Configurar o encaminhamento de portas ASA versão 9 com NAT

Contents

Introduction

Este documento descreve como configurar o Redirecionamento de Portas (Encaminhamento) e os recursos de Tradução de Endereço de Rede (NAT) externos no Software Adaptive Security Appliance (ASA) Versão 9.x, com o uso do CLI ou do Adaptive Security Device Manager (ASDM).

Consulte o Guia de Configuração do ASDM do Cisco ASA Series Firewall para obter informações adicionais.

Prerequisites

Requirements

Consulte Configurando o Acesso de Gerenciamento para permitir que o dispositivo seja configurado pelo ASDM.

Componentes Utilizados

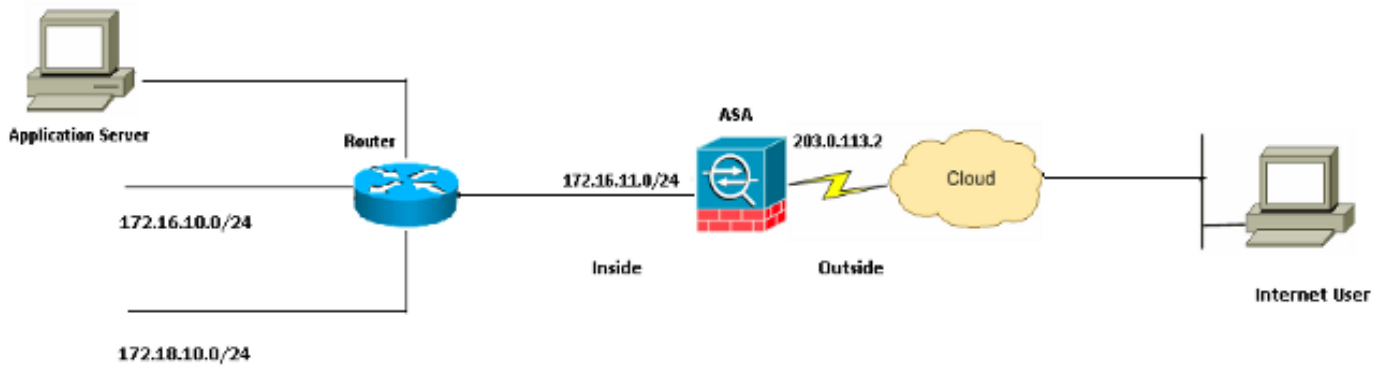
As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco ASA 5525 Series Security Appliance versão 9.x ou posterior
- ASDM versão 7.x e posterior

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

Configurar

Diagrama de Rede



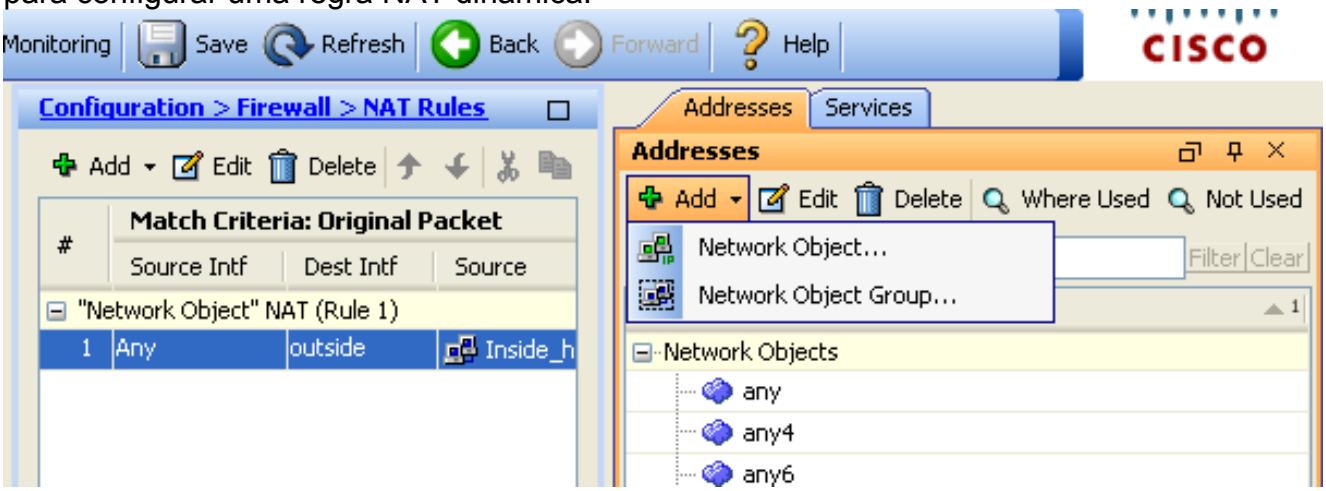
Os esquemas de endereço IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Permitir que hosts internos acessem redes externas com PAT

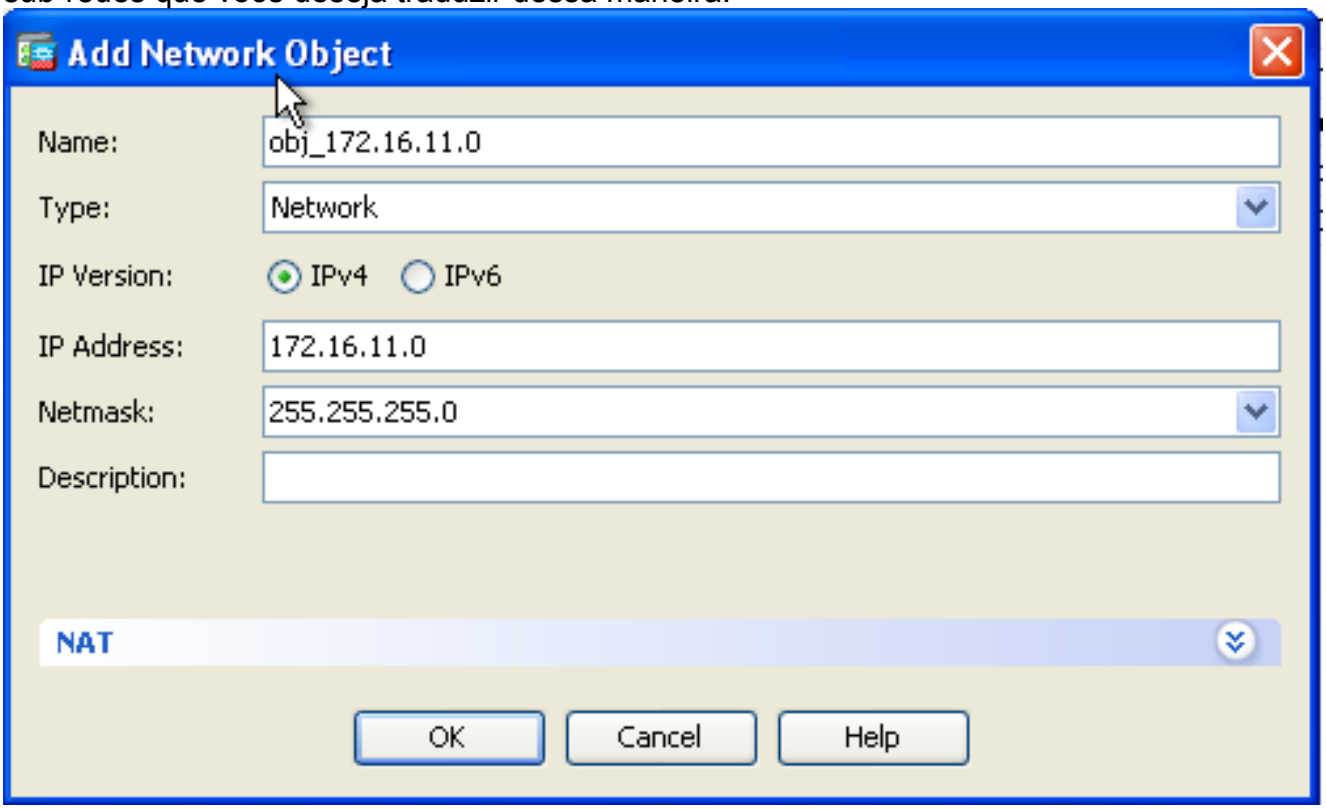
Se você quiser que os hosts internos compartilhem um único endereço público para conversão, use a Conversão de Endereço de Porta (PAT - Port Address Translation). Uma das configurações PAT mais simples envolve a conversão de todos os hosts internos para parecerem o endereço IP da interface externa. Essa é a configuração PAT típica usada quando o número de endereços IP roteáveis disponíveis no ISP é limitado a apenas alguns, ou talvez apenas um.

Conclua estas etapas para permitir que hosts internos acessem redes externas com PAT:

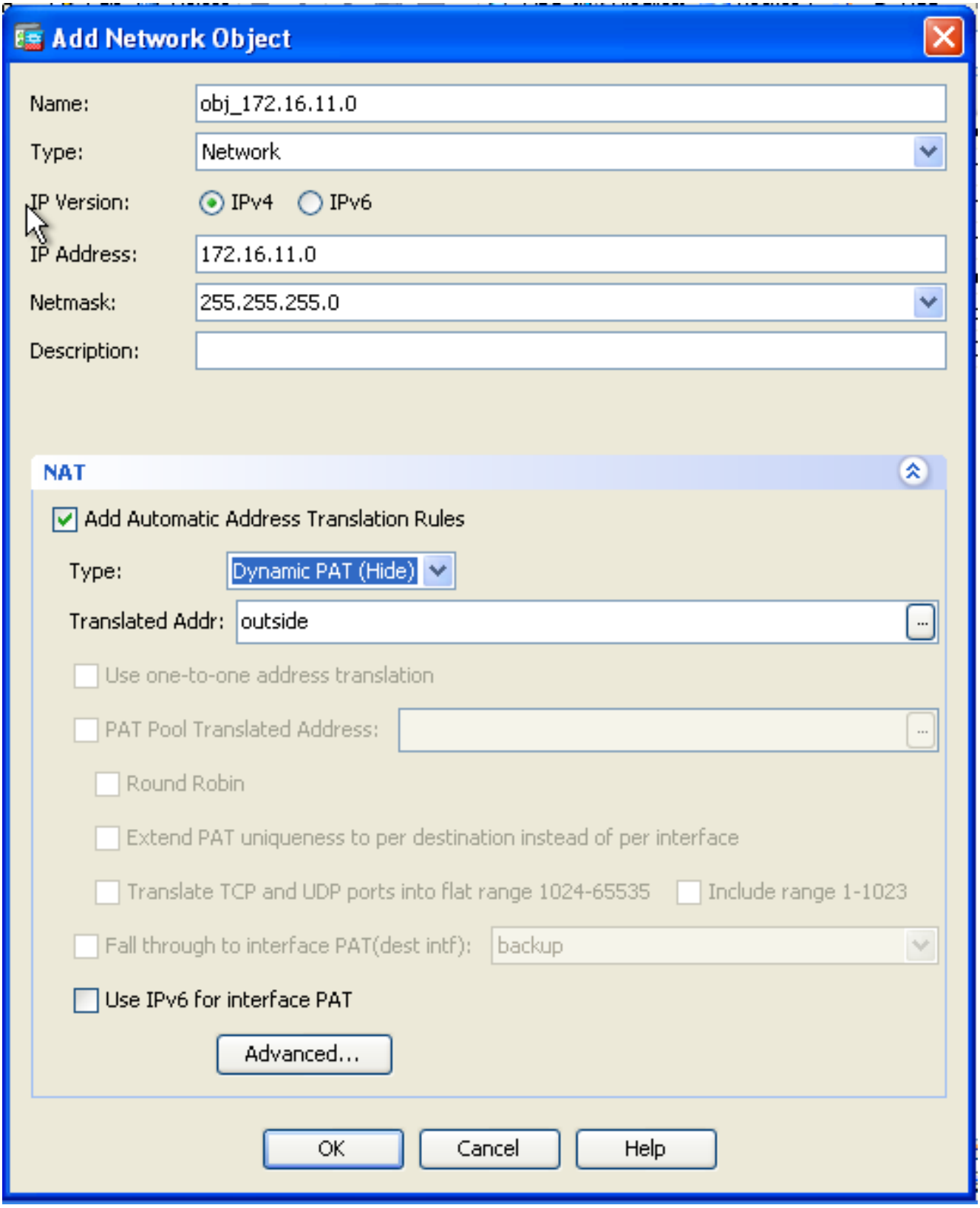
1. Selecione **Configuration > Firewall > NAT Rules**. Clique em **Add** e escolha **Network Object** para configurar uma regra NAT dinâmica.



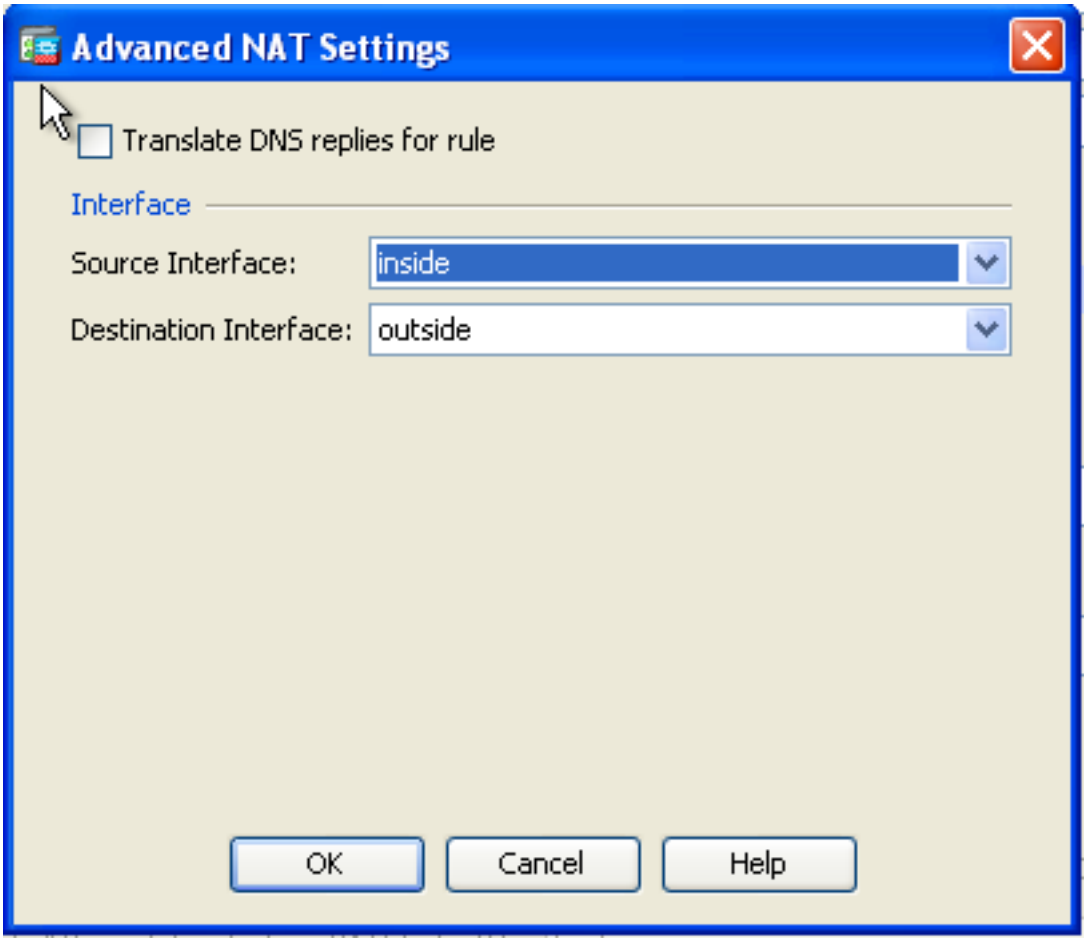
2. Configure a rede/host/intervalo para o qual o **PAT dinâmico** é necessário. Neste exemplo, uma das sub-redes internas foi selecionada. Esse processo pode ser repetido para outras sub-redes que você deseja traduzir dessa maneira.



3. Expanda NAT. Marque a caixa de seleção **Add Automatic Address Translation Rules**. Na lista suspensa Tipo, escolha **PAT dinâmico (Ocultar)**. No campo **Translated Addr**, escolha a opção para refletir a interface externa. Clique em **Advanced** (Avançado).



4. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. Clique em **OK** e clique em **Aplicar** para que as alterações tenham efeito.



Esta é a saída CLI equivalente para esta configuração PAT:

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

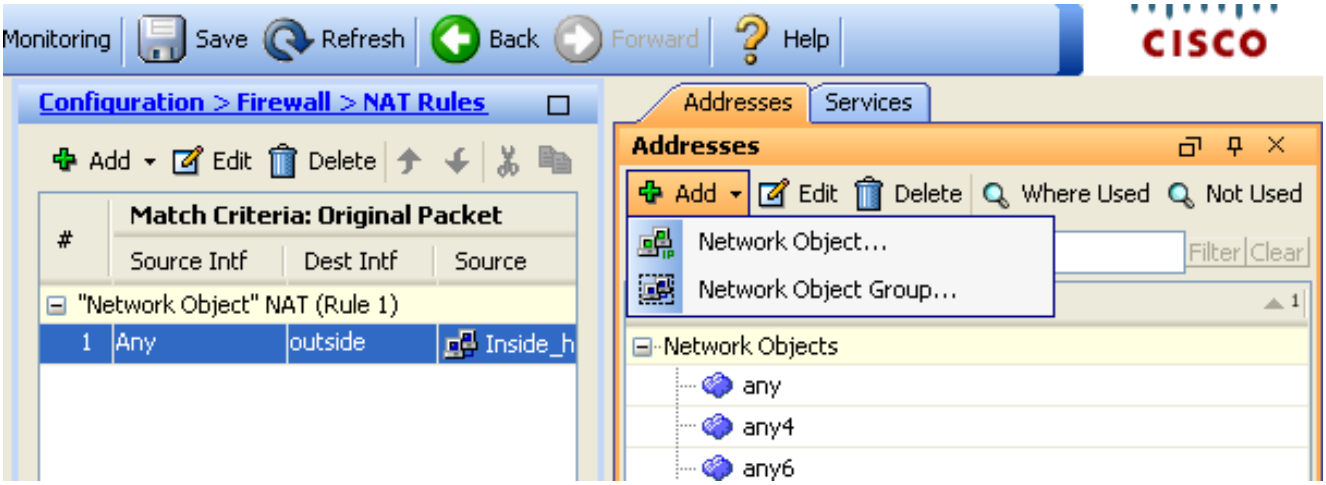
Permitir o Acesso de Host Internos às Redes Externas via NAT

Você pode permitir que um grupo de hosts/redes internos acesse o mundo externo com a configuração das regras de NAT dinâmico. Diferentemente do PAT, o NAT dinâmico aloca endereços convertidos de um pool de endereços. Como resultado, um host é mapeado para seu próprio endereço IP convertido e dois hosts não podem compartilhar o mesmo endereço IP convertido.

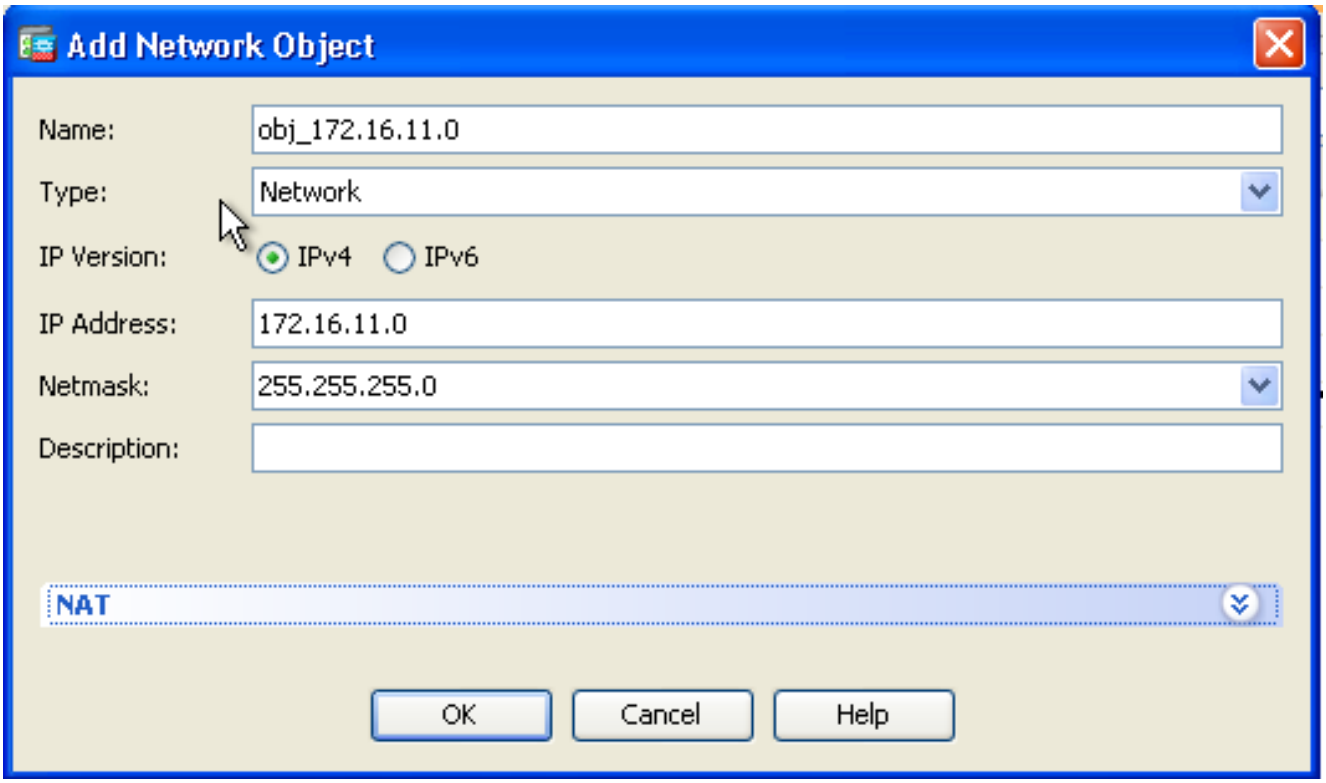
Para fazer isso, você precisa selecionar o endereço real dos hosts/redes para receber acesso e eles precisam ser mapeados para um pool de endereços IP traduzidos.

Conclua estas etapas para permitir que hosts internos acessem redes externas com NAT:

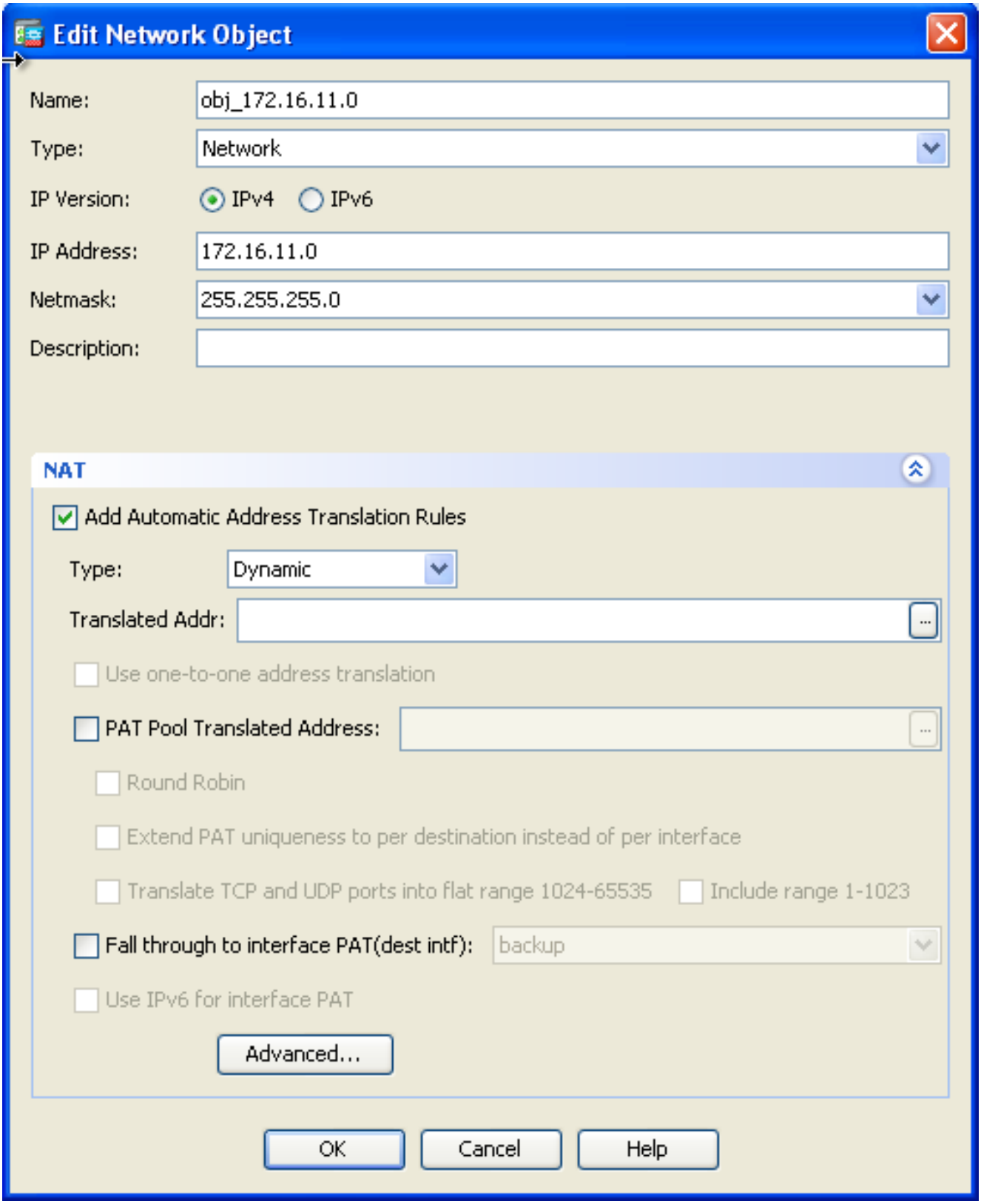
1. Selecione **Configuration > Firewall > NAT Rules**. Clique em **Add** e escolha **Network Object** para configurar uma regra NAT dinâmica.



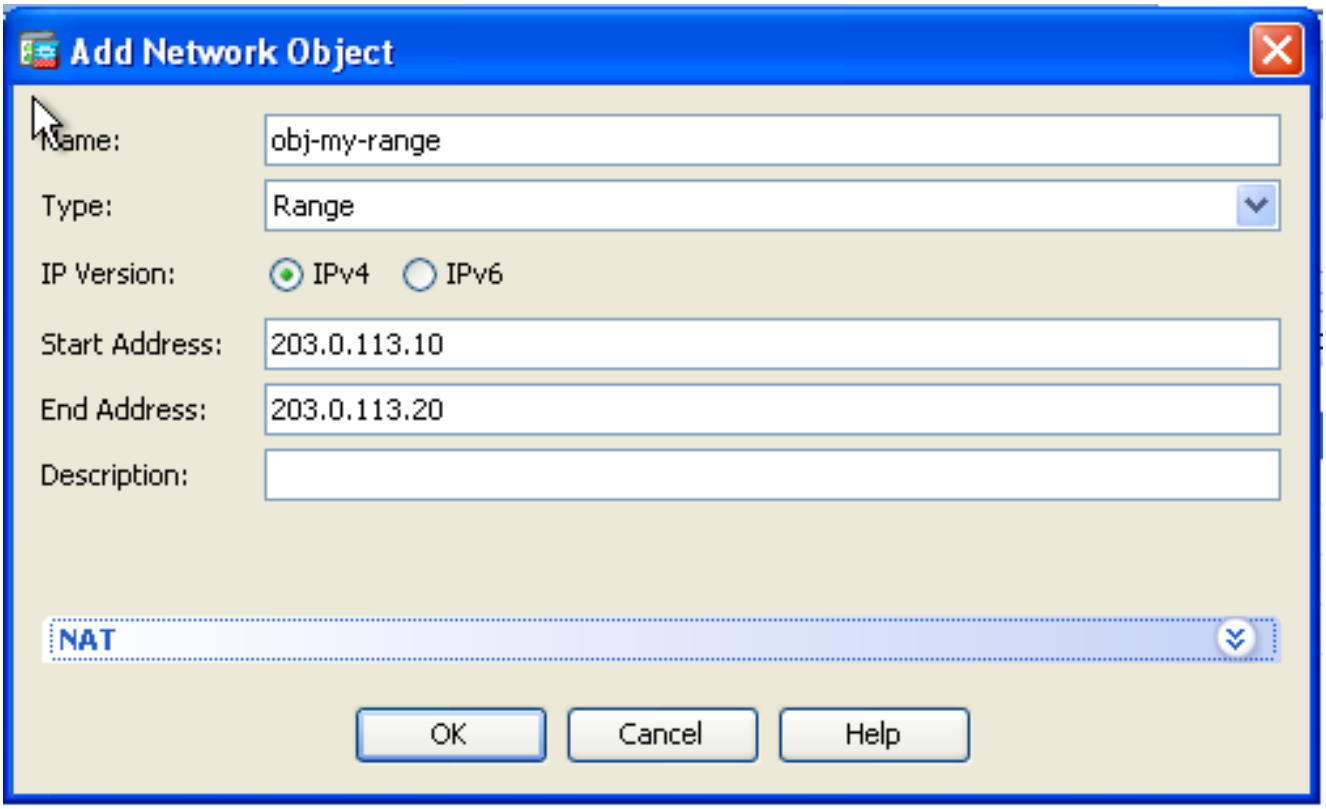
2. Configure a rede/host/intervalo para o qual o PAT dinâmico é necessário. Neste exemplo, toda a *rede interna* foi selecionada.



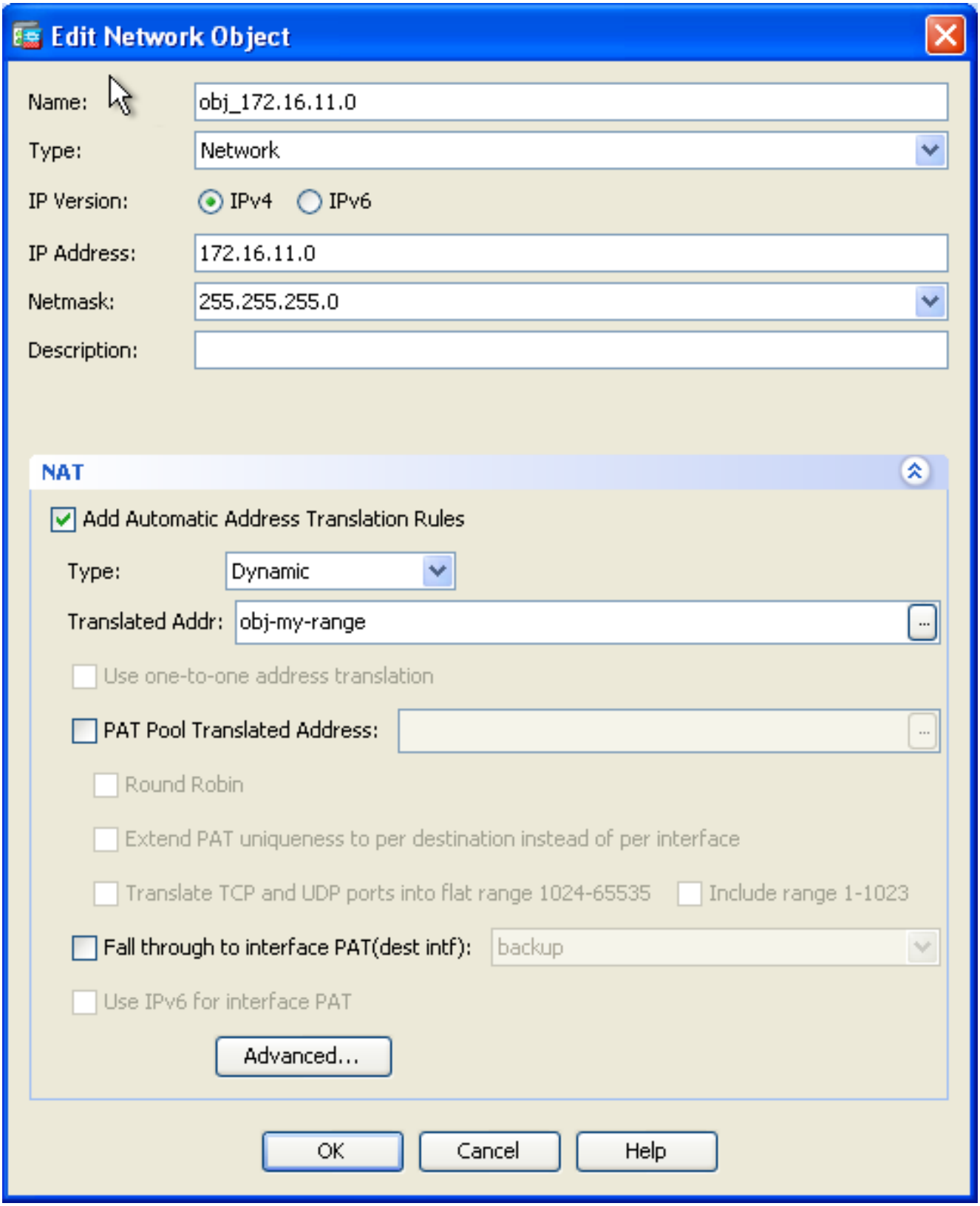
3. Expanda NAT. Marque a caixa de seleção **Add Automatic Address Translation Rules**. Na lista suspensa Tipo, escolha **Dinâmico**. No campo Endereço traduzido, escolha a seleção apropriada. Clique em **Advanced** (Avançado).



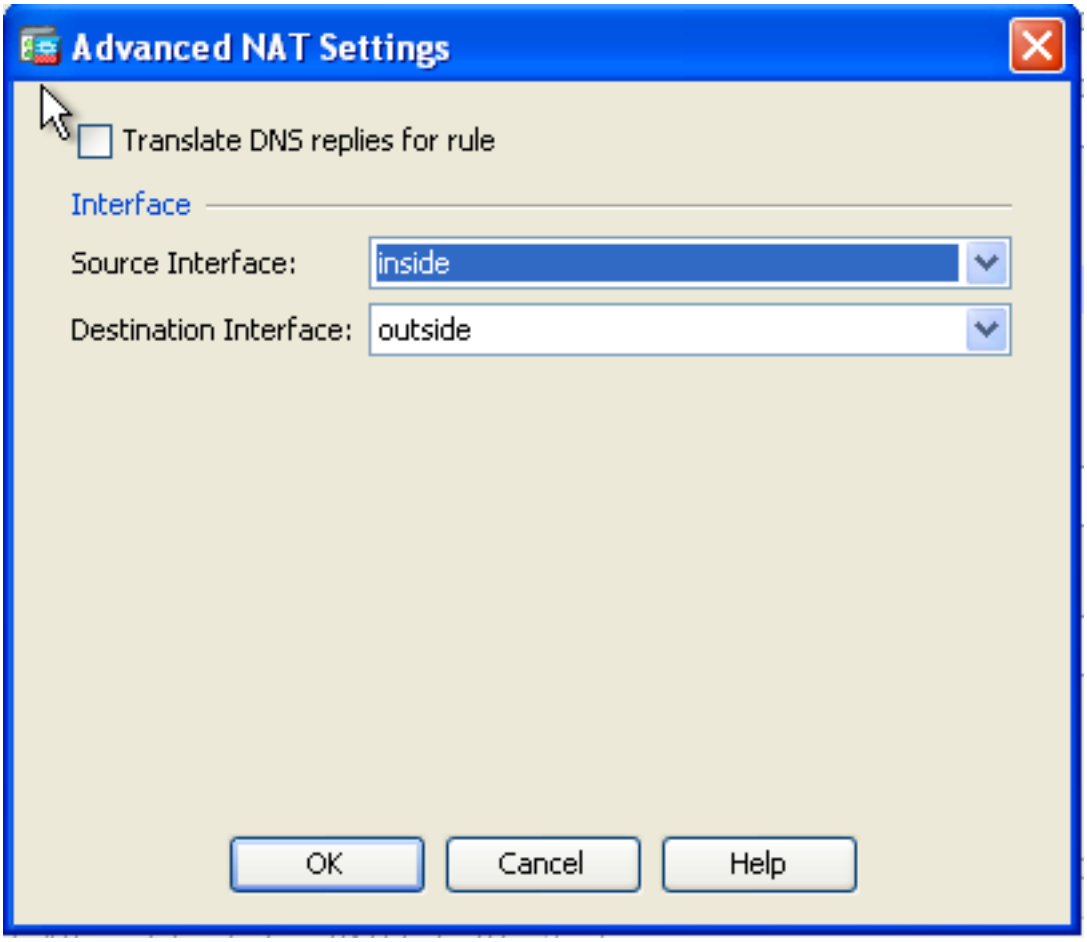
4. Clique em **Add** para adicionar o objeto de rede. Na lista suspensa Tipo, escolha **Intervalo**. Nos campos Endereço inicial e Endereço final, insira os endereços IP PAT inicial e final. Click **OK**.



5. No campo Endereço traduzido, escolha o objeto de endereço. Clique em **Advanced** para selecionar as interfaces de origem e destino.



6. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. Clique em **OK** e clique em **Aplicar** para que as alterações tenham efeito.

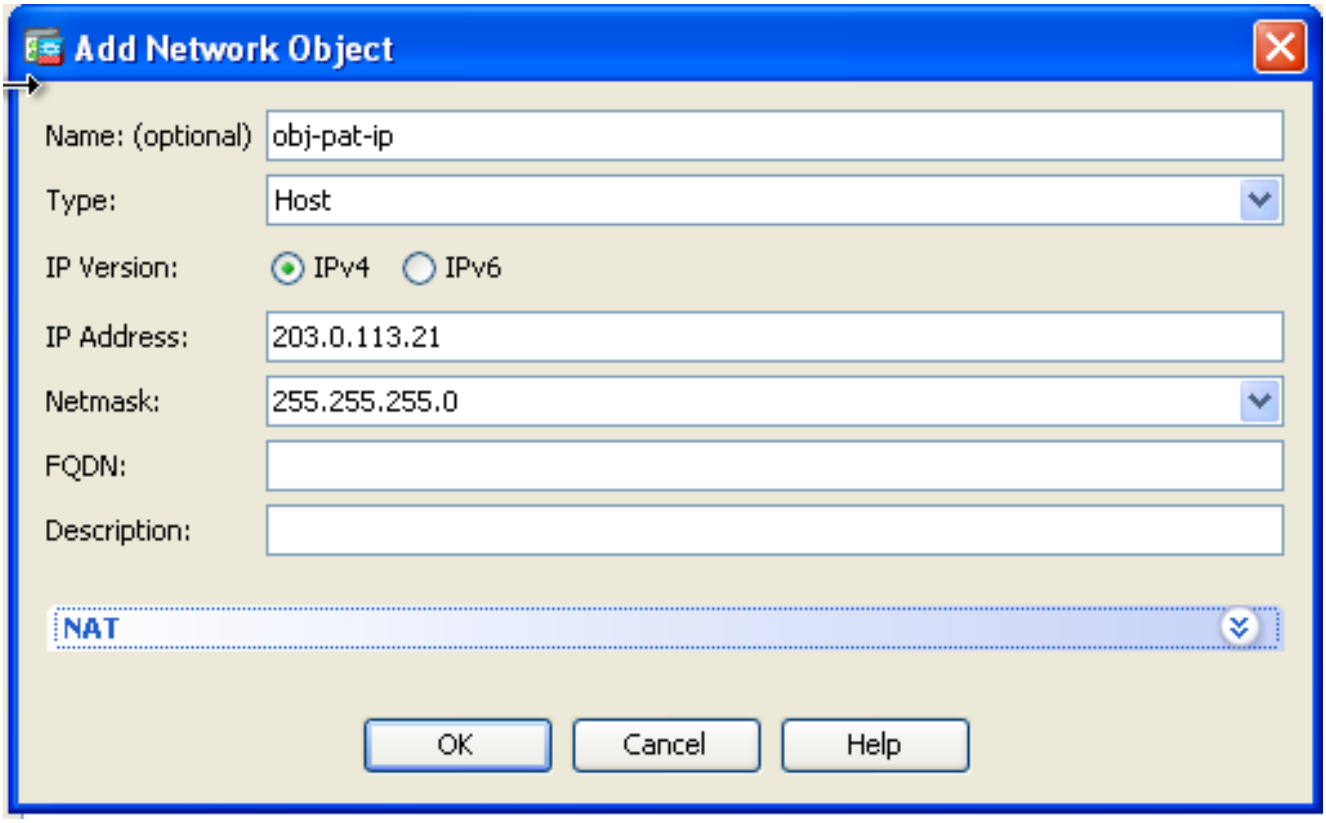


Esta é a saída CLI equivalente para esta configuração do ASDM:

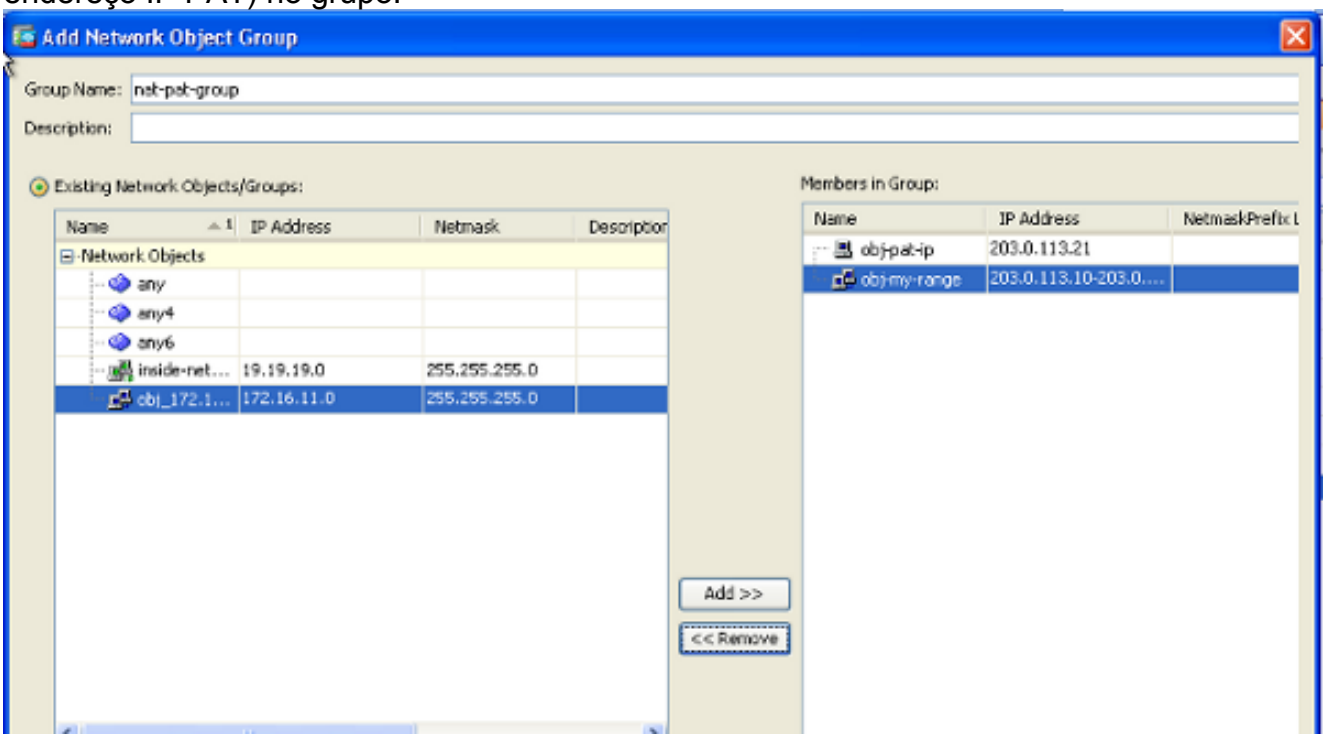
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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

De acordo com essa configuração, os hosts na rede 172.16.11.0 são convertidos para qualquer endereço IP do pool NAT, 203.0.113.10 - 203.0.113.20. Se o pool mapeado tiver menos endereços que o grupo real, você poderá ficar sem endereços. Como resultado, você pode tentar implementar o NAT dinâmico com backup PAT dinâmico ou pode tentar expandir o pool atual.

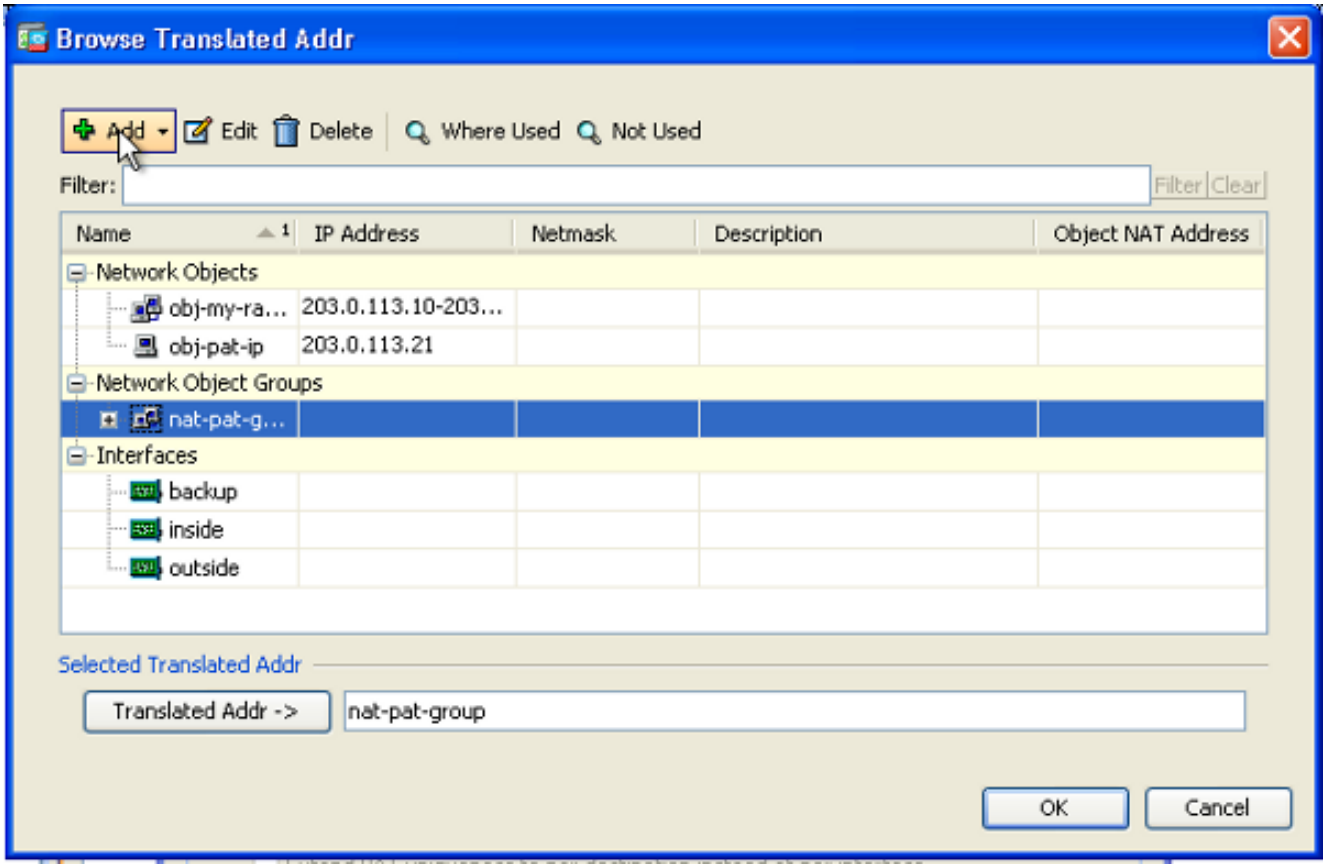
1. Repita as etapas 1 a 3 na configuração anterior e clique em **Add** novamente para adicionar um objeto de rede. Na lista suspensa Tipo, escolha **Host**. No campo Endereço IP, insira o endereço IP de backup do PAT. Click **OK**.



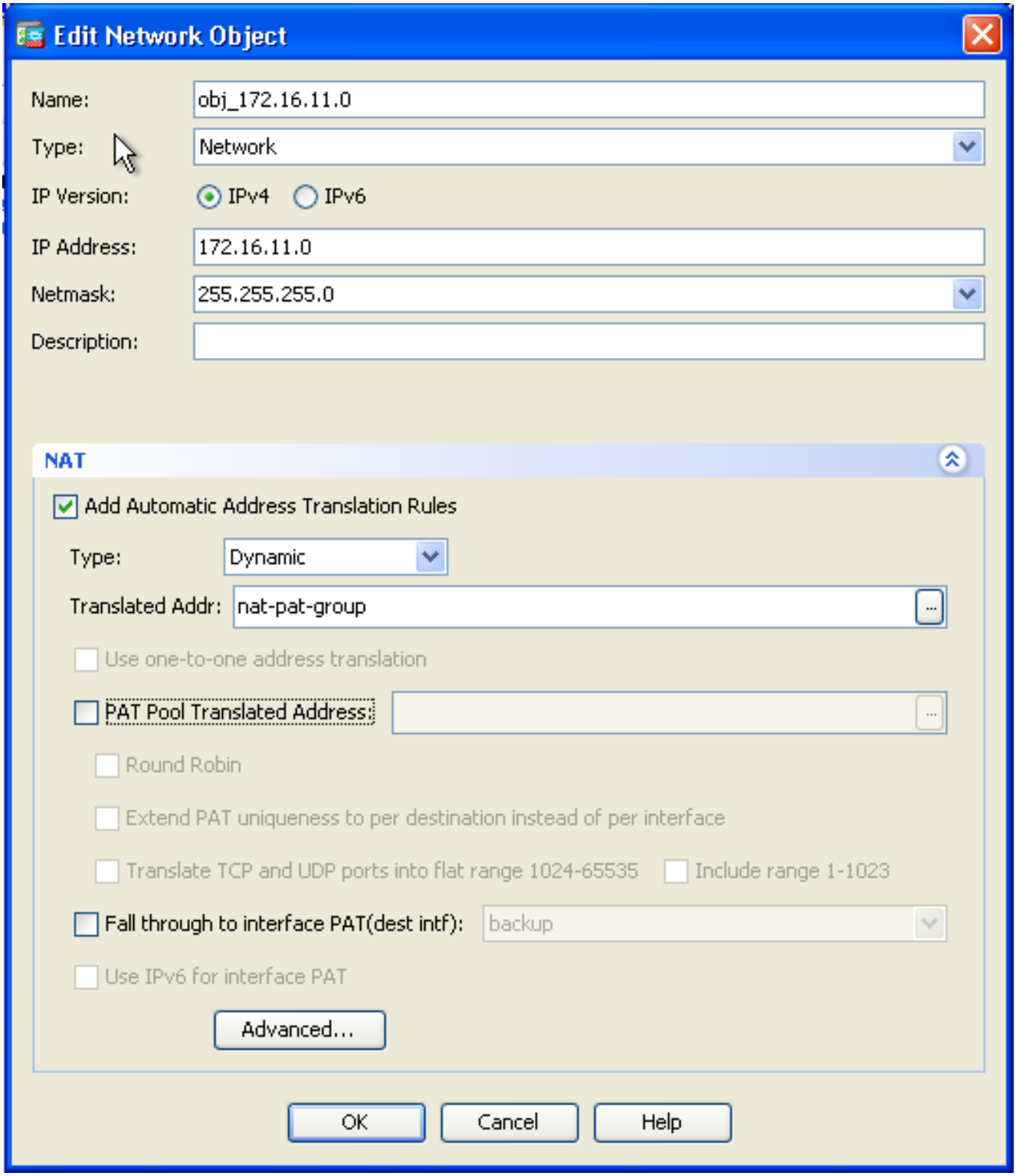
2. Clique em **Adicionar** para adicionar um grupo de objetos de rede. No campo Nome do grupo, insira um nome de grupo e **adicione** ambos os objetos de endereço (intervalo NAT e endereço IP PAT) no grupo.



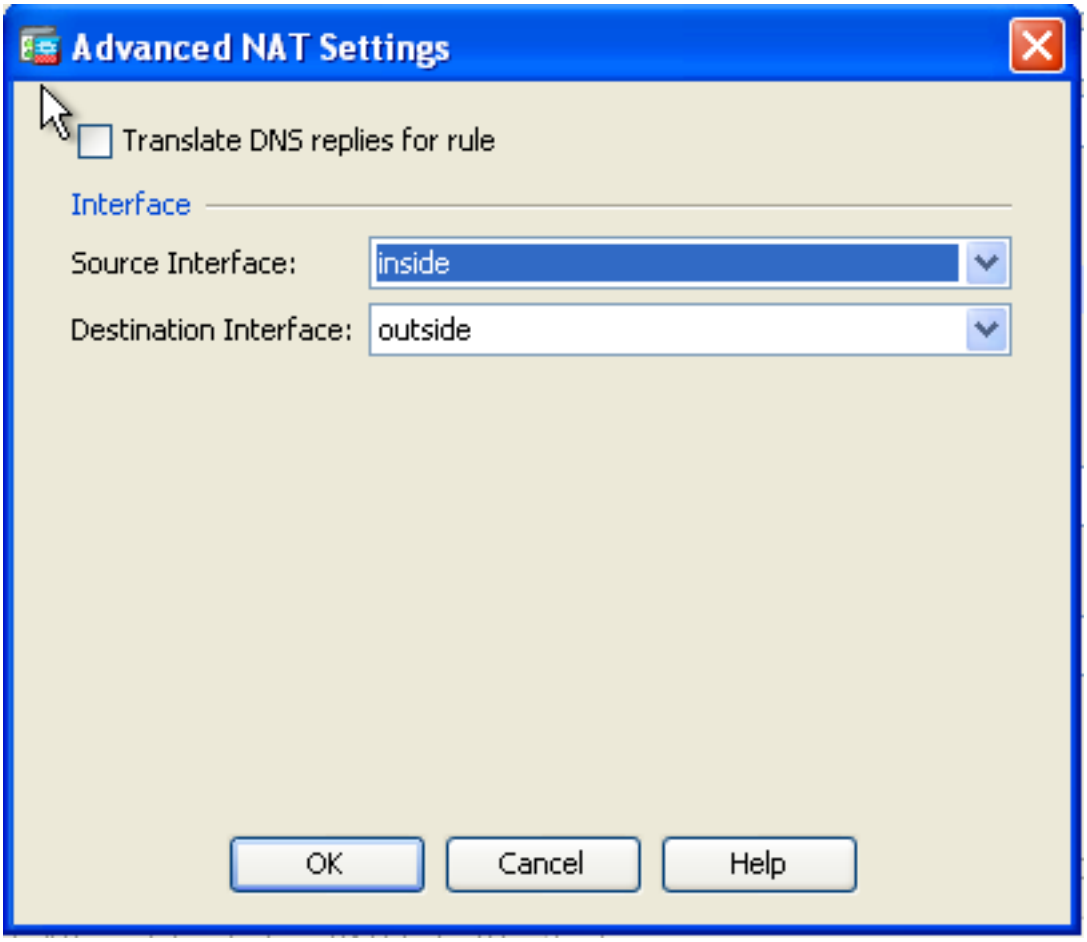
3. Escolha a regra NAT configurada e altere o endereço convertido para o grupo recém-configurado 'nat-pat-group' (era anteriormente 'obj-my-range'). Click **OK**.



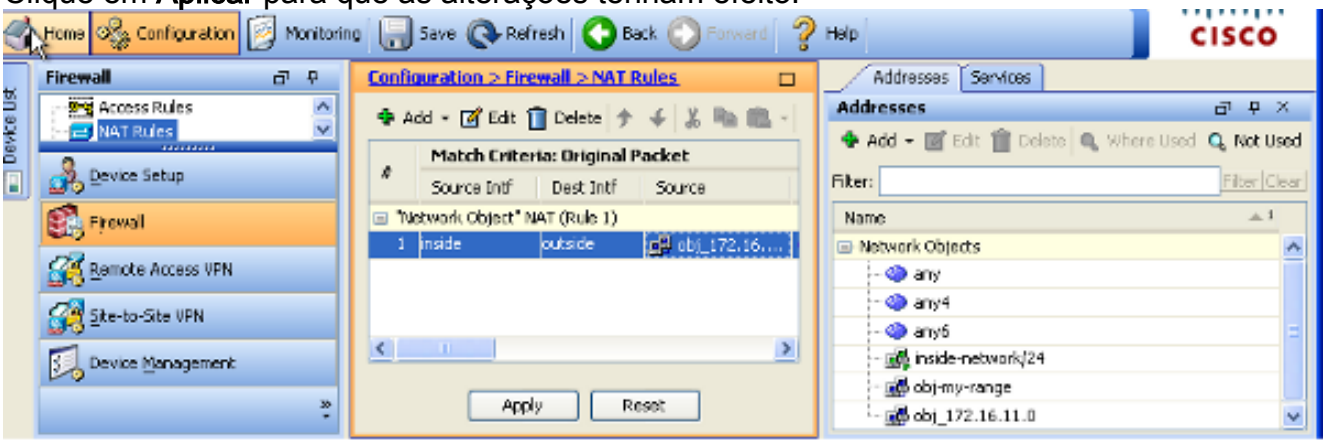
4. Clique em **OK** para adicionar a regra NAT. Clique em **Advanced** para selecionar as interfaces de origem e destino.



5. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. Click **OK**.



6. Clique em **Aplicar** para que as alterações tenham efeito.



Esta é a saída CLI equivalente para esta configuração do ASDM:

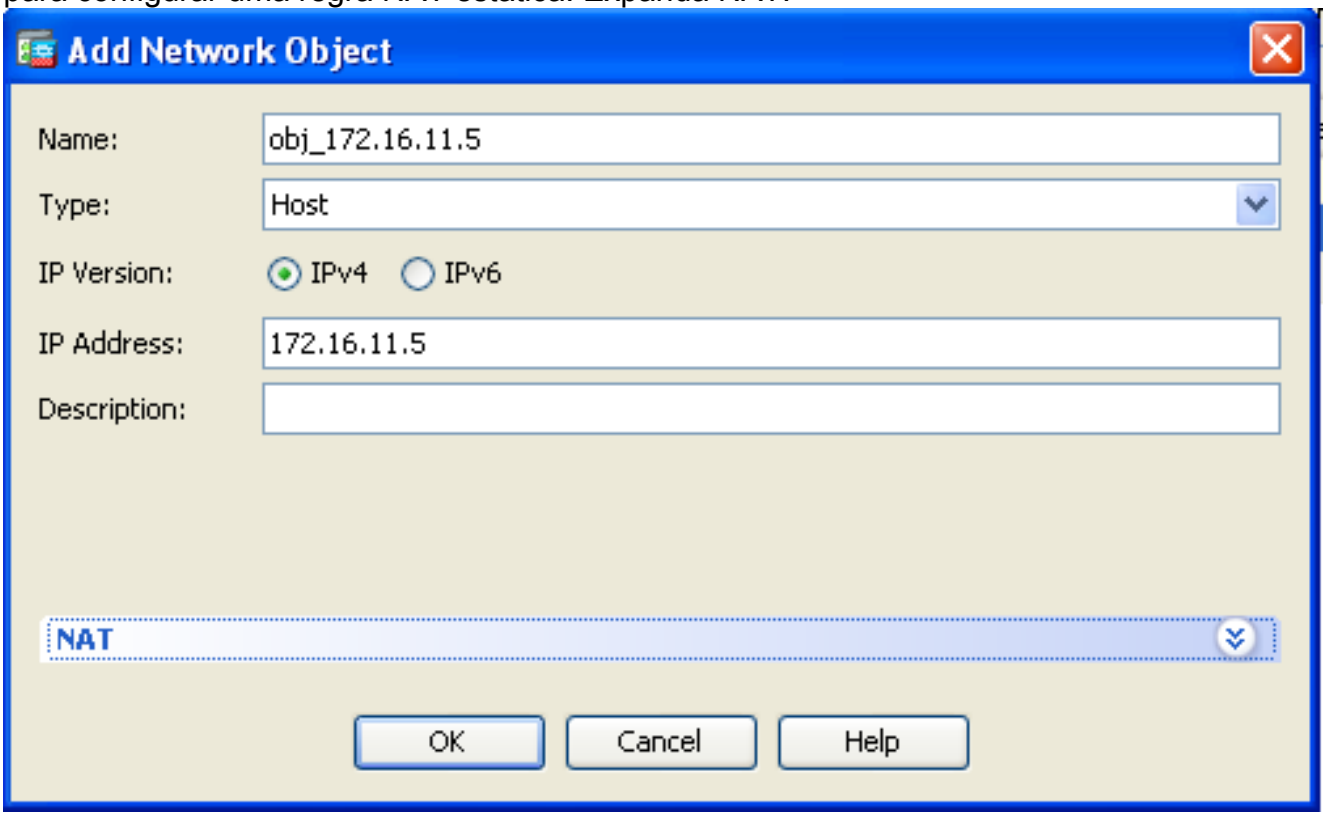
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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
```

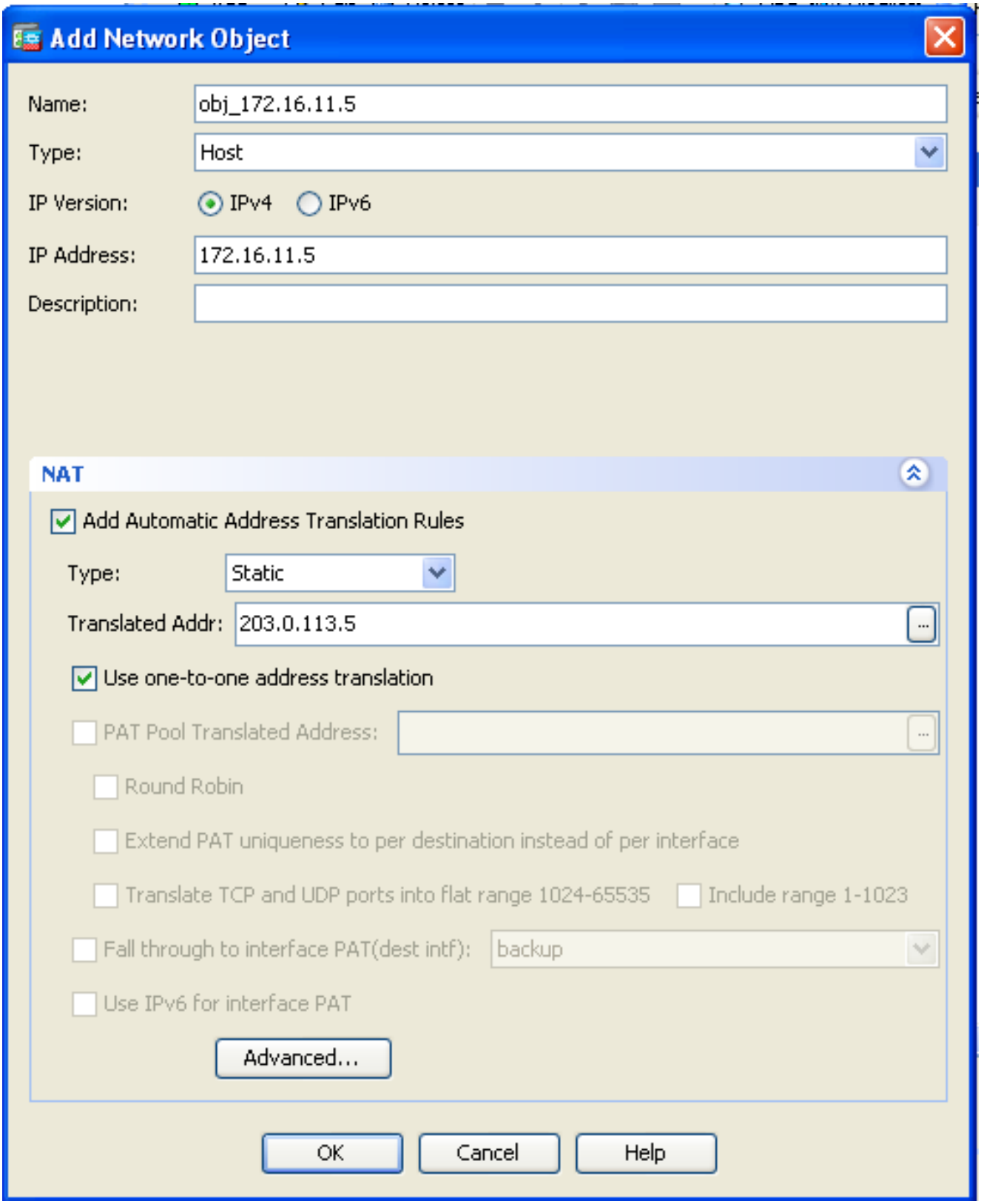
Permita o acesso dos hosts não confiáveis aos hosts em sua rede confiável

Isso pode ser obtido através da aplicação de uma conversão de NAT estático e uma regra de acesso para permitir esses hosts. Você deve configurá-lo sempre que um usuário externo desejar acessar qualquer servidor que esteja em sua rede interna. O servidor na rede interna pode ter um endereço IP privado que não seja roteável na Internet. Como resultado, você precisa converter esse endereço IP privado em um endereço IP público por meio de uma regra de NAT estático. Suponha que você tenha um servidor interno (172.16.11.5). Para que isso funcione, você precisa converter esse endereço IP de servidor privado em um endereço IP público. Este exemplo descreve como implementar o NAT estático bidirecional para converter 172.16.11.5 em 203.0.113.5.

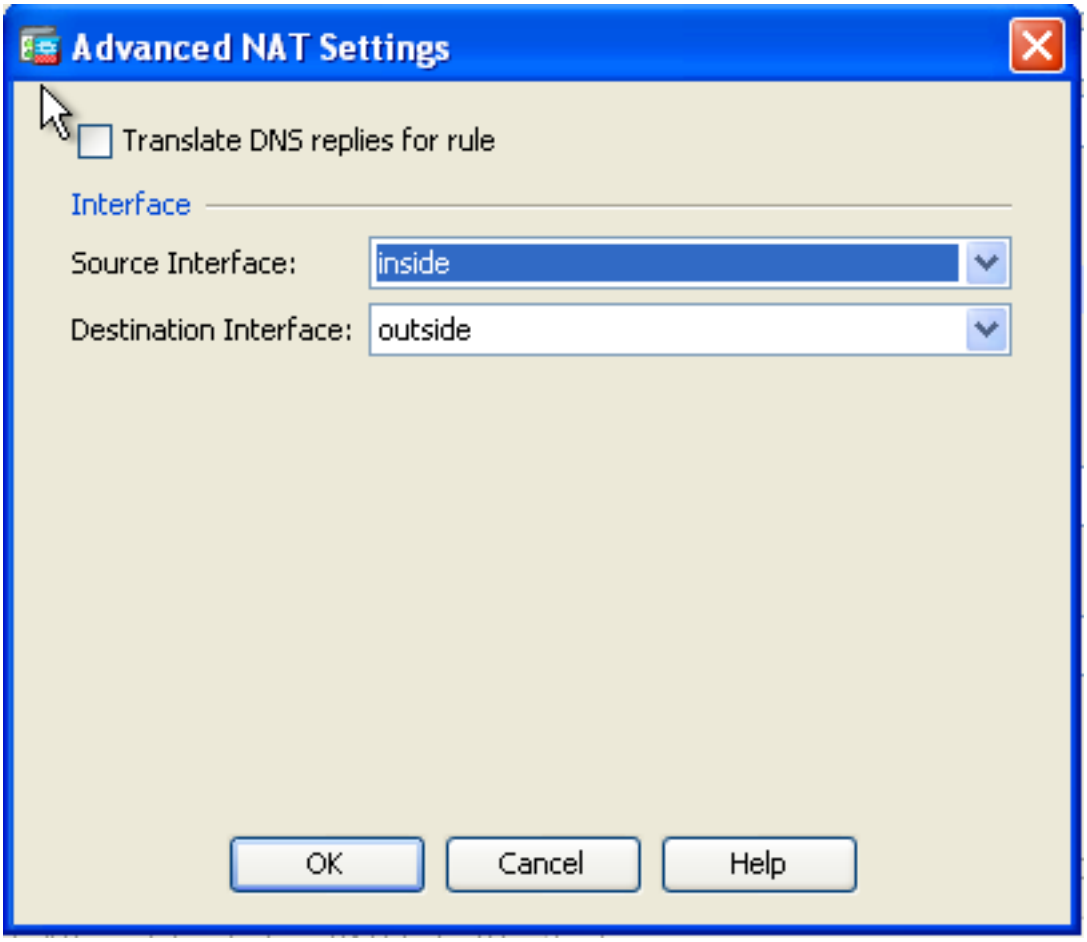
1. Selecione **Configuration > Firewall > NAT Rules**. Clique em **Add** e escolha **Network Object** para configurar uma regra NAT estática. Expanda NAT.



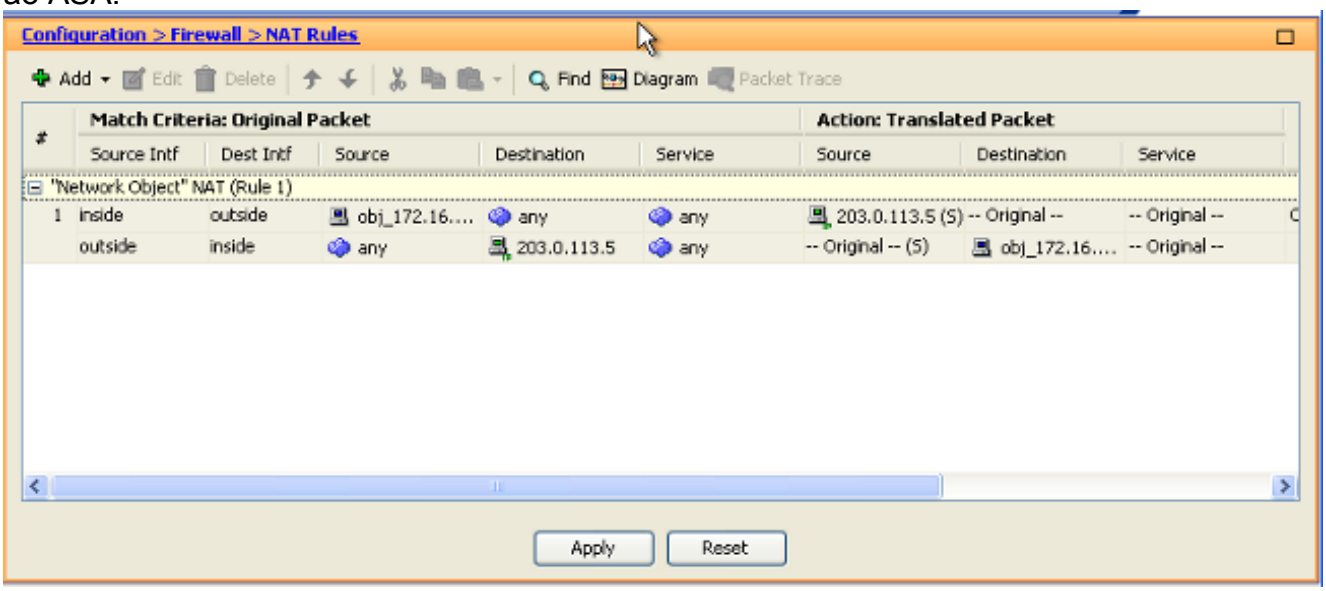
2. Marque a caixa de seleção **Add Automatic Address Translation Rules**. Na lista suspensa Tipo, escolha **Estático.** No campo Endereço traduzido, insira o endereço IP. Clique em **Advanced** para selecionar as interfaces de origem e destino.



3. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. Click **OK**.



4. Você pode ver a entrada de NAT estático configurada aqui. Clique em **Apply** para enviar isso ao ASA.



Esta é a saída CLI equivalente para esta configuração NAT:

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

NAT de identidade estática

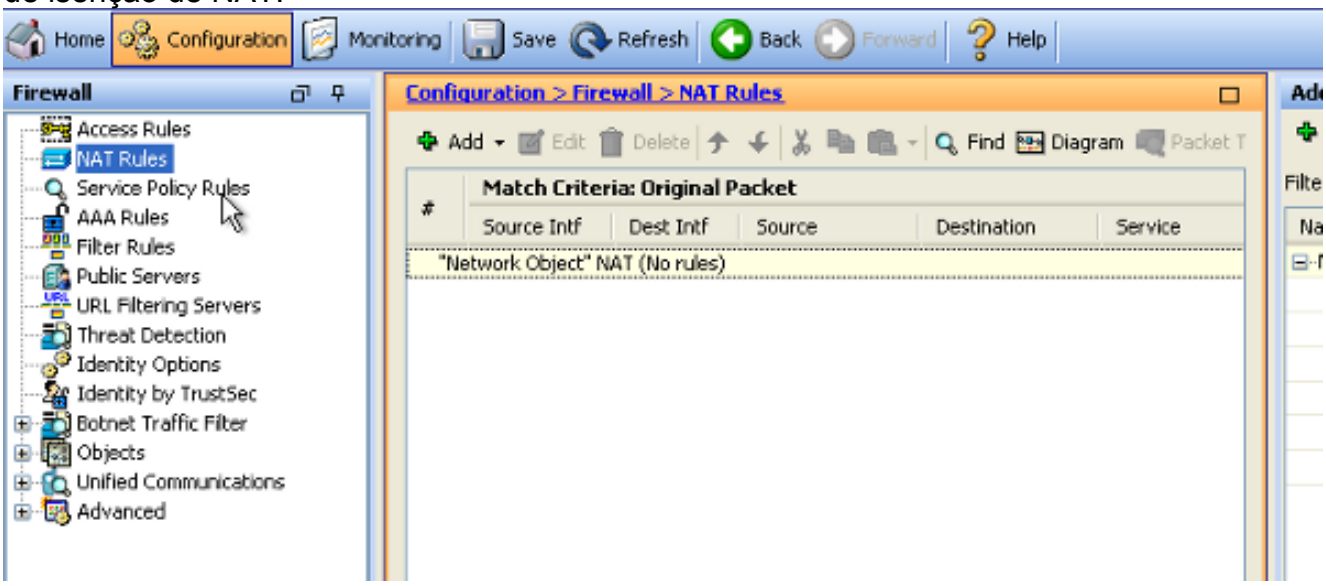
NAT Isento é um recurso útil em que os usuários internos tentam acessar um host/servidor VPN remoto ou algum host/servidor hospedado atrás de qualquer outra interface do ASA sem concluir

um NAT. Para conseguir isso, o servidor interno, que tem um endereço IP privado, pode ter a identidade convertida para si mesmo e que, por sua vez, tem permissão para acessar o destino que executa um NAT.

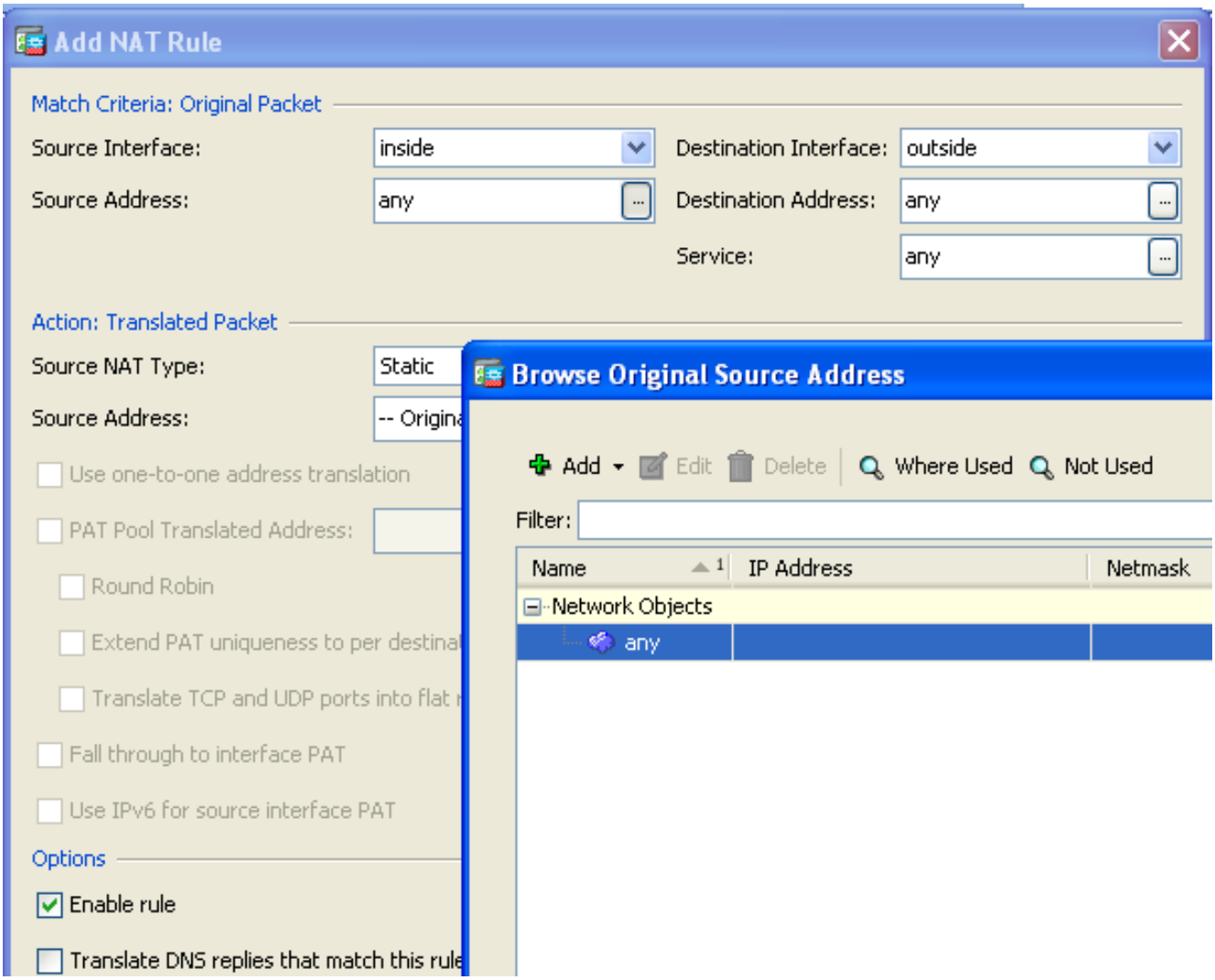
Neste exemplo, o host interno 172.16.11.15 precisa acessar o servidor VPN remoto 172.20.21.15.

Conclua estas etapas para permitir que hosts internos acessem a rede VPN remota com a conclusão de um NAT:

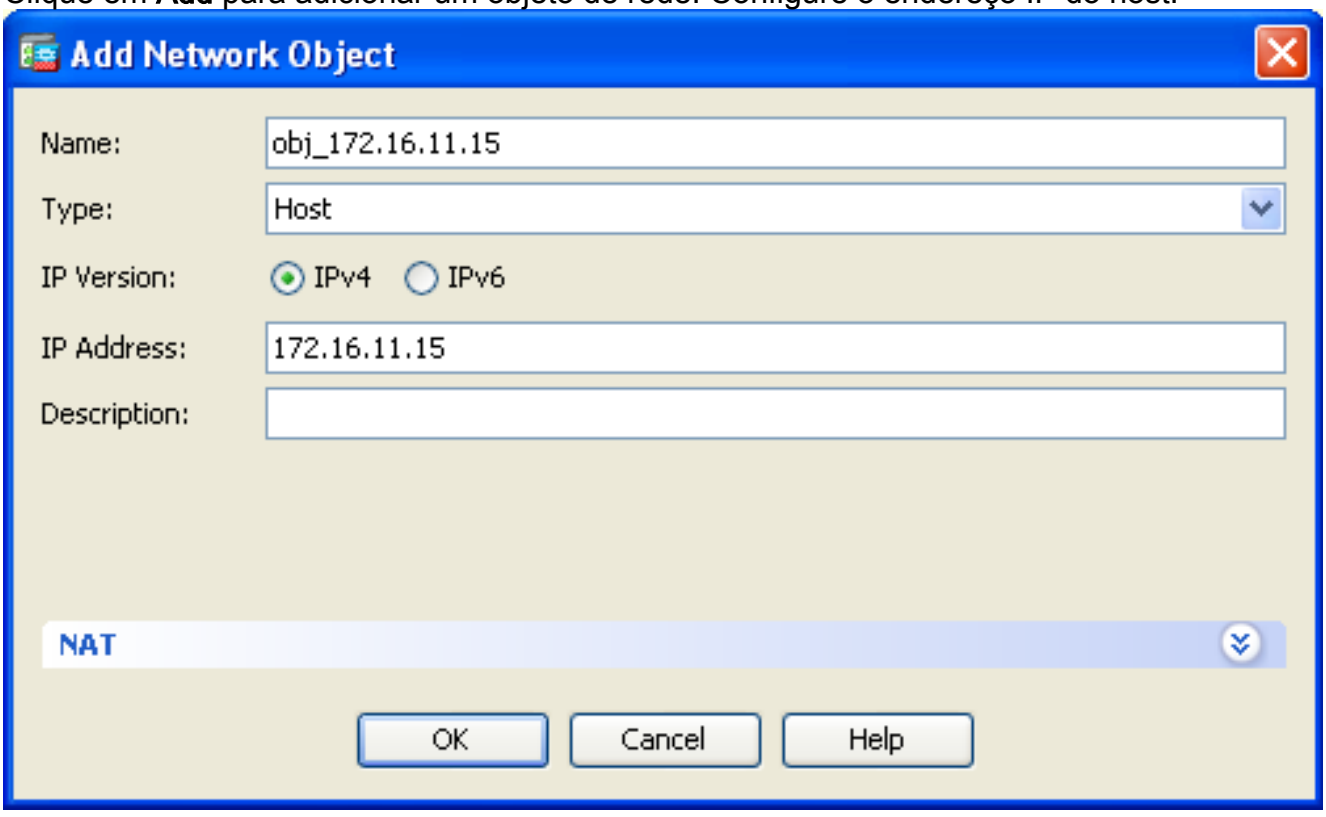
1. Selecione **Configuration** > **Firewall** > **NAT Rules**. Clique em **Add** para configurar uma regra de isenção de NAT.



2. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. No campo Endereço de origem, escolha a entrada apropriada.

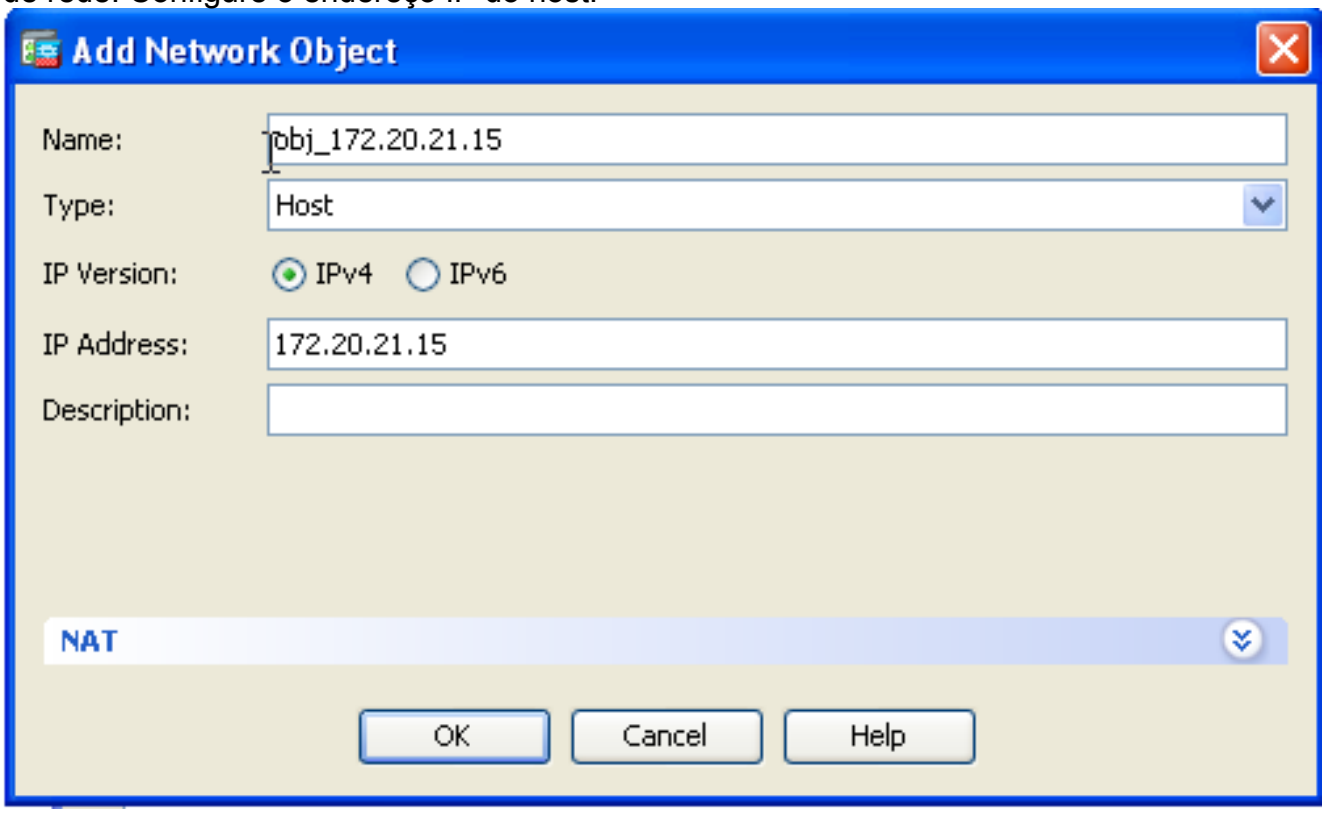


3. Clique em **Add** para adicionar um objeto de rede. Configure o endereço IP do host.

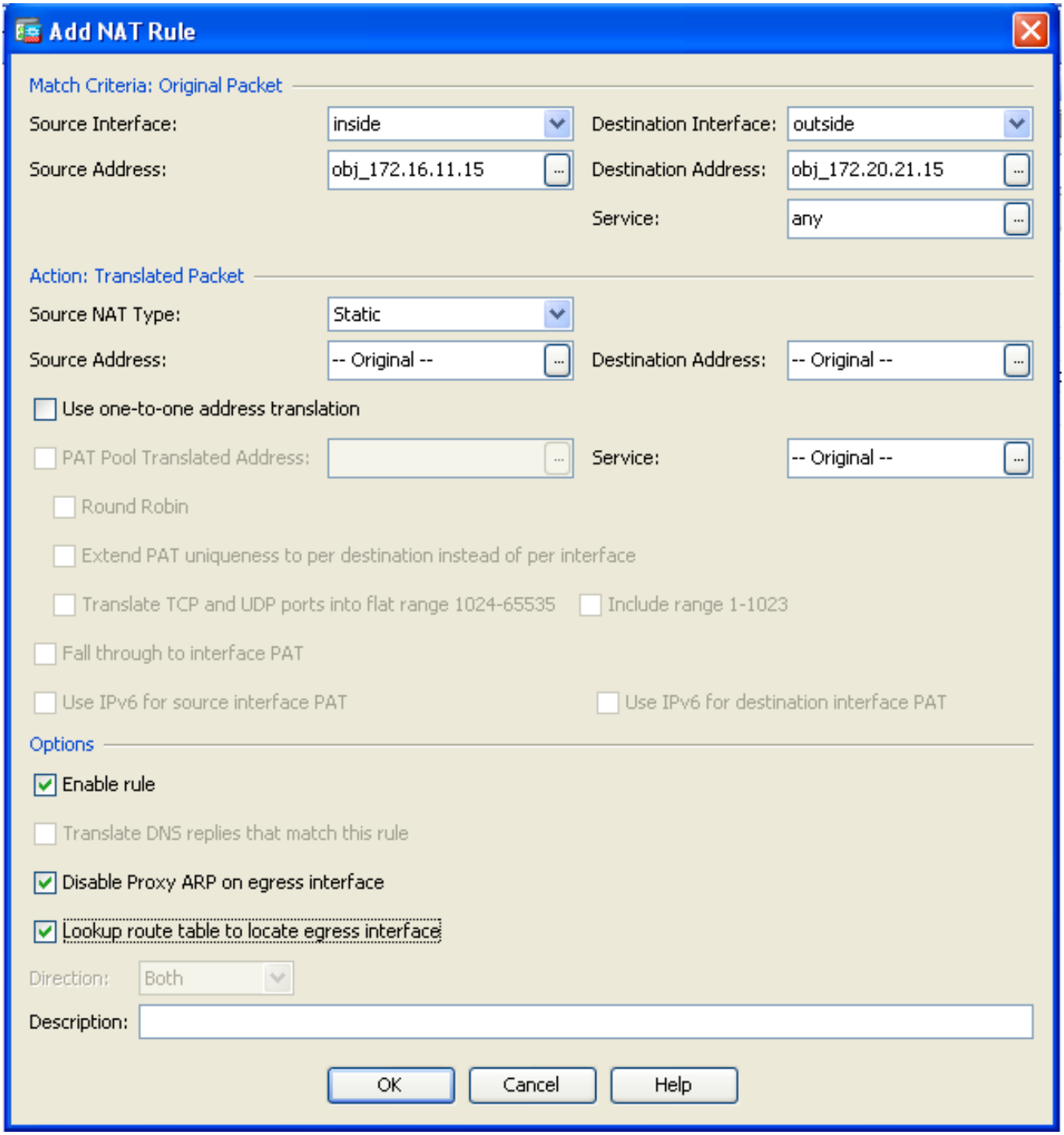


4. Da mesma forma, procure o **endereço de destino**. Clique em **Add** para adicionar um objeto

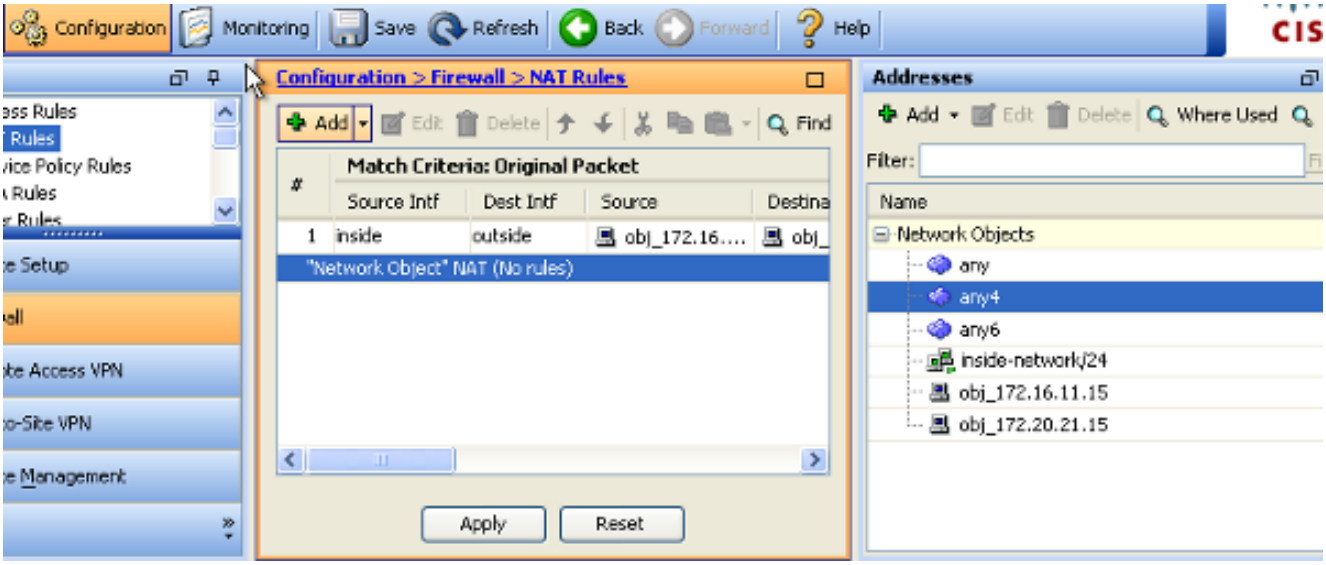
de rede. Configure o endereço IP do host.



5. Escolha os objetos configurados Endereço origem e Endereço destino. Marque as caixas de seleção **Disable Proxy ARP on egress interface** e **Lookup route table to locate egress interface**. Click **OK**.



6. Clique em **Aplicar** para que as alterações tenham efeito.



Esta é a saída CLI equivalente para a configuração NAT Isento de NAT ou Identity NAT:

```
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 (encaminhamento) com estático

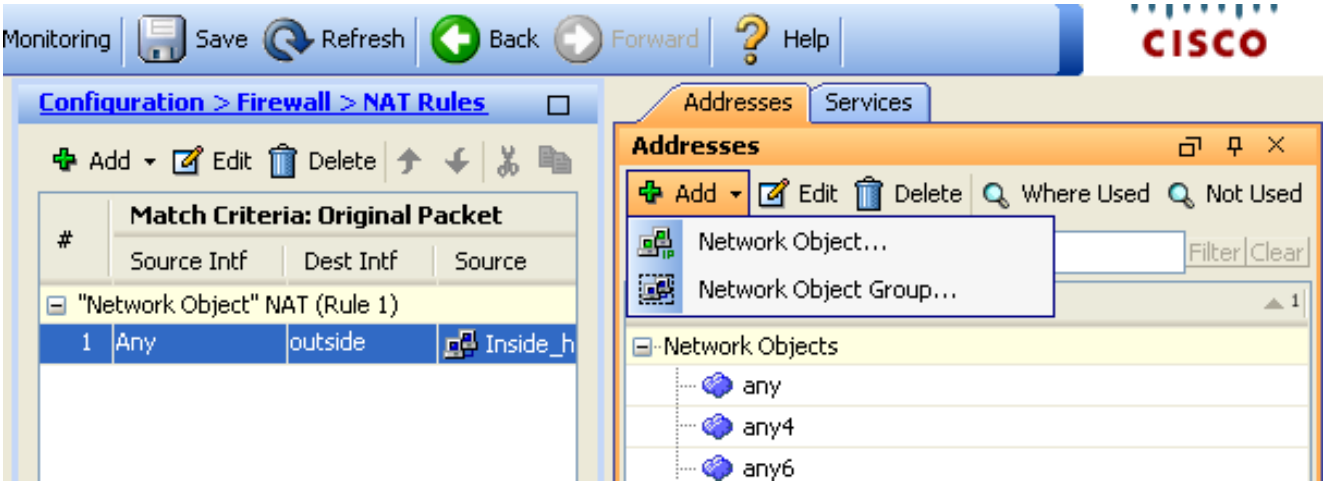
O encaminhamento de portas ou o redirecionamento de portas é um recurso útil no qual os usuários externos tentam acessar um servidor interno em uma porta específica. Para conseguir isso, o servidor interno, que tem um endereço IP privado, pode ser convertido em um endereço IP público que, por sua vez, tem acesso permitido para a porta específica.

Neste exemplo, o usuário externo deseja acessar o servidor SMTP, 203.0.113.15 na porta 25. Isso é feito em duas etapas:

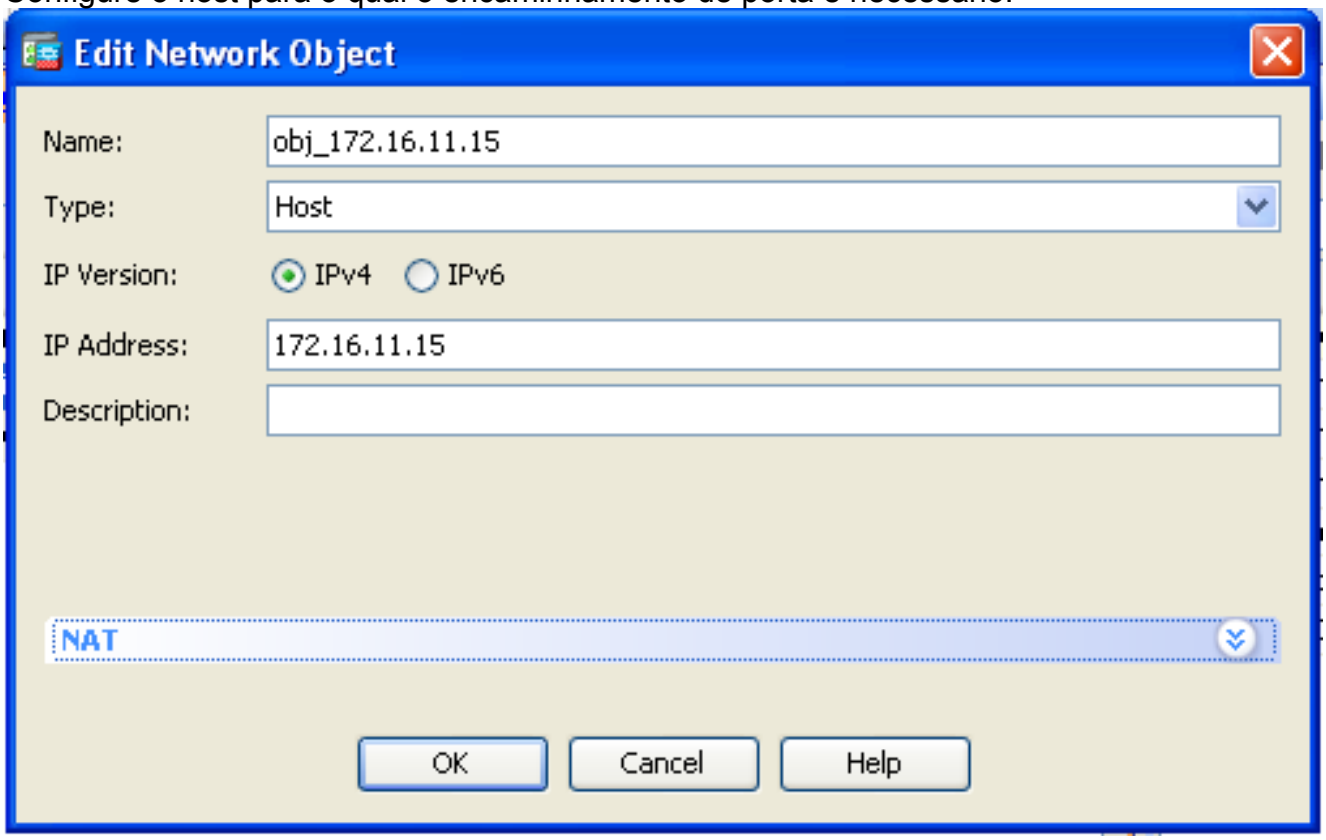
1. Converta o servidor de correio interno, 172.16.11.15 na porta 25, para o endereço IP público, 203.0.113.15 na porta 25.
2. Permita o acesso ao servidor de correio público, 203.0.113.15 na porta 25.

Quando o usuário externo tenta acessar o servidor, 203.0.113.15 na porta 25, esse tráfego é redirecionado para o servidor de correio interno, 172.16.11.15 na porta 25.

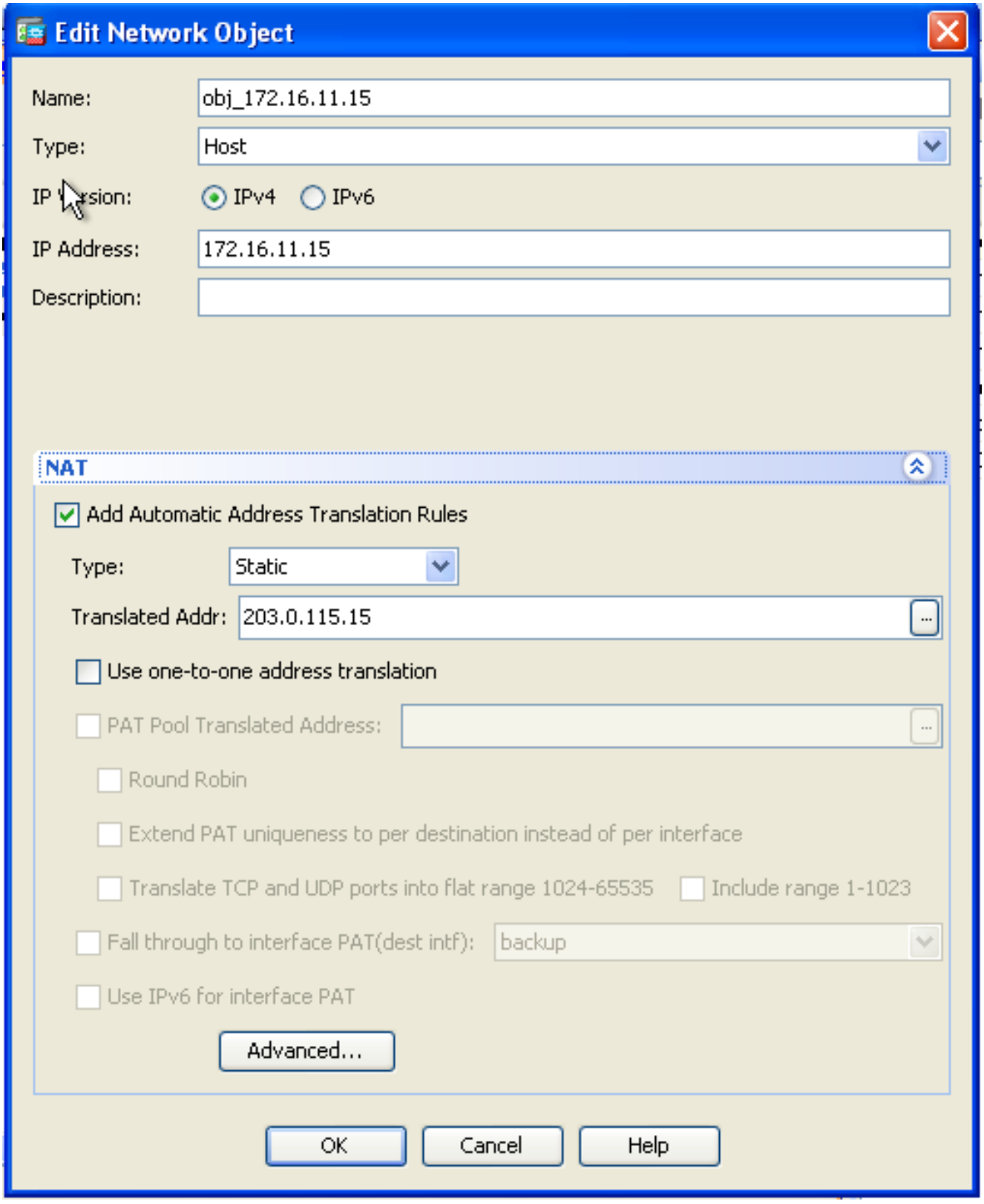
1. Selecione **Configuration > Firewall > NAT Rules**. Clique em **Add** e escolha **Network Object** para configurar uma regra NAT estática.



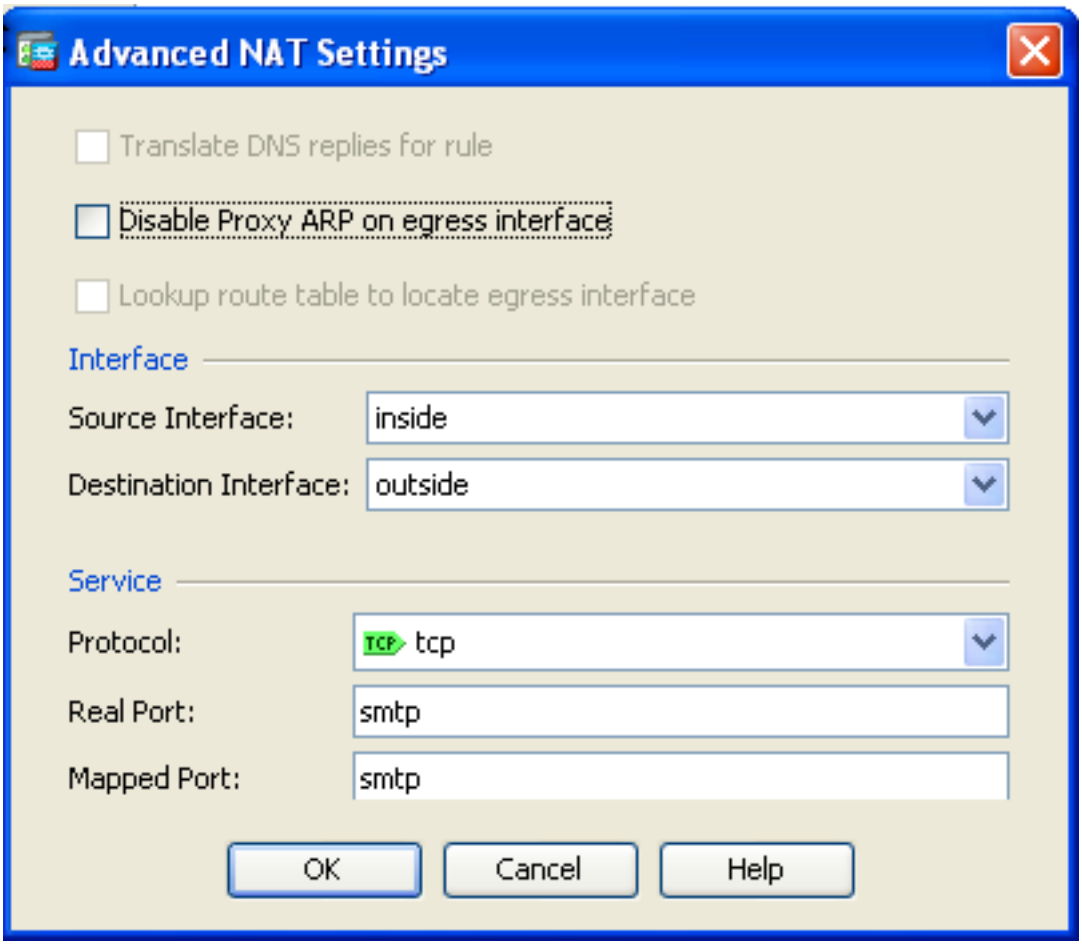
2. Configure o host para o qual o encaminhamento de porta é necessário.



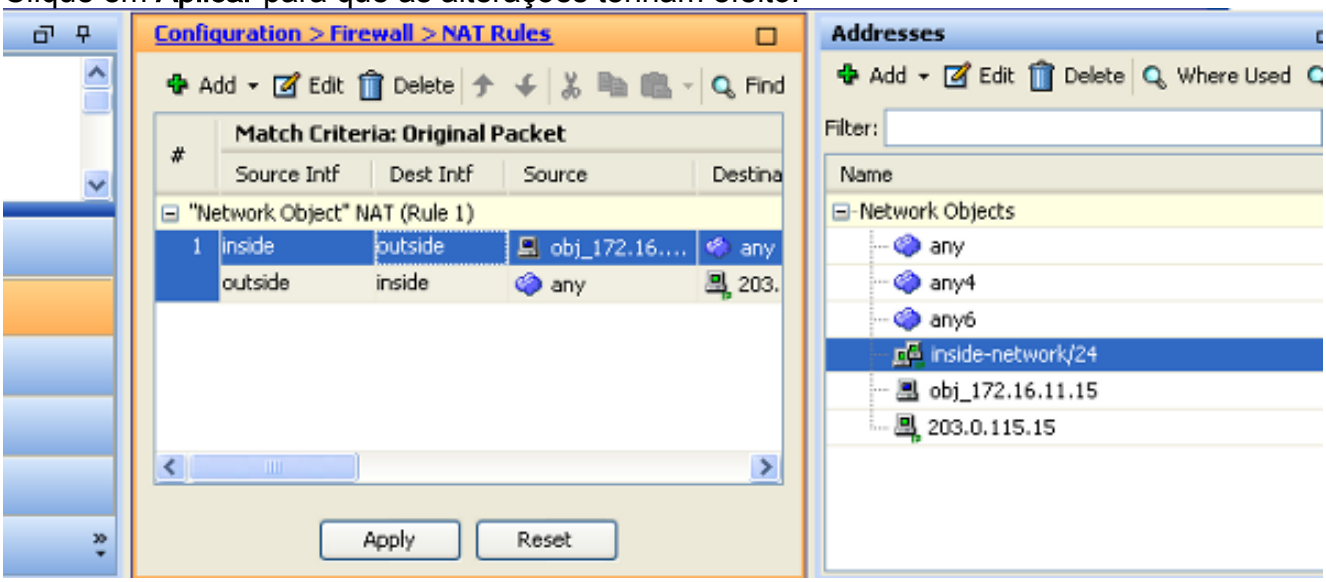
3. Expanda NAT. Marque a caixa de seleção **Add Automatic Address Translation Rules**. Na lista suspensa Tipo, escolha **Estático**. No campo Endereço traduzido, insira o endereço IP. Clique em **Advanced** para selecionar as interfaces de serviço, origem e destino.



4. Nas listas suspensas Interface de Origem e Interface de Destino, escolha as interfaces apropriadas. Configure o serviço. Click **OK**.



5. Clique em **Aplicar** para que as alterações tenham efeito.



Esta é a saída CLI equivalente para esta configuração NAT:

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

Verificar

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

O Cisco CLI Analyzer (somente clientes registrados) aceita alguns comandos show. Use o Cisco

CLI Analyzer para visualizar uma análise da saída do comando show.

Acesse um site via HTTP com um navegador da Web. Este exemplo usa um site hospedado em 198.51.100.100. Se a conexão for bem-sucedida, essa saída poderá ser vista na CLI do ASA.

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 Web é permitido de volta pelo firewall porque ele corresponde a uma ***conexão*** na tabela de conexão do firewall. O tráfego que corresponde a uma conexão preexistente é permitido através do firewall sem ser bloqueado por uma ACL de interface.

Na saída anterior, o cliente na interface interna estabeleceu uma conexão com o host 198.51.100.100 fora da interface externa. Essa conexão é feita com o protocolo TCP e está ociosa por seis segundos. Os sinalizadores de conexão indicam o estado atual dessa conexão. Mais informações sobre sinalizadores de conexão podem ser encontradas em Sinalizadores de Conexão 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 gera syslogs durante a operação normal. Os syslogs variam em verbosidade com base na configuração de registro. A saída mostra dois syslogs que são vistos no nível seis, ou o nível 'informativo'.

Neste exemplo, há dois syslogs gerados. A primeira é uma mensagem de log que indica que o firewall criou uma conversão, especificamente uma conversão TCP dinâmica (PAT). Ele indica o endereço IP e a porta origem e o endereço IP e a porta convertidos à medida que o tráfego atravessa as interfaces internas para as externas.

O segundo syslog indica que o firewall criou uma conexão em sua tabela de conexão para esse tráfego específico entre o cliente e o servidor. Se o firewall foi configurado para bloquear essa tentativa de conexão, ou algum outro fator inibiu a criação dessa conexão (restrições de recursos ou uma possível configuração incorreta), o firewall não gerará um log que indique que a conexão foi criada. Em vez disso, registraria um motivo para a conexão ser negada ou uma indicação sobre qual fator inibiu a conexão de ser criada.

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
```

A funcionalidade do packet tracer no ASA permite especificar um pacote *simulado* e ver todas as várias etapas, verificações e funções pelas quais o firewall passa ao processar o tráfego. Com essa ferramenta, é útil identificar um exemplo de tráfego que você acredita *poder* passar pelo firewall e usar essa tupla de 5 para simular o tráfego. No exemplo anterior, o packet tracer é usado para simular uma tentativa de conexão que atenda a estes critérios:

- O pacote simulado chega por dentro.
- O protocolo usado é o TCP.
- O endereço IP simulado do cliente é 172.16.11.5.
- O cliente envia o tráfego originado na porta 1234.
- O tráfego é destinado a um servidor no endereço IP 198.51.100.100.
- O tráfego é destinado à porta 80.

Observe que não houve menção à interface externa no comando. Isso é feito pelo design do packet tracer. A ferramenta informa como o firewall processa esse tipo de tentativa de conexão, o que inclui como o rotearia e de que interface. Mais informações sobre o Packet Tracer podem ser encontradas em Rastreando Pacotes com o Packet Tracer.

Capturar

Aplicar captura

```
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>
O firewall ASA pode capturar o tráfego que entra ou sai de suas interfaces. Essa funcionalidade de captura é fantástica porque pode comprovar definitivamente se o tráfego chega ou sai de um firewall. O exemplo anterior mostrou a configuração de duas capturas chamadas capin e capout nas interfaces interna e externa, respectivamente. Os comandos capture usaram a palavra-chave match, que permite que você seja específico sobre qual tráfego deseja capturar.

Para a captura capin**,** você indicou que queria corresponder o tráfego visto na interface interna (entrada ou saída) que corresponde ao host TCP 172.16.11.5 host 198.51.100.100. Em outras palavras, você quer capturar qualquer tráfego TCP que é enviado do host 172.16.11.5 para o host 198.51.100.100 ou vice-versa. O uso da palavra-chave match permite que o firewall capture esse tráfego bidirecionalmente. O comando capture definido para a interface externa não faz referência ao endereço IP do cliente interno porque o firewall conduz o PAT nesse endereço IP do cliente. Como resultado, você não pode fazer correspondência com esse endereço IP do cliente. Em vez disso, este exemplo usa any para indicar que todos os endereços IP possíveis corresponderiam a essa condição.

Depois de configurar as capturas, você tentará estabelecer uma conexão novamente e continuará a exibir as capturas com o comando **show capture** <capture_name> . Neste exemplo, você pode ver que o cliente conseguiu se conectar ao servidor como evidente pelo handshake triplo do TCP visto nas capturas.

Troubleshoot

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

Informações Relacionadas

- Exemplo da configuração de syslog do ASA
- Capturas de pacotes do ASA com CLI e Exemplo de Configuração do ASDM
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.