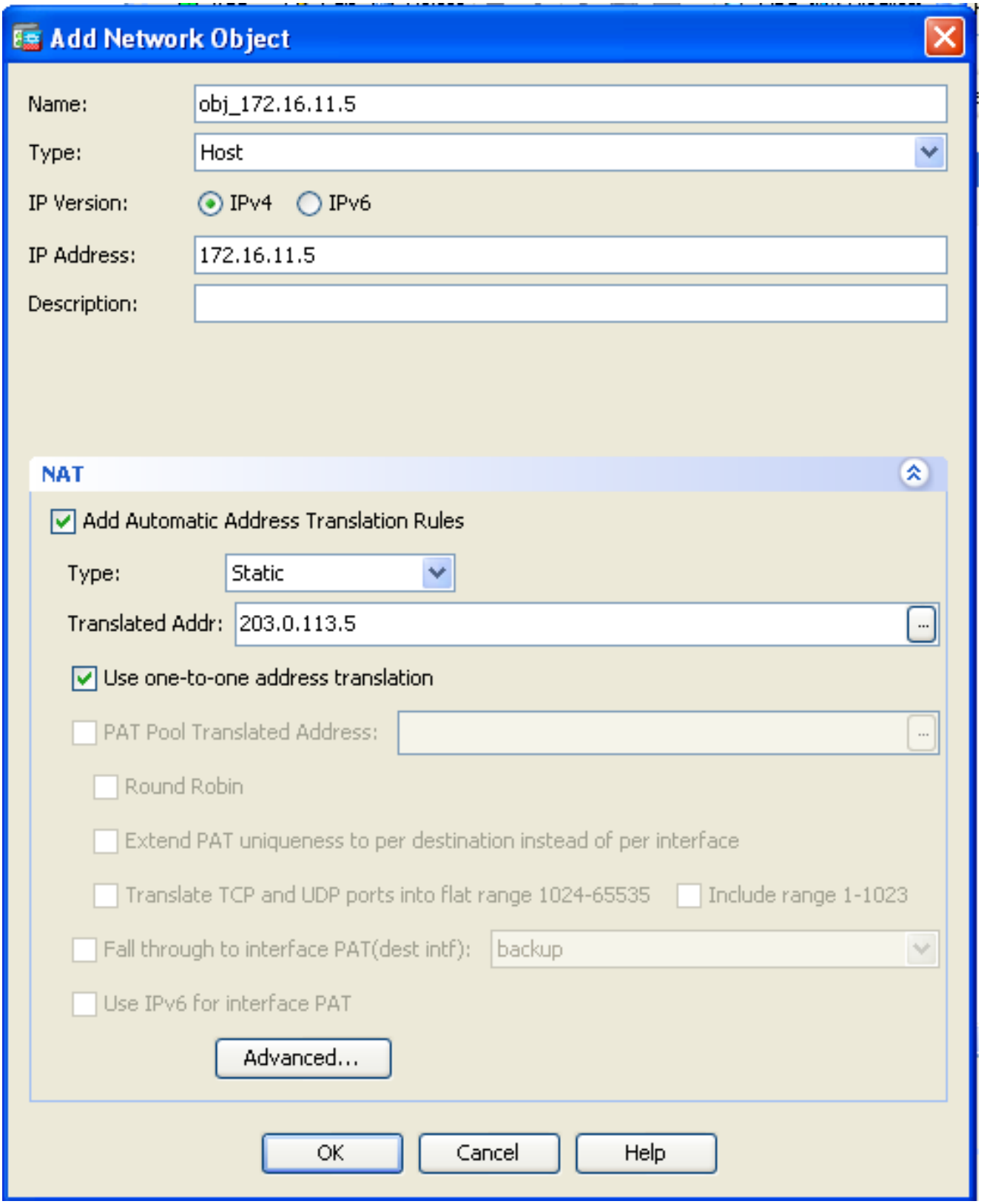
允许不受信任的主机访问受信任的网络中的主机

这可以通过静态NAT转换和访问规则的应用程序达到允许那些主机。您要求配置此，每当外部用户希望访问在您的内部网络坐的所有服务器。在不是可路由的在互联网的内部网络的服务器将有一个专用IP地址。结果，您需要翻译该专用IP地址到公网IP地址通过一个静态NAT规则。假设您有一个内部服务器(172.16.11.5)。为了做此工作，您需要翻译此私有服务器IP地址到公网IP地址。此示例描述如何实现双向静态NAT翻译172.16.11.5到203.0.113.5。

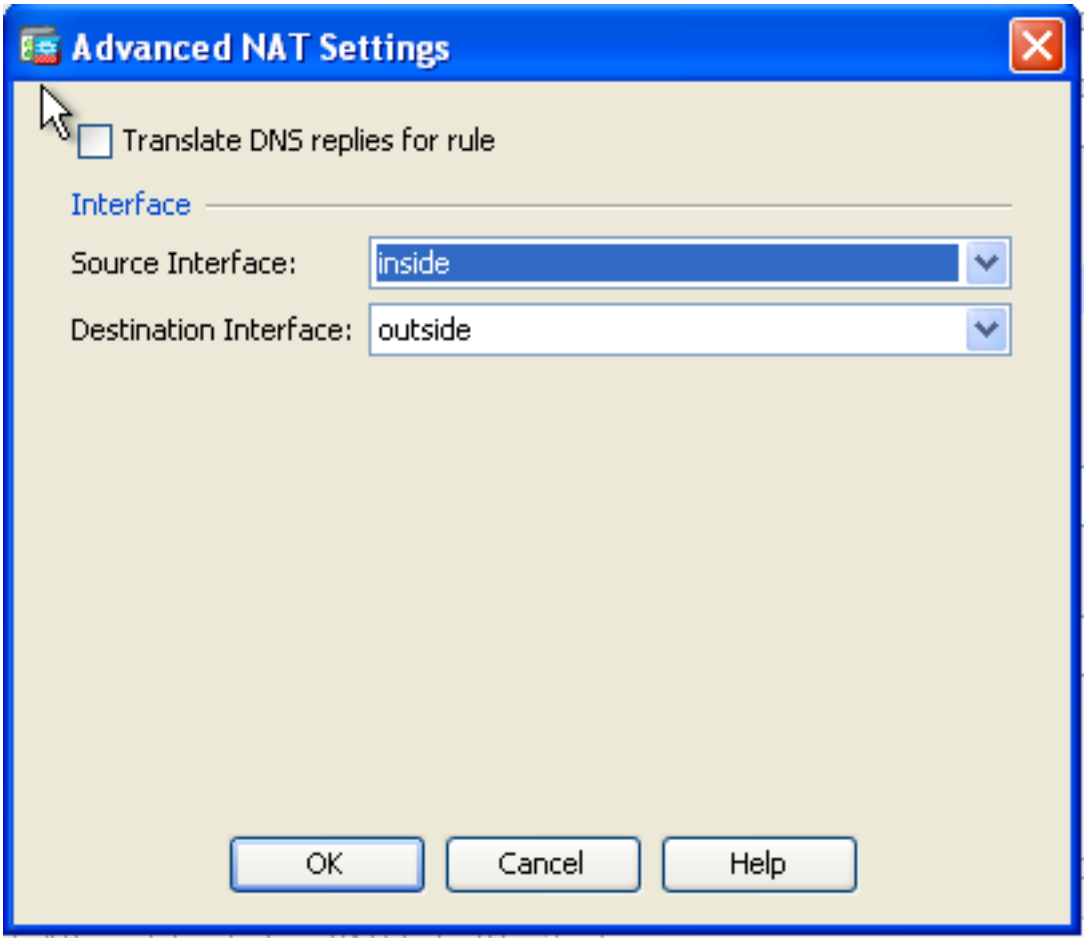
1. 选择**Configuration>防火墙> NAT规则**。单击**添加**然后选择**网络对象**为了配置一个静态NAT规则。展开NAT。



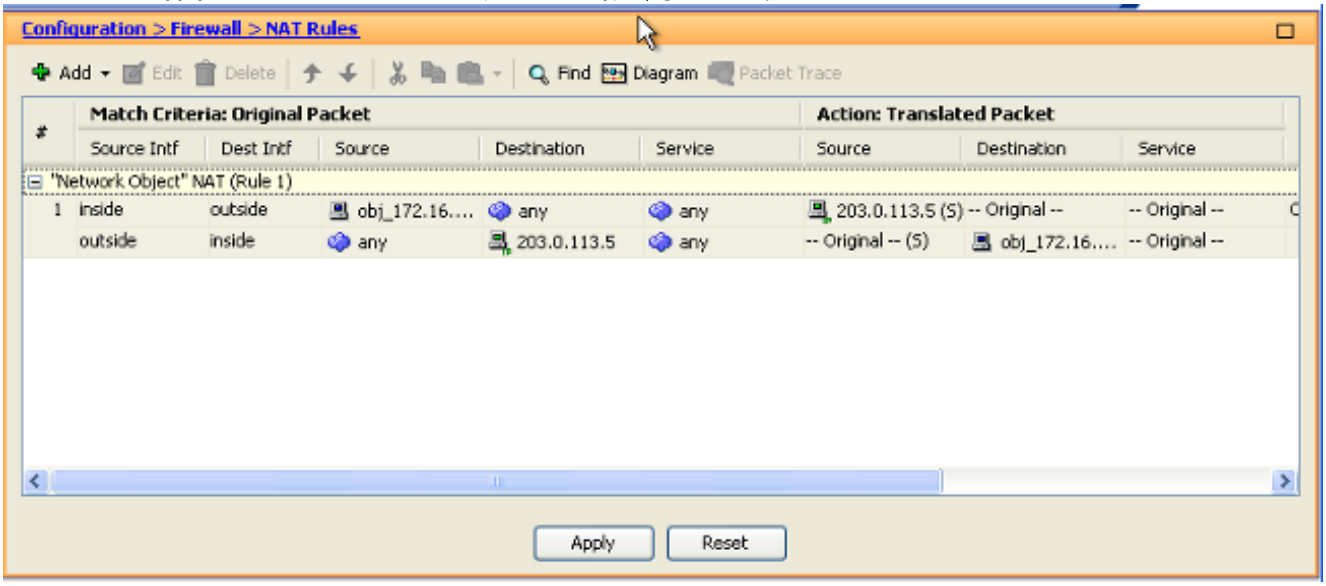
2. 检查**添加自动地址转换规则**复选框。在类型下拉列表中，请选择**静态。**在翻译的地址字段，请输入IP地址。单击**先进**为了选择源和目的接口。



3. 在源接口和目的地接口下拉列表中，请选择适当的接口。单击 Ok。



4. 您能看到已配置的静态NAT条目此处。单击**应用**为了发送此到ASA。



这是为此NAT配置输出的等同CLI ：

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

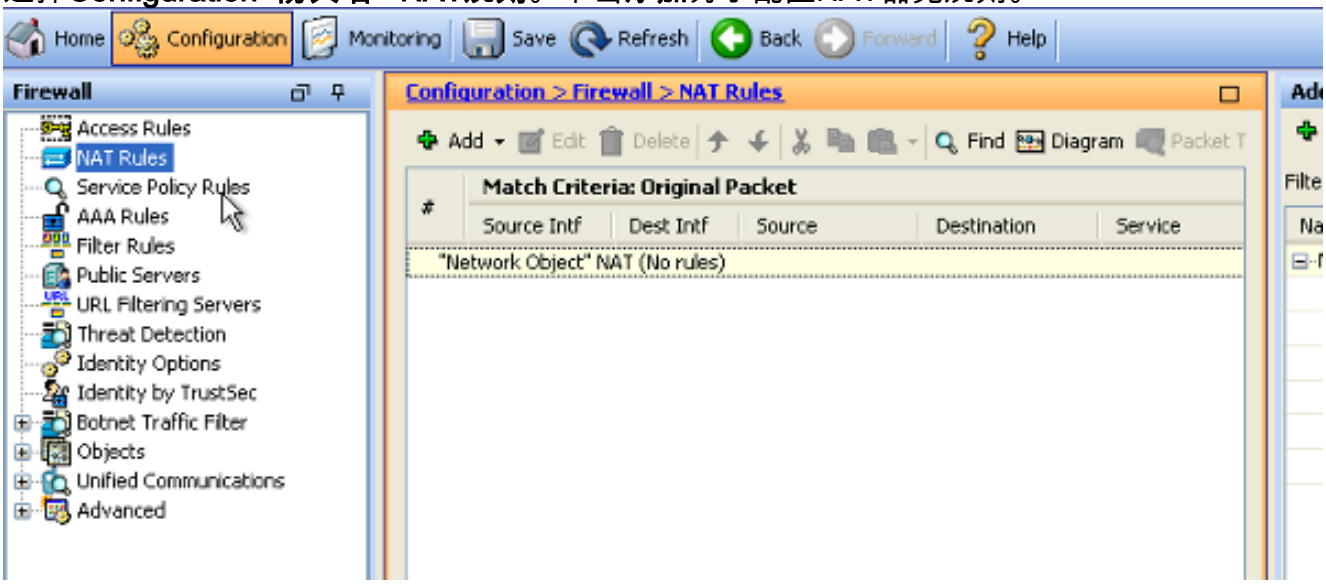
静态标识NAT

豁免的NAT是内部的用户设法访问远程VPN主机/服务器的有用的功能或者一些在ASA的其他接口后服务器主机主机/，不用NAT的完成。为了达到此，内部服务器，有一个专用IP地址，将是标识翻译对，并且反过来允许访问目的地执行NAT的本身。

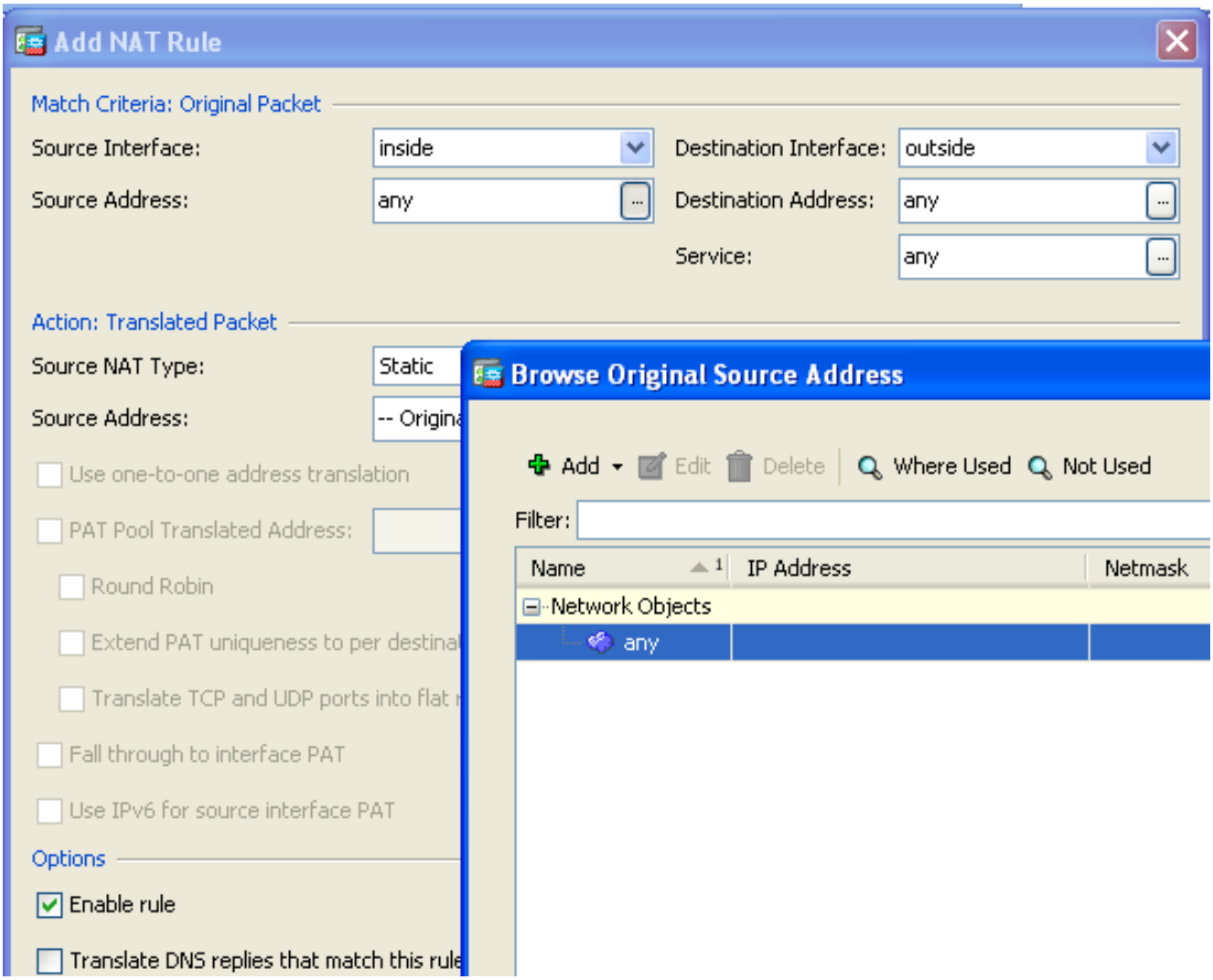
在本例中，内部主机172.16.11.15需要访问远程VPN服务器172.20.21.15。

完成这些步骤为了允许内部主机对远程VPN网络的访问与NAT:的完成

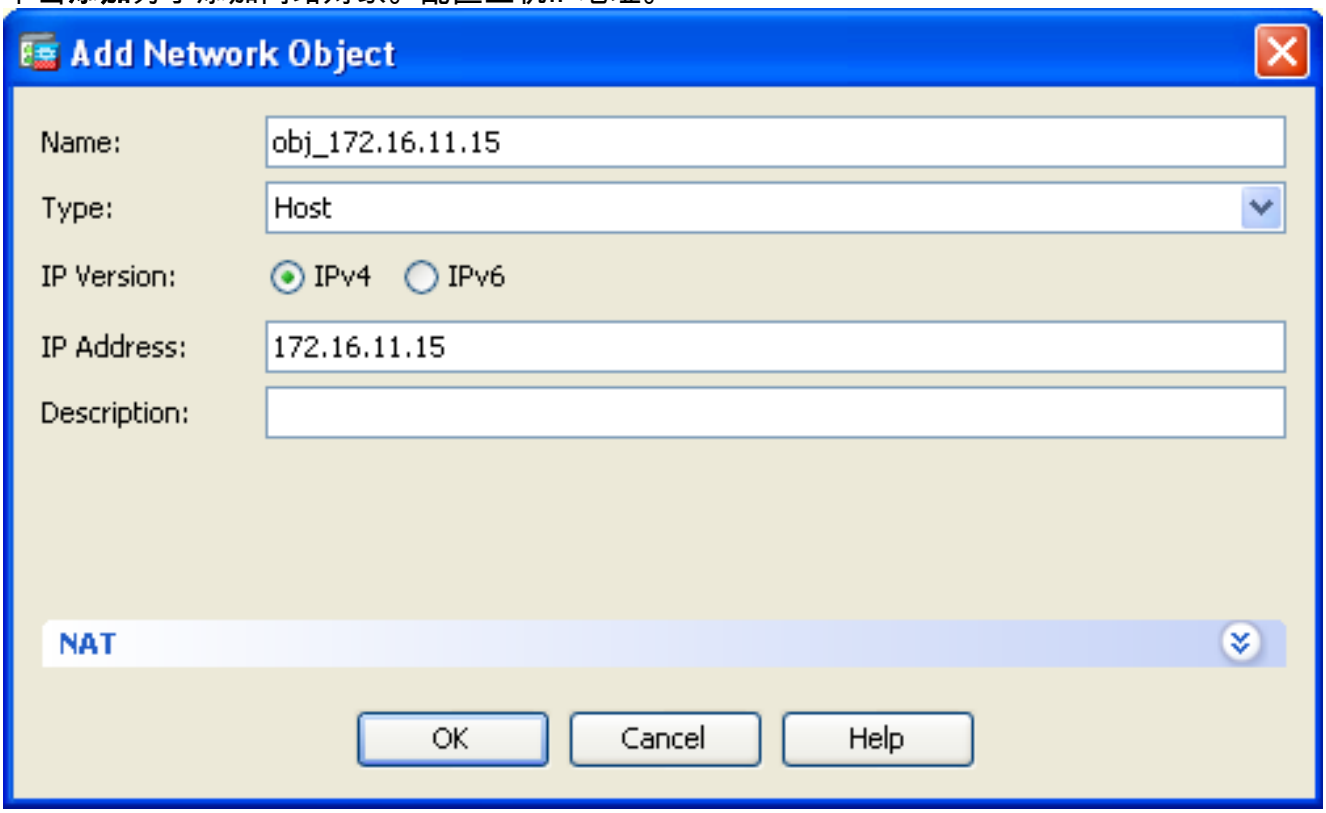
1. 选择**Configuration>防火墙> NAT规则**。单击**添加**为了配置NAT豁免规则。



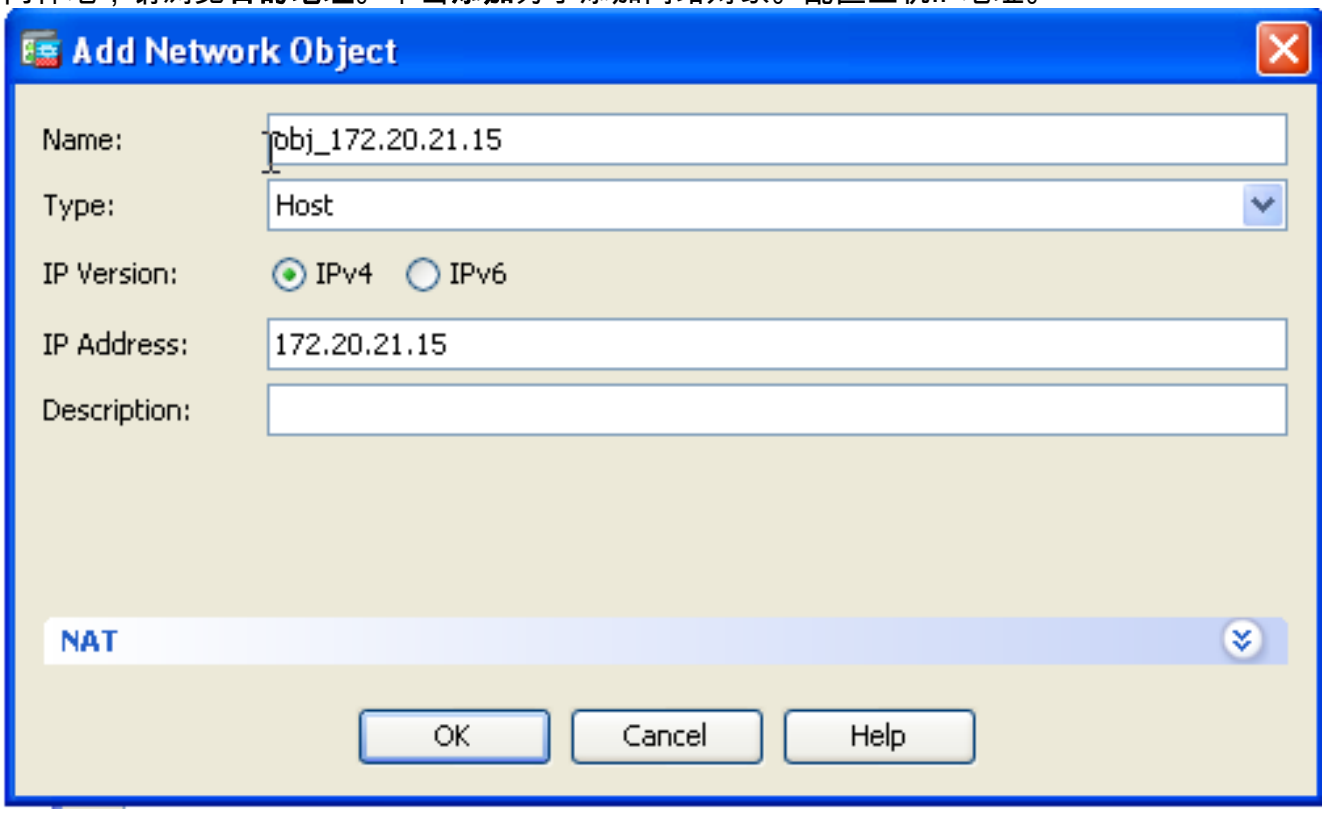
2. 在源接口和目的地接口下拉列表中，请选择适当的接口。在源地址域，请选择appropriate条目。



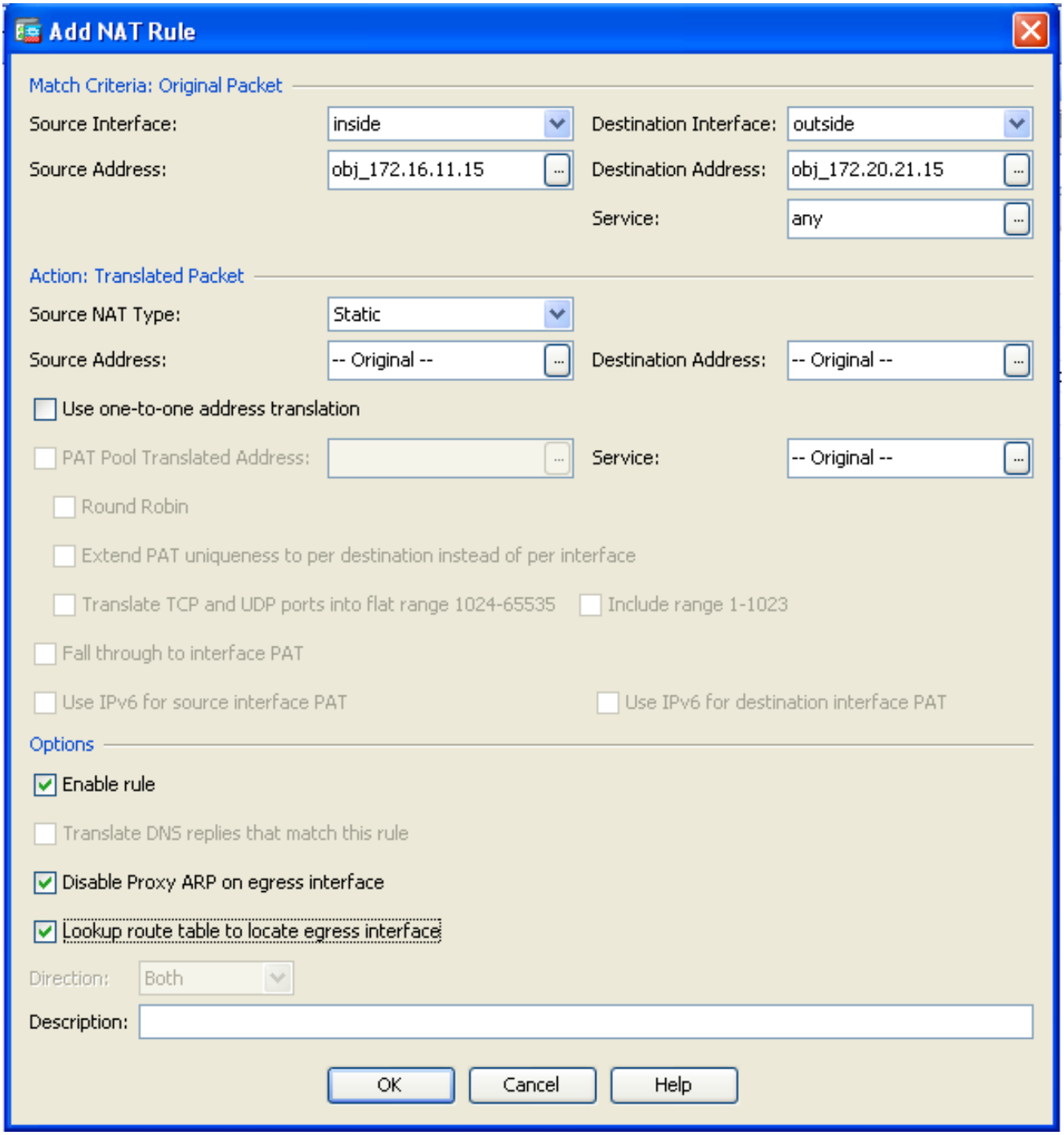
3. 单击**添加**为了添加网络对象。配置主机IP地址。



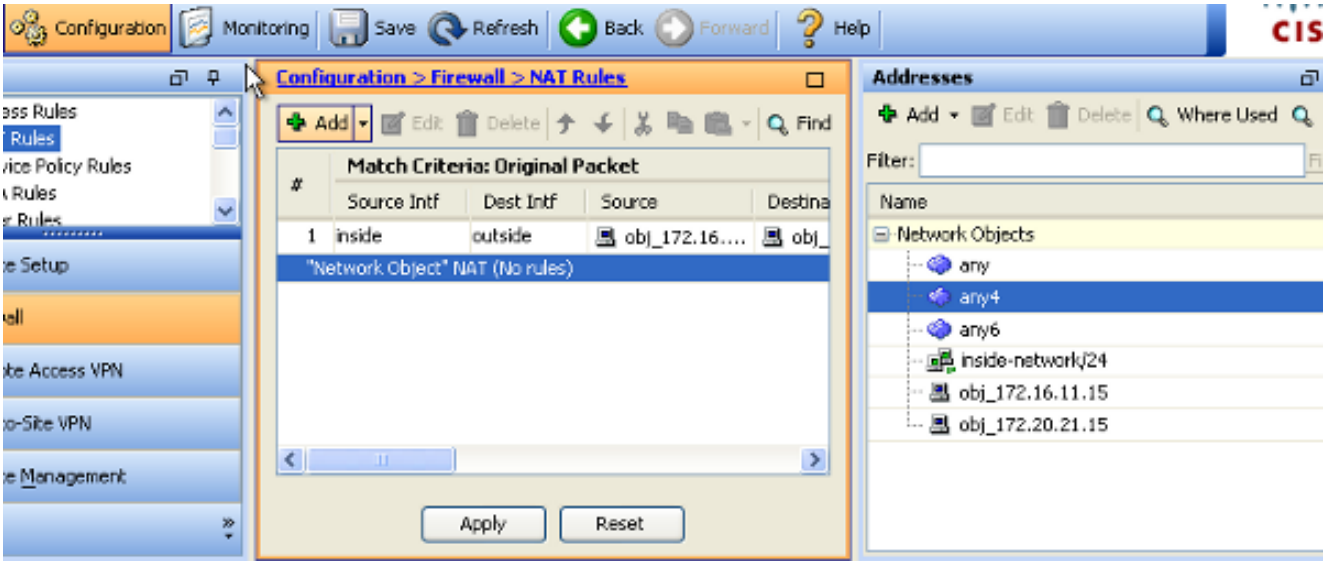
4. 同样地，请浏览**目的地址**。单击**添加**为了添加网络对象。配置主机IP地址。



5. 选择已配置的源地址和目的地址对象。检查**在出口接口**和**查找路由表的禁用代理ARP找出出口接口**复选框。单击 Ok。


Add NAT Rule
Match Criteria: Original Packet
Source Interface:
inside
Destination Interface:
outside
Source Address:
obj_172.16.11.15
Destination Address:
obj_172.20.21.15
Service:
any
Action: Translated Packet
Source NAT Type:
Static
Source Address:
-- Original --
Destination Address:
-- Original --
Use one-to-one address translation
PAT Pool Translated Address:
Service:
-- Original --
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:
Both
Description:
OK
Cancel
Help

6. 单击**运用**使更改生效。



这是为NAT输出的等同CLI豁免或标识NAT配置：

```
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
```

端口重定向(转发)与静态

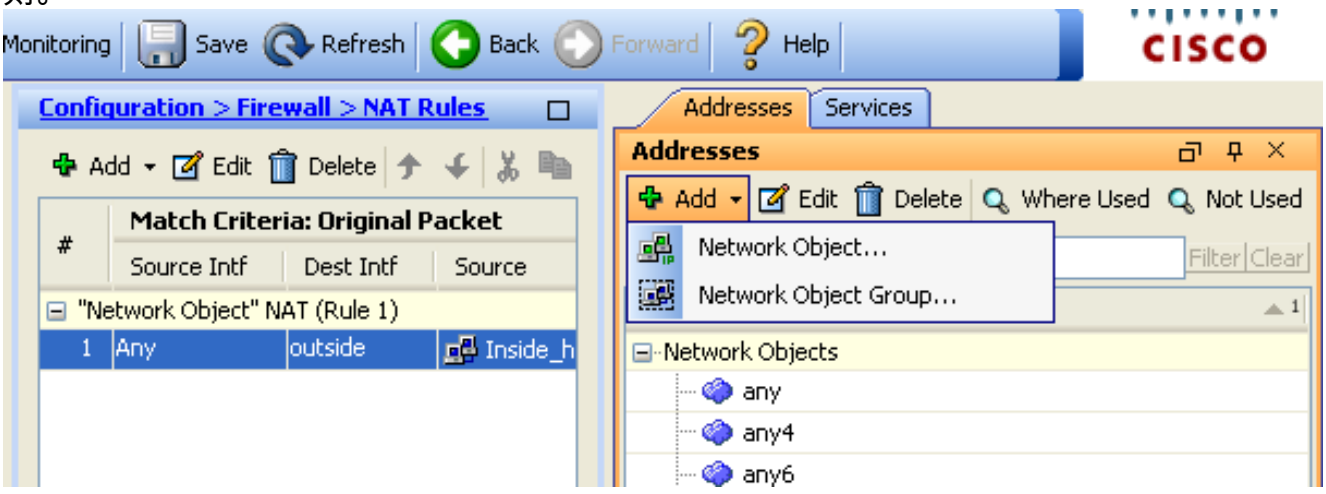
波尔特转发或端口重定向是外部用户设法访问在一个特定端口的一个内部服务器的有用的功能。为了达到此，内部服务器，有一个专用IP地址，将翻译对为特定端口反过来允许访问的公网IP地址。

在本例中，外部用户要在端口25访问SMTP服务器， 203.0.115.15。这在两个步骤完成：

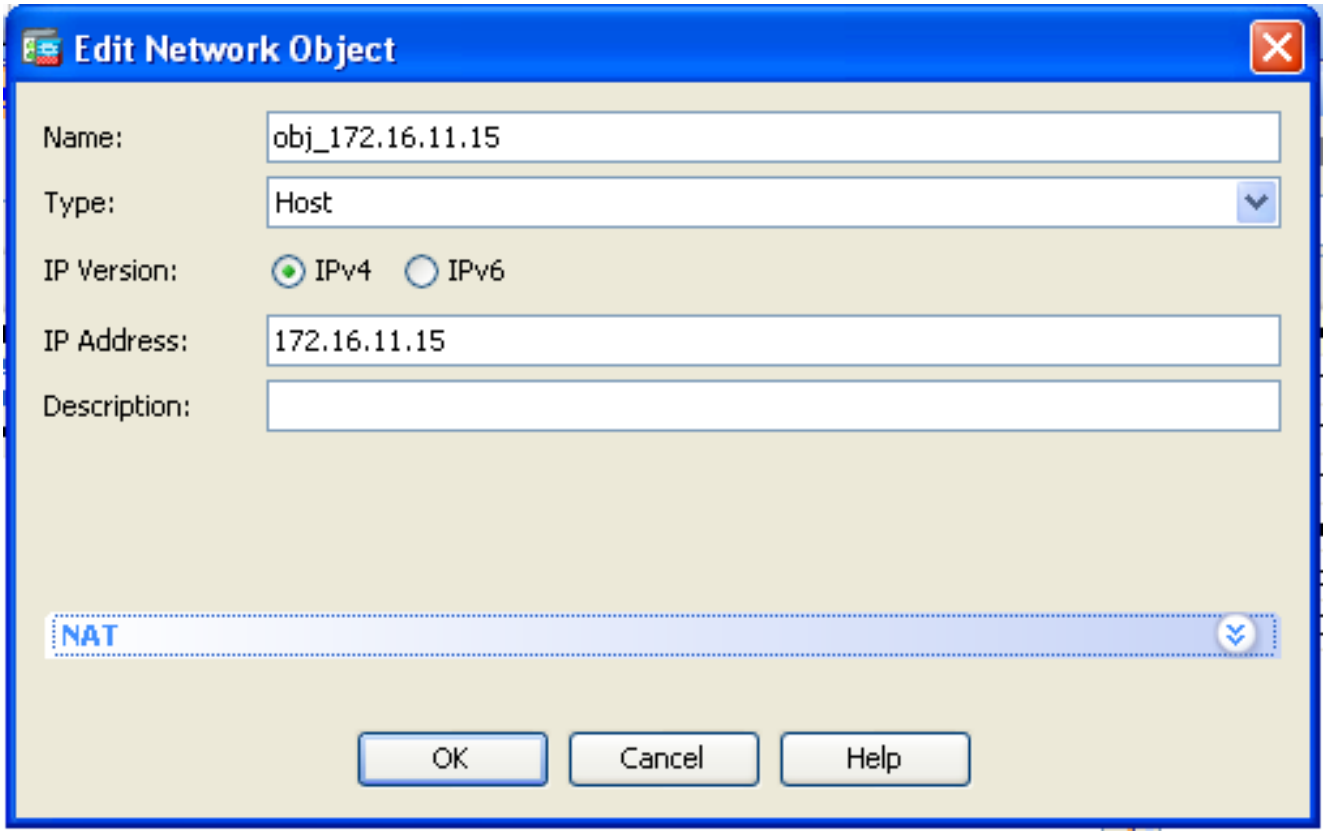
1. 翻译内部邮件服务器，在端口25的172.16.11.15，对公网IP地址， 203.0.115.15在端口25。
2. 对公共邮件服务器的允许，在端口25的203.0.115.15。

当外部用户设法访问服务器时，在端口25的203.0.115.15，此流量重定向到内部邮件服务器，172.16.11 15在端口25。

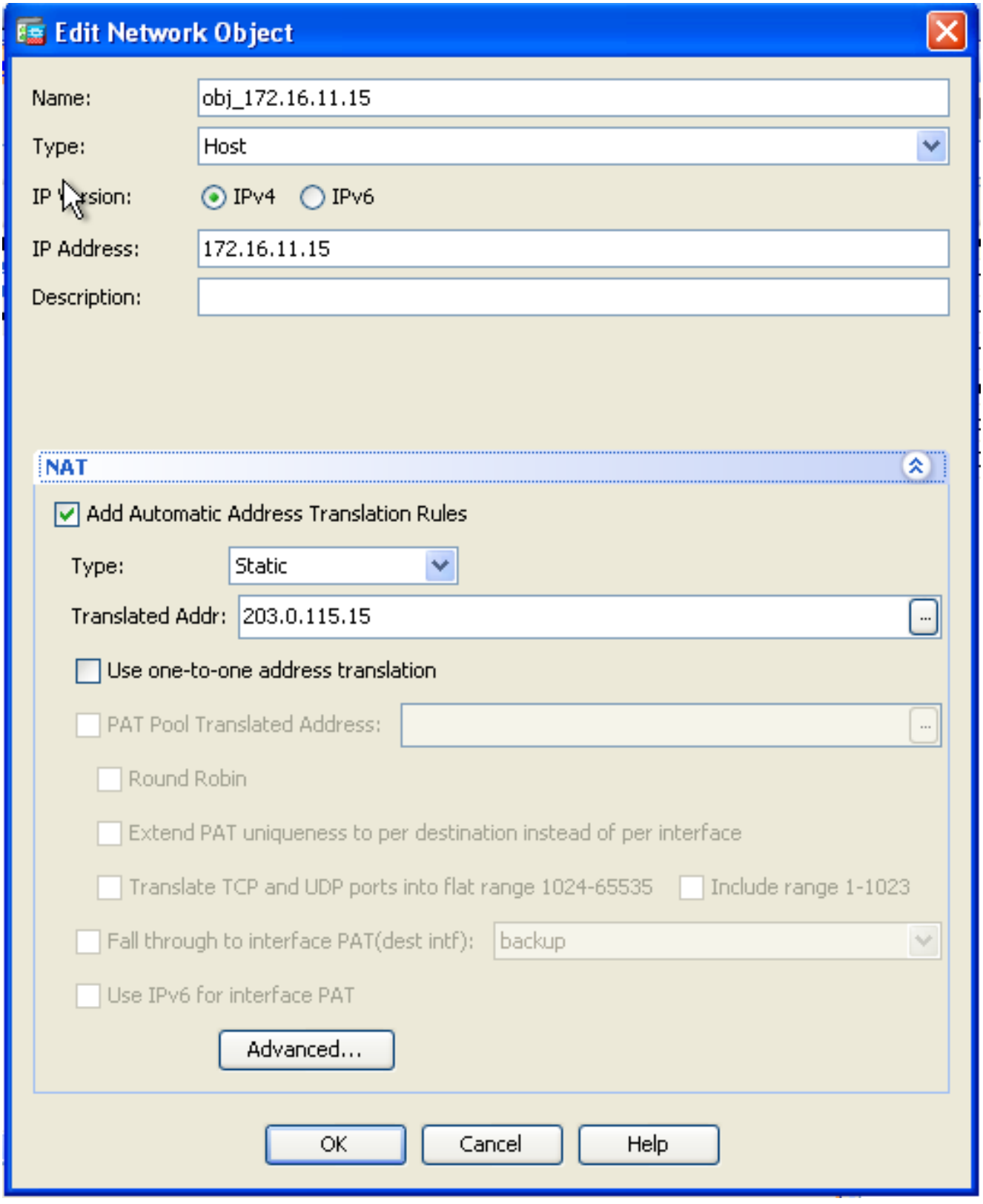
1. 选择**Configuration>防火墙> NAT规则**。单击**添加**然后选择**网络对象**为了配置一个静态NAT规则。



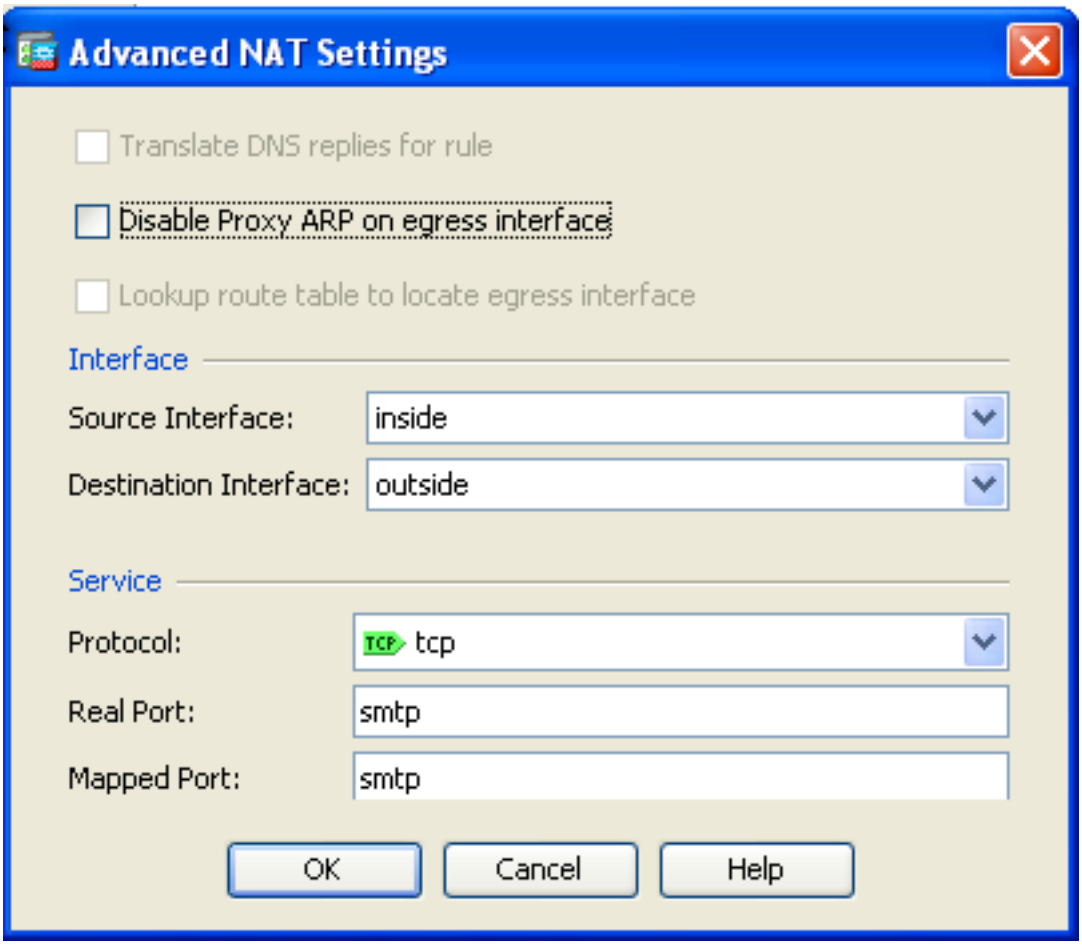
2. 配置端口转发要求的主机。



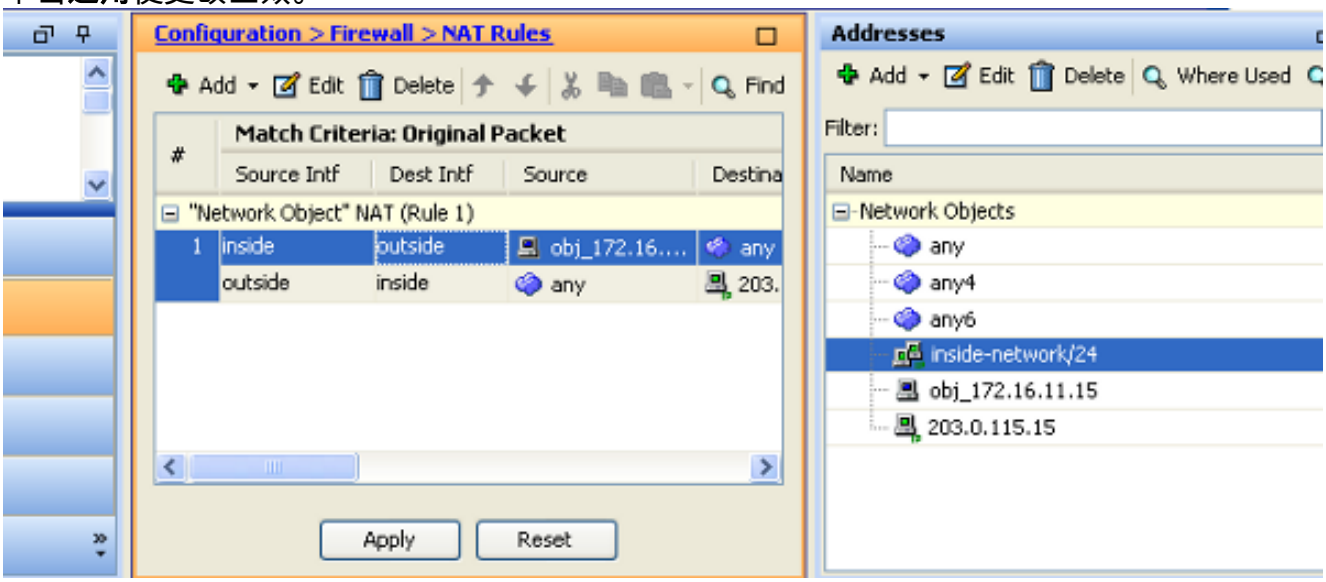
3. 展开NAT。检查**添加自动地址转换规则**复选框。在类型下拉列表中，请选择**静态**。在翻译的地址字段，请输入IP地址。单击**先进**为了选择服务和源和目的接口。



4. 在源接口和目的地接口下拉列表中，请选择适当的接口。配置服务。单击 Ok。



5. 单击**运用**使更改生效。



这是为此NAT配置输出的等同CLI ：

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.115.15 service tcp smtp smtp
```

验证

使用本部分可确认配置能否正常运行。

确定Cisco CLI分析器(仅限注册用户)支持**显示**命令。请使用Cisco CLI分析器为了查看show命令输出分析。

通过与Web浏览器的HTTP访问网站。此示例使用主机在198.51.100.100的一个站点。如果连接是成功的，此输出在ASA CLI能被看到。

连接

```
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
```

ASA是状态防火墙，并且从Web服务器的回程数据流允许上一步通过防火墙，因为在防火墙连接表里匹配一***连接***。匹配连接事先存在的流量通过防火墙允许，不用阻塞由接口ACL。

在上一个输出中，内部接口的客户端建立了对198.51.100.100主机的连接外部接口。此联系用TCP协议建立和是空闲在六秒。连接标志指示此连接的当前状态。关于连接标志的更多信息可以在ASA TCP连接标志找到。

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防火墙在正常操作时生成Syslog。Syslog在根据操作日志配置的冗余排列。输出显示被看到在级别六的两Syslog，或者'信息性'级别。

在本例中，有生成的两Syslog。第一是表明的日志消息防火墙建立了转换，特别地一个动态TCP转换(PAT)。当流量从里面横断到外部接口，它指示源IP地址和端口和转换后的IP地址和端口。

第二Syslog表明防火墙在其此特定的流量的连接表里建立了连接在客户端和服务器之间。如果防火墙配置为了阻塞此连接尝试，或者某个其他要素禁止了此连接(资源约束或一可能的误配置)的创建，防火墙不会生成表明的日志连接被建立了。反而它将记录连接的一个原因能拒绝或关于什么要素的一个征兆从创建禁止了连接。

packet tracer

```
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
```

在ASA的数据包跟踪程序功能允许您指定一*被模拟的*数据包和发现所有多种步骤，检查，并且作用防火墙审阅，当处理流量时。使用此工具，识别您相信*应该*允许穿过防火墙流量的示例是有用的，并且使用5-tupple为了模拟流量。在前一个示例中，数据包跟踪程序用于为了模拟满足这些标准的连接尝试：

- 被模拟的数据包在里面到达。
- 使用的协议是TCP。
- 被模拟的客户端IP地址是172.16.11.5。
- 客户端发送从端口发出的流量1234。
- 流量被注定到在IP地址198.51.100.100的一个服务器。
- 流量被注定到端口80。

注意没有接口的提及从外部在命令。这是由数据包跟踪程序设计。工具如何告诉您防火墙处理那种连接尝试，包括如何将路由它，并且在哪个接口外面。关于数据包跟踪程序的更多信息可以在有数据包跟踪程序。的跟踪数据包找到

捕获

应用捕获

```
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 198.51.100.100ASA#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 32768ASA#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防火墙能捕获进入或离开其接口的流量。此捕获功能是意想不到的，因为能明确证明流量是否到达在，或者分支从，防火墙。前一个示例显示名为capin和capout的两个捕获的配置在各自内部和外部接口。捕获命令使用了匹配关键字，允许您是特定关于什么流量您要捕获。

对于捕获capin，您表明您在该的内部接口要匹配流量被看到(入口或出口)匹配TCP主机172.16.11.5主机198.51.100.100。换句话说，从主机172.16.11.5发送主机198.51.100.100或反之亦然的您要捕获所有TCP数据流。使用匹配关键字允许防火墙捕获该流量双向。因为防火墙执行在该客户端IP地址的PAT capture命令定义外部接口的不参考内部客户端IP地址。结果，您不能配比与该客户端IP地址。反而，此示例使用其中任一为了表明所有可能的IP地址将匹配该情况。

在您配置捕获后，您然后会尝试再建立连接，并且继续查看捕获用**显示捕获*<capture_name>***命令。在本例中，您能看到客户端能连接到服务器如明显由在捕获看到的TCP三通的握手。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- ASA Syslog配置示例
- 有CLI和ASDM配置示例的ASA数据包捕获
- 技术支持和文档 - Cisco Systems