Configurar a transmissão da porta da versão ASA 9.x com NAT

Índice

Introdução

Este documento explica como configurar o redirecionamento de porta (transmissão) e as características da tradução de endereço de rede externa (NAT) na versão de software adaptável 9.x da ferramenta de segurança (ASA), com o uso do CLI ou do Security Device Manager adaptável (ASDM).

Refira o guia de configuração ASDM do Series Firewall de Cisco ASA para a informação adicional.

Pré-requisitos

Requisitos

Refira configurar o acesso de gerenciamento a fim permitir que o dispositivo seja configurado pelo ASDM.

Componentes Utilizados

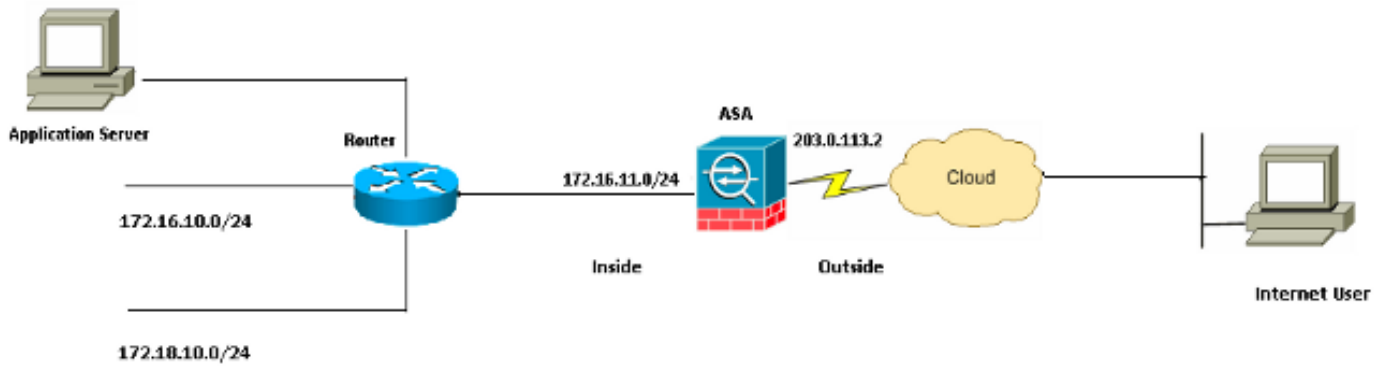
As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software 9.x da ferramenta de segurança do 5525 Series de Cisco ASA e mais tarde
- Versão 7.x e mais recente ASDM

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



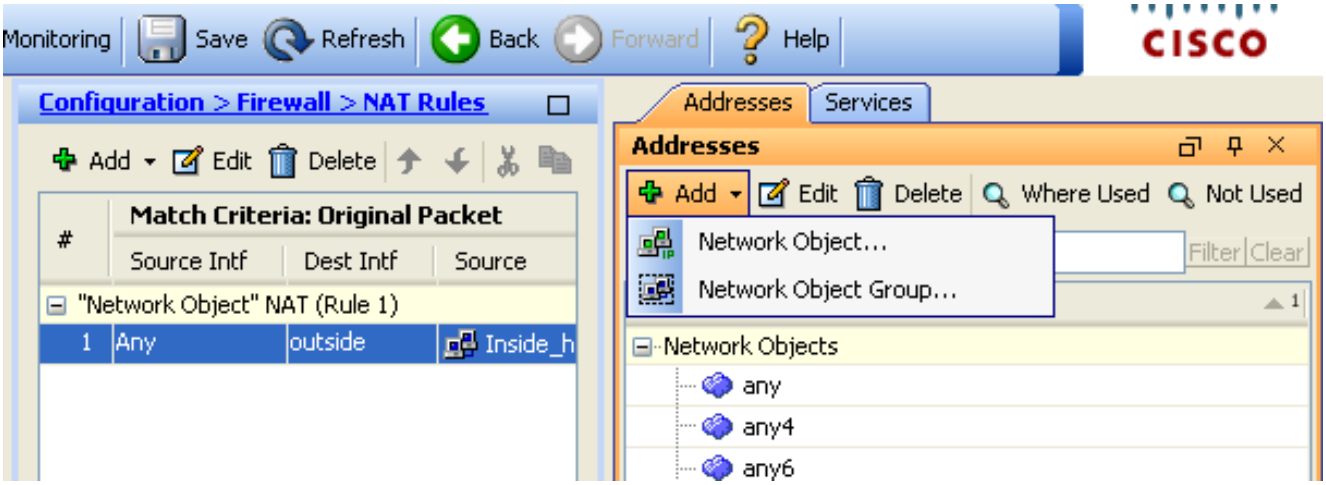
Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Permita o acesso dos host internos às redes externas com PANCADINHA

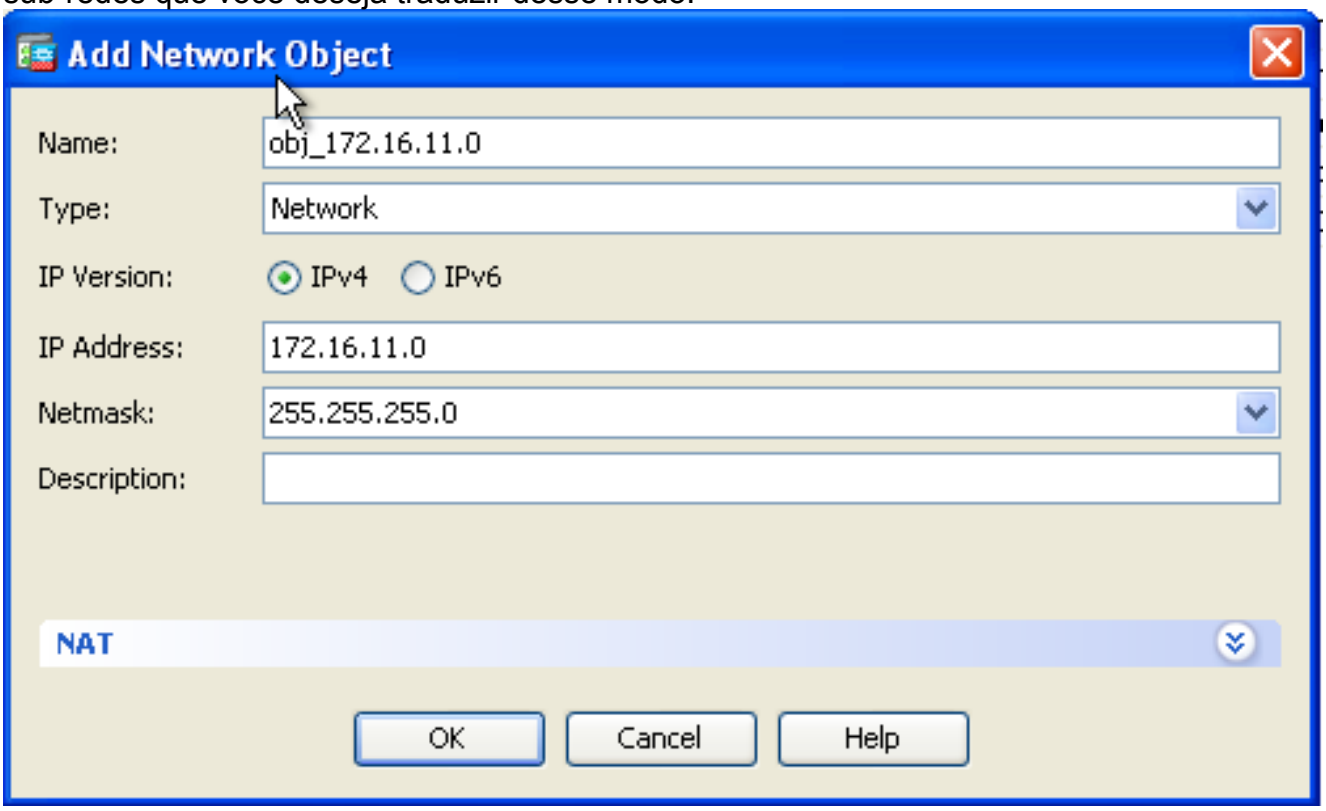
Se você quer host internos compartilhar de um único endereço público para a tradução, use a tradução de endereço de porta (PAT). Uma das configurações as mais simples da PANCADINHA envolve a tradução de todos os host internos para olhar como o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface externa. Esta é a configuração típica da PANCADINHA que é usada quando o número de endereços IP roteável disponíveis do ISP é limitado somente a alguns, ou talvez apenas um.

Termine estas etapas a fim permitir o acesso dos host internos às redes externas com PANCADINHA:

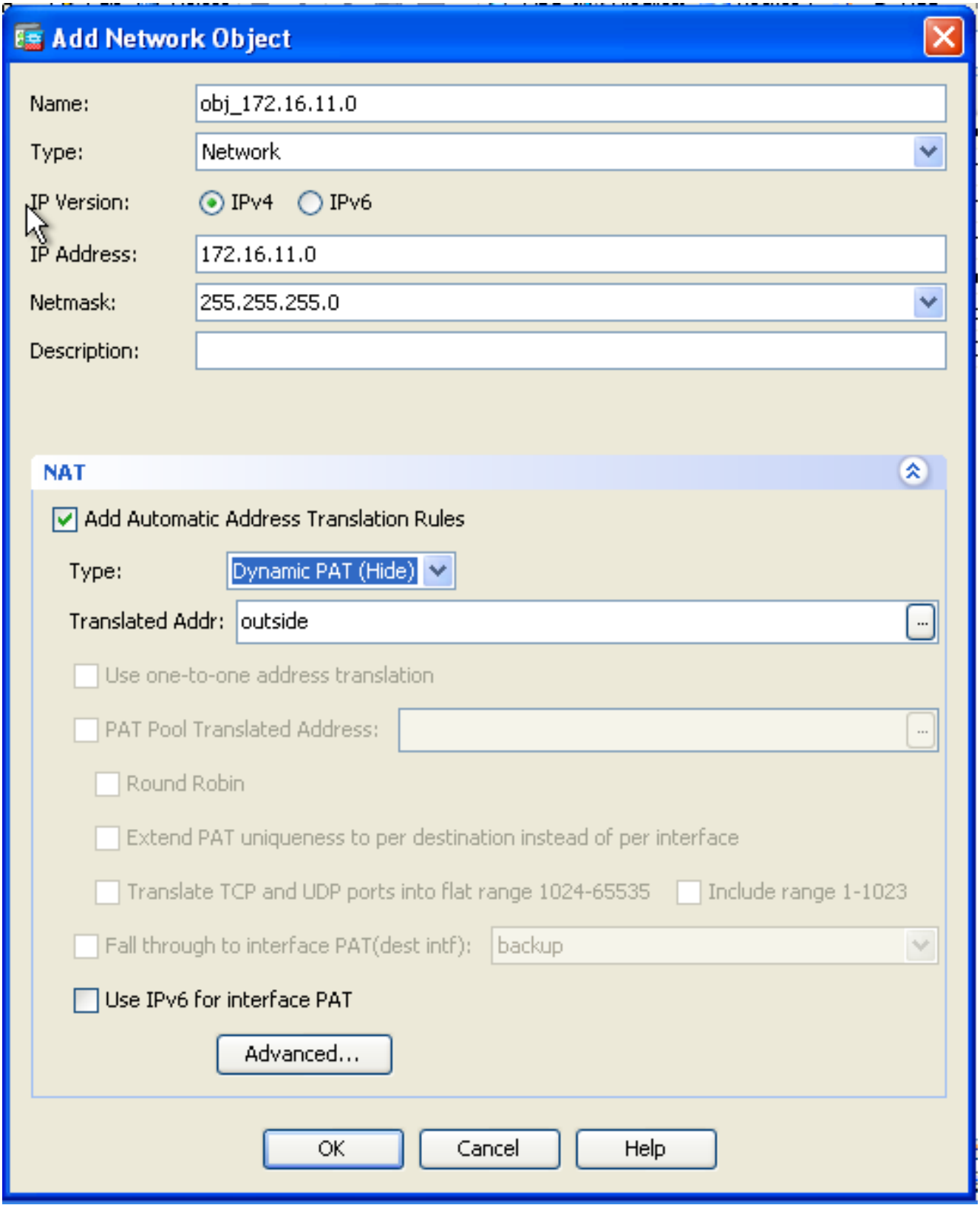
1. Escolha a **configuração** > o **Firewall** > as **regras NAT**. O clique **adiciona** e escolhe então o **objeto de rede** a fim configurar uma regra dinâmica NAT.



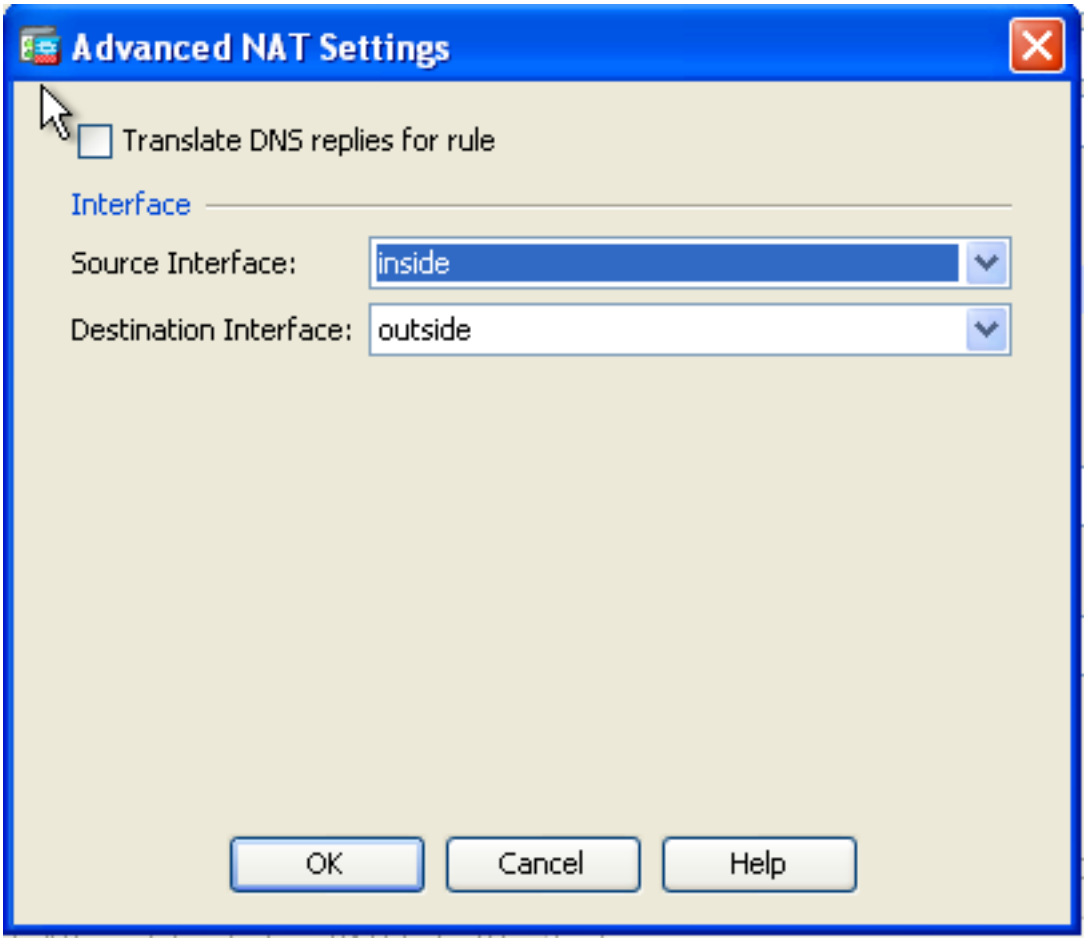
2. Configurar a rede/host/escala para que a **PANCADINHA dinâmica** é exigida. Neste exemplo, uma das sub-redes internas foi selecionado. Este processo pode ser repetido para outras sub-redes que você deseja traduzir desse modo.



3. Expanda o NAT. Verifique a caixa de verificação **automática das regras de tradução de endereço adicionar**. No tipo lista de drop-down, escolha a **PANCADINHA dinâmica (couro cru)**. No campo **traduzido do ADDR**, escolha a opção refletir a interface externa. Clique **avançado**.



4. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. Clique a **APROVAÇÃO** e o clique **aplica-se** para que as mudanças tomem o efeito.



Este é o CLI equivalente output para esta configuração da PANCADINHA:

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

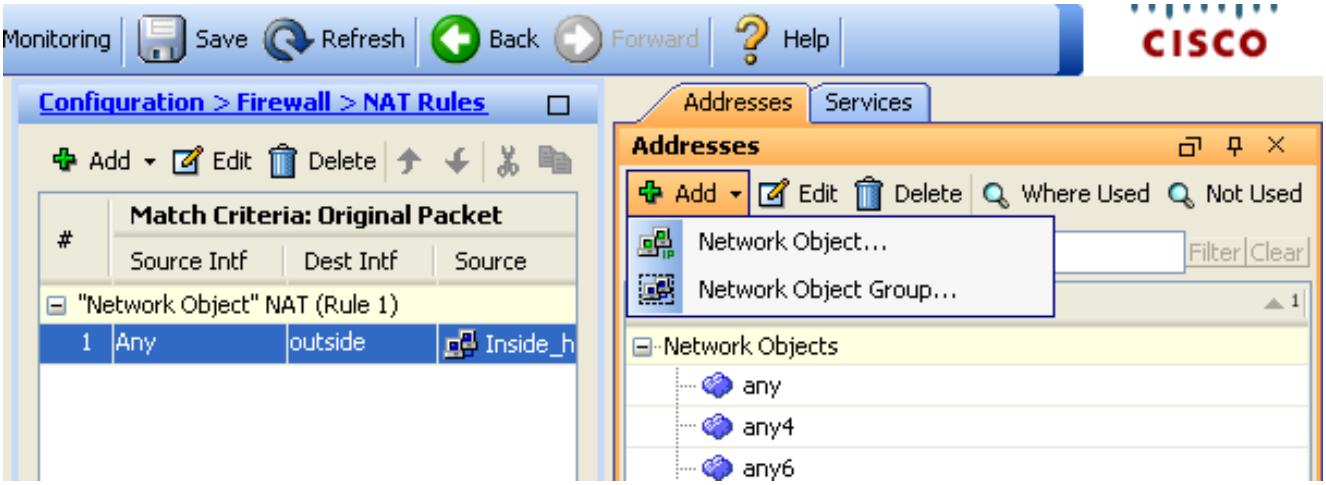
Permitir o Acesso de Host Internos às Redes Externas via NAT

Você poderia permitir que um grupo de host internos/redes alcance o mundo exterior com a configuração das regras dinâmicas NAT. Ao contrário da PANCADINHA, o NAT dinâmico atribui endereços traduzido de um conjunto de endereço. Em consequência, um host é traçado a seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido e dois anfitriões não podem compartilhar do mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido.

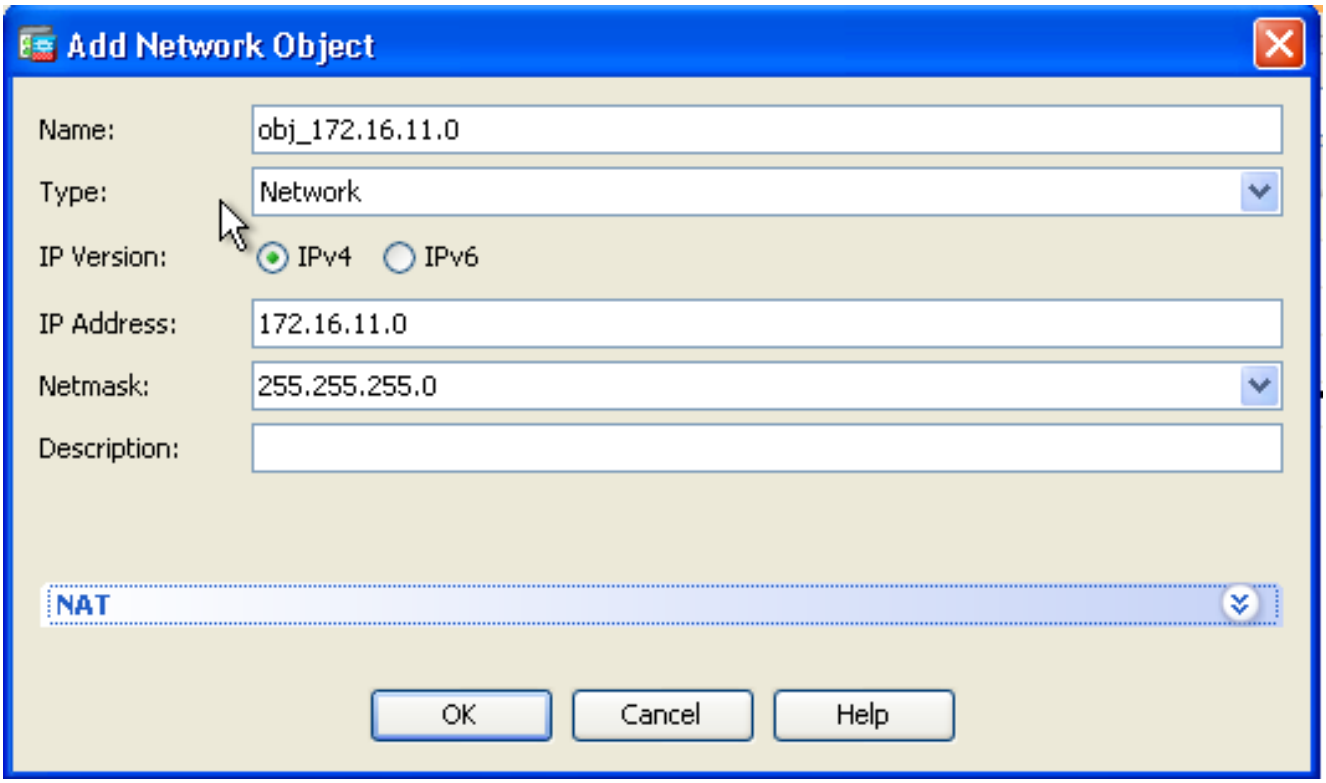
A fim realizar isto, você precisa de selecionar o endereço real dos anfitriões/redes para ser dados o acesso e então têm que ser traçados a um pool de endereços IP de Um ou Mais Servidores Cisco ICM NT traduzidos.

Termine estas etapas a fim permitir o acesso dos host internos às redes externas com NAT:

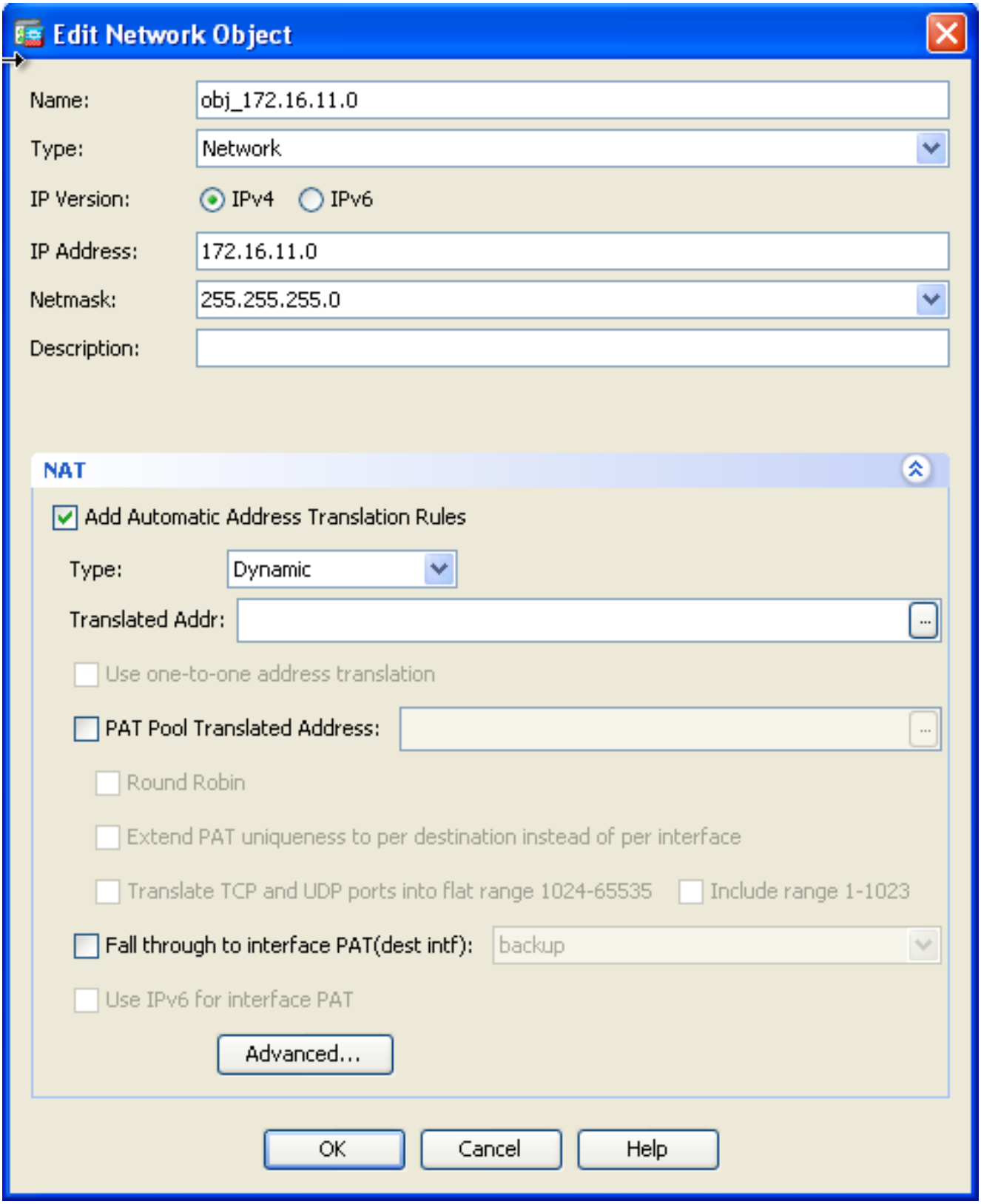
1. Escolha a **configuração** > o **Firewall** > as **regras NAT**. O clique **adiciona** e escolhe então o **objeto de rede** a fim configurar uma regra dinâmica NAT.



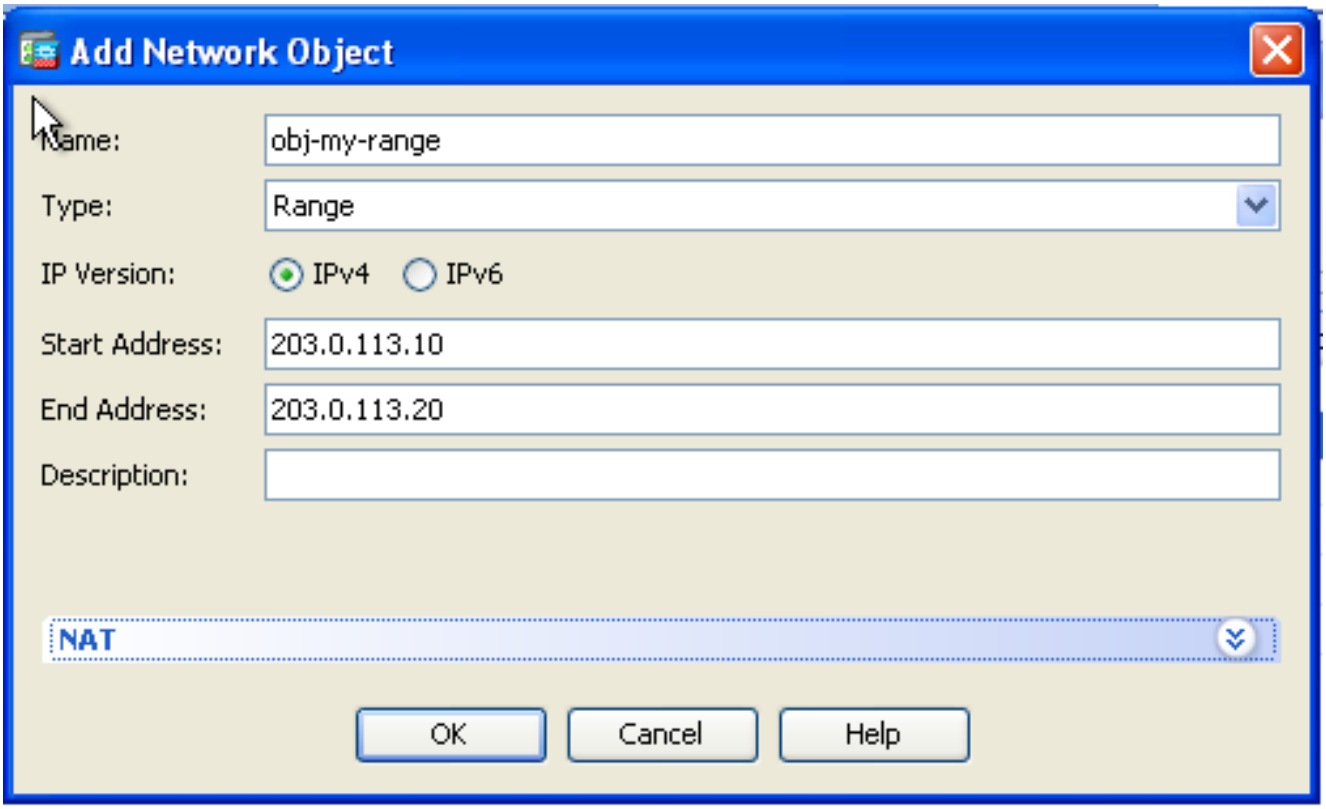
2. Configurar a rede/host/escala para que a PANCADINHA dinâmica é exigida. Neste exemplo, a *rede interna* inteira foi selecionada.



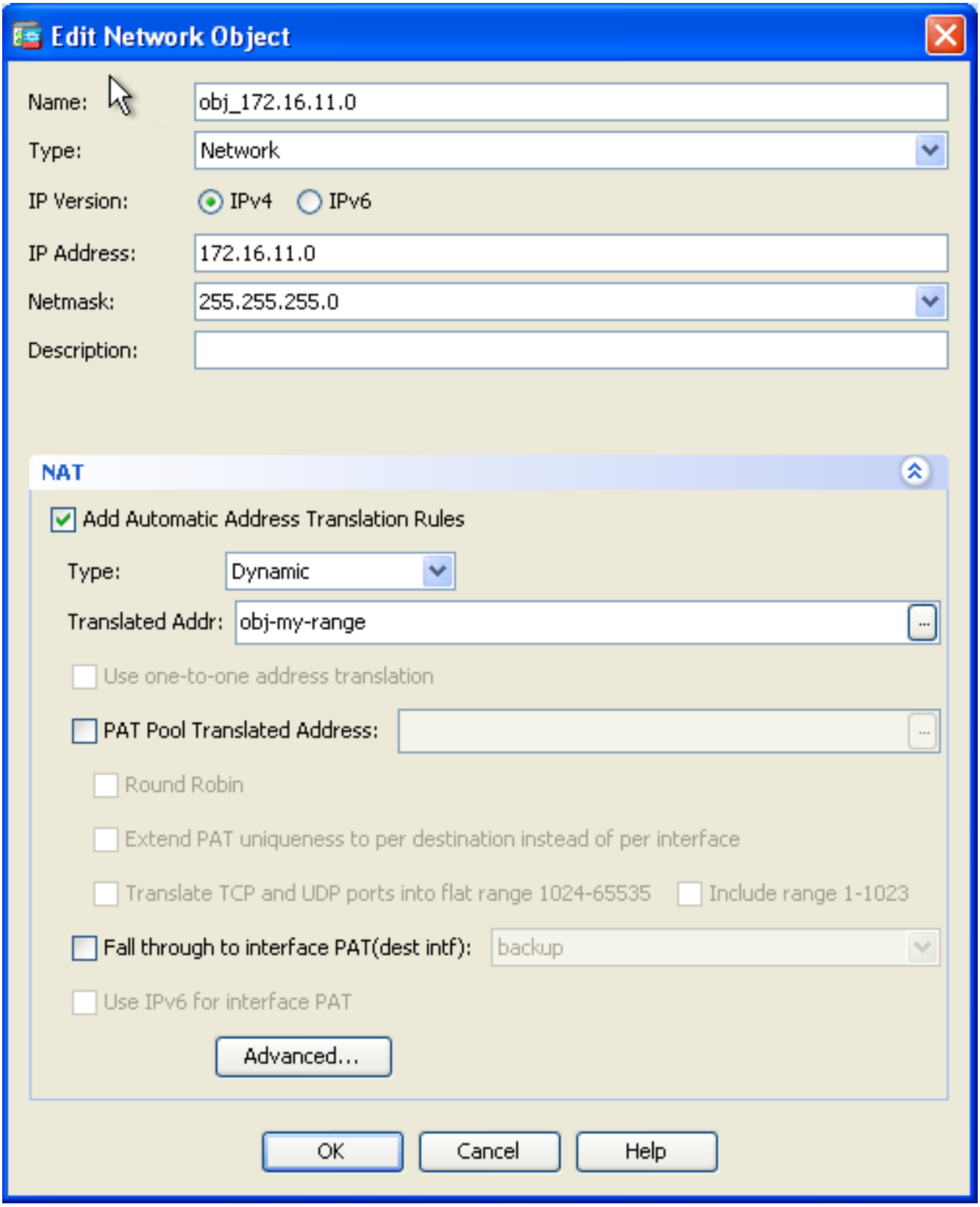
3. Expanda o NAT. Verifique a caixa de verificação **automática das regras de tradução de endereço adicionar**. No tipo lista de drop-down, escolha **dinâmico**. No campo traduzido do ADDR, escolha a seleção apropriada. Clique **avançado**.



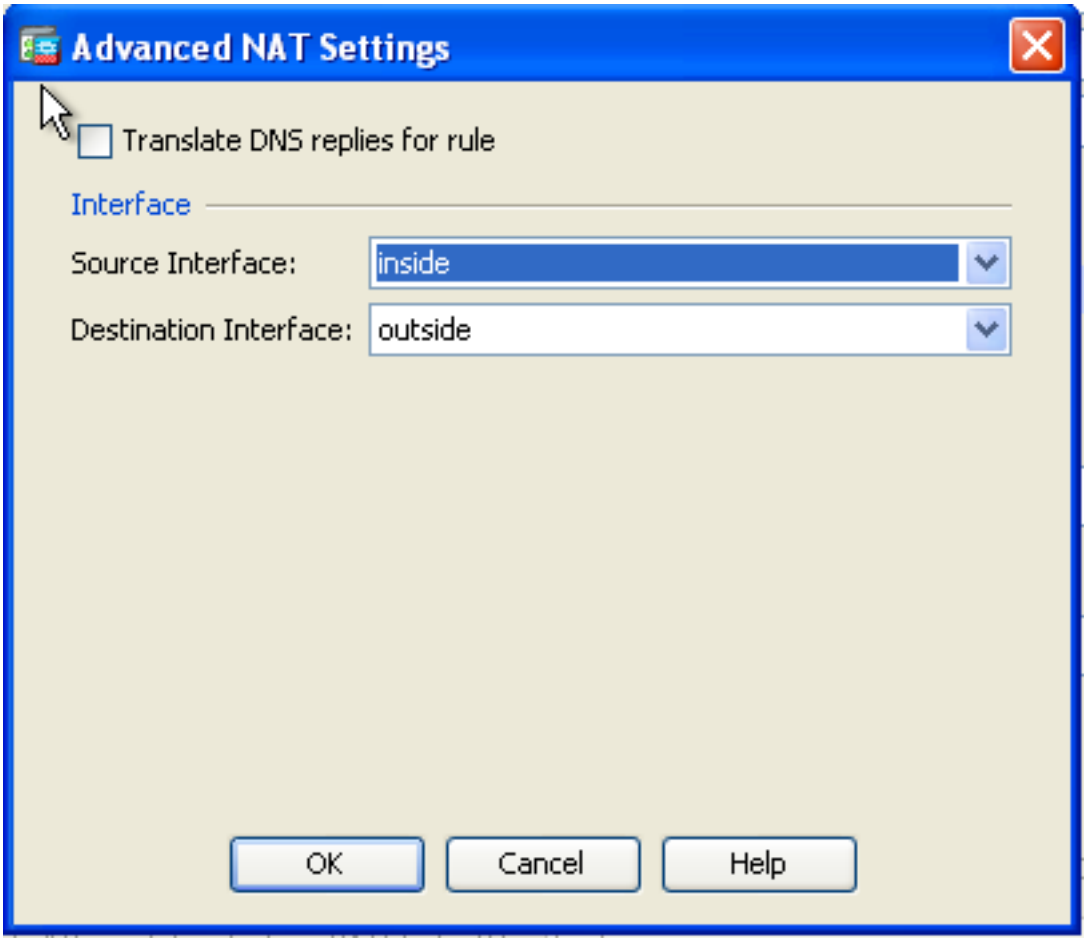
4. O clique **adiciona** para adicionar o objeto de rede. No tipo lista de drop-down, escolha a **escala**. Nos campos de endereço do endereço de início e da extremidade, incorpore os endereços IP de Um ou Mais Servidores Cisco ICM NT começando e de término da PANCADINHA. Clique em **OK**.



5. No campo traduzido do ADDR, escolha o objeto do endereço. Clique **avançado** a fim selecionar a fonte e as interfaces de destino.



6. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. Clique a **APROVAÇÃO** e o clique **aplica-se** para que as mudanças tomem o efeito.

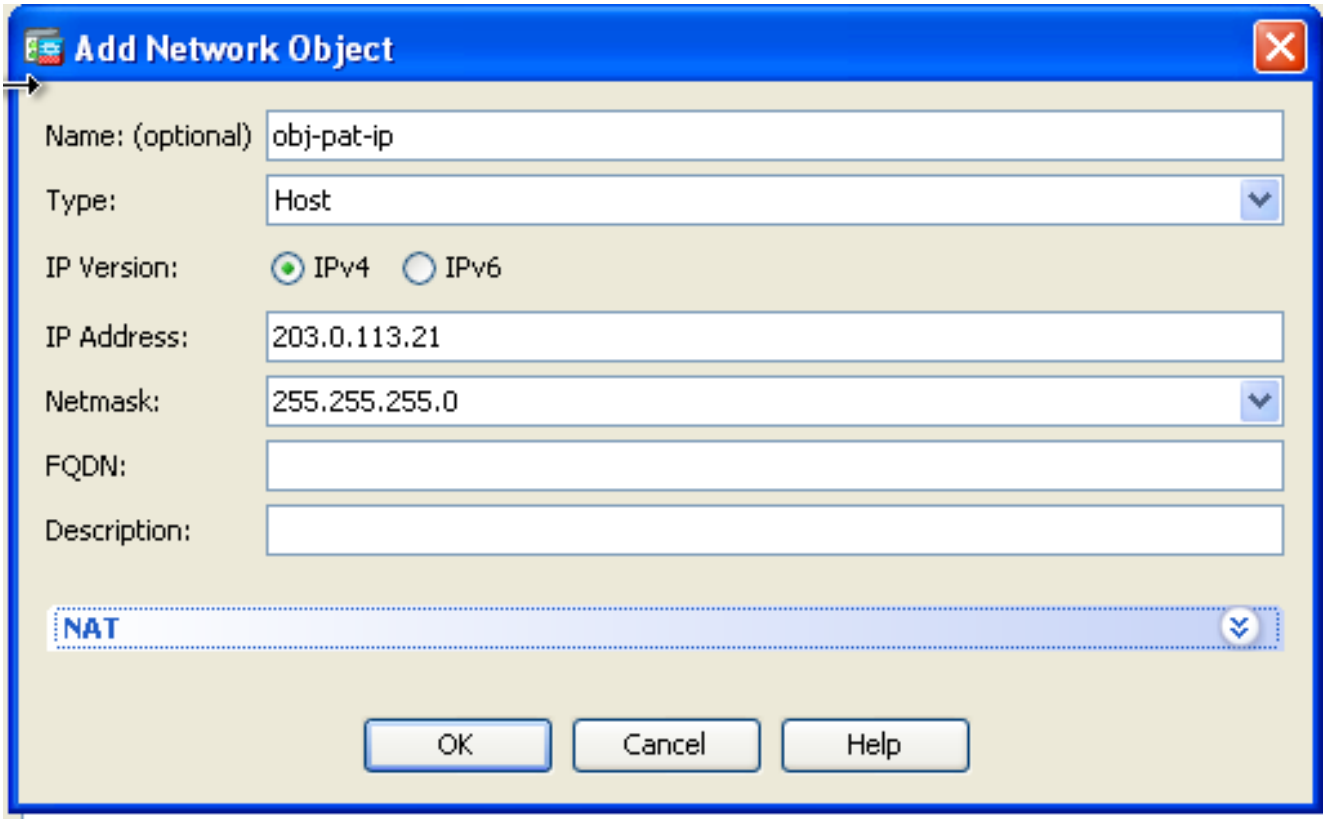


Este é o CLI equivalente output para esta configuração ASDM:

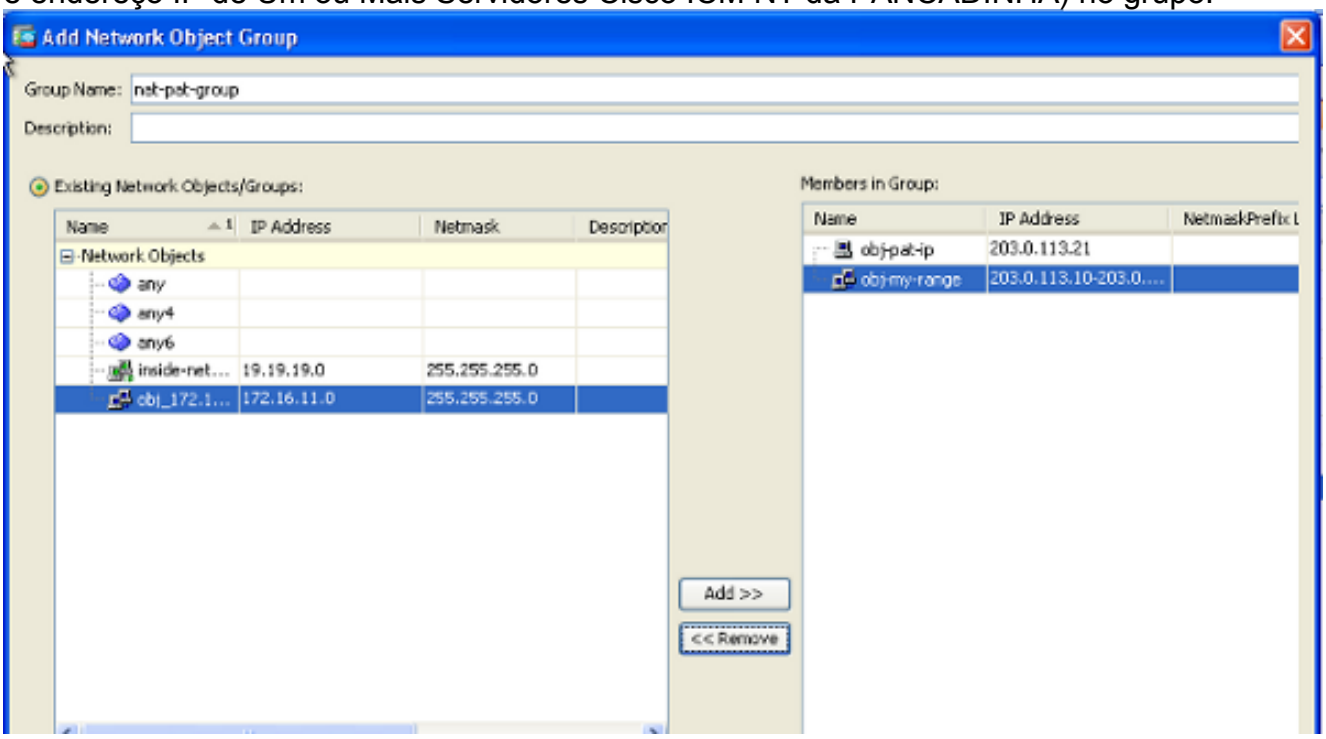
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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

Conforme esta configuração, os anfitriões na rede de 172.16.11.0 obterão traduzidos a todo o endereço IP de Um ou Mais Servidores Cisco ICM NT do conjunto NAT, 203.0.113.10 - 203.0.113.20. Se o pool traçado tem menos endereços do que o grupo real, você poderia ser executado fora dos endereços. Em consequência, você poderia tentar executar o NAT dinâmico com backup dinâmico da PANCADINHA ou você poderia tentar expandir o pool existente.

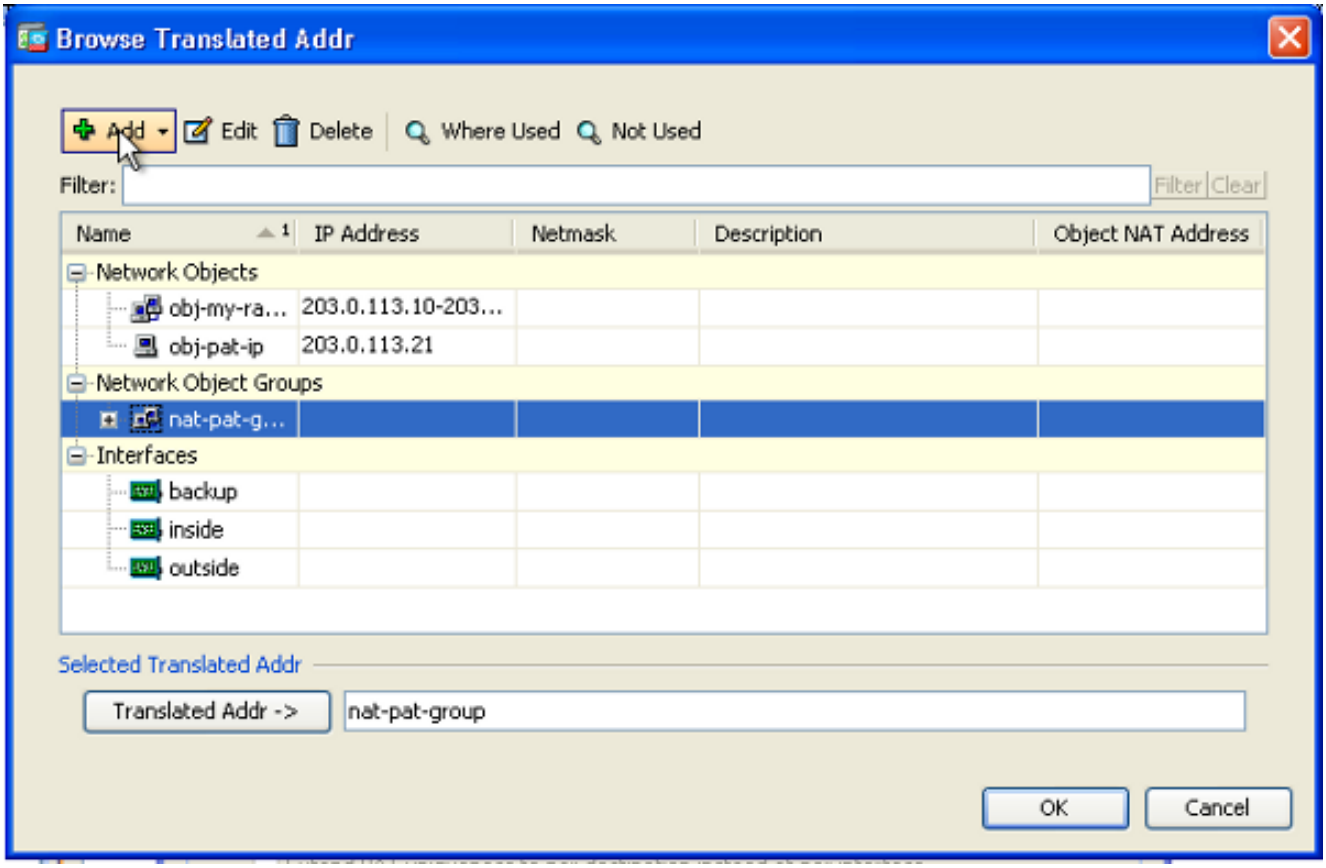
1. Repita etapas 1 3 na configuração precedente e o clique **adiciona** mais uma vez a fim adicionar um objeto de rede. No tipo lista de drop-down, escolha o **host**. No campo do endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do backup da PANCADINHA. Clique em **OK**.



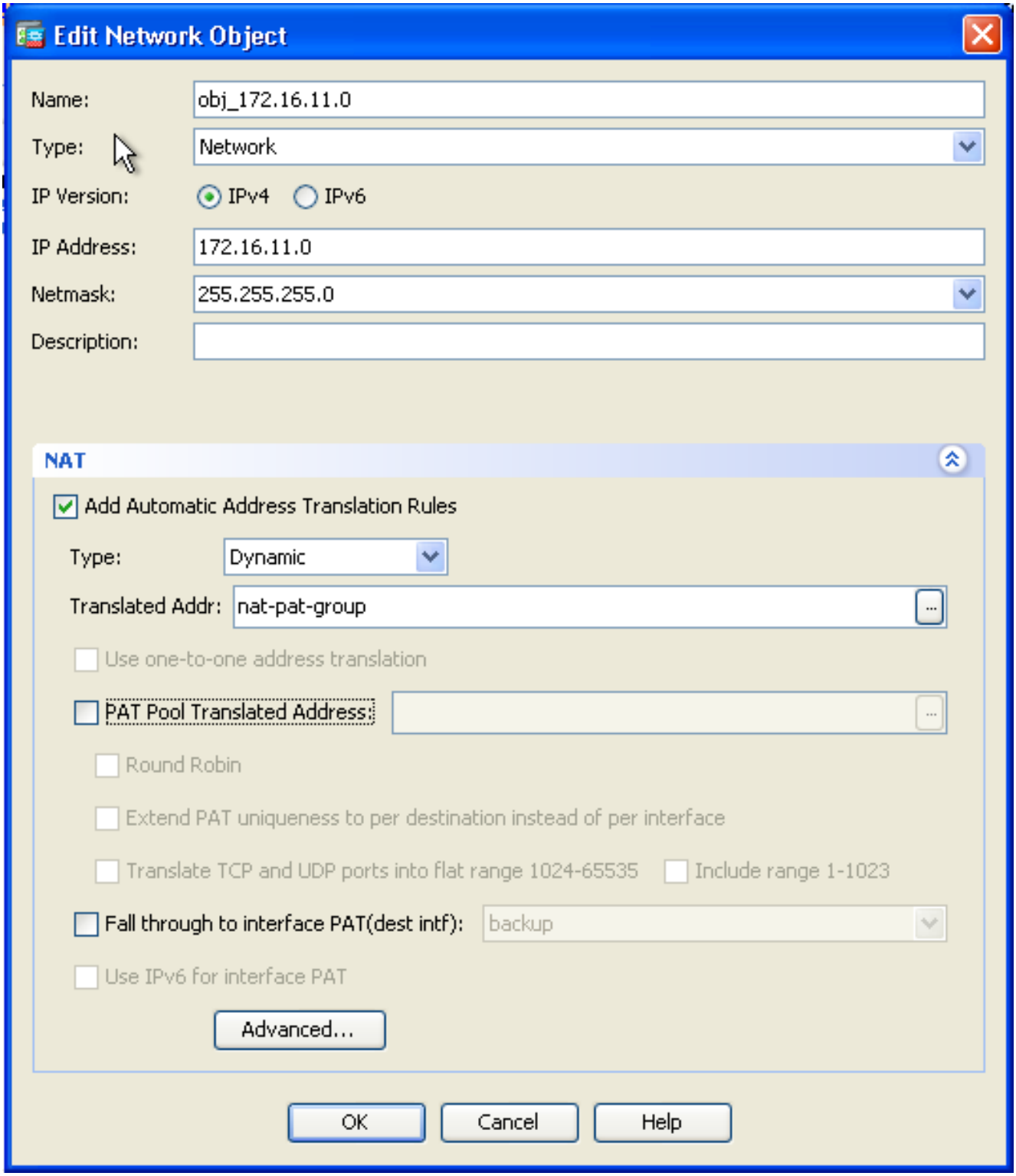
2. O clique **adiciona** para adicionar um grupo de objeto de rede. No campo de nome do grupo, dê entrada com um nome do grupo e **adicionar** ambos os objetos do endereço (escala NAT e endereço IP de Um ou Mais Servidores Cisco ICM NT da PANCADINHA) no grupo.



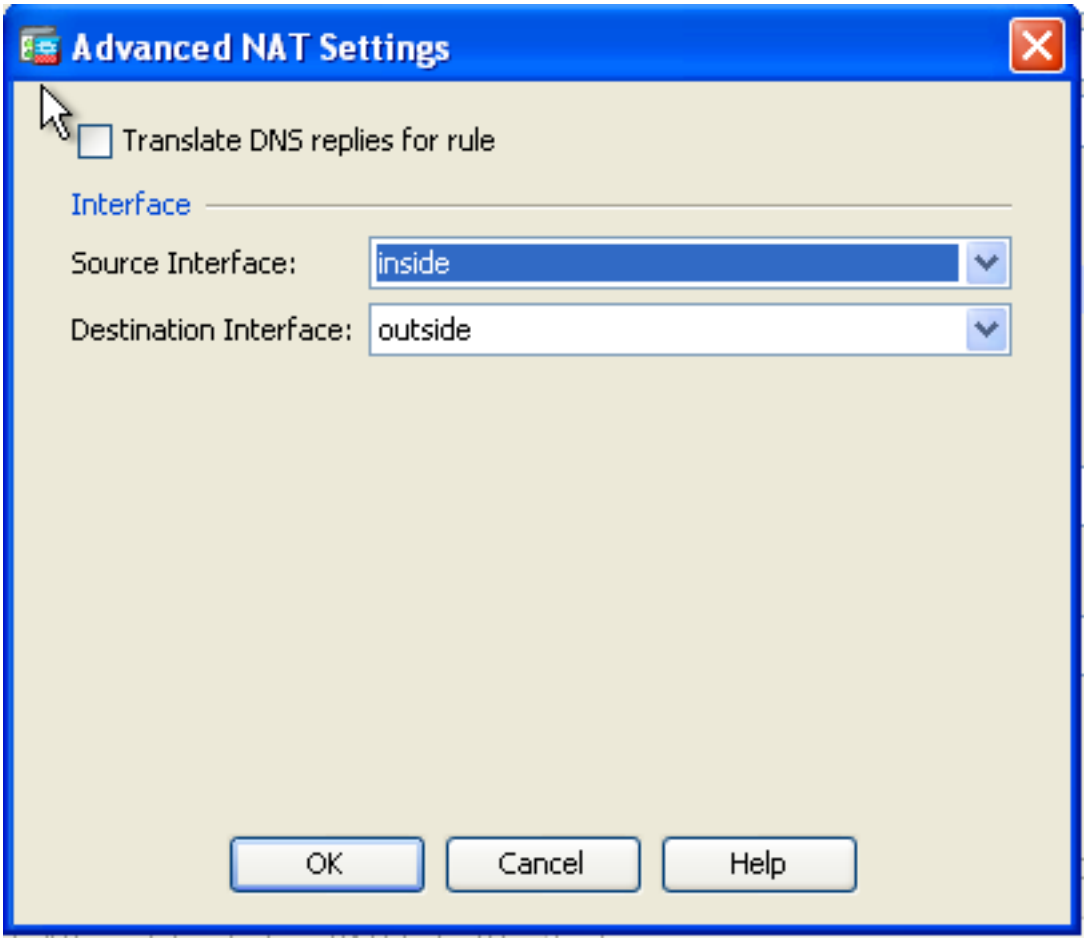
3. Escolha a regra configurada NAT e mude o ADDR traduzido para ser “NAT-pancadinha-grupo” do grupo recentemente configurado (era previamente a “OBJ-meu-escala "). Clique em **OK**.



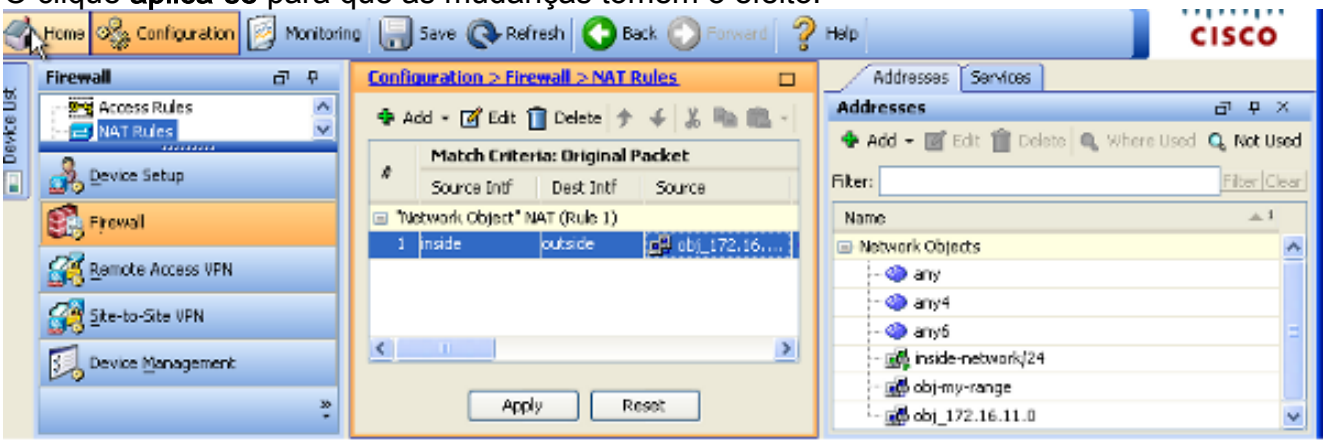
4. Clique a **APROVAÇÃO** a fim adicionar a regra NAT. Clique **avançado** a fim selecionar a fonte e as interfaces de destino.



5. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. Clique em **OK**.



6. O clique **aplica-se** para que as mudanças tomem o efeito.



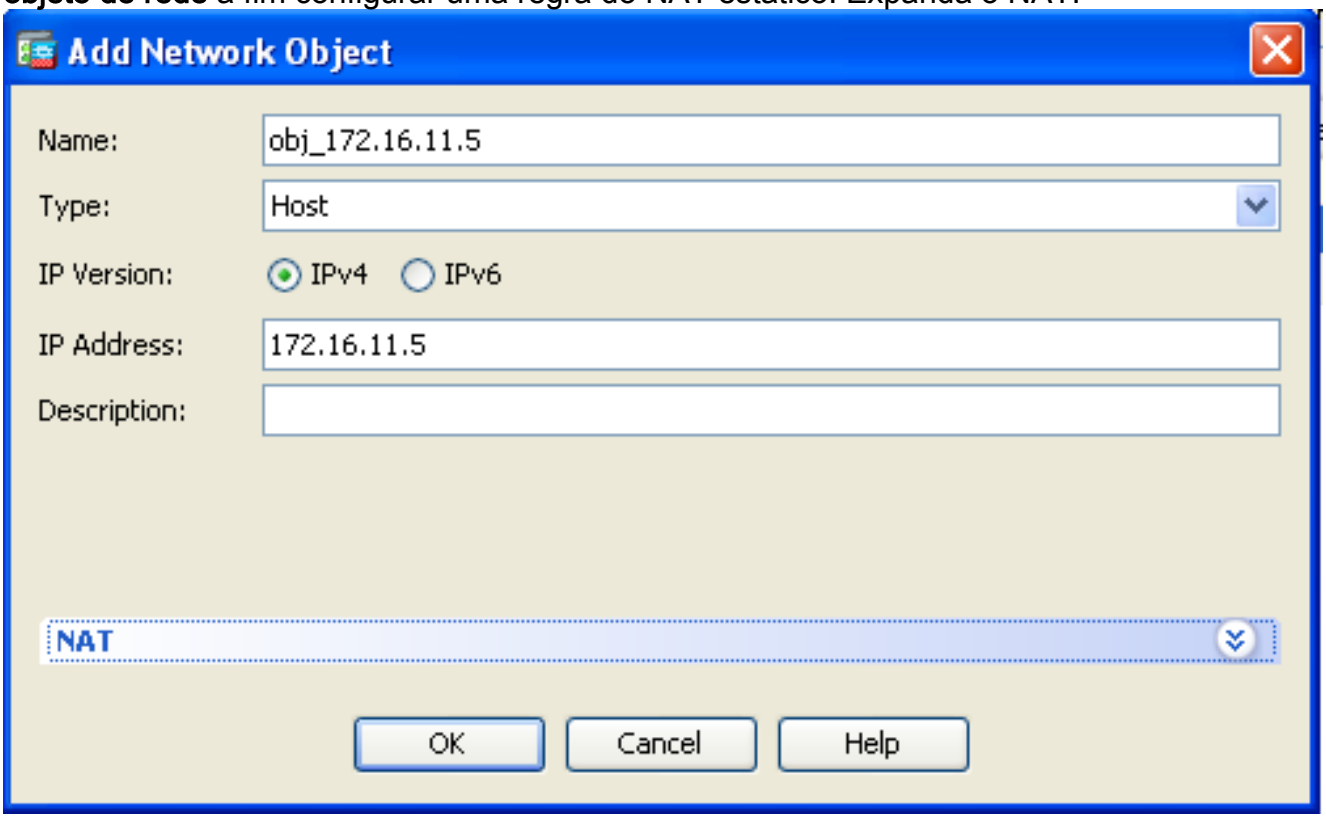
Este é o CLI equivalente output para esta configuração ASDM:

```
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
```

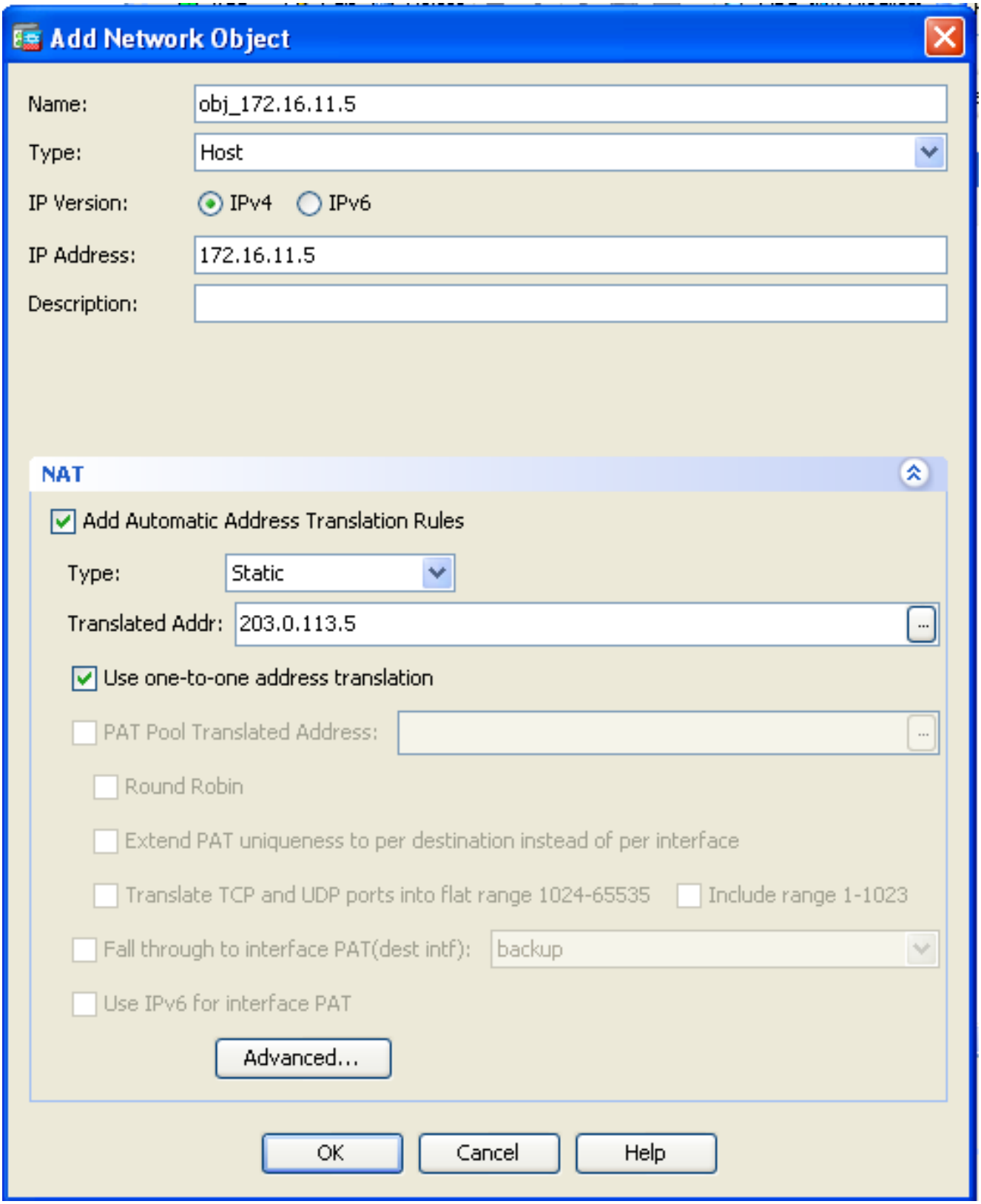
Permita o acesso dos hosts não confiáveis aos hosts em sua rede confiável

Isto pode ser conseguido com o aplicativo de uma tradução NAT estática e de uma regra do acesso permitir aqueles anfitriões. Você é exigido configurar este sempre que um usuário externo gostaria de alcançar todo o server que se sentar em sua rede interna. O server na rede interna terá um endereço IP privado que não seja roteável no Internet. Em consequência, você precisa de traduzir esse endereço IP privado a um endereço IP público com uma regra do NAT estático. Supõe que você tem um servidor interno (172.16.11.5). A fim fazer este trabalho, você precisa de traduzir este endereço IP do servidor privado a um endereço IP público. Este exemplo descreve como executar o NAT estático bidirecional para traduzir 172.16.11.5 a 203.0.113.5.

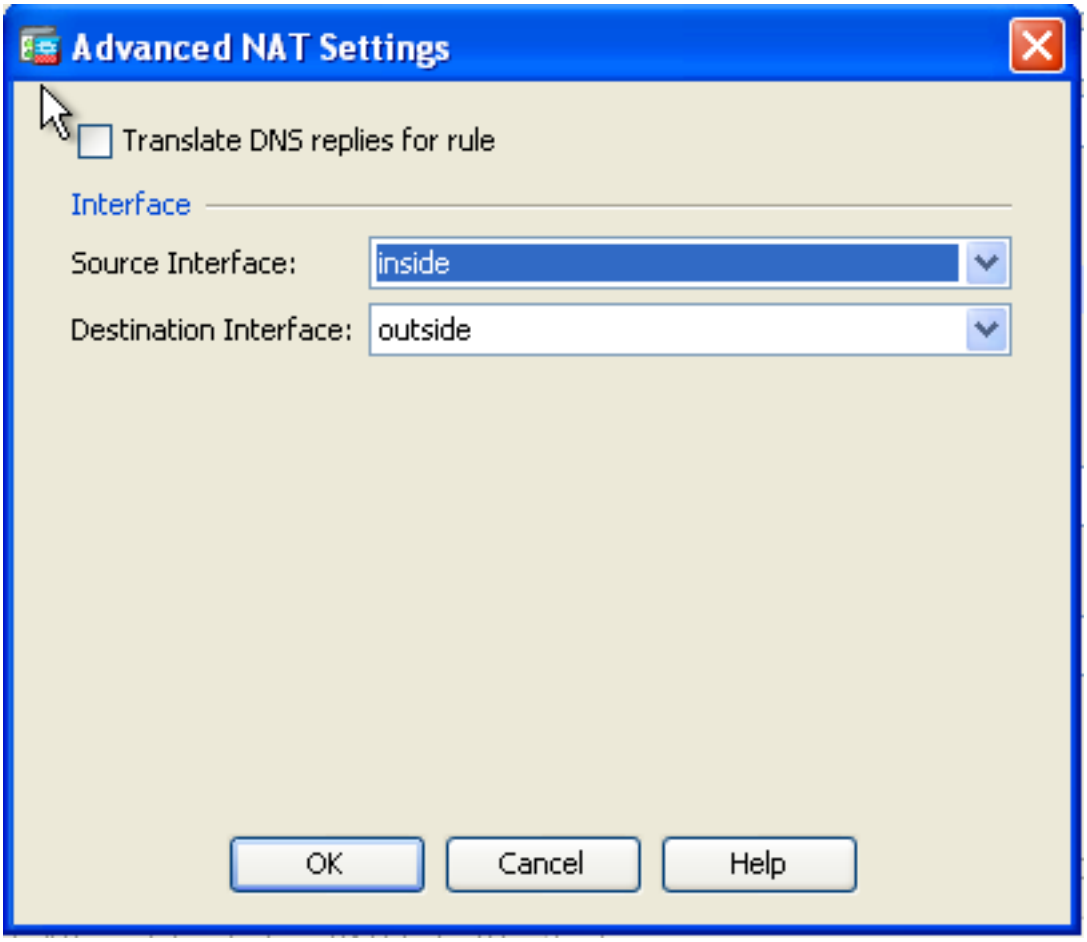
1. Escolha a **configuração** > o **Firewall** > as **regras NAT**. O clique **adiciona** e escolhe então o **objeto de rede** a fim configurar uma regra do NAT estático. Expanda o NAT.



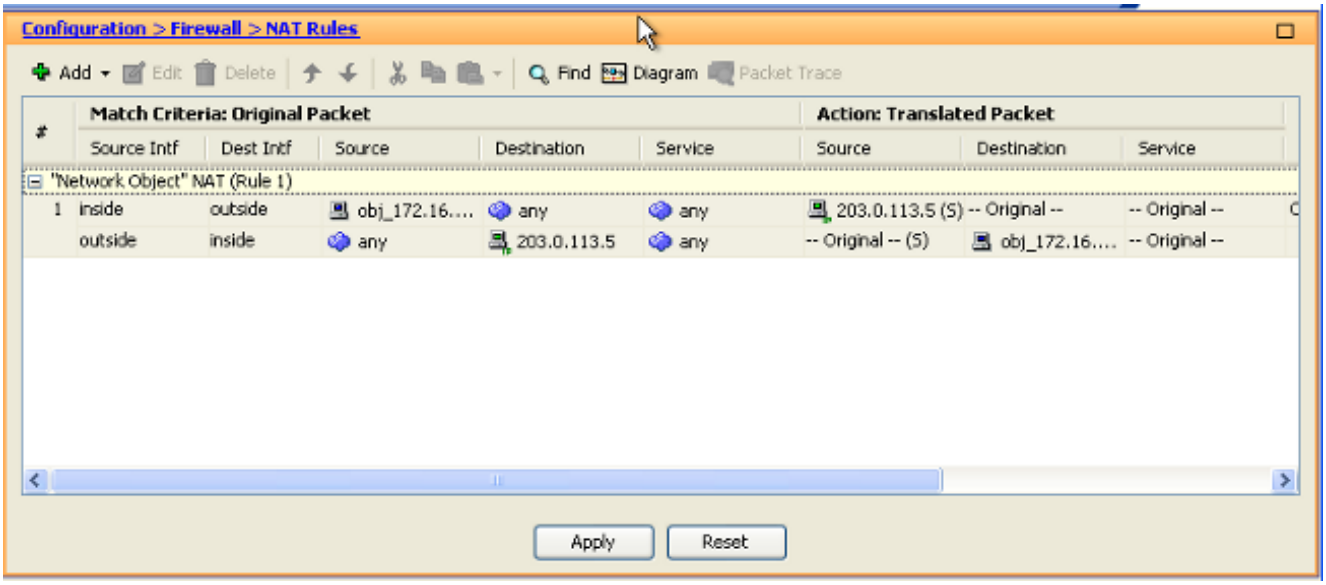
2. Verifique a caixa de verificação **automática das regras de tradução de endereço adicionar**. No tipo lista de drop-down, escolha a **estática.** No campo traduzido do ADDR, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT. Clique **avançado** a fim selecionar a fonte e as interfaces de destino.



3. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. Clique em **OK**.



4. Você pode ver a entrada NAT estática configurada aqui. O clique **aplica-se** a fim enviar este ao ASA.



Este é o CLI equivalente output para esta configuração de NAT:

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

Identidade estática NAT

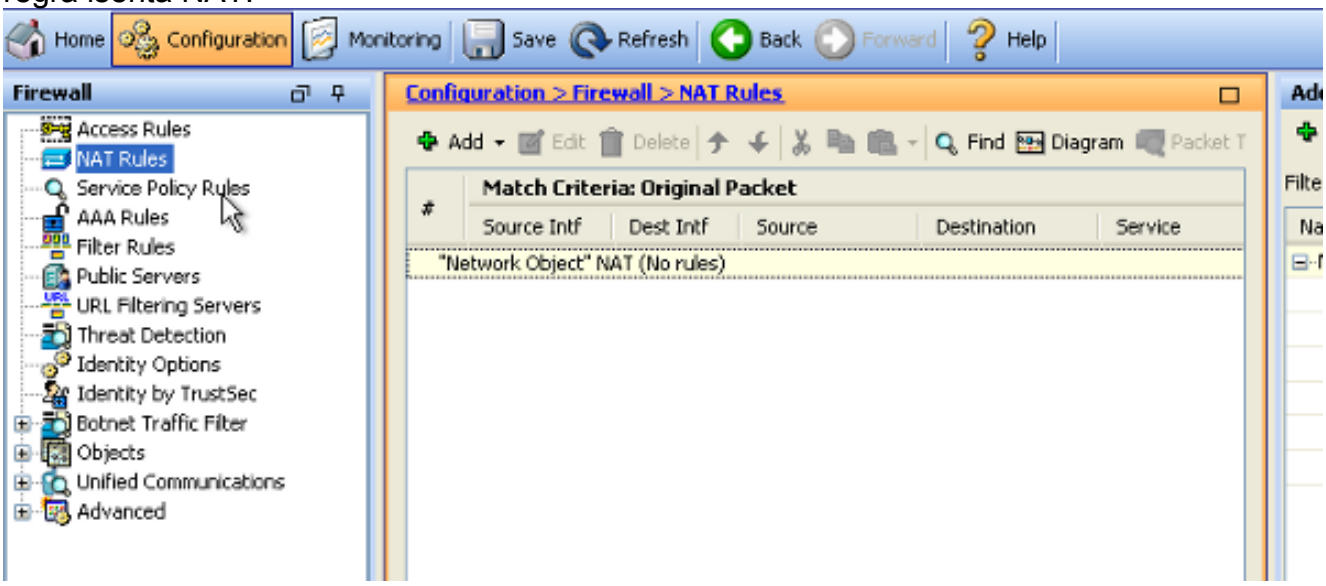
O NAT isento é uns recursos úteis onde os usuários internos tentem alcançar um host remoto/server VPN ou alguns host/server hospedado atrás de toda a outra relação do ASA sem conclusão de um NAT. A fim conseguir isto, o servidor interno, que têm um endereço IP privado,

será identidade traduzida a se e que é permitido por sua vez alcançar o destino que executa um NAT.

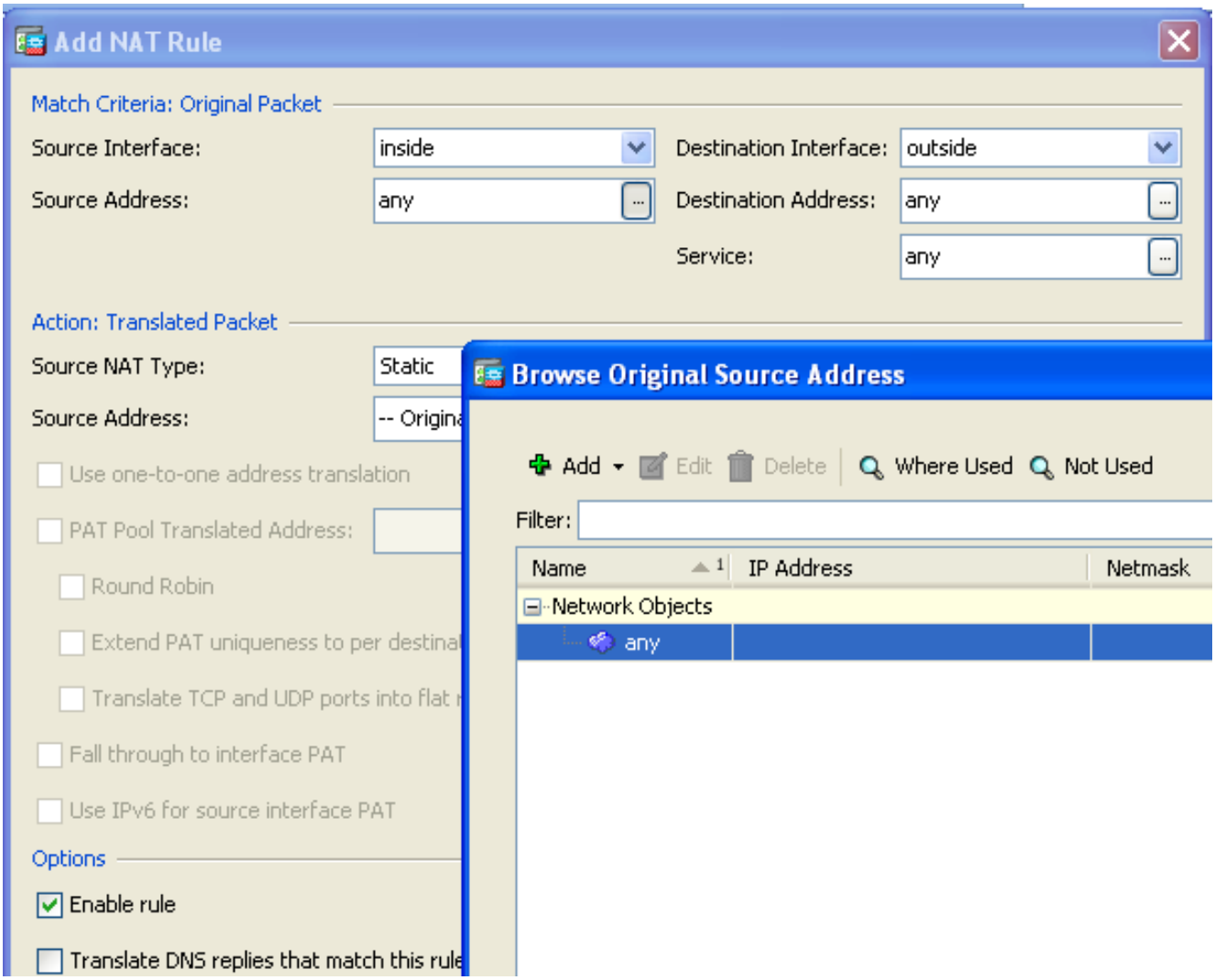
Neste exemplo, o host interno 172.16.11.15 precisa de alcançar o servidor de VPN remoto 172.20.21.15.

Termine estas etapas a fim permitir o acesso dos host internos à rede VPN remota com conclusão de um NAT:

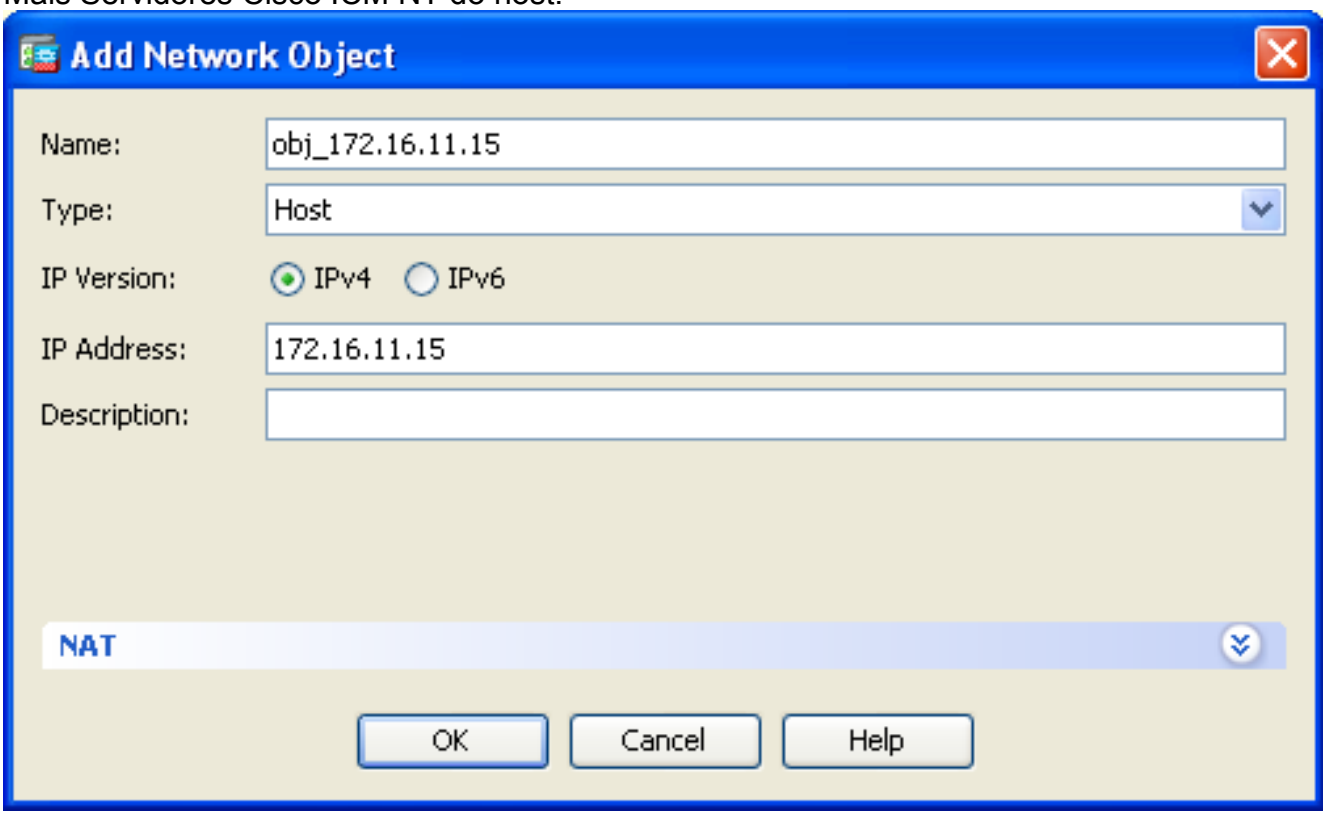
1. Escolha a **configuração** > o **Firewall** > as **regras NAT**. O clique **adiciona** a fim configurar uma regra isenta NAT.



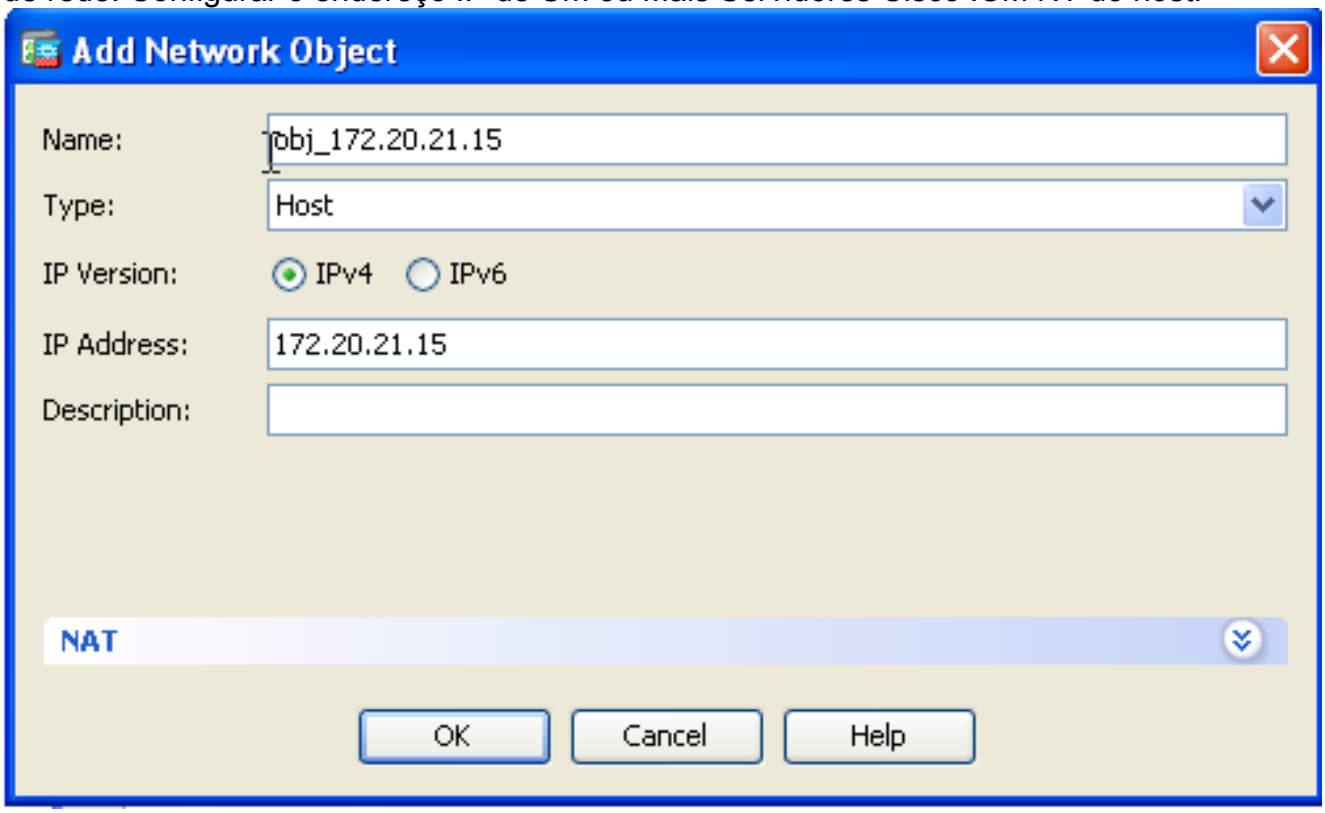
2. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. No campo de endereço de origem, escolha a entrada apropriada.



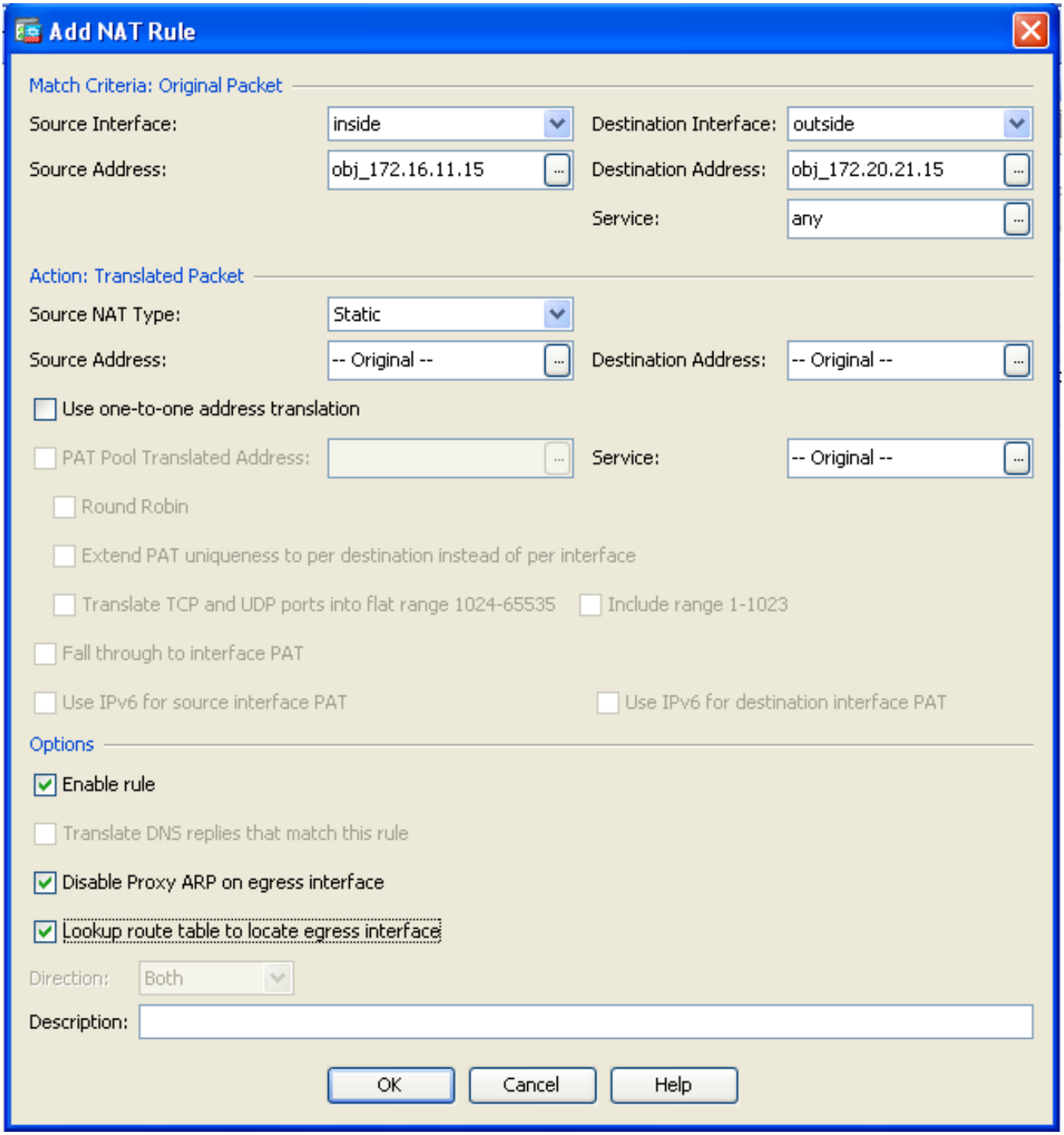
3. O clique **adiciona** a fim adicionar um objeto de rede. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT do host.



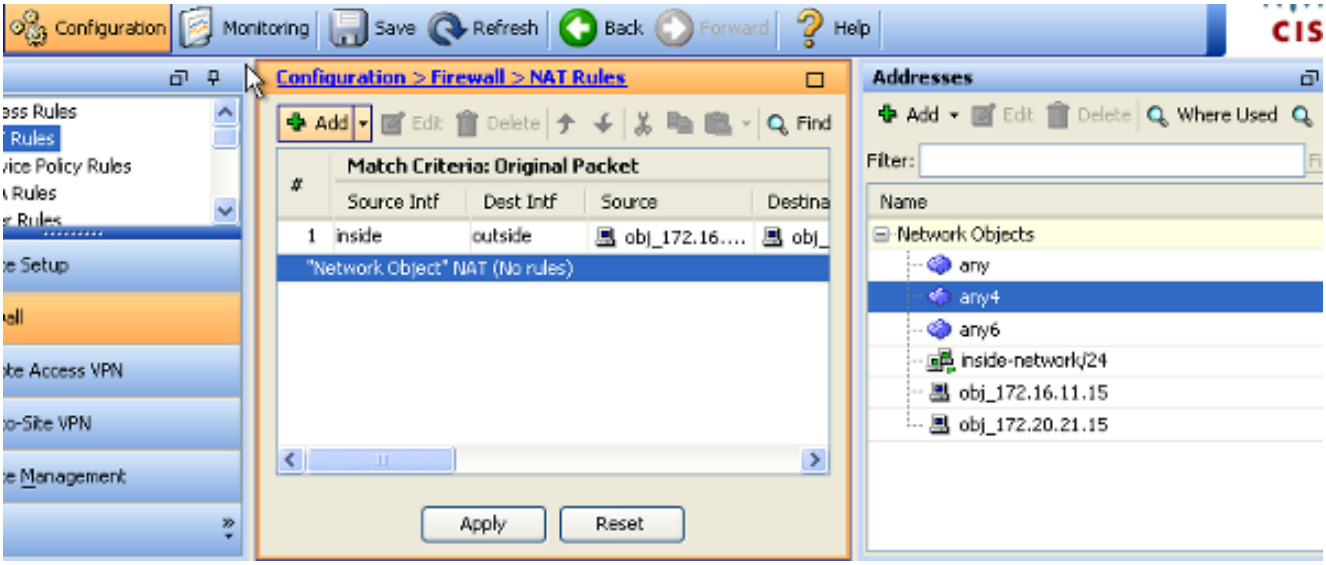
4. Similarmente, consulte o **endereço de destino**. O clique **adiciona** a fim adicionar um objeto de rede. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT do host.



5. Escolha os objetos configurados do endereço de origem e do endereço de destino. Verifique o **proxy ARP do desabilitação na interface de saída** e na **tabela de rota da consulta para encontrar** caixas de seleção da **interface de saída**. Clique em **OK**.



6. O clique **aplica-se** para que as mudanças tomem o efeito.



Este é o CLI equivalente output para o NAT isento ou a configuração de NAT da identidade:

```
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
```

Redirecionamento de porta (transmissão) com estática

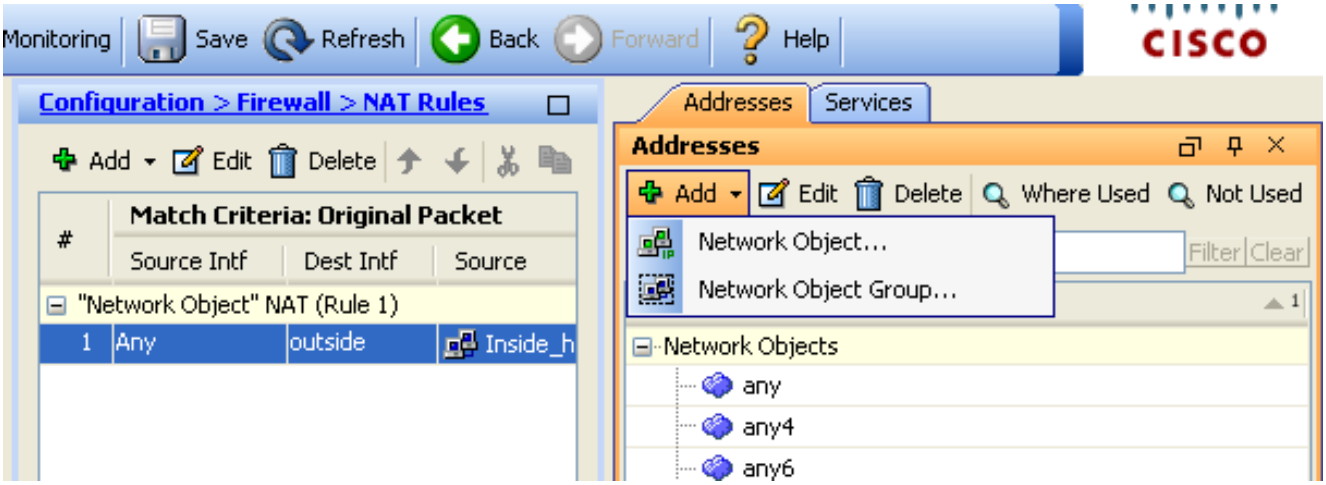
A transmissão ou o redirecionamento de porta da porta são uns recursos úteis onde os usuários externos tentem alcançar um servidor interno em uma porta específica. A fim conseguir isto, o servidor interno, que tem um endereço IP privado, será traduzido a um endereço IP público que seja permitido por sua vez o acesso para a porta específica.

Neste exemplo, o usuário externo quer alcançar o servidor SMTP, 203.0.115.15 na porta 25. Isto é realizado em duas etapas:

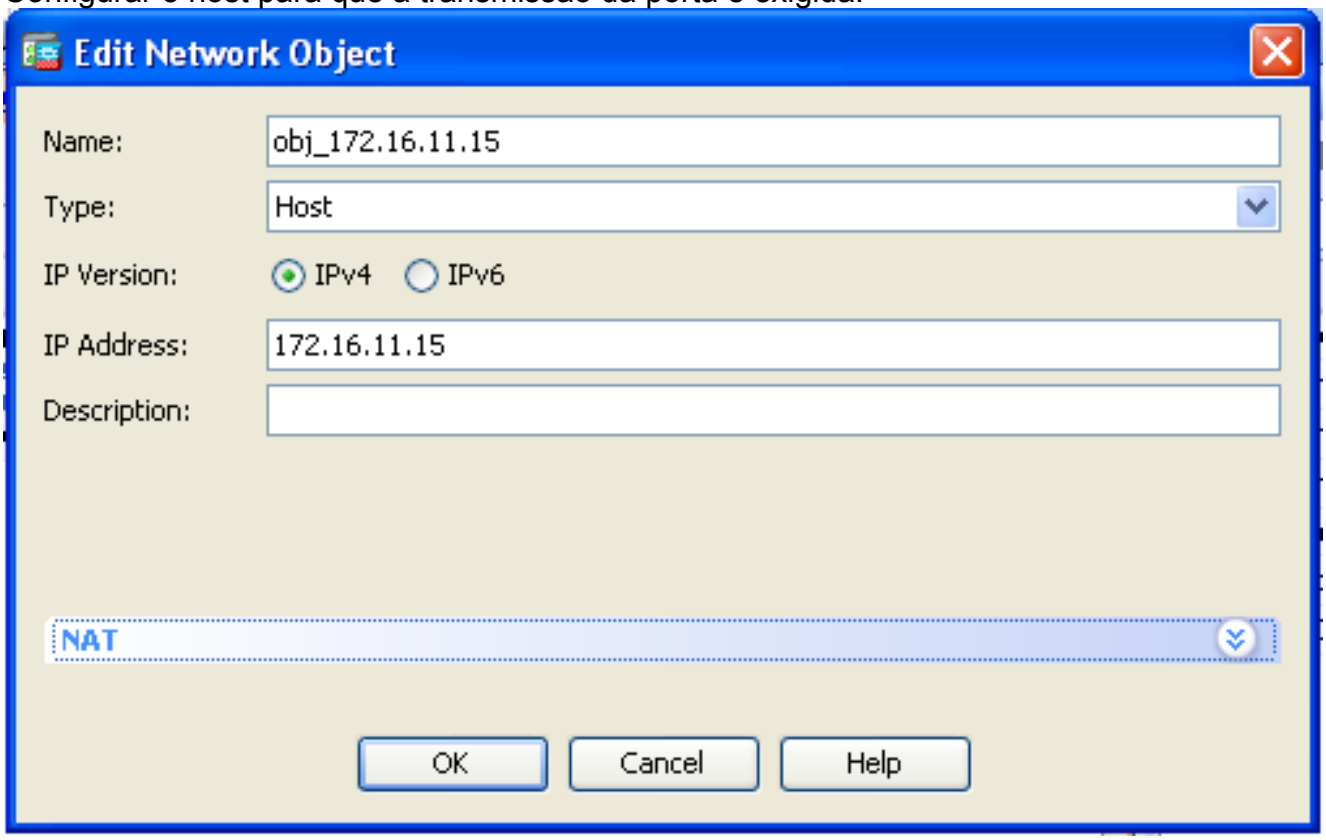
1. Traduza o servidor de e-mail interno, 172.16.11.15 na porta 25, ao endereço IP público, 203.0.115.15 na porta 25.
2. Permita o acesso ao mail server público, 203.0.115.15 na porta 25.

Quando o usuário externo tenta alcançar o server, 203.0.115.15 na porta 25, este tráfego está reorientado ao servidor de e-mail interno, 172.16.11 15 na porta 25.

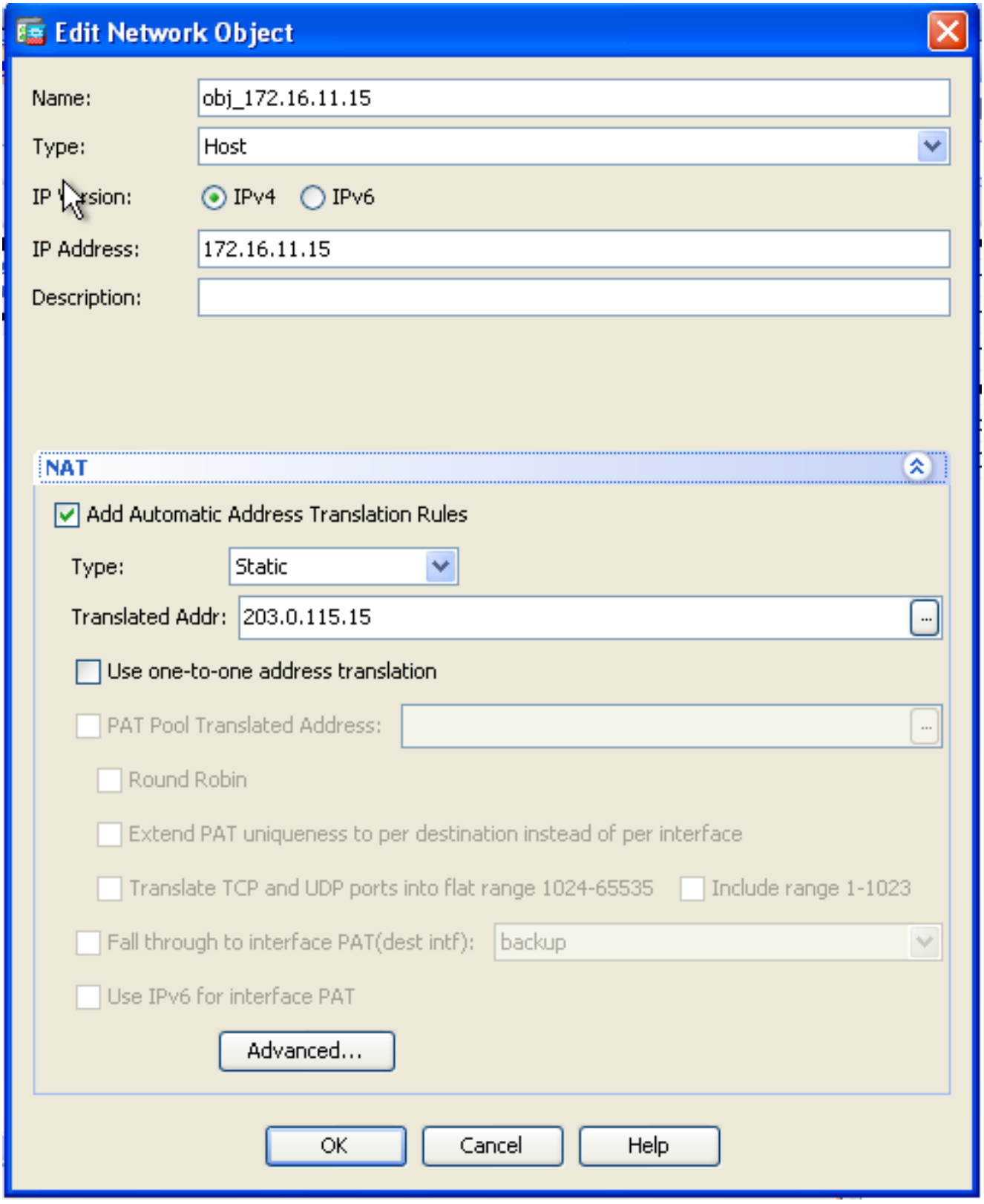
1. Escolha a **configuração > o Firewall > as regras NAT**. O clique **adiciona** e escolhe então o **objeto de rede** a fim configurar uma regra do NAT estático.



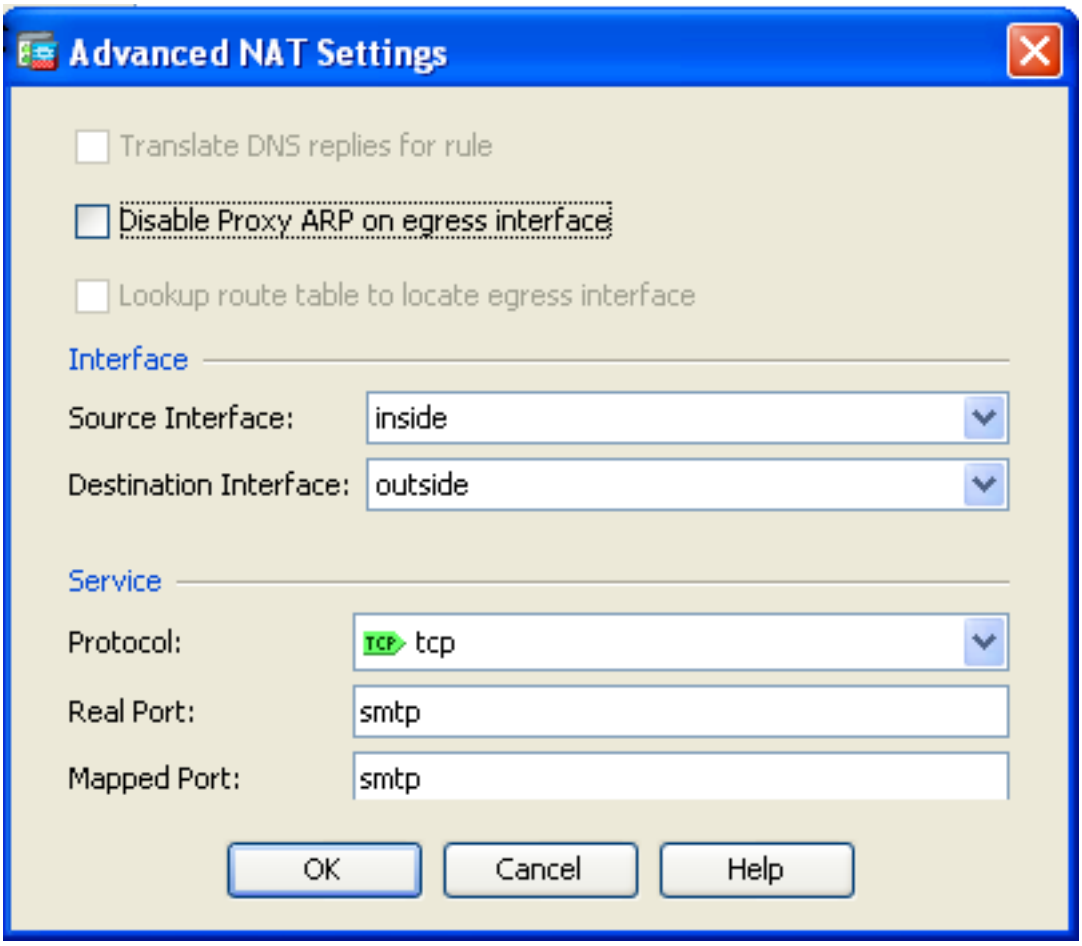
2. Configurar o host para que a transmissão da porta é exigida.



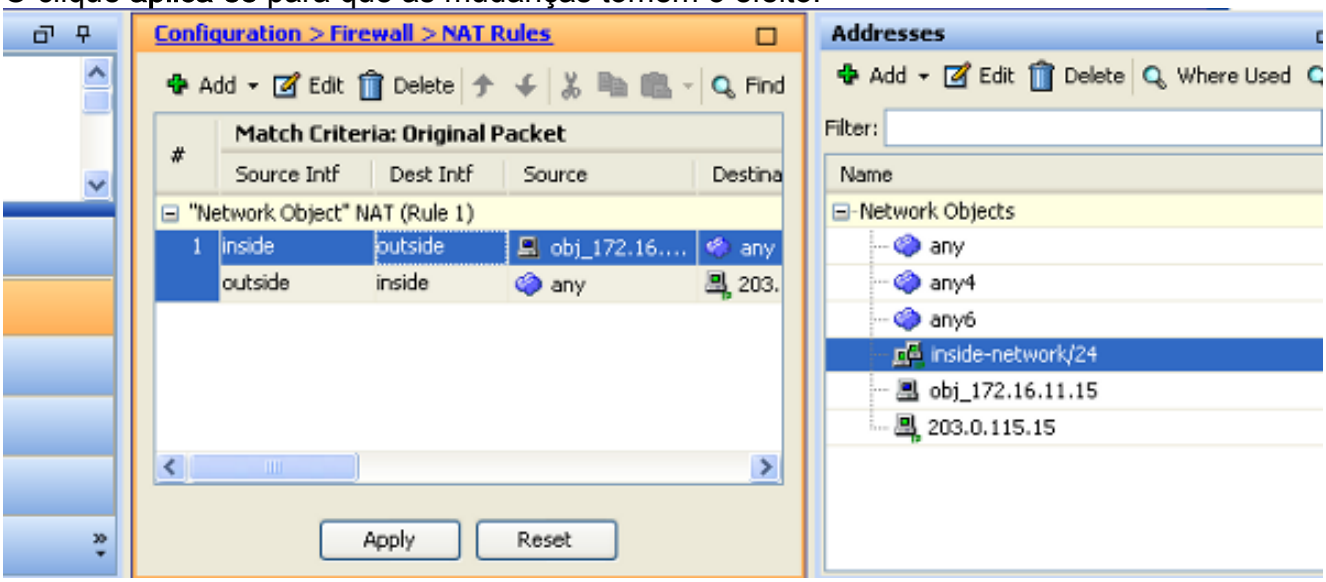
3. Expanda o NAT. Verifique a caixa de verificação **automática das regras de tradução de endereço adicionar**. No tipo lista de drop-down, escolha a **estática**. No campo traduzido do ADDR, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT. Clique **avançado** a fim selecionar o serviço e a fonte e as interfaces de destino.



4. Nas listas de drop-down da interface de origem e da interface de destino, escolha as relações apropriadas. Configurar o serviço. Clique em **OK**.



5. O clique **aplica-se** para que as mudanças tomem o efeito.



Este é o CLI equivalente output para esta configuração de NAT:

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O analisador do CLI Cisco (clientes registrados somente) apoia determinados comandos de exibição. Use o analisador do CLI Cisco a fim ver uma análise do emissor de comando de

execução.

Alcance um site através do HTTP com um navegador da Web. Este exemplo usa um local que seja hospedado em 198.51.100.100. Se a conexão é bem sucedida, esta saída pode ser considerada no ASA CLI.

Conexão

```
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
```

O ASA é um firewall stateful, e o tráfego de retorno do servidor de Web é permitido para trás com o Firewall porque combina uma *conexão na* tabela de conexão do Firewall. Trafique que combina uma conexão que preexista seja permitida com o Firewall sem ser obstruída por uma relação ACL.

Na saída precedente, o cliente na interface interna estabeleceu uma conexão ao host de 198.51.100.100 fora da interface externa. Esta conexão é feita com o protocolo de TCP e foi inativa por seis segundos. As bandeiras da conexão indicam o estado atual desta conexão. Mais informação sobre bandeiras da conexão pode ser encontrada em bandeiras da conexão de TCP ASA.

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)
```

O Firewall ASA gerencie Syslog durante a operação normal. Os Syslog variam na verbosidade baseada na configuração de registro. A saída mostra dois Syslog que são vistos a nível seis, ou o nível “informativo”.

Neste exemplo, há dois Syslog gerados. O primeiro é um mensagem de registro que indique que o Firewall construiu uma tradução, especificamente uma tradução dinâmica TCP (PANCADINHA). Indica o endereço IP de origem e a porta e o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta traduzidos enquanto o tráfego atravessa do interior às interfaces externas.

O segundo Syslog indica que o Firewall construiu uma conexão em sua tabela de conexão para este tráfego específico entre o cliente e servidor. Se o Firewall foi configurado a fim obstruir esta tentativa de conexão, ou algum outro fator inibiu a criação desta conexão (confinamentos de recurso ou um possível erro de configuração), o Firewall não geraria um log que indicasse que a conexão esteve construída. Em lugar de registraria uma razão para que a conexão seja negada ou uma indicação sobre que fator inibiu a conexão da criação.

Projétil luminoso do pacote

```
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
```

A funcionalidade do projétil luminoso do pacote no ASA permite que você especifique um pacote *simulado* e considere todas as várias etapas, verificações, e funções que o Firewall atravessa quando processa o tráfego. Com esta ferramenta, é útil identificar um exemplo do tráfego que você acredita *deve* ser reservado passar com o Firewall, e usa-se que 5-tupple a fim simular o tráfego. No exemplo anterior, o projétil luminoso do pacote é usado a fim simular uma tentativa de conexão que encontre estes critérios:

- O pacote simulado chega no interior.
- O protocolo usado é TCP.
- O endereço IP cliente simulado é 172.16.11.5.
- O cliente envia o tráfego originado da porta 1234.
- O tráfego é destinado a um server no endereço IP 198.51.100.100.
- O tráfego é destinado à porta 80.

Observe que não havia nenhuma menção da relação fora no comando. Isto é pelo projeto do projétil luminoso do pacote. A ferramenta di-lo como os processos do Firewall que a tentativa do tipo de conexão, que inclui como a distribuiria, e fora de que relação. Mais informação sobre o projétil luminoso do pacote pode ser encontrada em uns pacotes de seguimento com projétil luminoso do pacote.

Captação

Aplique a captação

```
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>
```

O Firewall ASA pode capturar o tráfego que incorpora ou deixa suas relações. Esta funcionalidade da captação é fantástica porque pode definitivamente provar se o tráfego chega em, ou sae de, um Firewall. O exemplo anterior mostrou a configuração de duas captações nomeadas capin e capout nas interfaces internas e externas respectivamente. Os comandos

capture usaram a palavra-chave do fósforo, que permite que você seja específico sobre que tráfego você quer capturar.

Para o capin da captação**,** você indicou que você quis combinar o tráfego visto na interface interna (ingresso ou saída) esse host 198.51.100.100 de 172.16.11.5 do host dos fósforos TCP. Ou seja você quer capturar todo o tráfego TCP que for enviado do host 172.16.11.5 para hospedar 198.51.100.100 ou vice versa. O uso da palavra-chave do fósforo permite que o Firewall capture esse tráfego bidirecional. O comando capture definido para a interface externa não provê o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente interno porque o Firewall conduz a PANCADINHA nesse endereço IP cliente. Em consequência, você não pode combinar com esse endereço IP cliente. Em lugar de, este exemplo usa alguns a fim indicar que todos os endereços IP de Um ou Mais Servidores Cisco ICM NT possíveis combinariam essa circunstância.

Depois que você configura as captações, você tentaria então estabelecer outra vez uma conexão, e continua ver as captações com o comando do ***<capture_name> da*** **captação da mostra**. Neste exemplo, você pode ver que o cliente podia conectar ao server como evidente pelo aperto de mão da 3-maneira TCP visto nas captações.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Exemplo de configuração do Syslog ASA
- Capturas de pacote de informação ASA com CLI e exemplo da configuração ASDM
- Suporte Técnico e Documentação - Cisco Systems