PIX/ASA 7.x: Mova Redirection(Forwarding) com nat, o global, estática e comandos access-list

Índice

Introdução

A fim de maximizar a segurança quando você implementa o Cisco PIX Security Appliance versão 7.0, é importante compreender como os pacotes trafegam entre interfaces de segurança mais elevada e interfaces de segurança mais baixa quando os comandos **nat-control**, **nat**, **global**, **static**, **access-list** e **access-group** são usados. Este documento explica as diferenças entre esses comandos e também como configurar o Redirecionamento de Portas (Encaminhamento) e os recursos da Tradução de Endereço de Rede (NAT) externa no PIX Software versão 7.x com o uso da interface de linha de comando ou do Adaptive Security Device Manager (ASDM).

Nota: Algumas opções no ASDM 5.2 ou posterior podem ser diferentes do que as opções do ASDM 5.1. Consulte a documentação do ASDM para obter mais informações.

Pré-requisitos

Requisitos

Consulte Permitindo o Acesso HTTPS para o ASDM para permitir que o dispositivo seja configurado pelo ASDM.

Componentes Utilizados

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

- Cisco PIX 500 Series Security Appliance Software versão 7.0 ou posterior
- ASDM versão 5.x ou posterior

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.

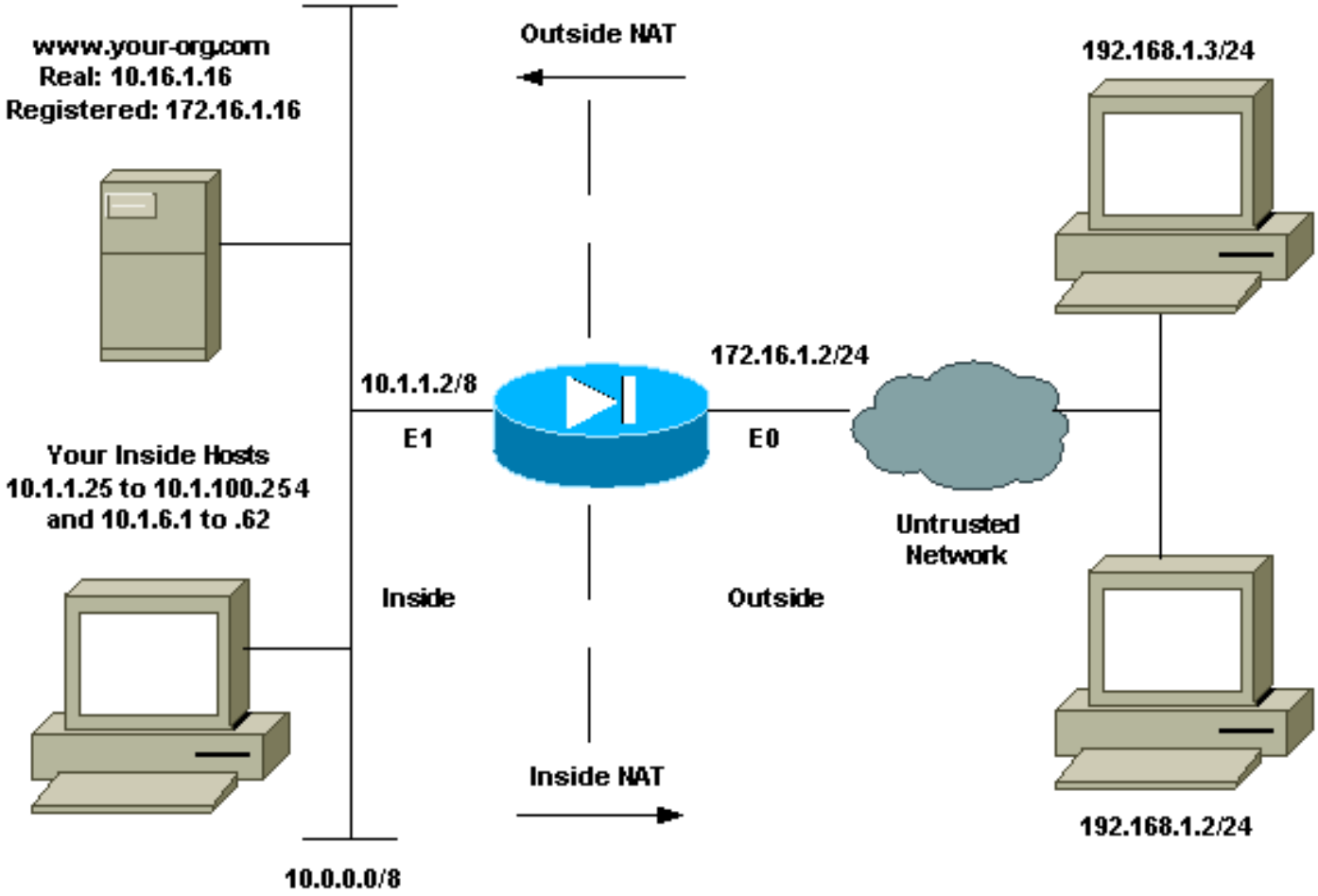
Produtos Relacionados

Você também pode usar esta configuração com o Cisco ASA Security Appliance versão 7.x ou posterior.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

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.

Configuração inicial

Os nomes das interfaces são:

- **interface ethernet 0** — nameif outside
- **interface ethernet 1** — nameif inside

Nota: Para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados).

Permitir o Acesso de Externo

O acesso externo descreve conexões de uma interface de nível de segurança mais elevado para uma interface de nível de segurança mais baixo. Isso inclui conexões de dentro para fora, dentro de DMZs (Zonas Desmilitarizadas) e DMZs para fora. Isso também pode incluir conexões de uma DMZ para outra, desde que a interface de origem da conexão possua um nível de segurança mais elevado do que a de destino. Revise a configuração do "nível de segurança" nas interfaces do PIX para confirmar isso.

Este exemplo mostra o nível de segurança e a configuração do nome da interface:

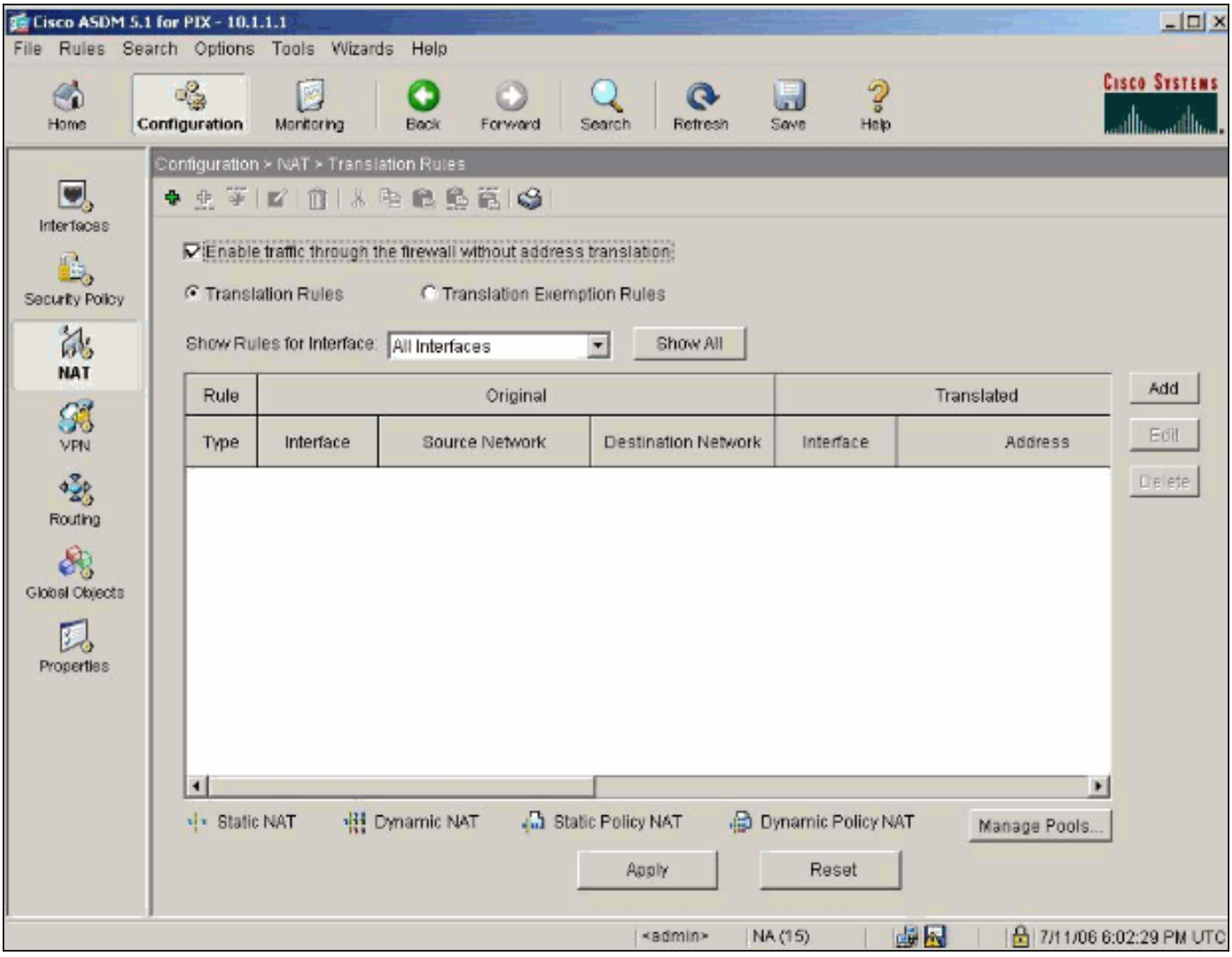
```
pix(config)#interface ethernet 0 pix(config-if)#security-level 0 pix(config-if)#nameif outside
pix(config-if)#exit
```

O PIX 7.0 apresenta o comando **nat-control**. Você pode usar o comando **nat-control no** modo de configuração para especificar se o NAT é necessário para as comunicações externas. Com o controle do NAT habilitado, a configuração das regras do NAT é necessária para permitir o tráfego de saída, como no caso das versões anteriores do PIX Software. Se o controle do NAT estiver desabilitado (**nenhum nat-control**), os host internos poderão se comunicar com as redes externas sem a configuração de uma regra de NAT. No entanto, se houver host internos que não possuam endereços públicos, você precisará configurar o NAT para esses hosts.

Para configurar o controle do NAT com o uso do ASDM, selecione a guia Configuration da janela ASDM Home e escolha **NAT no** menu de recursos.

Permita o tráfego através do firewall sem tradução: Esta opção foi apresentada no PIX versão 7.0(1). Quando esta opção é marcada, nenhum comando **nat-control** é executado na configuração. Este comando significa que nenhuma tradução é necessária para atravessar o firewall. Esta opção é normalmente marcada somente quando os host internos possuem endereços IP públicos ou a topologia da rede não exige que os host internos sejam traduzidos para nenhum endereço IP.

Se os host internos possuírem endereços IP privados, essa opção deverá ser desmarcada de modo que os host internos possam ser traduzidos para um endereço IP público e acessar a Internet.



Há duas políticas que são necessárias para permitir o acesso externo com controle do NAT. O primeiro é um método de conversão. Ele pode ser uma tradução estática com o uso do comando

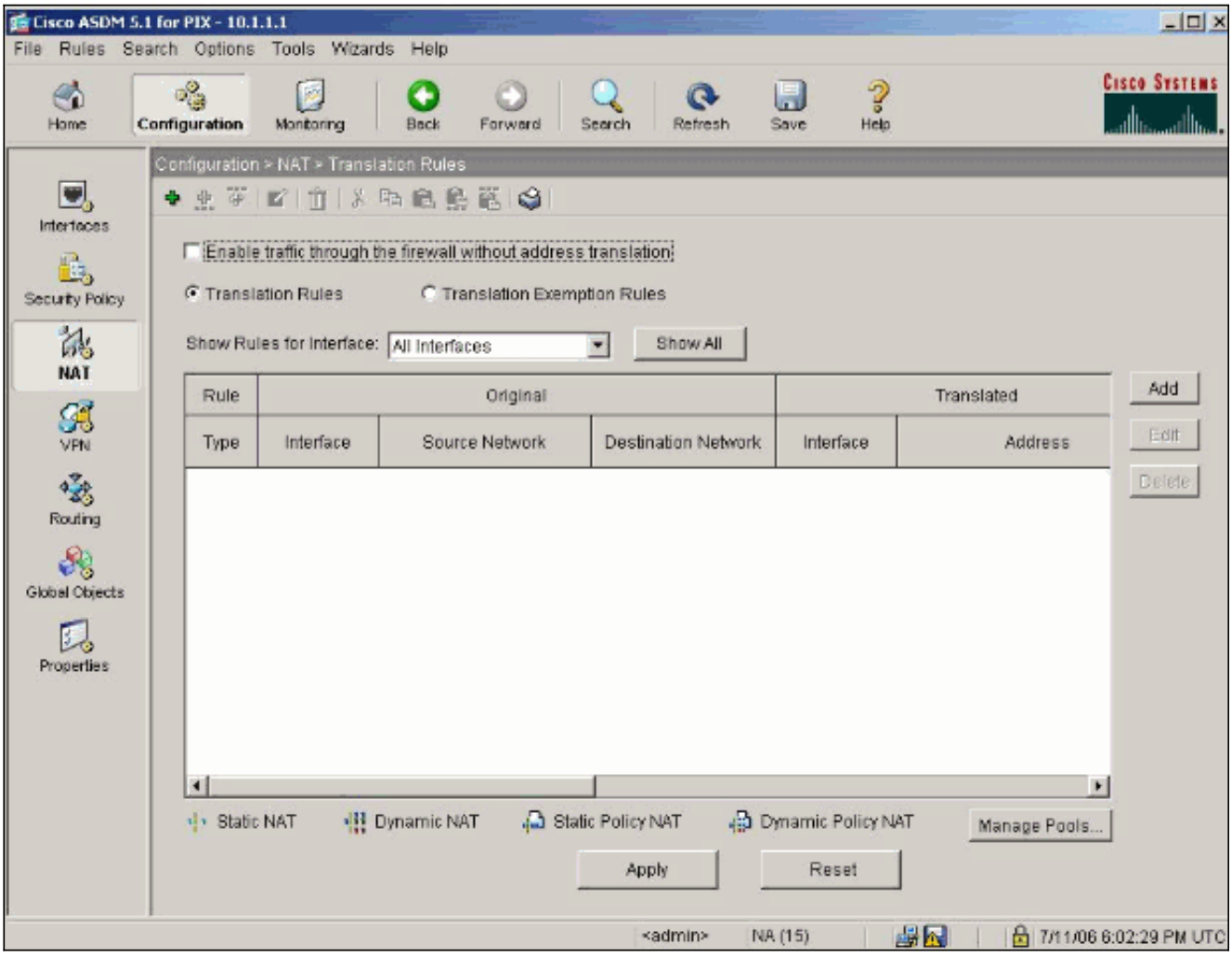
static ou uma tradução dinâmica com o uso de uma regra **nat/global**. Isso não será necessário se o controle do NAT estiver desabilitado e seus host internos possuírem endereços públicos.

A outra exigência para o acesso externo (que se aplica independentemente do NAT estar habilitado ou desabilitado) é se há uma lista de controle de acesso (ACL) presente. Se houver uma ACL, ela deverá permitir o acesso do host de origem ao host de destino com o uso do protocolo e da porta específicos. Por padrão, não há restrições de acesso às conexões externas por meio do PIX. Isso significa que, se não houver nenhuma ACL configurada para a interface de origem, a conexão externa será permitida por padrão se houver um método de tradução configurado.

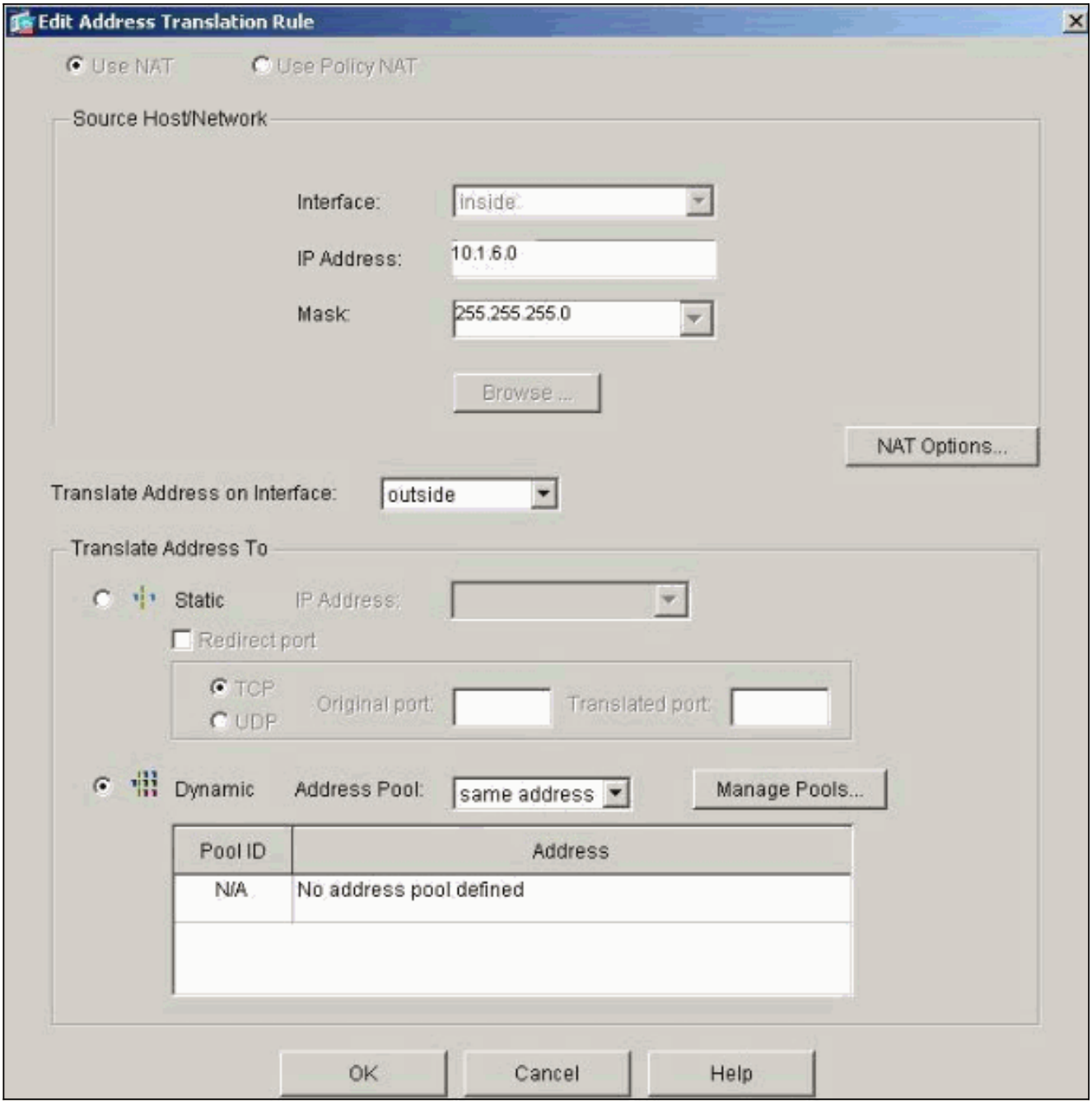
Permitir o Acesso de Host Internos às Redes Externas via NAT

Essa configuração concede a todos os hosts da sub-rede 10.1.6.0/24 acesso ao meio externo. Para fazer isso, use os comandos **nat** e **global** conforme demonstrado neste procedimento.

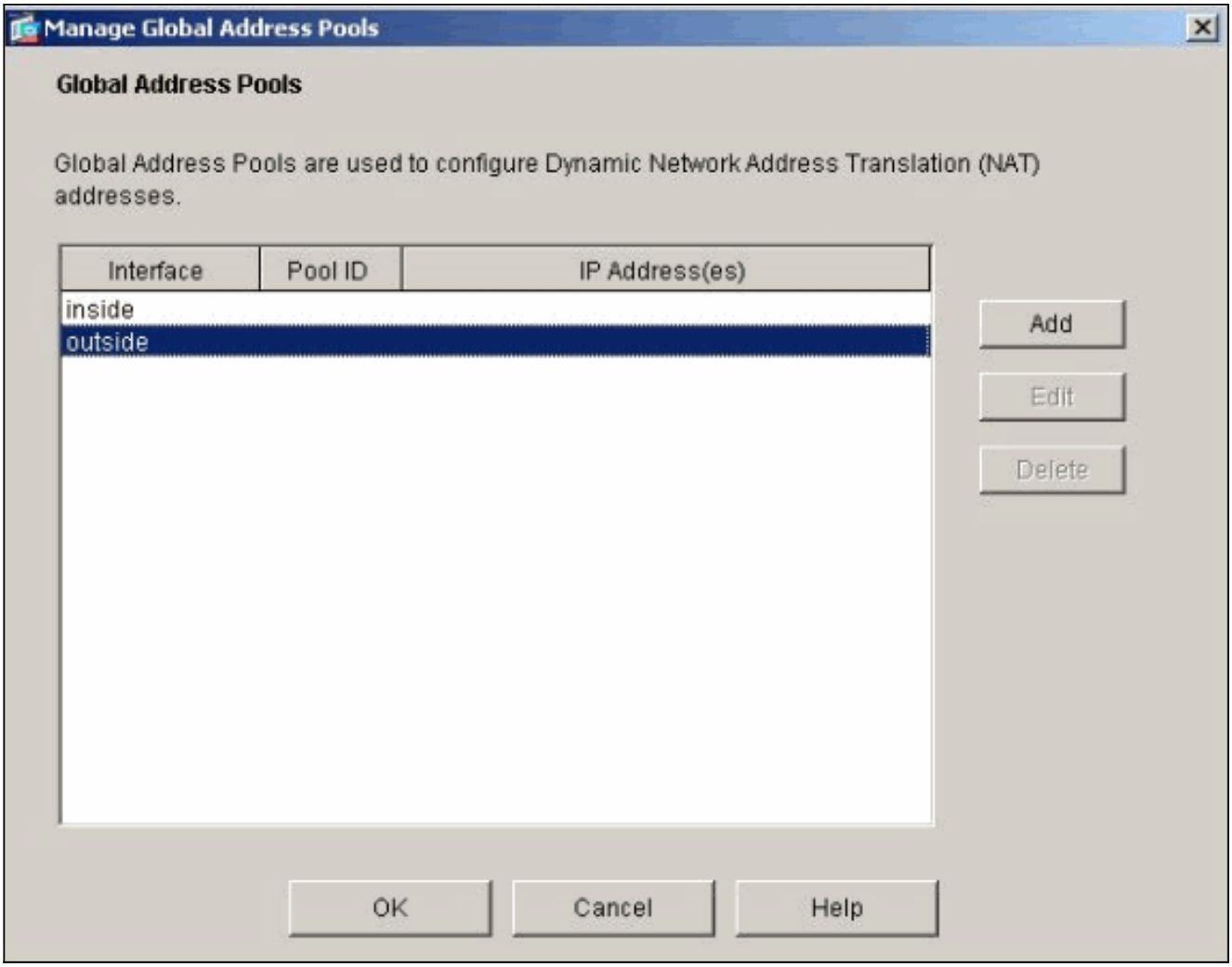
1. Defina o grupo interno que você deseja incluir para o NAT.
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. Especifique um pool de endereços na interface externa na qual os hosts definidos na declaração de NAT são traduzidos.
   ```
   global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
   ```
3. Use o ASDM para criar seu pool de endereços global. Escolha **Configuration > Features > NAT** e desmarque **Enable traffic through the firewall without address translation**. Em seguida, clique em **Add** para configurar a regra de NAT.



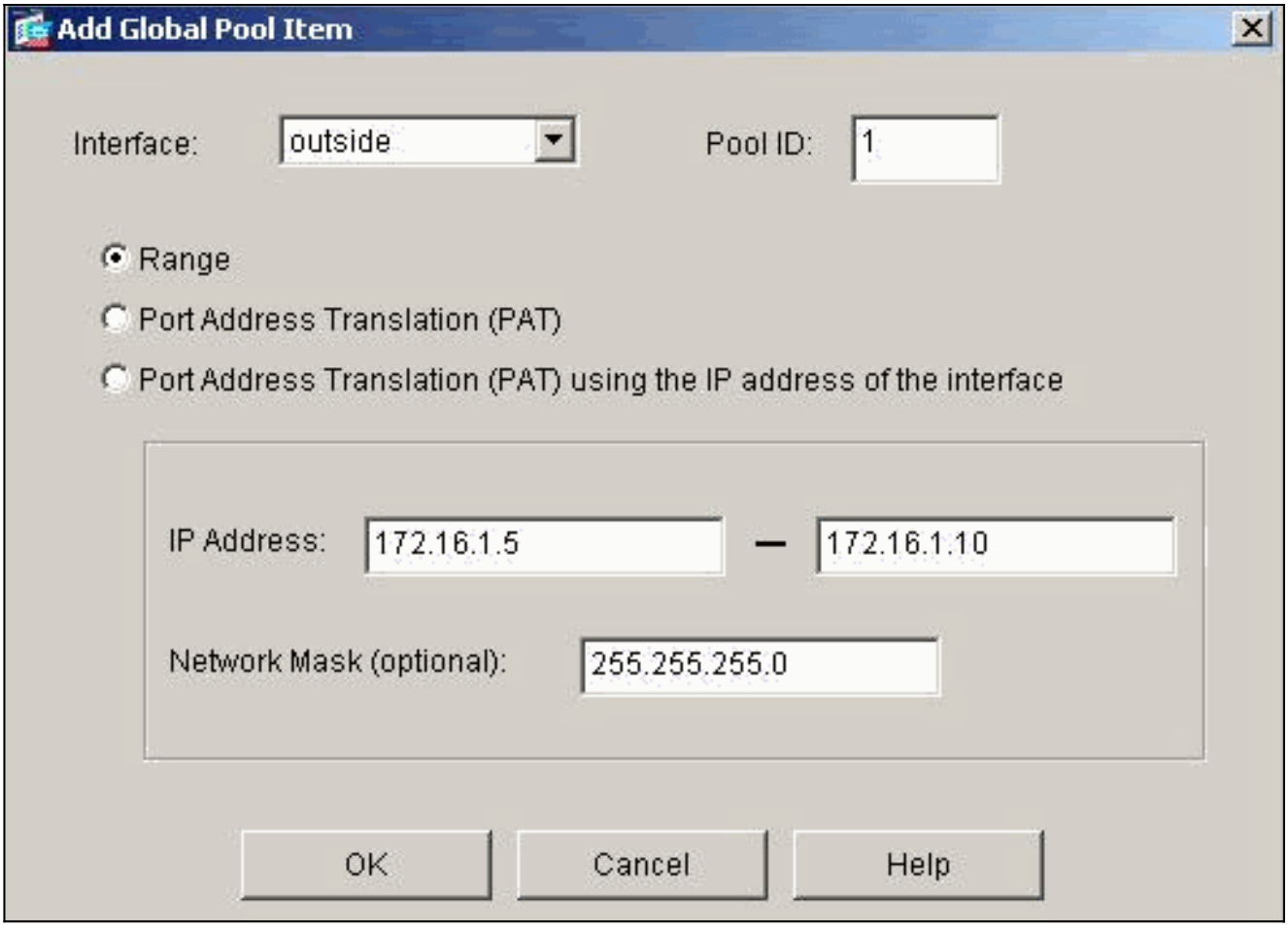
4. Clique em **Manage Pools** para definir os endereços do pool de NAT.



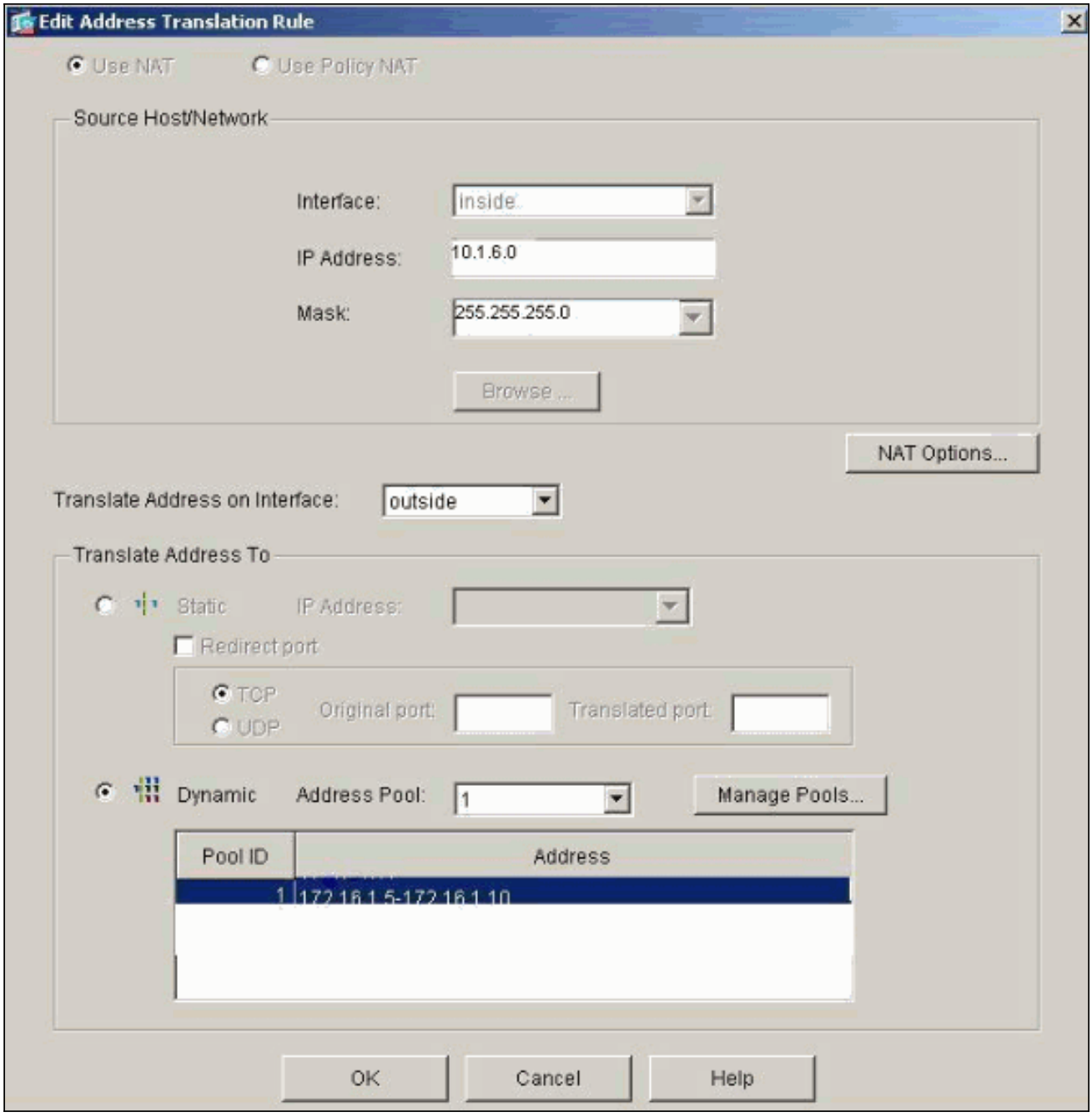
5. Escolha **Outside > Add** e escolha um intervalo para especificar um pool de endereços.



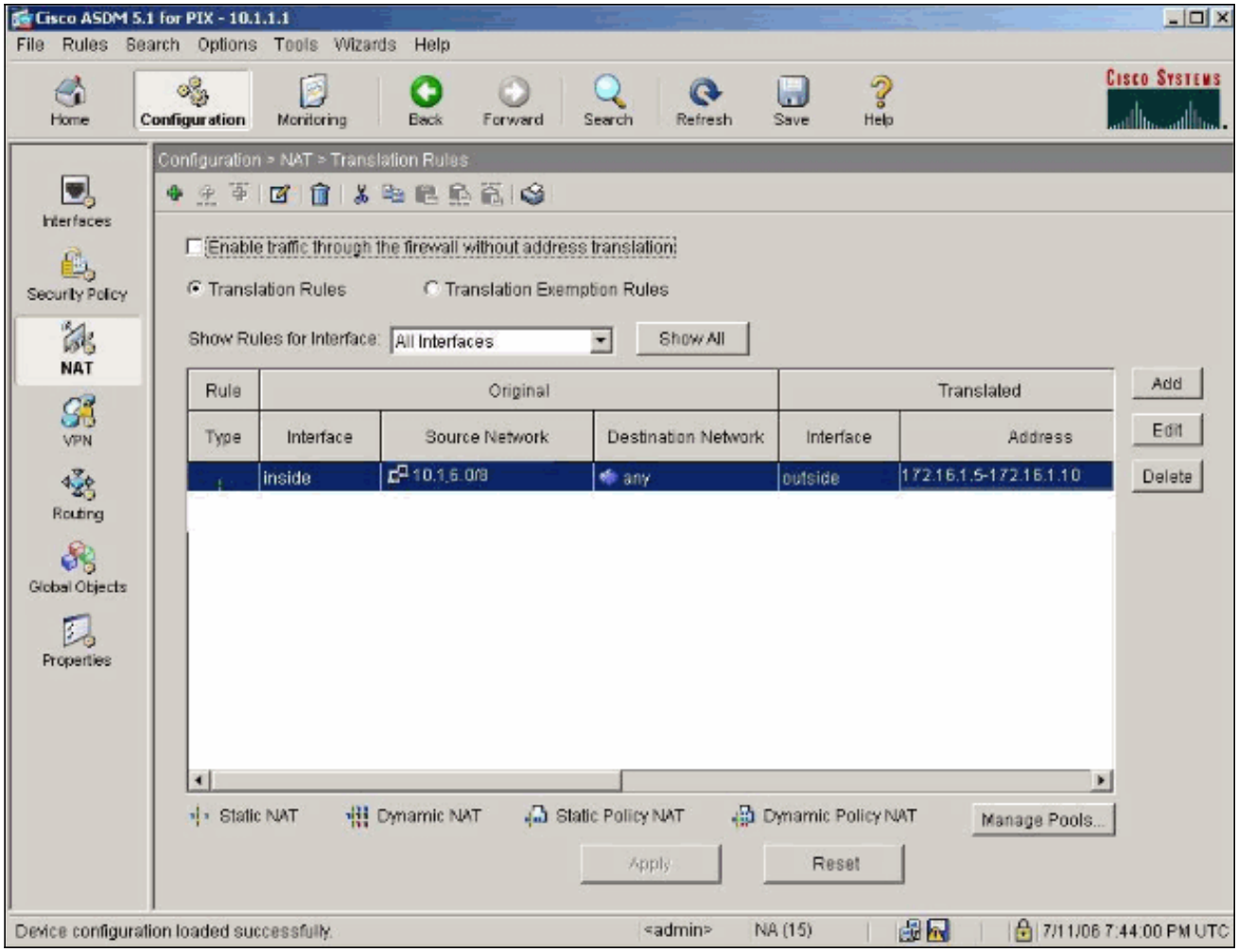
6. Insira seu intervalo de endereços, um ID de Pool e clique em **OK**.



7. Escolha **Configuration > Features > NAT > Translation Rules** para criar a regra de tradução.
8. Escolha **Inside** como a interface de origem e insira os endereços que deseja traduzir com o NAT.
9. Para Translate Address on Interface, selecione **Outside**, escolha **Dynamic** e selecione o pool de endereços que acabou de configurar.
10. Clique em
    OK.



11. A tradução é mostrada nas regras de tradução em **Configuration > Features > NAT > Translation Rules**.



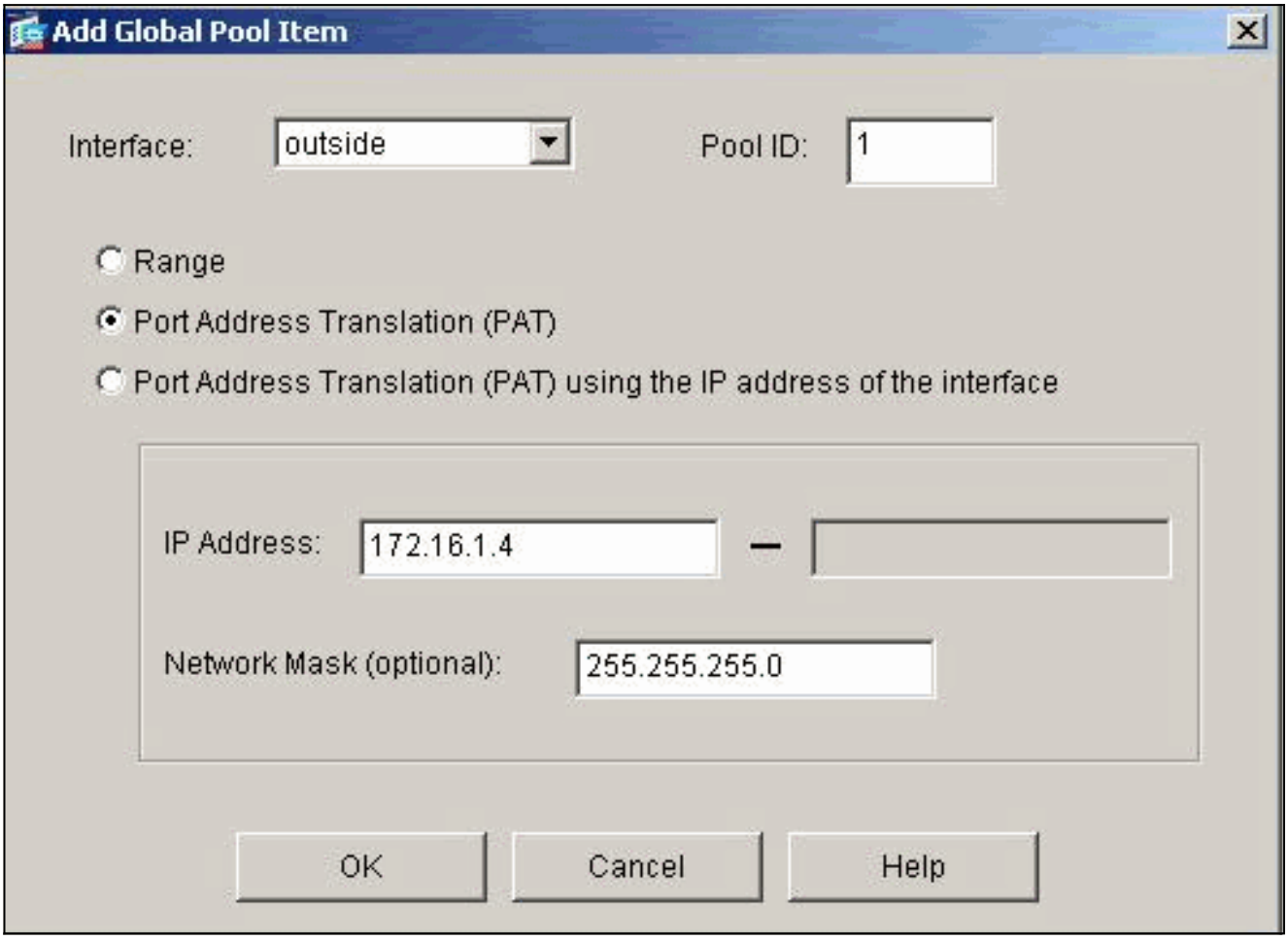
Agora os hosts internos podem acessar as redes externas. Quando hosts internos iniciam uma conexão com o exterior, eles são convertidos para um endereço do conjunto global. Os endereços são atribuídos do pool global na forma "primeiro a chegar, primeiro a ser traduzido" e começam a partir do menor endereço do pool. Por exemplo, se o host 10.1.6.25 for o primeiro a iniciar uma conexão com o meio externo, ele receberá o endereço 172.16.1.5. O próximo host receberá 172.16.1.6 e assim por diante. Esta não é uma tradução estática, e o timeout da tradução é excedido após um período de inatividade definido pelo comando **timeout xlate hh: milímetro: ss** . Se houver mais host internos do que endereços no pool, o endereço final no pool será usado para a Tradução de Endereço de Porta (PAT).

Permitir o Acesso de Host Internos às Redes Externas via PAT

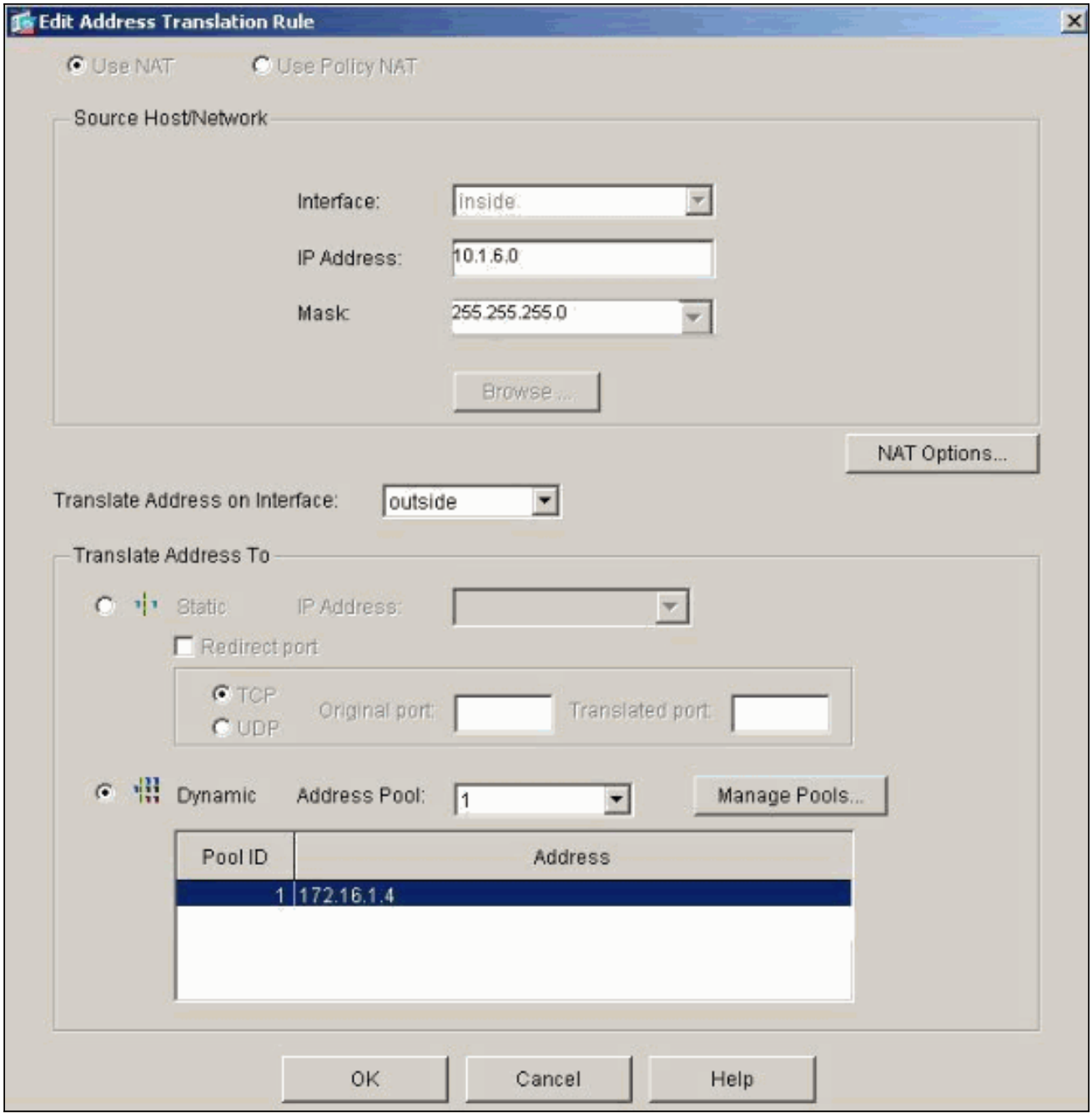
Se desejar que os host internos compartilhem um único endereço público para a tradução, use o PAT. Se a **declaração global** especificar um endereço, esse endereço terá a porta traduzida. O PIX permite uma conversão de porta por interface, e essa conversão suporta até 65.535 objetos xlate ativos para o endereço global único. Conclua estes passos para permitir o acesso dos host internos às redes externas com o uso do PAT.

1. Defina o grupo interno que você deseja incluir no PAT (ao usar 0 0, você seleciona todos os host internos.)
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. Especifique o endereço global que deseja usar para o PAT. Esse pode ser o endereço da interface.
   ```
   global (outside) 1 172.16.1.4 netmask 255.255.255.0
   ```

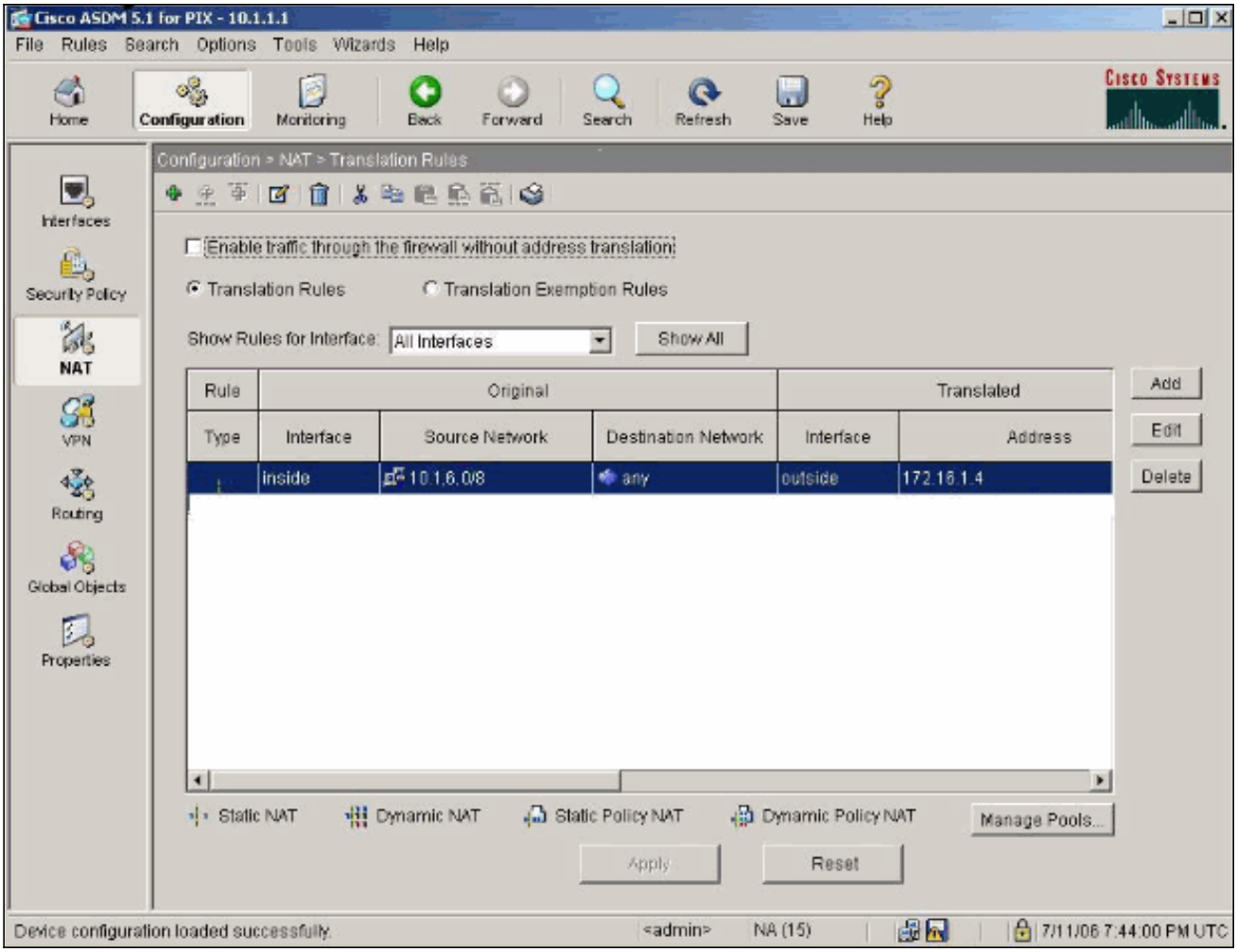
3. No ASDM, escolha **Configuration > Features > NAT** e desmarque **Enable traffic through the firewall without address translation**.
4. Clique em **Add** para configurar a regra de NAT.
5. Escolha **Manage Pools** para configurar seu endereço PAT.
6. Escolha o **Outside > Add** e clique em **Port Address Translation (PAT)** para configurar um único endereço para o PAT.
7. Insira um endereço, um ID de Pool e clique em **OK**.



8. Escolha **Configuration > Features > NAT > Translation Rules** para criar a regra de tradução.
9. Selecione **Inside** como a interface de origem e insira os endereços que deseja traduzir com o NAT.
10. Para Translate Address on Interface, selecione **Outside**, escolha **Dynamic** e selecione o pool de endereços que acabou de configurar. Clique em **OK**.



11. A tradução é mostrada nas regras de tradução em **Configuration > Features > NAT > Translation Rules**.



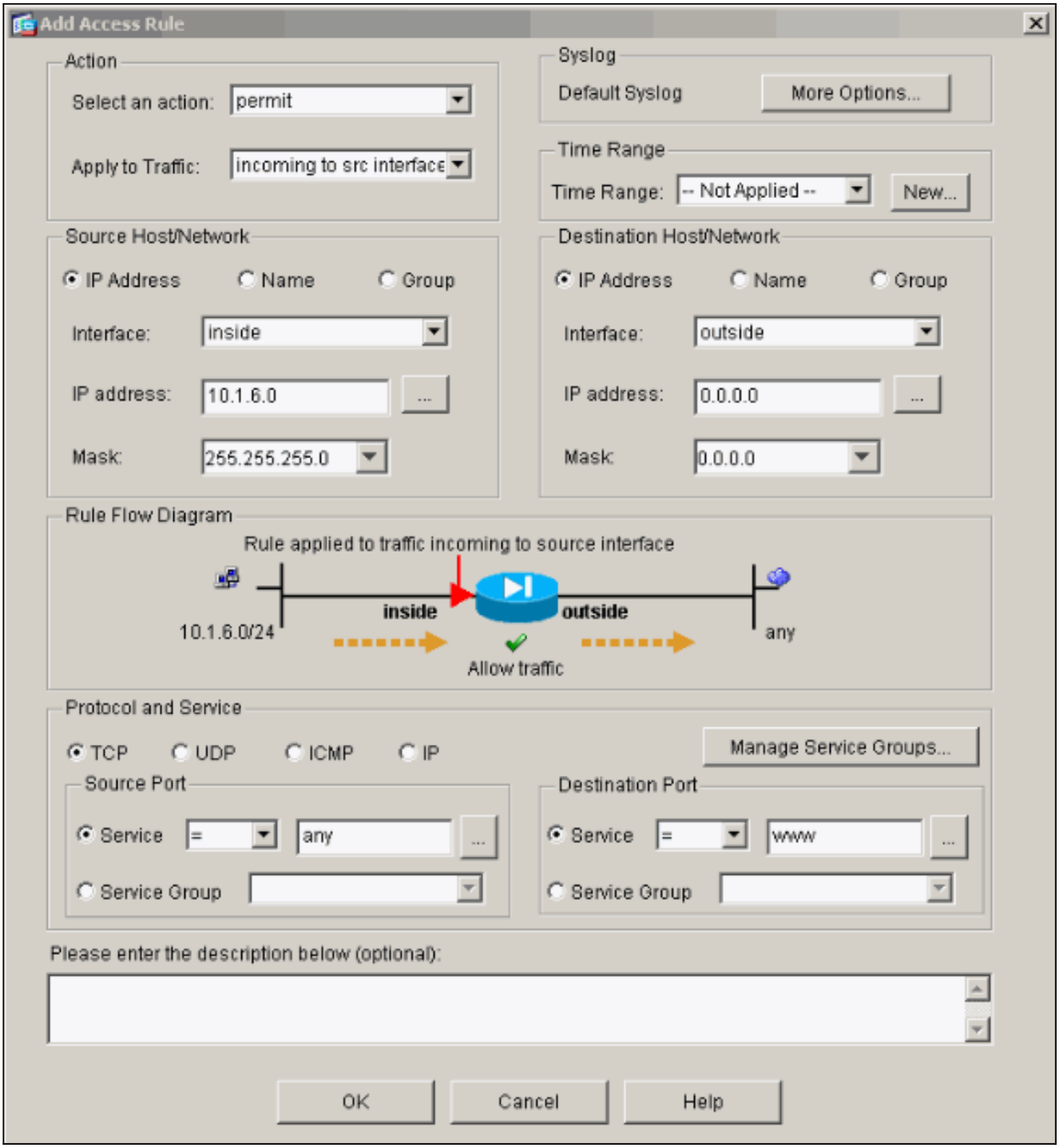
Há algumas coisas a considerar quando você usa o PAT.

- Os endereços IP que você especificar para o PAT não poderão pertencer a outro pool de endereços global.
- O PAT não funciona com aplicações H.323, servidores de nome de cache e o Point-to-Point Tunneling Protocol (PPTP). O PAT funciona com o Domain Name Service (DNS), FTP e FTP passivo, HTTP, email, RPC, rshell, Telnet, filtragem de URL e traceroute externo.
- Não use o PAT quando precisar executar aplicativos multimídia através do firewall. Os aplicativos multimídia podem entrar em conflito com os mapeamentos de porta fornecidos pelo PAT.
- No PIX Software Release 4.2(2), o recurso PAT não funciona com pacotes de dados IP que chegam em ordem reversa. O PIX Software Release 4.2(3) corrige este problema.
- Os endereços IP no pool de endereços global especificado com o **comando global** exigem entradas de DNS reverso a fim de garantir que todos os endereços da rede externa possam ser acessados via PIX. Para criar mapeamentos de DNS reversos, use um registro DNS Pointer (PTR) no arquivo de mapeamento de endereços em nome para cada endereço global. Sem as entradas de PTR, os sites podem experimentar conectividade lenta ou intermitente à Internet e as solicitações de FTP falham constantemente.Por exemplo, se um endereço IP global é 192.168.1.3 e o nome de domínio para o PIX Security Appliance é pix.caguana.com, o registro PTR é:`3.1.1.175.in-addr.arpa. IN PTR pix3.caguana.com`
  `4.1.1.175.in-addr.arpa. IN PTR pix4.caguana.com & so on.`

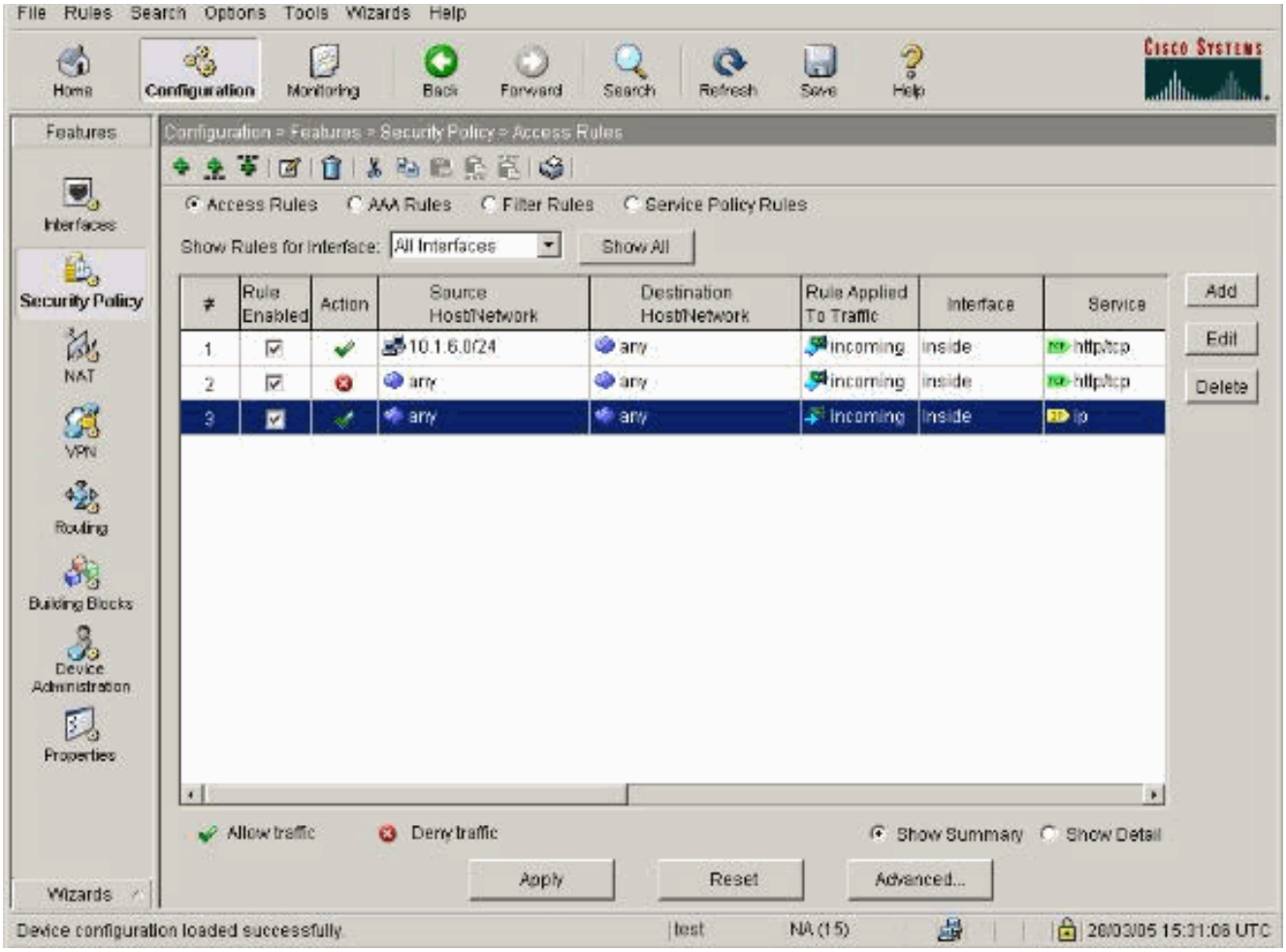
Restrigir o Acesso de Host Internos a Redes Externas

Se houver um método de tradução válido definido para o host de origem, e nenhuma ACL definida para a interface do PIX de origem, então a conexão externa será permitida por padrão. No entanto, em alguns casos é necessário restringir o acesso externo baseado na fonte, no destino, no protocolo e/ou na porta. Para fazer isso, configure uma ACL com o comando **access-list** e aplique-o à interface do PIX de origem da conexão com o comando **access-group**. Você pode aplicar ACLs do PIX 7.0 tanto na direção de entrada quanto na de saída. Este procedimento é um exemplo que permite o acesso externo HTTP a uma sub-rede, mas nega a todos os demais hosts o acesso HTTP ao meio externo ao mesmo tempo em que permite todo o tráfego IP restante para todo mundo.

1. Defina a ACL.
   access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www access-list acl_outbound deny tcp any any eq www access-list acl_outbound permit ip any any **Nota:** As ACLs do PIX diferem das ACLs dos roteadores Cisco IOS® no sentido em que o PIX não usa uma máscara curinga como o Cisco IOS. Ele usa uma máscara de sub-rede regular na definição de ACL. Assim como ocorre com os roteadores Cisco IOS, a ACL do PIX possui uma declaração "negar tudo" implícita no final.**Nota:** As entradas de lista de acesso novas serão adicionadas ao fim dos ACE existentes. Se você precisa um ACE específico processado primeiramente, você pode usar a `linha` palavra-chave na lista de acesso. Este é um sumário do comando example:`access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any`
2. Aplique a ACL à interface interna.
   access-group acl_outbound in interface inside
3. Use o ASDM para configurar a primeira entrada da lista de acesso no passo 1 para permitir o tráfego HTTP de 10.1.6.0/24. Escolha **Configuration > Features > Security Policy > Access Rules**.
4. Clique em **Add**, insira as informações mostradas nesta janela e clique em **OK**.



5. Após você inserir as três entradas da lista de acesso, escolha **Configuration> Feature > Security Policy > Access Rules** para exibir estas regras.



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

A maioria das organizações precisam permitir o acesso de hosts não confiáveis aos recursos em suas redes confiáveis. Um exemplo comum é um servidor Web interno. Por padrão, o PIX nega conexões dos host externos para os host internos. Para permitir essa conexão no modo de controle do NAT, use o comando **static** com os comandos **access-list** e **access-group**. Se o controle do NAT estiver desabilitado, somente os comandos **access-list e access-group** serão necessários se nenhuma tradução for executada.

Aplique ACLs às interfaces com um comando **access-group**. Este comando associa a ACL à interface para examinar o tráfego que flui em uma direção específica.

Ao contrário dos comandos **nat** e **global** que permitem a saída do tráfego dos hosts internos, o comando **static** cria uma tradução em dois sentidos que permite que o tráfego dos hosts internos para fora e dos hosts externos para dentro se você adicionar as ACLs/grupos apropriados.

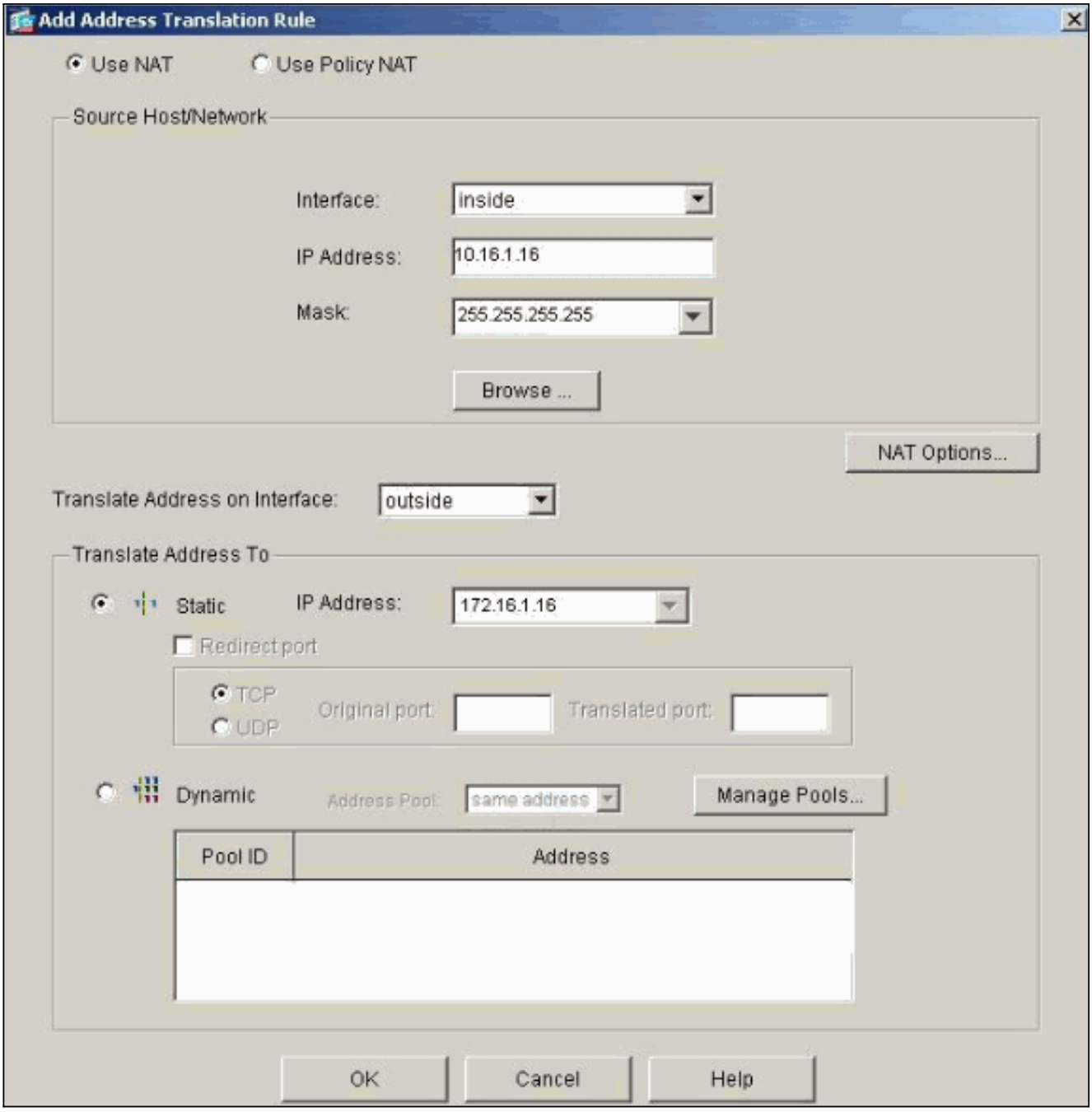
Nos exemplos de configuração do PAT mostrados neste documento, se um host externo tentar se conectar ao endereço global, ele poderá ser usado por milhares de hosts internos. O comando **static** cria um mapeamento um a um. O comando **access-list** define que tipo de conexão é permitido para um host interno e é sempre exigido quando um host de segurança mais baixa se conecta a um host de segurança mais elevada. O comando **access-list** é baseado na porta e no protocolo e pode ser muito permissivo ou muito restritivo com base em que o administrador de sistema quer conseguir.

O diagrama de rede neste documento ilustra o uso destes comandos para configurar o PIX para permitir que qualquer host não confiável se conecte ao servidor Web interno e permitir o acesso do host não confiável 192.168.1.1 a um serviço de FTP na mesma máquina.

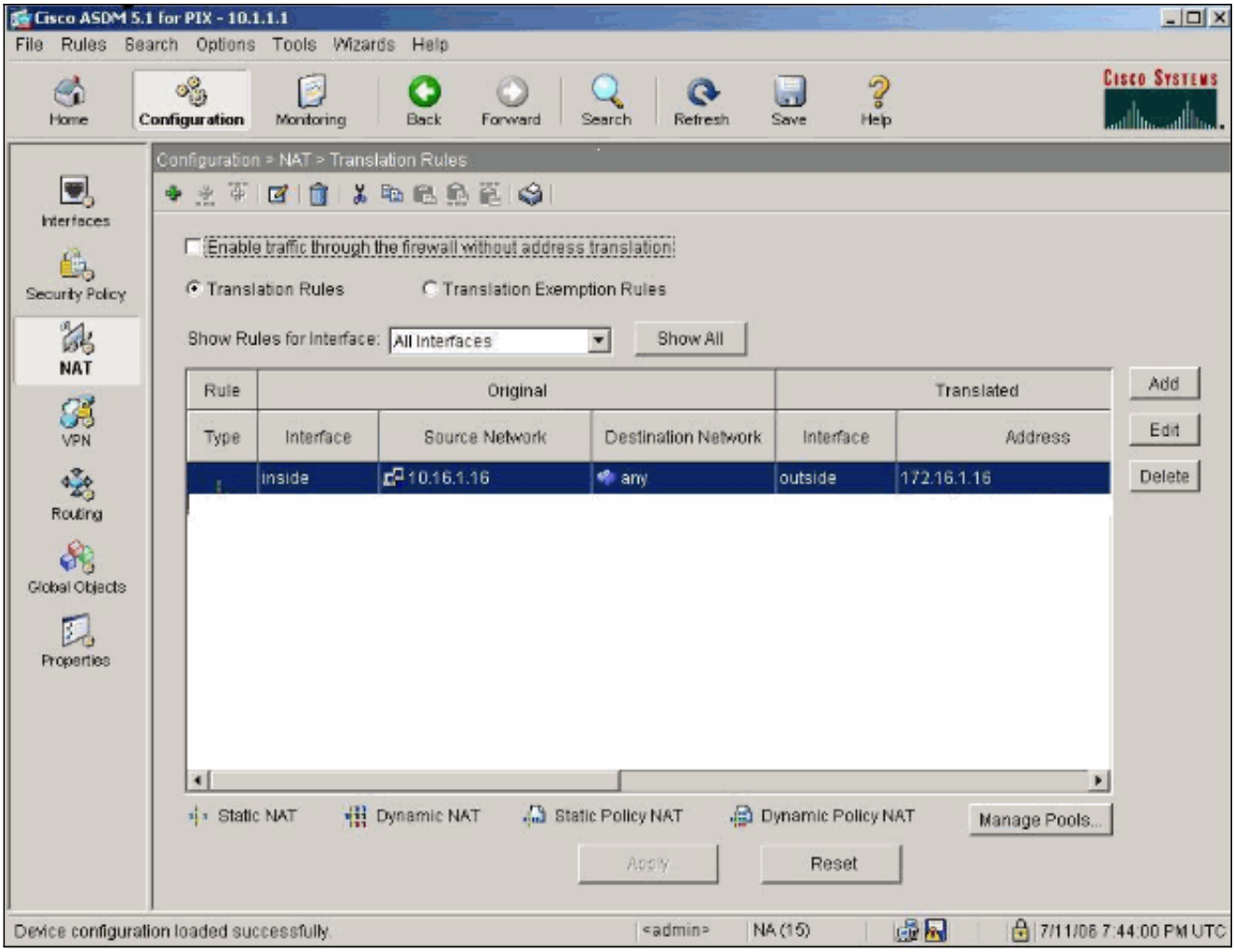
Usar ACL no PIX Versões 7.0 e posteriores

Conclua estes passos para o PIX Software versão 7.0 ou posterior com o uso de ACLs.

1. Se o controle do NAT estiver habilitado, defina uma tradução de endereço estático do servidor Web interno para um endereço externo/global.
   `static (inside, outside) 172.16.1.16 10.16.1.16`
2. Defina quais hosts podem se conectar em quais portas do seu servidor Web/FTP.
   `access-list 101 permit tcp any host 172.16.1.16 eq www access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp`
3. Aplique à ACL à interface externa.
   `access-group 101 in interface outside`
4. **Escolha Configuration > Features > NAT** e clique em **Add** para criar esta tradução estática com o ASDM.
5. Selecione **inside** como a interface de origem e insira o endereço interno para o qual deseja criar uma tradução estática.
6. Escolha **Static** e insira o endereço externo que você deseja traduzir no campo de endereço IP. Clique em
   OK.



7. A tradução é mostrada nas regras de tradução quando você escolhe **Configuration > Features > NAT > Translation Rules**.



8. Use o procedimento Restringir o Acesso de Hosts Internos a Redes Externas para inserir as entradas de **access-list**.**Nota:** Seja cuidadoso ao implementar estes comandos. Se você implementar o comando **access-list 101 permit ip any any**, qualquer host na rede não confiável poderá acessar qualquer host na rede confiável com o uso do IP enquanto houver uma tradução ativa.

Desabilitar o NAT para Hosts/Redes Específicos

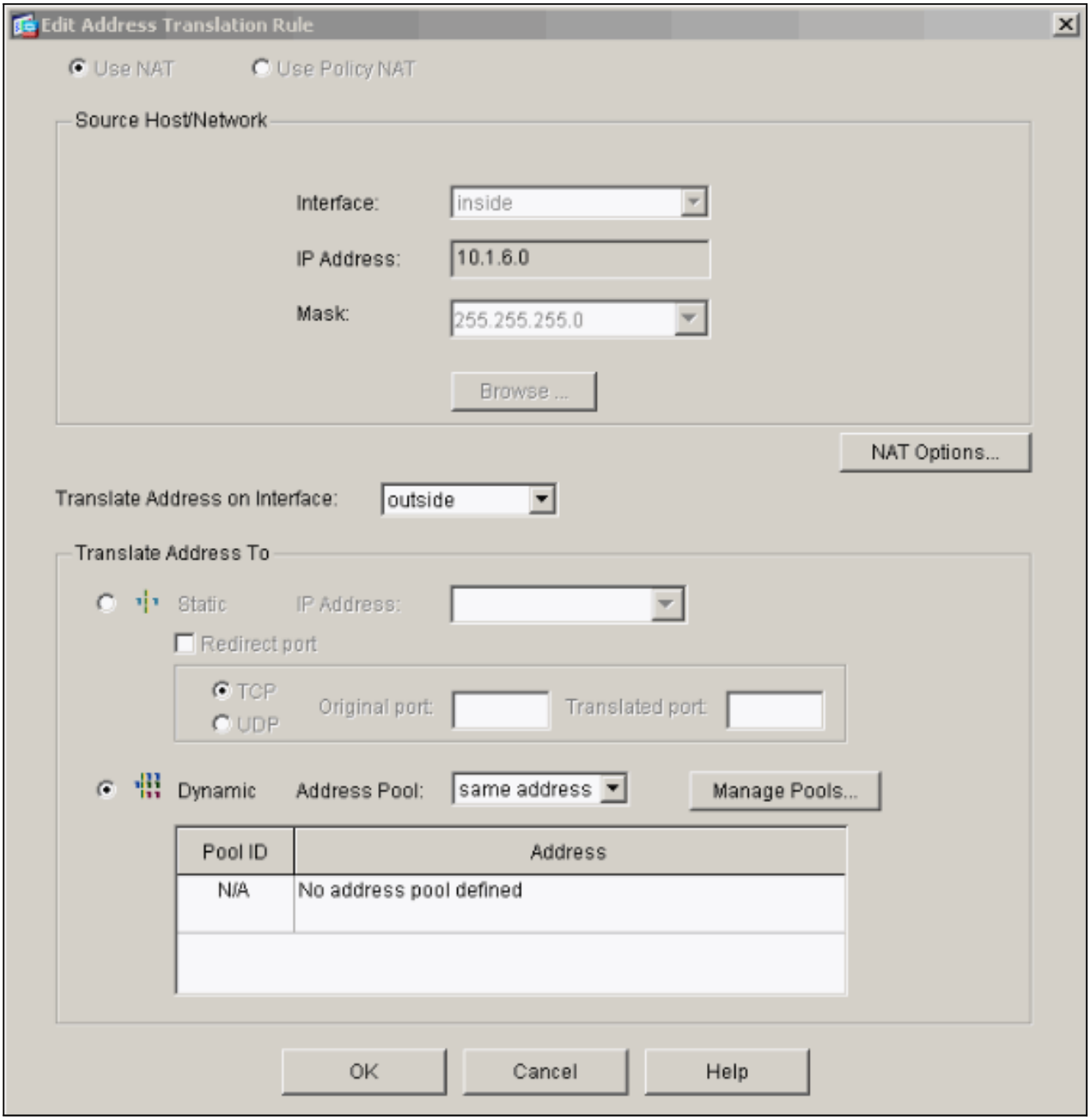
Se você usa o controle do NAT, possui alguns endereços públicos na rede interna e deseja que host internos específicos saiam da rede interna sem tradução, você poderá desabilitar o NAT para esses hosts com os comandos **nat 0** ou **static**.

Este é um exemplo do comando **nat**:

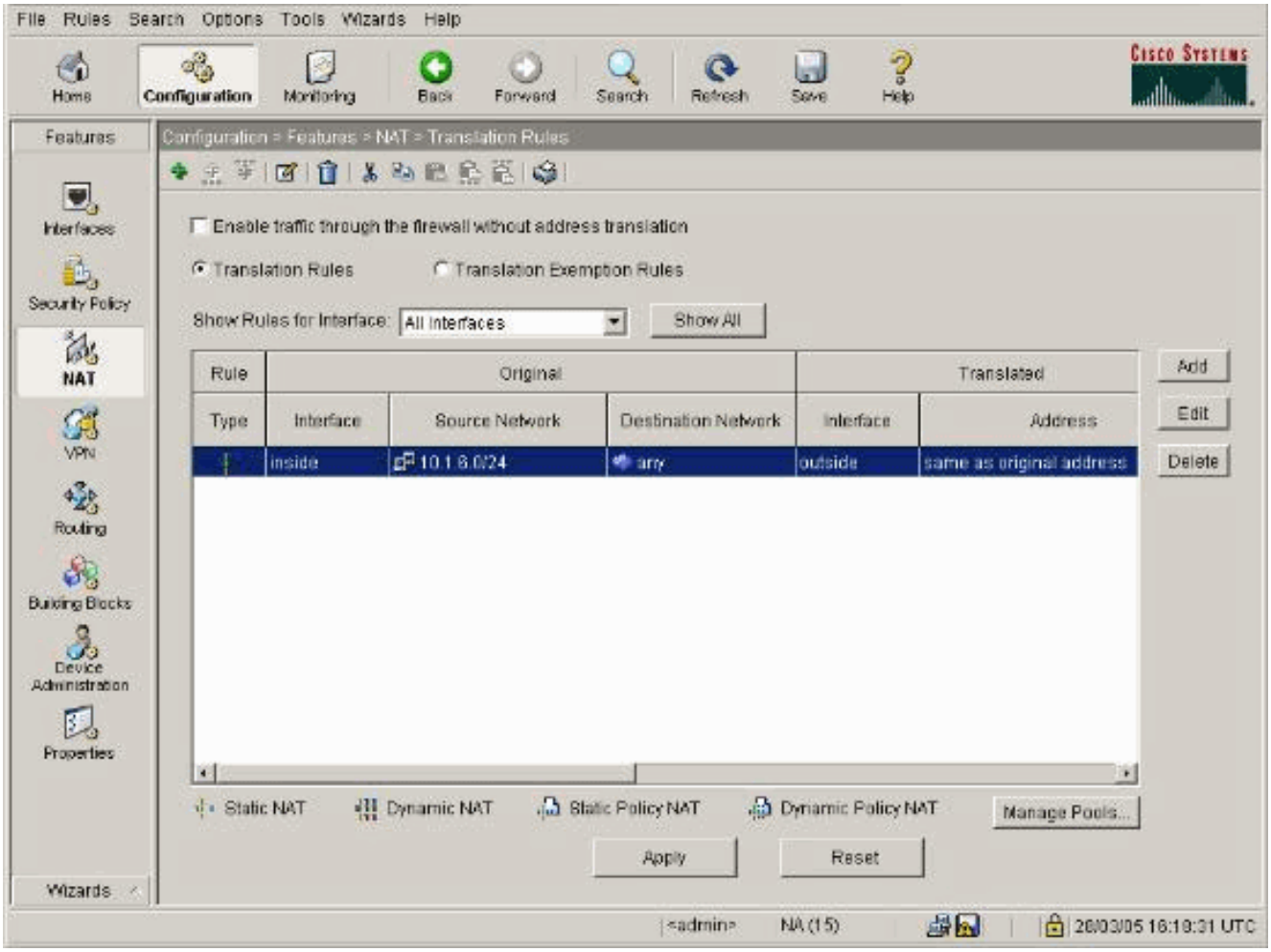
```
nat (inside) 0 10.1.6.0 255.255.255.0
```

Conclua estes passos para desabilitar o NAT para hosts/redes específicos com o uso do ASDM.

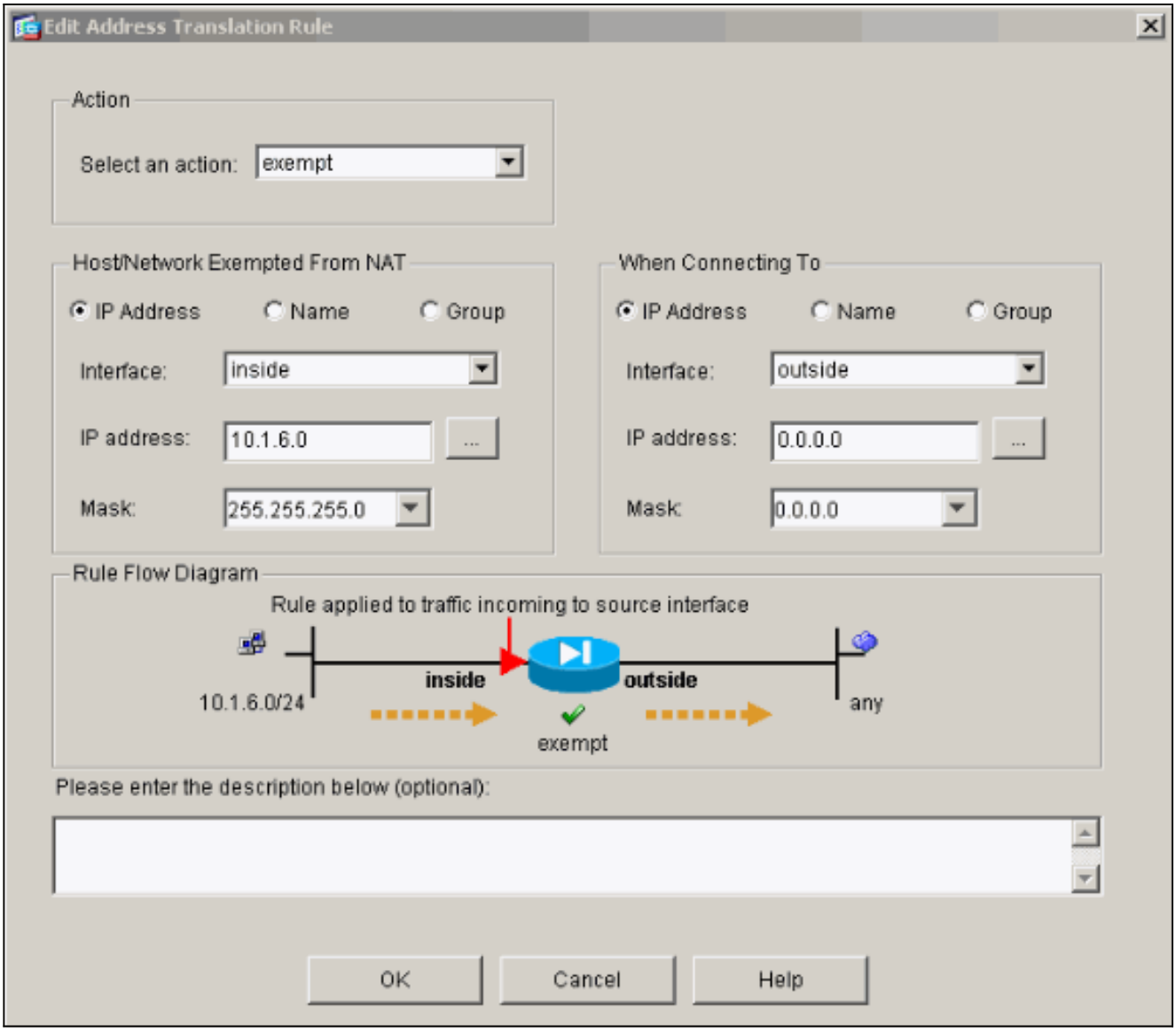
1. Escolha **Configuration > Features > NAT** e clique em **Add**.
2. Selecione **inside** como a interface de origem e insira o endereço interno/rede para o qual deseja criar uma tradução estática.
3. Escolha **Dynamic** e selecione o mesmo endereço para o pool de endereços. Clique em **OK**.



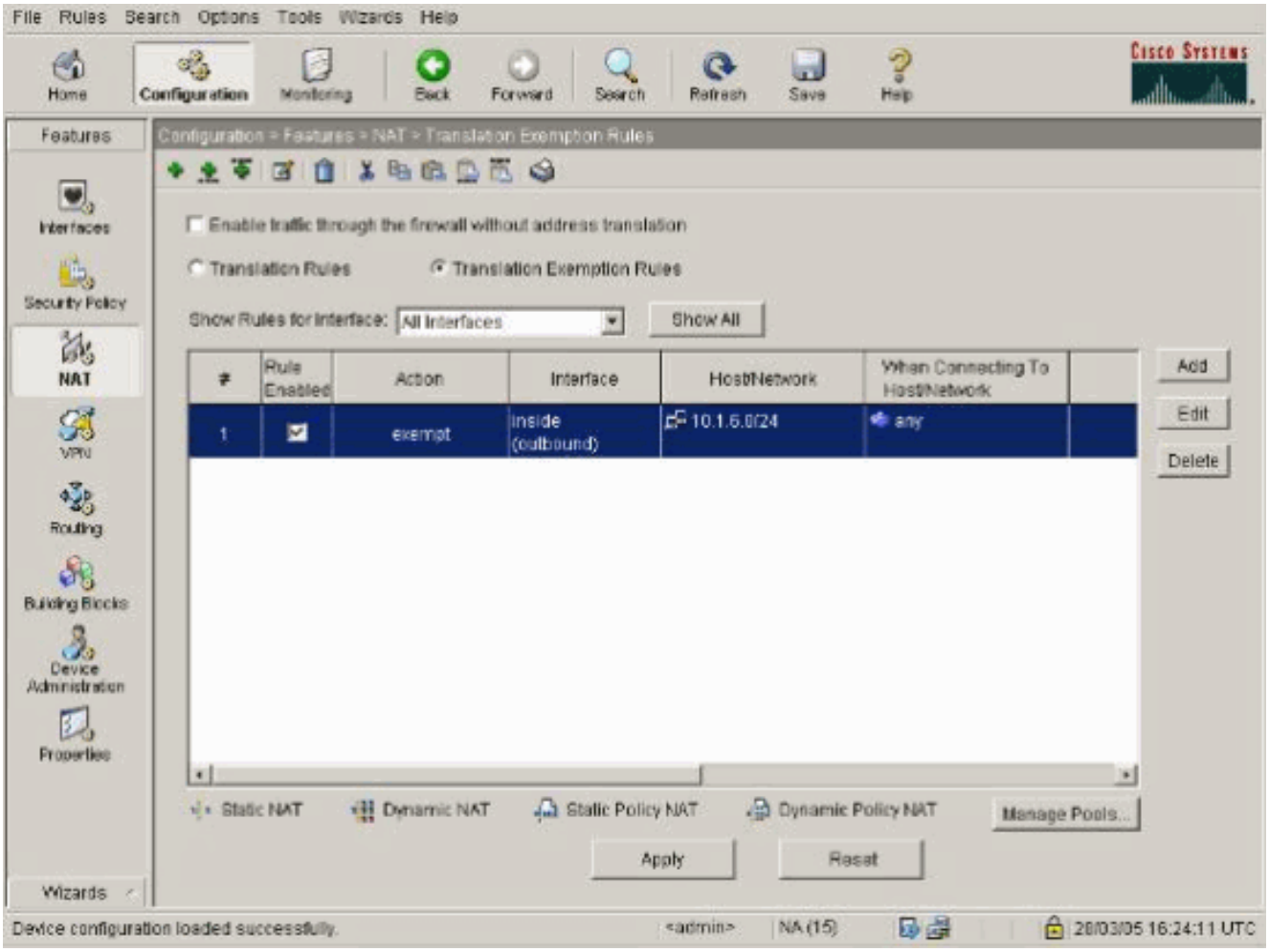
4. A nova regra é mostrada nas regras de tradução quando você escolhe **Configuration > Features > NAT > Translation Rules**.



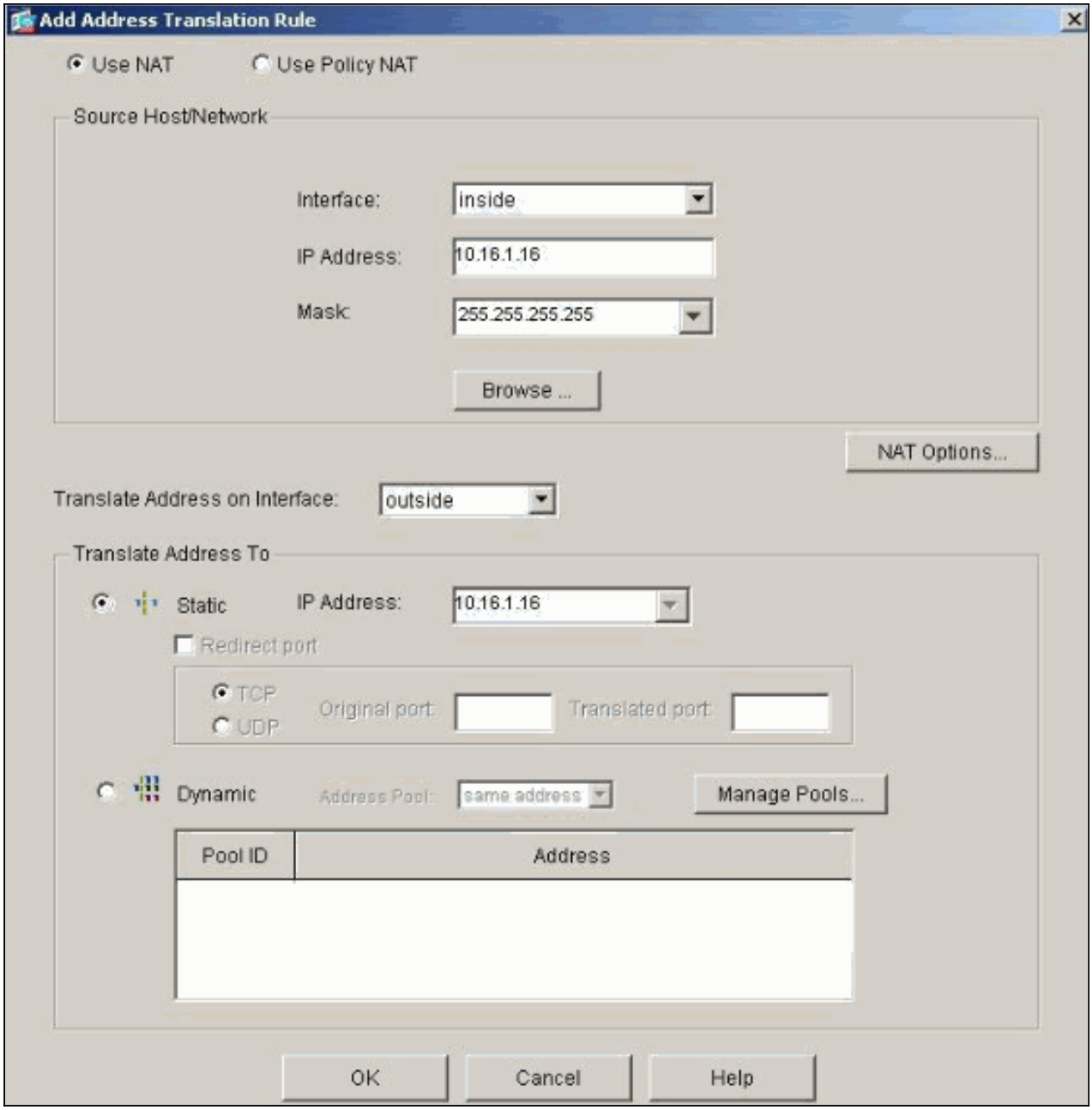
5. Se você usa ACLs, as quais possibilitam um controle mais preciso do tráfego que não deve ser traduzido (baseado na origem/destino), use esses comandos.
   `access-list 103 permit ip 10.1.6.0 255.255.255.0 any nat (inside) 0 access-list 103`
6. Use o ASDM e escolha **Configuration > Features > NAT > Translation Rules**.
7. Escolha **Translation Exemption Rules** e clique em **Add**.Este exemplo mostra como isentar o tráfego da rede 10.1.6.0/24 da tradução em qualquer
   lugar.



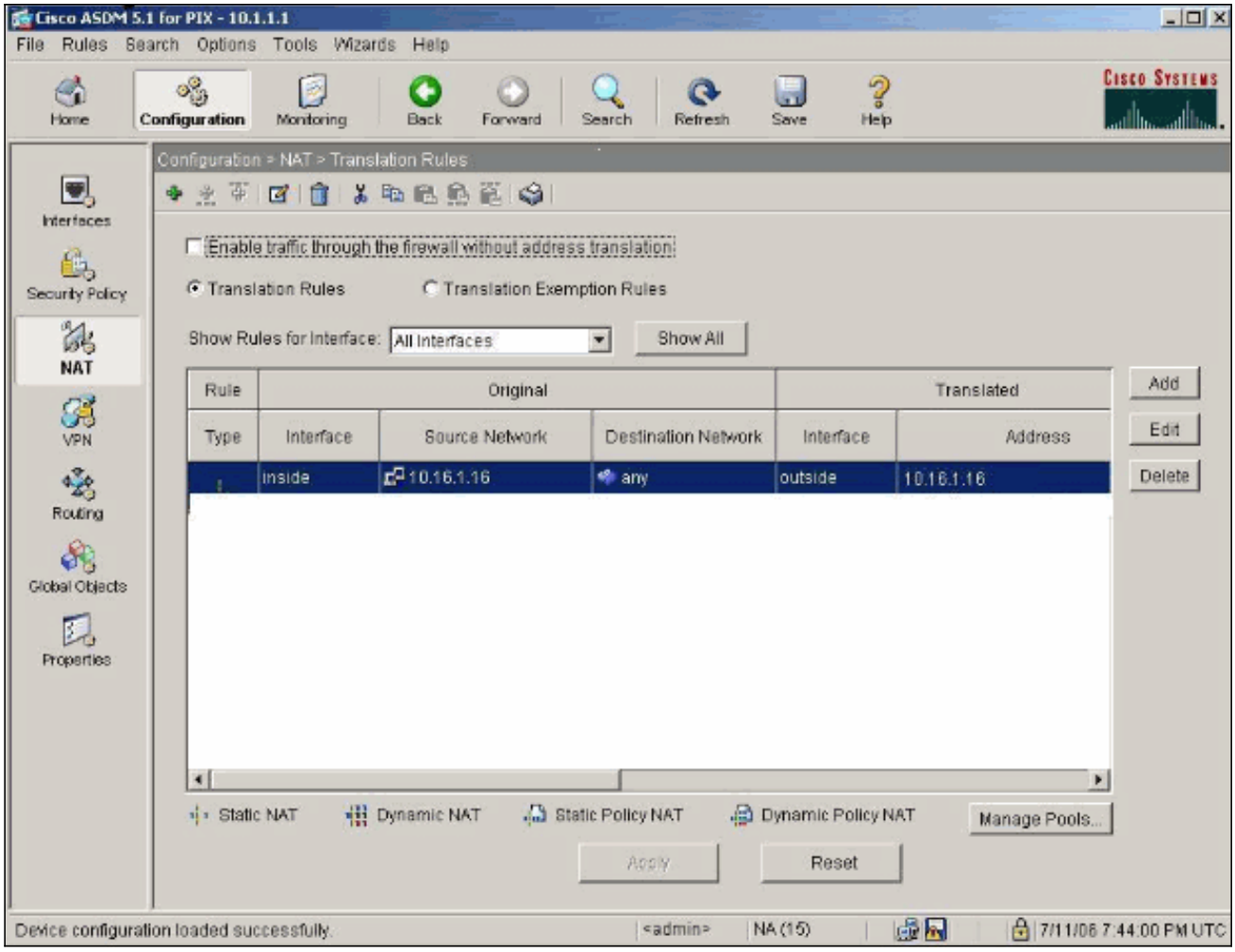
8. Escolha **Configuration > Features > NAT > Translation Exemption Rules** para exibir as novas regras.



9. O comando **static** para o servidor Web é alterado conforme mostrado neste exemplo.
   `static (inside, outside) 10.16.1.16 10.16.1.16`
10. No ASDM, escolha **Configuration > Features > NAT > Translation Rules**.
11. Selecione **Translation Rules** e clique em **Add**. Insira as informações de endereço de origem e selecione a **Static**. Insira o mesmo endereço no campo IP Address.



12. A tradução é mostrada nas regras de tradução quando você escolhe **Configuration > Features > NAT > Translation Rules**.



13. Se você usa ACLs, use estes comandos.
`access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside` Consulte a seção Restringir o Acesso de Hosts Internos a Redes Externas deste documento para obter informações adicionais sobre a configuração das ACLs no ASDM.Note a diferença entre quando você usa **nat 0** quando você especifica a rede/máscara em comparação com quando você usa uma ACL que usa uma rede/máscara que permita a iniciação de conexões somente do meio interno. O uso de ACLs com **nat 0**permite a iniciação de conexões pelo tráfego de saída ou de entrada. As interfaces do PIX precisam estar em sub-redes diferentes para evitar problemas de alcançabilidade.

Redirecionamento de Portas (Encaminhamento) com Statics

No PIX 6.0, a característica de Redirecionamento de Portas (Encaminhamento) foi adicionada a fim de permitir que os usuários externos se conectem a um endereço/porta IP particular e fazer com que o PIX reoriente o tráfego à porta/servidor interno apropriado. O comando **static** foi alterado. O endereço compartilhado pode ser um endereço único, um endereço de PAT de saída compartilhado, ou compartilhado com a interface externa. Esta característica está disponível no PIX 7.0.

Nota: Devido a limitações de espaço, os comandos são mostrados em duas linhas.

`static` *`[(internal_if_name, external_if_name)] {global_ip|interface}local_ip [netmask mask] [max_conns [emb_limit [norandomseq]]]`* **`static`** *`[(internal_if_name, external_if_name)] {tcp|udp} {global_ip|interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]`*

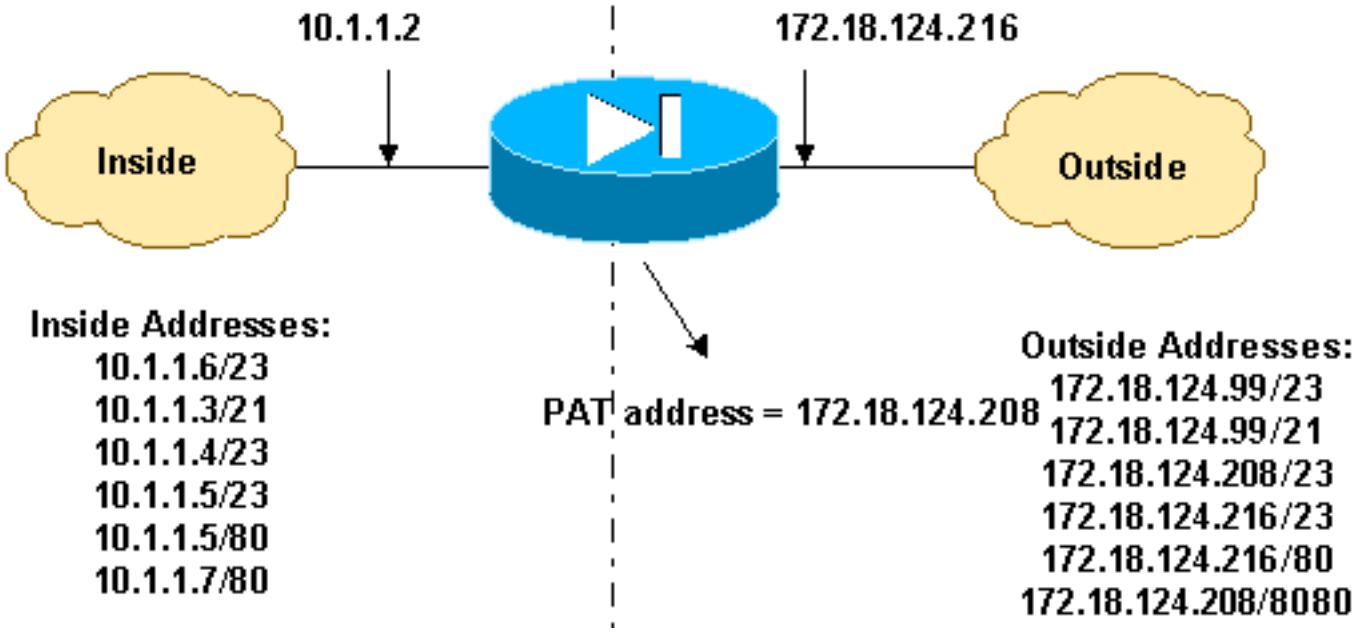
Nota: Se o NAT estático usa o endereço IP (global_IP) externo para traduzir, isso poderia causar uma tradução. Assim, use a palavra chave **interface** em vez do endereço IP na tradução estática.

Estes Redirecionamentos de Portas (Encaminhamentos) estão neste exemplo de rede:

- Os usuários externos direcionam solicitações de telnet para o endereço IP exclusivo 172.18.124.99, o qual é redirecionado pelo PIX para 10.1.1.6.
- Os usuários externos direcionam solicitações de FTP para endereços IP exclusivos 172.18.124.99, que o PIX redireciona para 10.1.1.3.
- Os usuários externos direcionam as solicitações de Telnet para o endereço PAT 172.18.124.208, o qual é redirecionado pelo PIX para 10.1.1.4.
- Os usuários externos direcionam requisições de Telnet para o endereço IP externo de PIX 172.18.124.216, que o PIX redireciona para 10.1.1.5.
- Os usuários externos direcionam a solicitação de HTTP para endereço IP externo 172.18.124.216 do PIX, o qual é redirecionado pelo PIX para 10.1.1.5.
- Os usuários externos direcionam solicitações de porta 8080 HTTP para o endereço PAT 172.18.124.208, o qual o PIX redireciona para a porta 80 10.1.1.7

Este exemplo também bloqueia o acesso de alguns usuários do meio interno para o externo com a ACL 100. Este passo é opcional. todo o tráfego é permitido no sentido de saída sem o ACL no lugar.

Diagrama de Rede - Redirecionamento de Portas (Encaminhamento)



Configuração parcial de PIX - Redirecionamento de porta

Esta configuração parcial ilustra o uso do Redirecionamento de Portas Estático (Encaminhamento). Consulte o diagrama de rede do Redirecionamento de Portas (Encaminhamento).

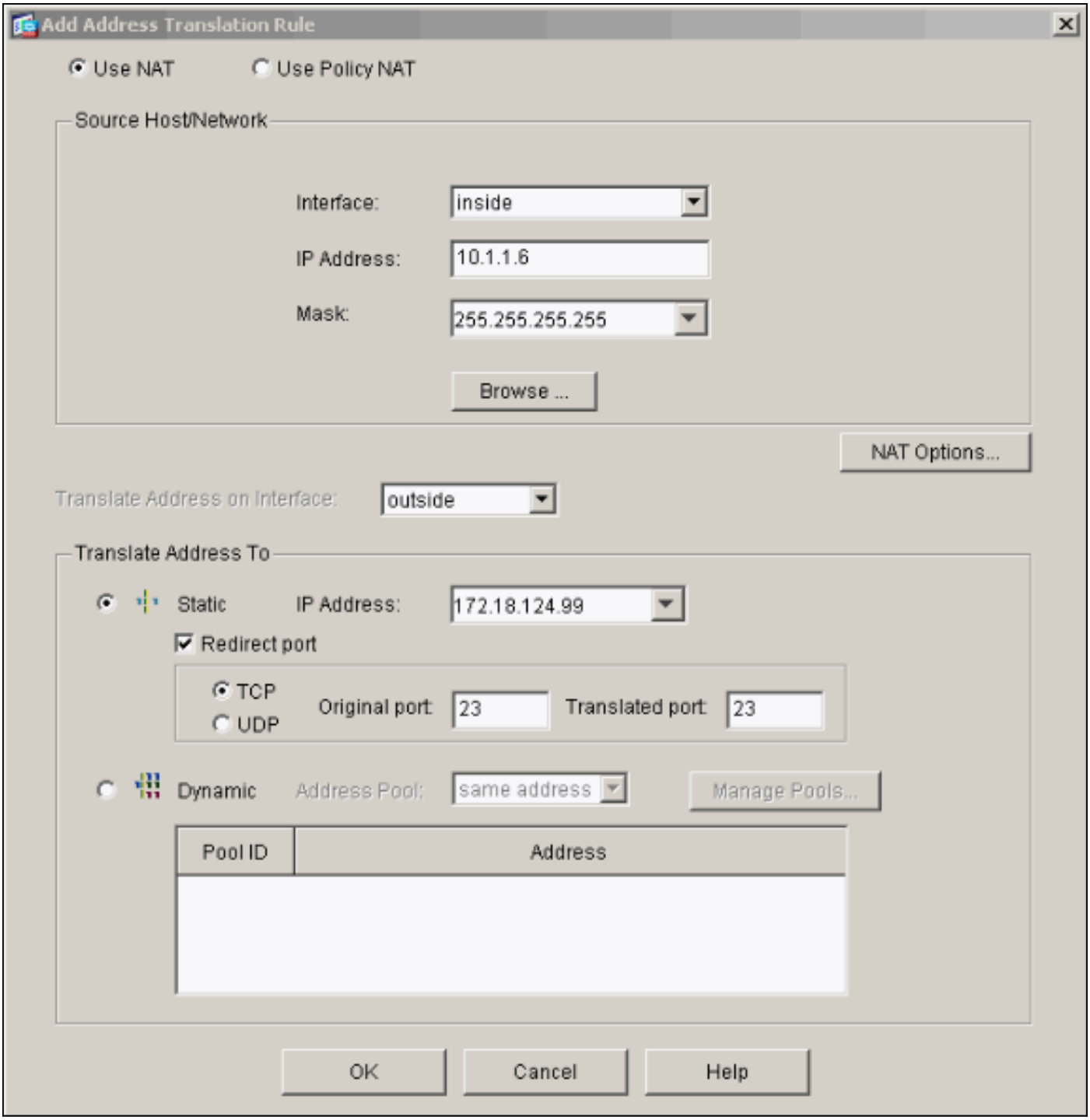
Configuração Parcial do PIX 7.x - Redirecionamento de Portas (Encaminhamento)
`fixup protocol ftp 21` `!--- Use of an outbound ACL is optional.` `access-list 100`

```
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

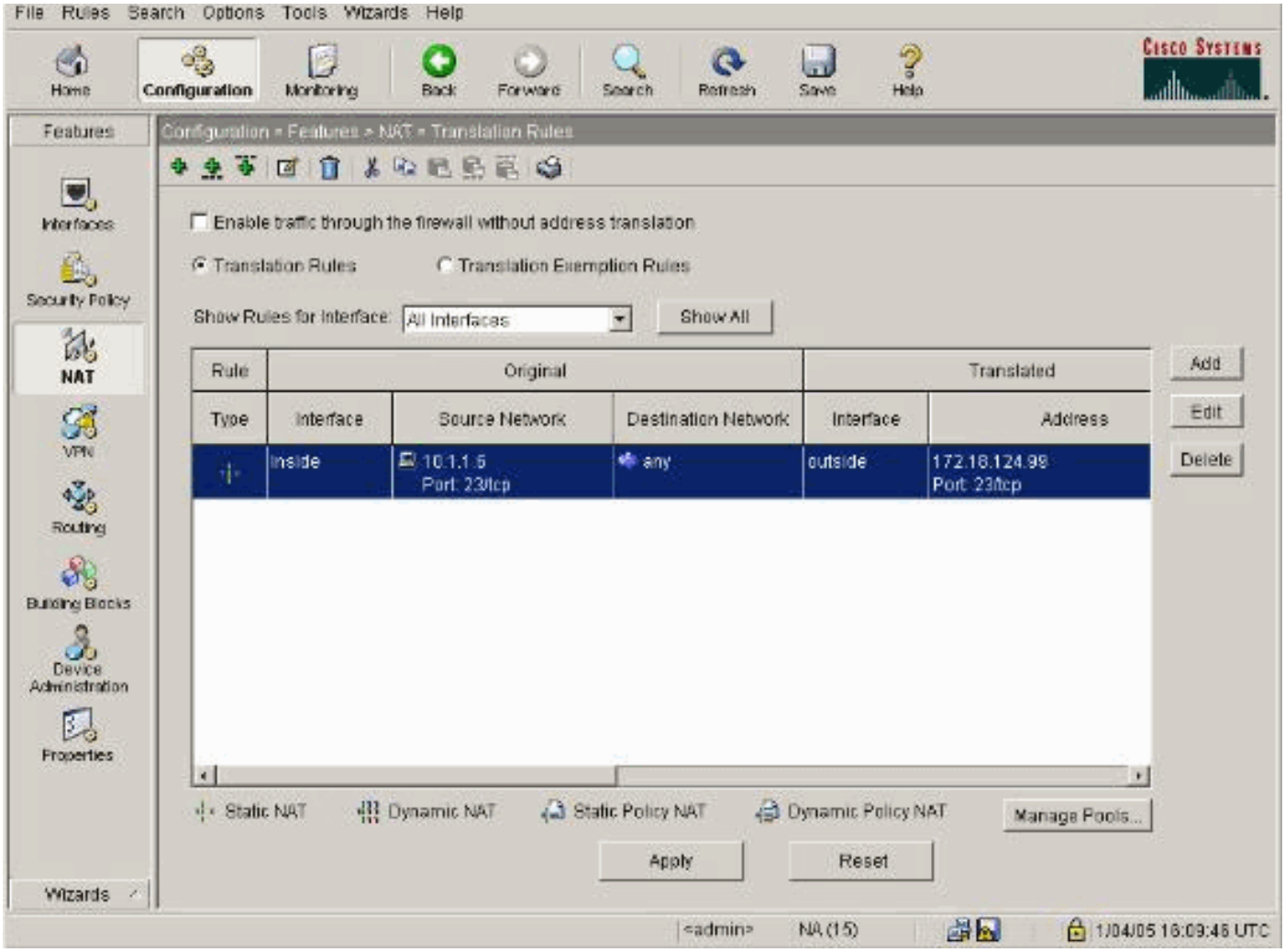
Nota: Se o PIX/ASA é configurado com o **noproxyarp do sysopt fora do** comando, a seguir não permite que o Firewall faça o proxy ARP e as traduções NAT estáticas no PIX/ASA. A fim resolver isto, remova o **noproxyarp do sysopt fora do** comando na configuração PIX/ASA e atualize então as entradas de ARP usando o ARP gratuito. Isto permite que as entradas NAT estáticas trabalhem muito bem.

Este procedimento é um exemplo de como configurar o Redirecionamento de Portas (Encaminhamento), o qual permite que usuários externos direcionem solicitações de Telnet para o endereço IP exclusivo 172.18.124.99 que é redirecionado pelo PIX para 10.1.1.6.

1. Use o ASDM e escolha **Configuration > Features > NAT > Translation Rules**.
2. Selecione **Translation Rules** e clique em **Add**.
3. Para o host/rede de origem, insira as informações do endereço IP interno.
4. Para Translate Address To, selecione a **Static**, insira o endereço IP externo e marque **Redirect port**.
5. Insira a pré-tradução e a informação de porta de porta de pós-tradução (este exemplo mantém a porta 23). Clique em **OK**.



A tradução é mostrada nas regras de tradução quando você escolhe **Configuration > Features > NAT > Translation Rules**.



Limitar Sessão de TCP/UDP Usando Static

Se desejar limitar as sessões de TCP ou UDP ao servidor interno colocado no PIX/ASA, use o comando **static**.

Especifica o número máximo de conexões TCP e UDP simultâneas para a sub-rede inteira. O padrão é 0, o que significa conexões ilimitadas (as conexões ociosas são fechadas após o timeout de ociosidade especificado pelo comando **timeout conn**.). Esta opção não se aplica ao NAT externo. O Security Appliance controla somente as conexões de uma interface de segurança mais elevada para uma interface de segurança mais baixa.

Limitar o número de conexões embrionárias protege você contra ataques de DoS. O Security Appliance usa o limite embrionário para acionar uma interceptação de TCP, a qual protege os sistemas internos contra ataques de DoS perpetrados pela inundação de uma interface com pacotes SYN do TCP. Uma conexão embrionária é uma solicitação de conexão que não terminou o handshake necessário entre a origem e o destino. Esta opção não se aplica ao NAT externo. O recurso de interceptação de TCP aplica-se somente aos hosts ou servidores em um nível de segurança mais elevado. Se você definir o limite embrionário para o NAT externo, o limite embrionário será ignorado.

Por exemplo:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100 !--- The maximum
number of simultaneous tcp connections the local IP !--- hosts are to allow is 500, default is 0
which means unlimited !--- connections. Idle connections are closed after the time specified !--
```

*- by the **timeout conn** command !--- The maximum number of embryonic connections per host is **100**.*

%PIX-3-201002: Too many connections on {static|xlate} global_address! nconns dos econns

Esta é uma mensagem relacionada à conexão. Esta mensagem é registrada quando o número máximo de conexões para o endereço estático especificado é excedido. A variável econns é o número máximo de conexões embriônicas e nconns é o número máximo de conexões permitidas para static ou xlate.

A ação recomendada é usar o comando **show static** para verificar o limite imposto nas conexões para um endereço estático. O limite é configurável.

%ASA-3-201011: O limite da conexão excedeu 1000/1000 para o pacote de entrada de 10.1.26.51/2393 a 10.0.86.155/135 na relação fora

Este Mensagem de Erro é devido à identificação de bug Cisco CSCsg52106 (clientes registrados somente). Consulte este bug para obter mais informações.

Lista de Acessos Baseada em Tempo

A criação de um intervalo de tempo não restringe o acesso ao dispositivo. O comando **time-range** define somente o intervalo de tempo. Depois que um intervalo de tempo é definido, você pode anexá-lo às regras de tráfego ou a uma ação.

Para implementar uma ACL baseada no período, use o comando **time-range** para definir horas específicas do dia e da semana. Em seguida, **use o comando access-list extended time-range** para ligar o intervalo de tempo a uma ACL.

O intervalo de tempo depende do relógio de sistema do Security Appliance. No entanto, o recurso funciona melhor com sincronização de NTP.

Depois que você criou um intervalo de tempo e entrou no modo de configuração do time-range, você pode definir parâmetros do intervalo de tempo com os comandos **absolute** e **periodic**. Para restaurar as configurações padrão para as palavras-chave absolute e periodic do comando **time-range** use o comando **default** no modo de configuração de time-range.

Para implementar uma ACL baseada no período, use o comando **time-range** para definir horas específicas do dia e da semana. Em seguida, **use o comando access-list extended time-range** para ligar o intervalo de tempo a uma ACL. O próximo exemplo liga uma ACL chamada "Sales" intervalo de tempo chamado "New York Minute":

Este exemplo cria um intervalo de tempo chamado "New York Minute" e entra no modo de configuração de time-range:

```
hostname(config)#time-range New_York_Minute hostname(config-time-range)#periodic weekdays 07:00 to 19:00 hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute hostname(config)#access-group Sales in interface inside
```

Informações a Serem Coletadas se Você Abrir uma Ocorrência de Suporte Técnico

Se você ainda precisar de auxílio e desejar abrir uma ocorrência junto ao Suporte Técnico da Cisco, certifique-

se de incluir estas informações de troubleshooting do seu PIX Security Appliance.
• Descrição do problema e detalhes relevantes da topologia. • Os passos que você seguiu para fazer o troubleshooting antes de abrir a ocorrência. • Saída do comando **show tech-support**. • Saída do comando **show log** após a execução do comando **logging buffered debugging** ou capturas do console que demonstrem o problema (se disponíveis). Anexe os dados coletados à sua ocorrência em formato de texto simples descompactado (.txt). Você pode anexar a informação à sua ocorrência na TAC Service Request Tool (somente clientes registrados). Se você não conseguir acessar a TAC Service Request Tool (somente clientes registrados), você poderá enviar as informações em um anexo de e-mail para attach@cisco.com com seu número de ocorrência na linha de assunto da sua mensagem.

Informações Relacionadas

- Página de Suporte do PIX Security Appliance
- Referências de comando PIX
- Troubleshooting e Alertas do Cisco Adaptive Security Device Manager (ASDM)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems