

PIX/ASA 7.x e FWSM: Indicações NAT e de PANCADINHA

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[O comando nat-control](#)

[Declarações NAT múltiplas com NAT 0](#)

[Vários conjuntos globais](#)

[Diagrama de Rede](#)

[Mistura NAT e declarações globais da PANCADINHA](#)

[Diagrama de Rede](#)

[Várias declarações NAT com lista de acesso NAT 0](#)

[Diagrama de Rede](#)

[Use a política NAT](#)

[Diagrama de Rede](#)

[NAT estático](#)

[Diagrama de Rede](#)

[Como contornar o NAT](#)

[Configurar a identidade NAT](#)

[Configurar a identidade estática NAT](#)

[Configurando a isenção NAT](#)

[Verificar](#)

[Troubleshooting](#)

[Mensagem de Erro recebido ao adicionar um PAT estático para a porta 443](#)

[ERRO: conflito do traçar-endereço com estática existente](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece exemplos de configurações básicas de Tradução de Endereço de Rede (NAT) e Tradução de Endereço de Porta (PAT) nos Cisco PIX/ASA Security Appliances. Os diagramas de rede simplificada são fornecidos. Consulte a documentação PIX/ASA para sua versão de software PIX/ASA para a informação detalhada.

Refira a [utilização nat, global, estática, a conduíte, e os comandos access-list e o redirecionamento de porta \(transmissão\) no PIX](#) a fim aprender mais sobre o **nat, global, estático, conduíte, e comandos access-list** e redirecionamento de porta (transmissão) em PIX 5.x e mais

tarde.

Refira a [utilização de indicações NAT e de PANCADINHA no firewall PIX segura Cisco](#) a fim aprender mais sobre os exemplos básicos NAT e configurações da PANCADINHA no firewall PIX segura Cisco.

Para obter mais informações sobre da configuração de NAT na versão ASA 8.3 e mais atrasado, refira a [informação sobre o NAT](#).

Nota: O NAT no modo transparente é apoiado da versão 8.x PIX/ASA. Refira o [NAT no modo transparente](#) para mais informação.

Pré-requisitos

Requisitos

Os leitores deste documento devem ser conhecedors sobre a ferramenta de segurança de Cisco PIX/ASA.

Componentes Utilizados

A informação neste documento é baseada na versão de software 7.0 da ferramenta de segurança da série do Cisco PIX 500 e mais atrasado.

Nota: Este original recertified com versão 8.x PIX/ASA.

Nota: Os comandos usados nestes documentam são aplicáveis ao módulo firewall service (FWSM).

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.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

O comando nat-control

O comando **nat-control** no PIX/ASA especifica que todo o tráfego com o Firewall deve ter uma entrada de tradução específica (indicação **nat** com uma harmonização de **global** ou uma **instrução estática**) para que esse tráfego passe com o Firewall. O comando **nat-control** assegura-se de que o comportamento de tradução seja o mesmo que versões de firewall PIX mais cedo de 7.0. A configuração padrão da versão 7.0 e mais recente PIX/ASA é a especificação do **comando no nat-control**. Com versão 7.0 e mais recente PIX/ASA, você pode mudar este comportamento quando você emite o **comando nat-control**.

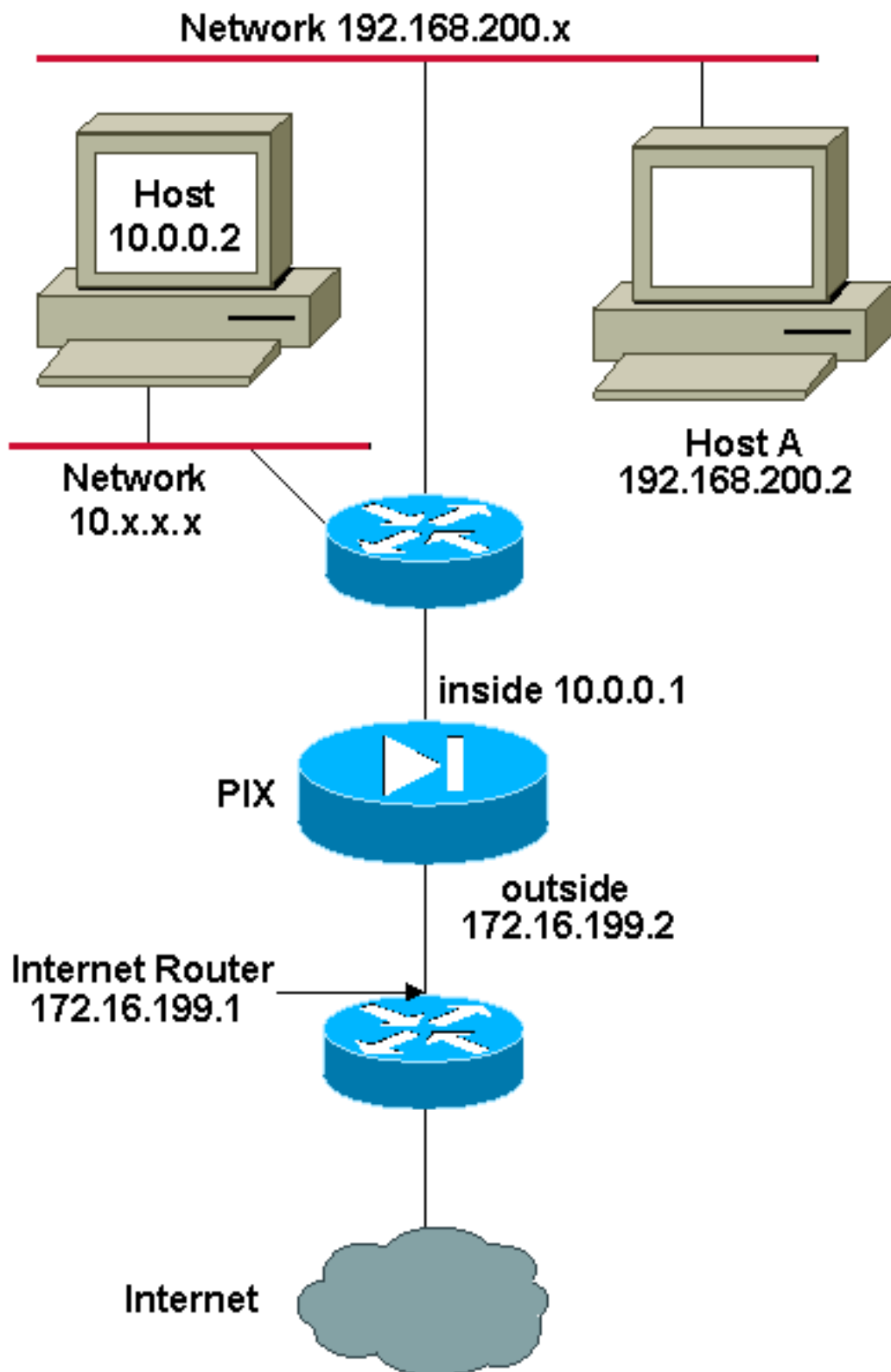
Com o **controle nat** desabilitado, os pacotes PIX/ASA para a frente de uma interface de

segurança mais elevada a um mais baixo sem uma entrada de tradução específica na configuração. A fim passar o tráfego de uma interface de segurança mais baixa a uma mais alta, use Listas de acesso para permitir o tráfego. O PIX/ASA então para a frente o tráfego. Este original centra-se sobre o comportamento da ferramenta de segurança PIX/ASA com o **controle nat** permitido.

Nota: Se você quer remover ou desabilitar a indicação do controle nat no PIX/ASA, você precisa de remover todas as declarações NAT da ferramenta de segurança. Geralmente, você precisa de remover o NAT antes que você desligue o controle NAT. Você tem que reconfigurar a declaração NAT no PIX/ASA para trabalhar como esperado.

[Declarações NAT múltiplas com NAT 0](#)

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Neste exemplo, o ISP fornece a gerente de rede um intervalo de endereço de 172.16.199.1 a 172.16.199.63. A gerente de rede decide atribuir 172.16.199.1 o à interface interna no roteador de Internet e 172.16.199.2 à interface externa do PIX/ASA.

O administrador de rede já teve um endereço do C da classe atribuído à rede, 192.168.200.0/24, e tem algumas estações de trabalho que usam estes endereços a fim alcançar o Internet. Estas

estações de trabalho não são ser endereço traduzido. Contudo, as novas estações de trabalho são atribuídas endereços na rede 10.0.0.0/8, e precisam de ser traduzidas.

A fim acomodar este projeto de rede, o administrador de rede deve usar duas declarações NAT e um conjunto global na configuração PIX/ASA enquanto esta saída mostra:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 192.168.200.0 255.255.255.0 0 0
```

```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

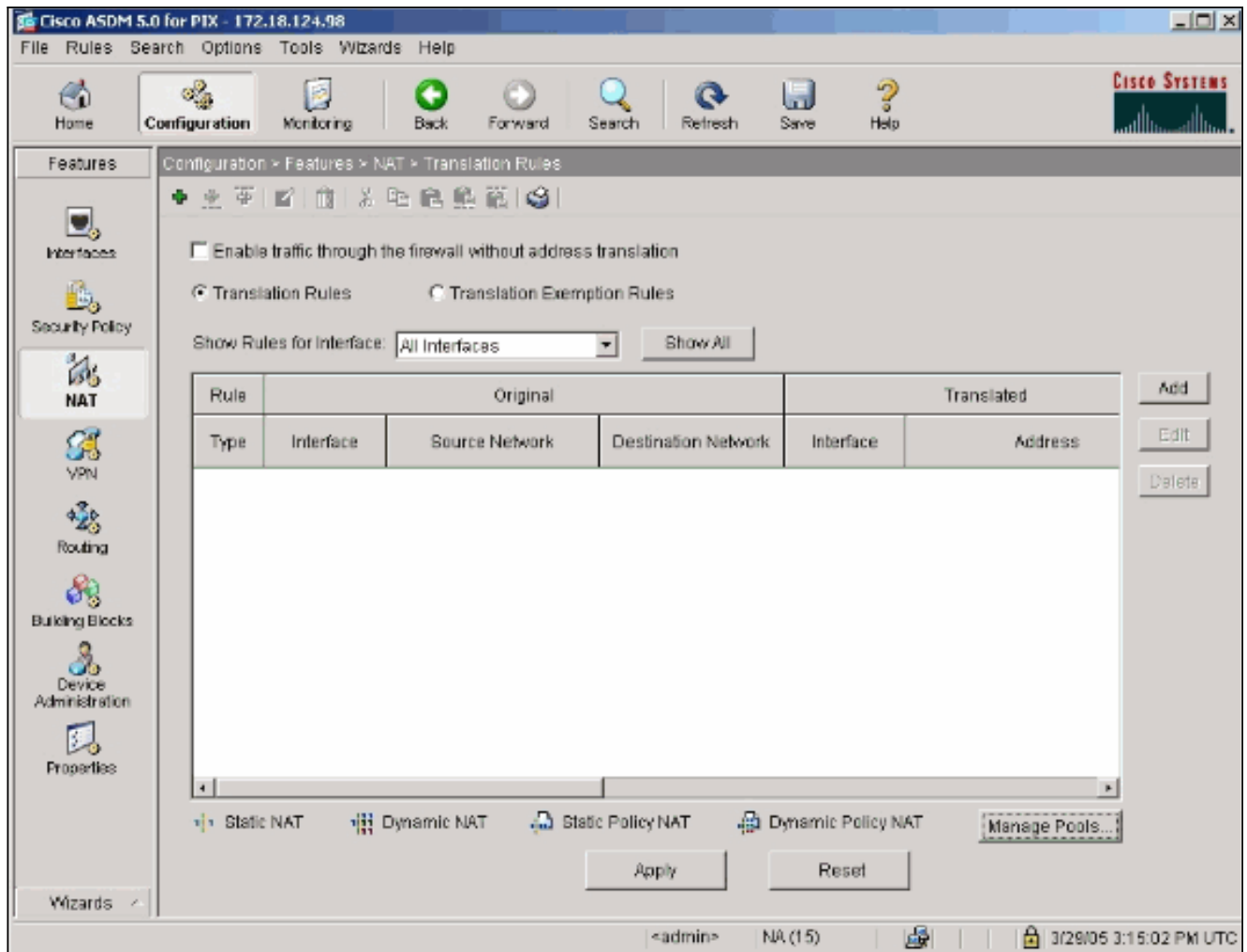
Esta configuração não traduz o endereço de origem de nenhum tráfego de saída da rede 192.168.200.0/24. Traduz um endereço de origem na rede 10.0.0.0/8 em um endereço da escala 172.16.199.3 a 172.16.199.62.

Estas etapas fornecem uma explicação de como aplicar esta mesma configuração com o uso do Security Device Manager adaptável (ASDM).

Nota: Execute todas as alterações de configuração com o CLI ou o ASDM. O uso do CLI e do ASDM para alterações de configuração causa muito o comportamento anormal em termos do que obtém aplicado pelo ASDM. Este não é um erro, mas ocorre devido a como o ASDM trabalha.

Nota: Quando você abre o ASDM, importa a configuração atual do PIX/ASA e trabalha dessa configuração quando você faz e aplica mudanças. Se uma mudança está feita no PIX/ASA quando a sessão ASDM estiver aberta, a seguir o ASDM já não trabalha com o que “pensa que” é a configuração atual do PIX/ASA. Seja certo fechar todas as sessões ASDM se você faz alterações de configuração através do CLI. Abra outra vez o ASDM quando você quer trabalhar através do GUI.

1. Lance o ASDM, consulte ao guia de configuração, e clique o **NAT**.
2. O clique **adiciona** a fim criar uma regra nova.



Uma nova janela aparece que permita que o usuário mude opções NAT para esta entrada NAT. Para este exemplo, execute o NAT nos pacotes que chegam na interface interna que é originado da rede 10.0.0.0/24 específica. O PIX/ASA traduz estes pacotes a um pool do IP dinâmico na interface externa. Depois que você incorpora a informação que descreve que tráfego ao NAT, define um pool dos IP address para o tráfego traduzido.

3. O clique **controla associações** a fim adicionar um IP pool novo.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

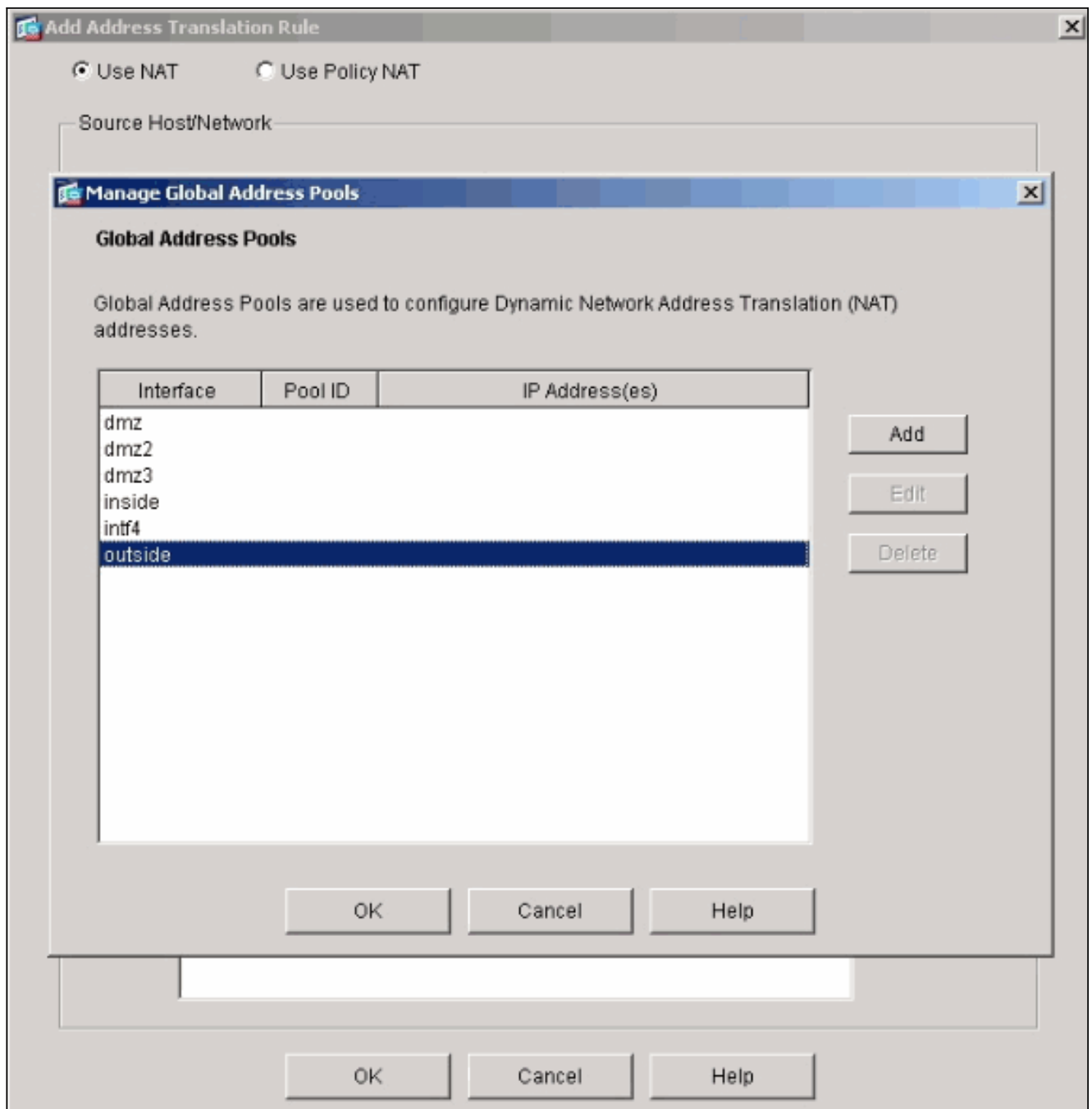
TCP Original port: Translated port:

UDP

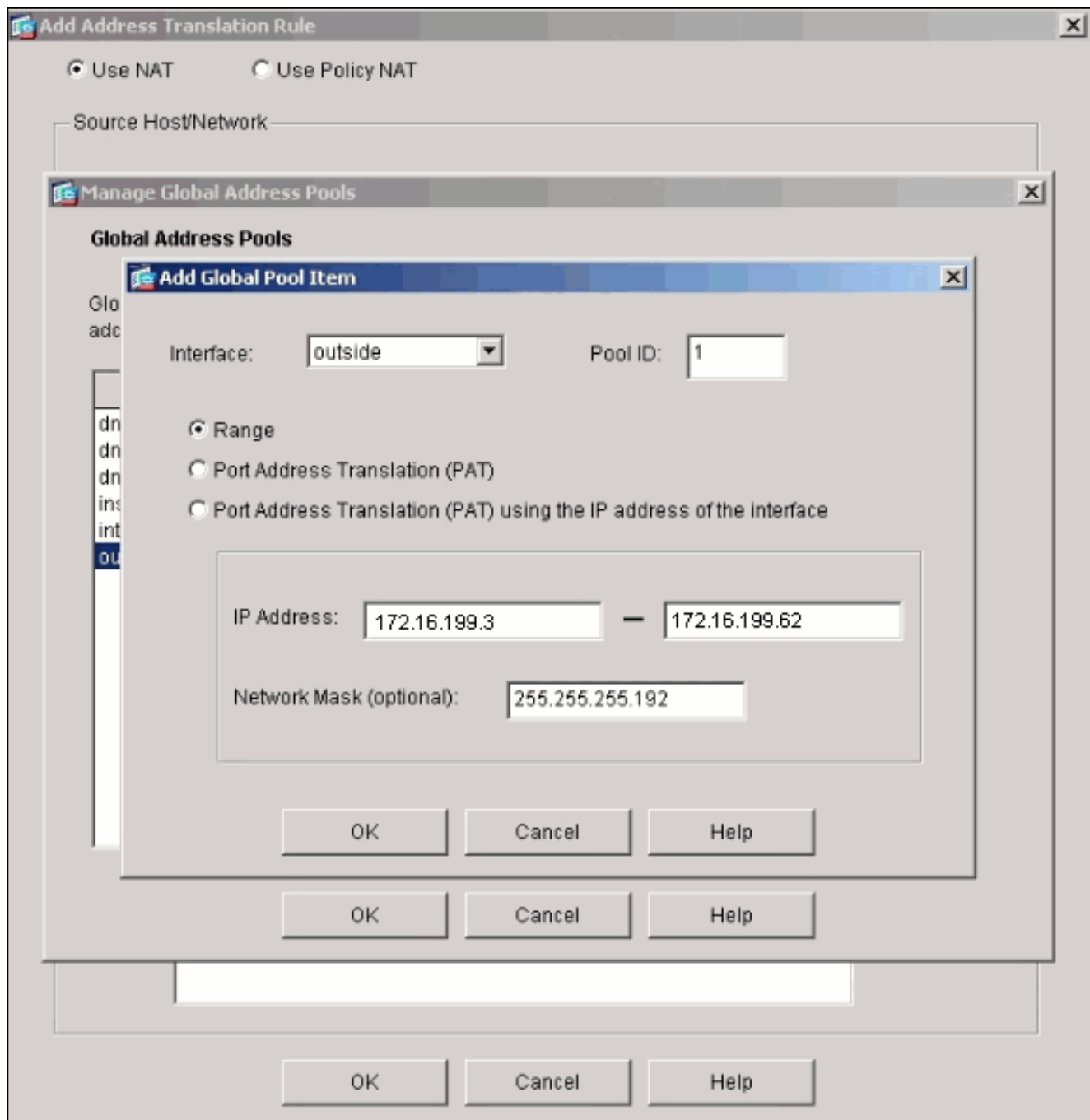
 Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

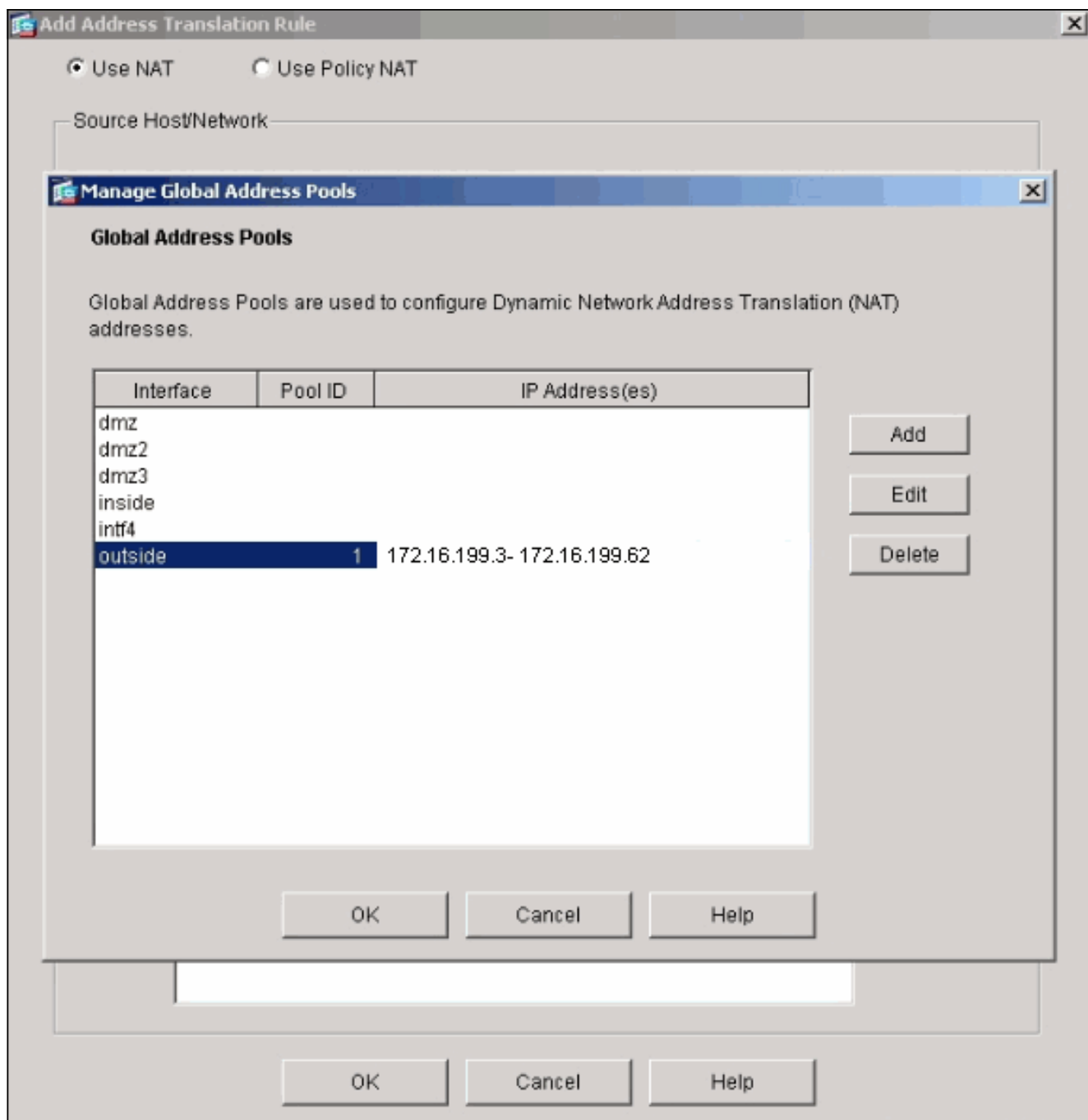
4. Escolha **fora**, e o clique **adiciona**.



5. Especifique a escala IP para o pool, e dê ao pool um número de ID do inteiro exclusivo.



6. Incorpore os valores apropriados, e clique a **APROVAÇÃO**.O pool novo é definido para a interface externa.



7. Depois que você define o pool, clique a **APROVAÇÃO** a fim retornar à janela de configuração da regra NAT. Certifique-se escolher o pool correto que você apenas criou sob a lista de drop-down do conjunto de endereços.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

TCP Original port: Translated port:

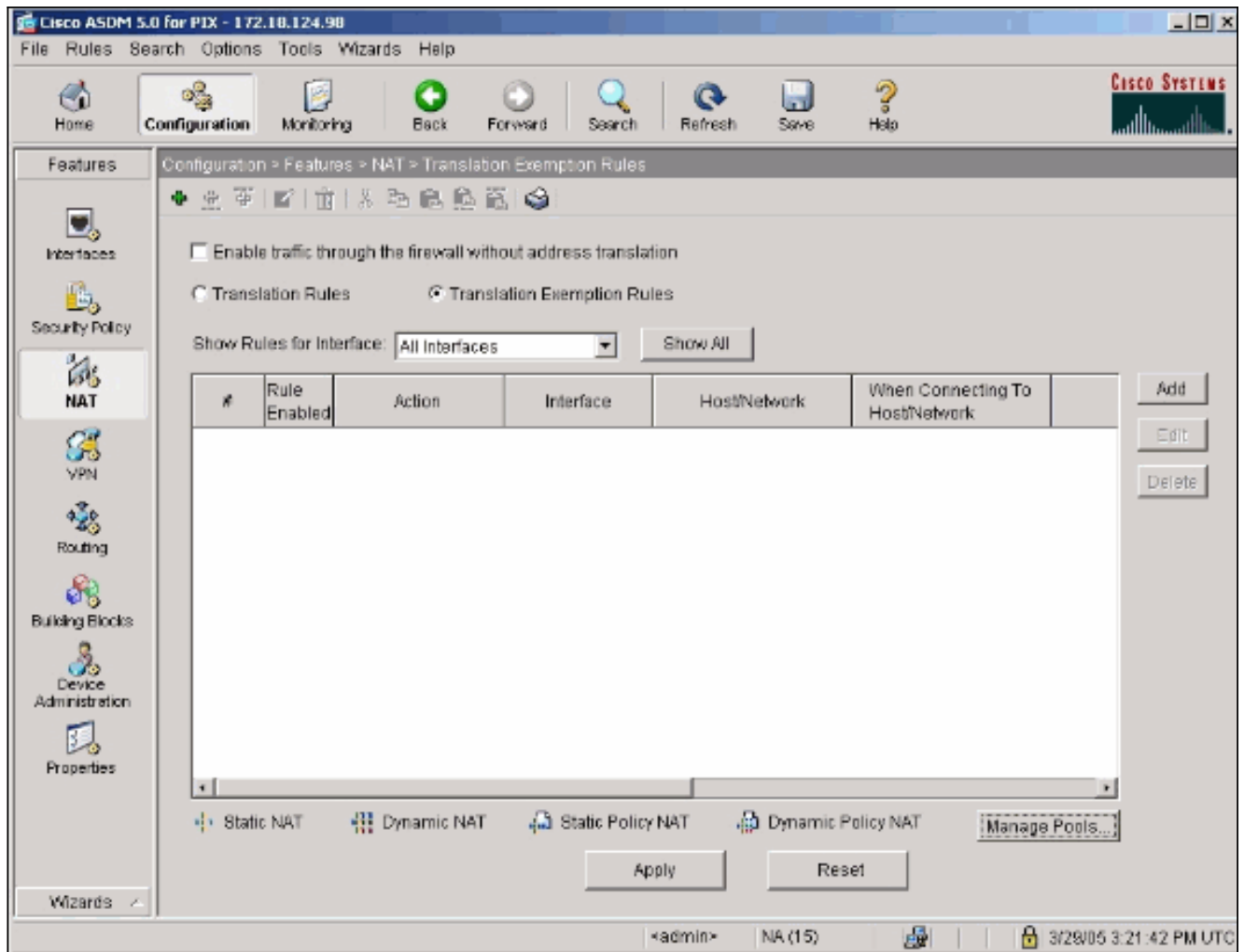
UDP

Dynamic Address Pool:

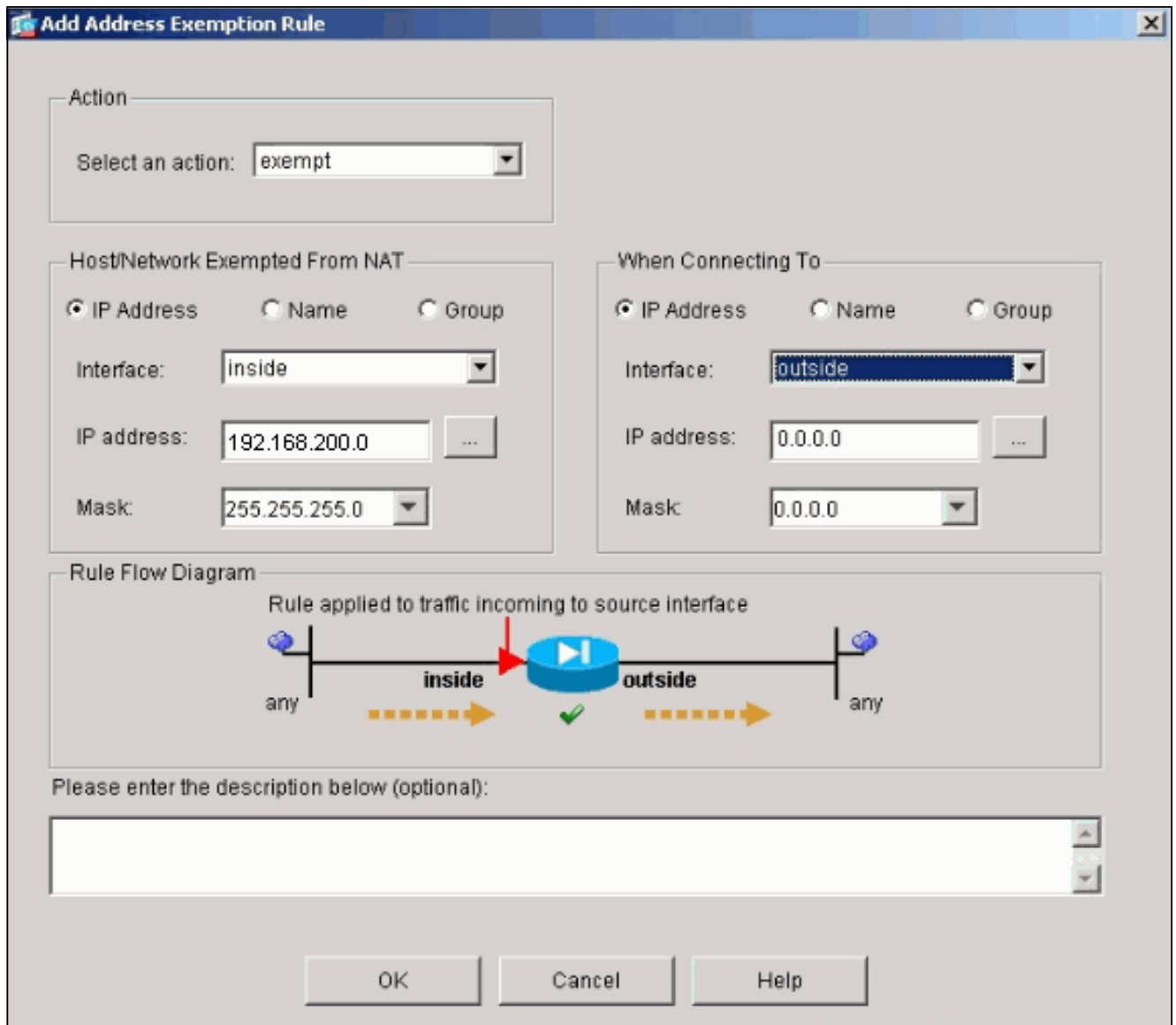
Pool ID	Address
1	172.16.199.3- 172.16.199.62

Você tem criado agora uma tradução NAT através da ferramenta de segurança. Contudo, você ainda precisa de criar a entrada NAT que especifica que tráfego não ao NAT.

8. Clique as **regras da isenção da tradução** situadas na parte superior do indicador, e clique-as então **adicionam** a fim criar uma regra nova.



9. Escolha a *interface interna* como a fonte, e especifique a sub-rede **192.168.200.0/24**. Saa “ao conectar” valores como os padrões.



As regras NAT são definidas agora.

10. O clique **aplica-se** a fim aplicar as mudanças à configuração em execução atualmente da ferramenta de segurança. Esta saída mostra as adições reais que são aplicadas à configuração PIX/ASA. São levemente diferentes dos comandos entered do método manual, mas são iguais.

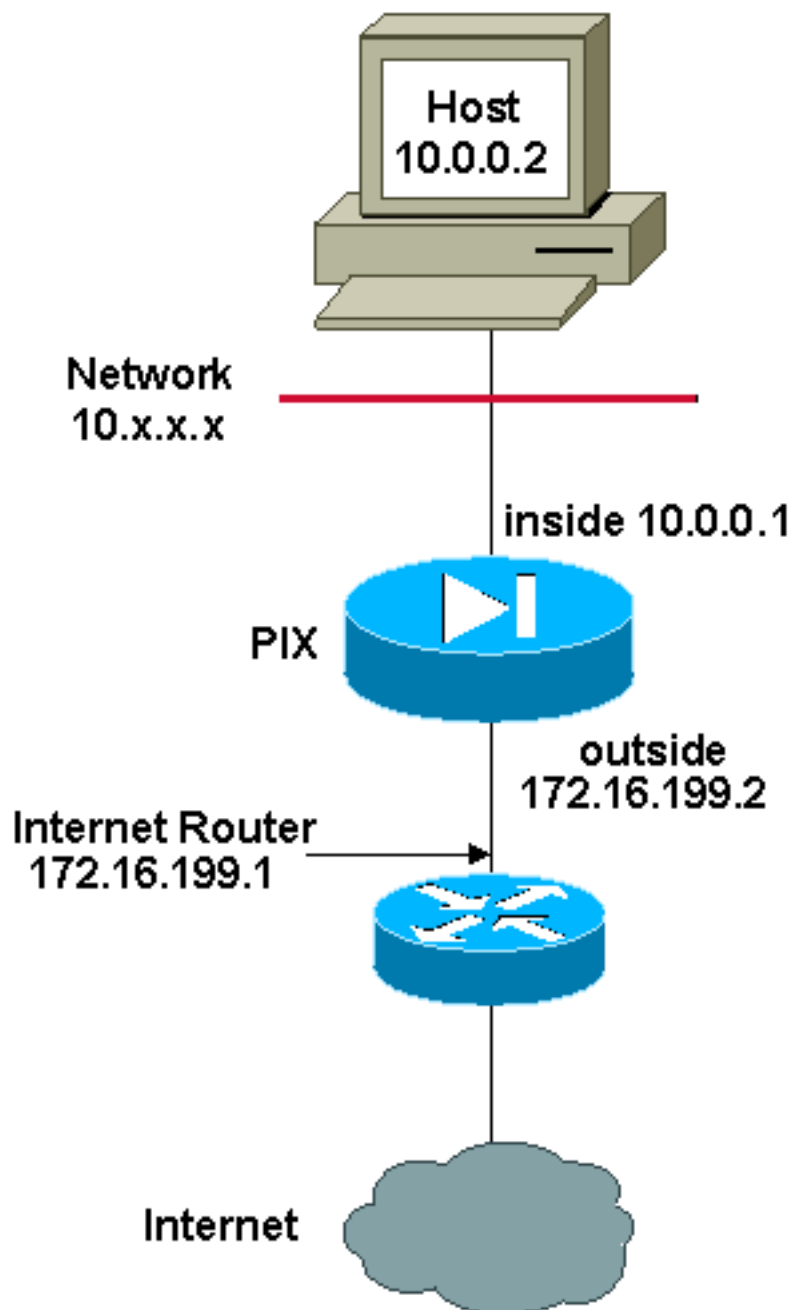
```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

Vários conjuntos globais

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Neste exemplo, a gerente de rede tem duas escalas dos IP address que se registram no Internet. A gerente de rede deve converter todos os endereços internos, que estão na escala 10.0.0.0/8, em endereços registrados. As escalas dos IP address que a gerente de rede deve usar são 172.16.199.1 com 172.16.199.62 e 192.168.150.1 com 192.168.150.254. A gerente de rede pode fazer esta com:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

No NAT dinâmico, a indicação mais específica é essa que toma a precedência quando você usa a mesma relação em global.

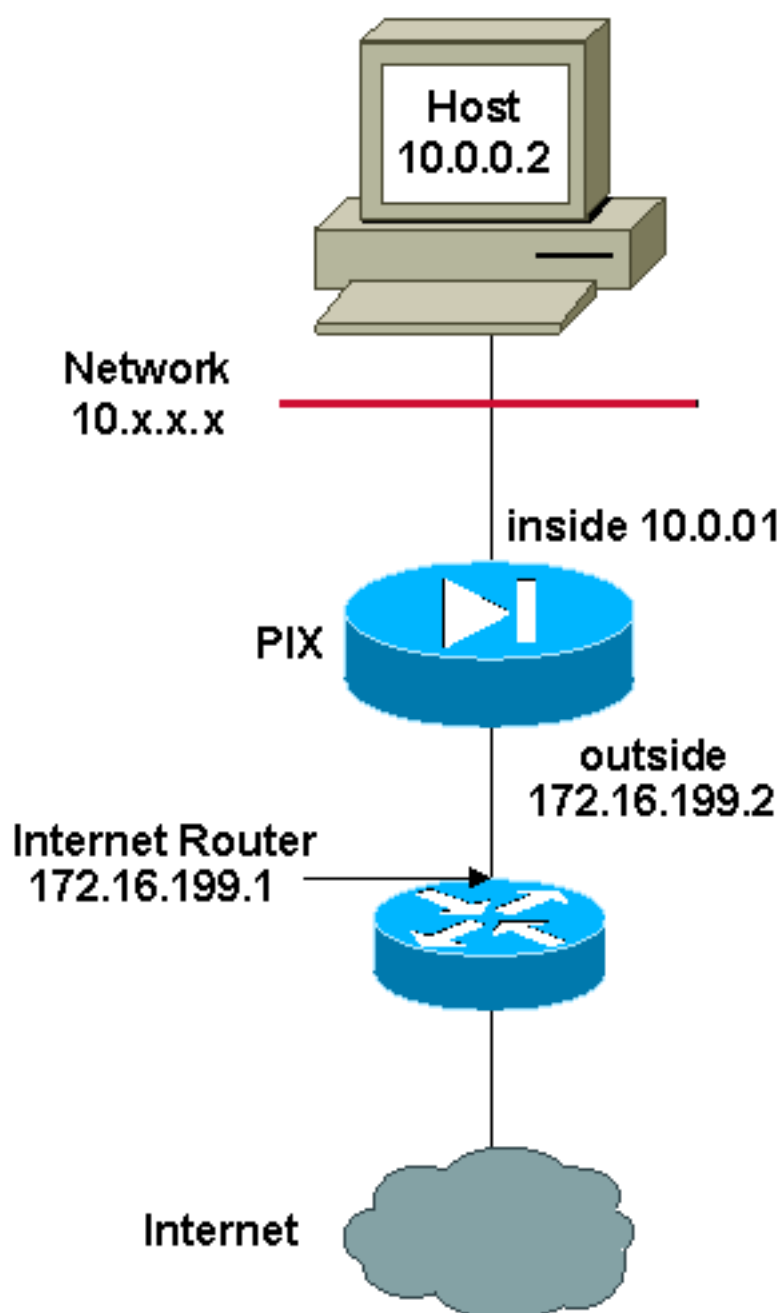
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Se você tem a rede interna como 10.1.0.0, o NAT 2 globais toma a precedência sobre 1 porque é mais específico para a tradução.

Nota: Um esquema de endereçamento de wildcard é usado na declaração NAT. Esta indicação diz o PIX/ASA para traduzir todo o endereço de fonte interna quando sai ao Internet. O endereço nesse comando pode ser mais específico, se desejado.

Mistura NAT e declarações globais da PANCADINHA

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente

roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Neste exemplo, o ISP fornece a gerente de rede um intervalo de endereço de 172.16.199.1 com 172.16.199.63 para o uso da empresa. A gerente de rede decide usar 172.16.199.1 para a interface interna no roteador de Internet e 172.16.199.2 para a interface externa no PIX/ASA. Você é deixado com 172.16.199.3 com 172.16.199.62 para usar-se para o conjunto NAT. Contudo, a gerente de rede sabe que, a qualquer altura, pode haver mais de sessenta povos que tenta sair do PIX/ASA. Consequentemente, a gerente de rede decide tomar 172.16.199.62 e fazer-lhe um endereço PAT de modo que os usuários múltiplos possam compartilhar de um endereço ao mesmo tempo.

```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192
```

```
global (outside) 1 172.16.199.62 netmask 255.255.255.192
```

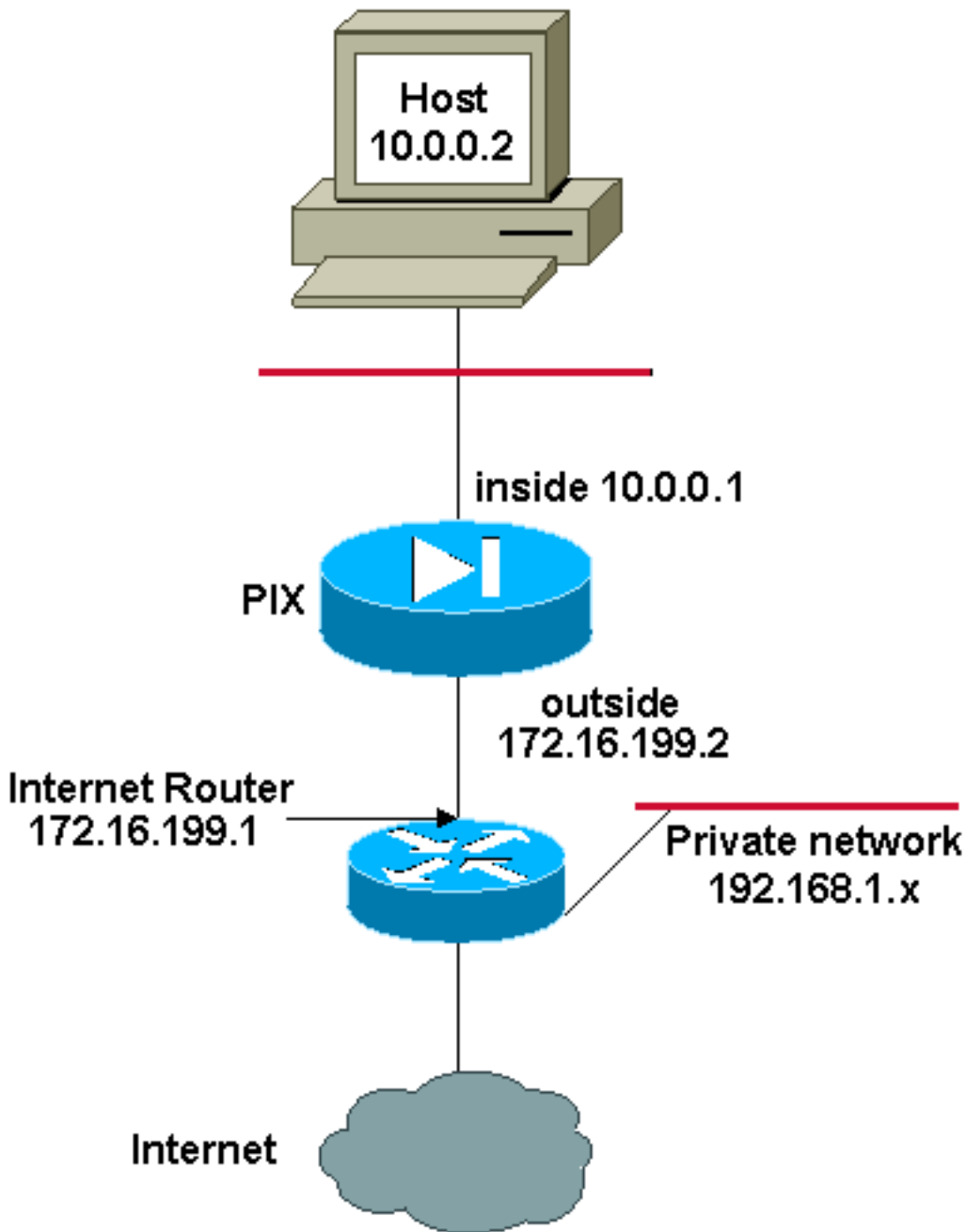
```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Estes comandos instruem o PIX/ASA traduzir o endereço de origem a 172.16.199.3 com 172.16.199.61 para que os primeiros cinquenta e nove usuários internos passem através do PIX/ASA. Depois que estes endereços são esgotados, o PIX a seguir traduz todos os endereços de origem subsequentes a 172.16.199.62 até que um dos endereços no conjunto NAT se torne livre.

Nota: Um esquema de endereçamento de wildcard é usado na declaração NAT. Esta indicação diz o PIX/ASA para traduzir todo o endereço de fonte interna quando sai ao Internet. O endereço neste comando pode ser mais específico se você deseja.

[Várias declarações NAT com lista de acesso NAT 0](#)

[Diagrama de Rede](#)



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Neste exemplo, o ISP fornece a gerente de rede um intervalo de endereço de 172.16.199.1 com 172.16.199.63. A gerente de rede decide atribuir 172.16.199.1 à interface interna no roteador de Internet e 172.16.199.2 à interface externa do PIX/ASA.

Contudo, nesta encenação um outro segmento de LAN privado é colocado fora do roteador de Internet. A gerente de rede um pouco não desperdiçaria endereços do conjunto global quando os anfitriões nestas duas redes falam entre si. A gerente de rede ainda precisa de traduzir o endereço de origem para todos os usuários internos (10.0.0.0/8) quando saem ao Internet.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list 101
```

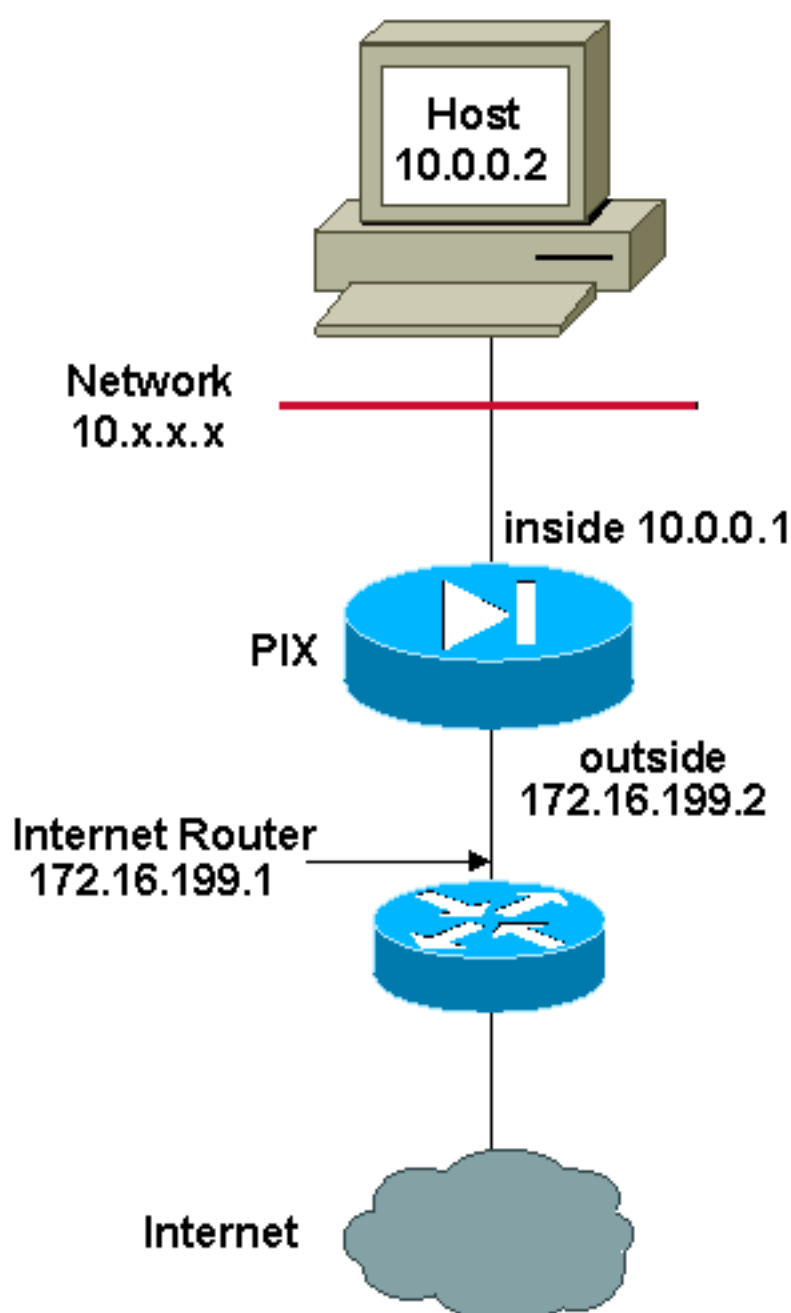
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Esta configuração não traduz aqueles endereços com um endereço de origem de 10.0.0.0/8 e um endereço de destino de 192.168.1.0/24. Traduz o endereço de origem de todo o tráfego iniciado de dentro da rede 10.0.0.0/8 e destinado para em qualquer lugar a não ser 192.168.1.0/24 em um endereço da escala 172.16.199.3 com 172.16.199.62.

Se você tem a saída de um **comando write terminal** de seu dispositivo Cisco, você pode usar a [ferramenta do Output Interpreter](#) ([clientes registrados somente](#)).

Use a política NAT

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que isso usado em um ambiente de

laboratório.

Quando você usa uma lista de acessos com o **comando nat** para toda a identificação NAT a não ser 0, a seguir você permite a política NAT.

Nota: A política NAT foi introduzida na versão 6.3.2.

A política NAT permite que você identifique o tráfego local para a tradução de endereços quando você especifica os endereços de remetente e destinatário (ou portas) em uma lista de acessos. O NAT regular usa /portas dos endereços de origem somente, visto que a política NAT usa ambas as /portas dos endereços de remetente e destinatário.

Nota: Todos os tipos da política de suporte NAT NAT à exceção da isenção NAT (**0 listas de acesso nat**). A isenção NAT usa um Access Control List a fim identificar os endereços locais, mas difere da política NAT que as portas não estão consideradas.

Com política NAT, você pode criar o NAT múltiplo ou as instruções estáticas que identificam o mesmo endereço local enquanto a combinação da /porta da fonte e da /porta do destino é original para cada indicação. Você pode então combinar endereços globais diferentes a cada par da /porta da fonte e da /porta do destino.

Neste exemplo, a gerente de rede fornece o acesso para o endereço IP de destino 192.168.201.11 para a porta 80 (Web) e a porta 23 (telnet), mas deve usar dois IP address diferentes como um endereço de origem. O endereço IP 172.16.199.3 é usado como o endereço de origem para a Web. O endereço IP 172.16.199.4 é usado para o telnet, e deve converter todos os endereços internos, que estão na escala 10.0.0.0/8. A gerente de rede pode fazer esta com:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11  
255.255.255.255 eq 80
```

```
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11  
255.255.255.255 eq 23
```

```
nat (inside) 1 access-list WEB
```

```
nat (inside) 2 access-list TELNET
```

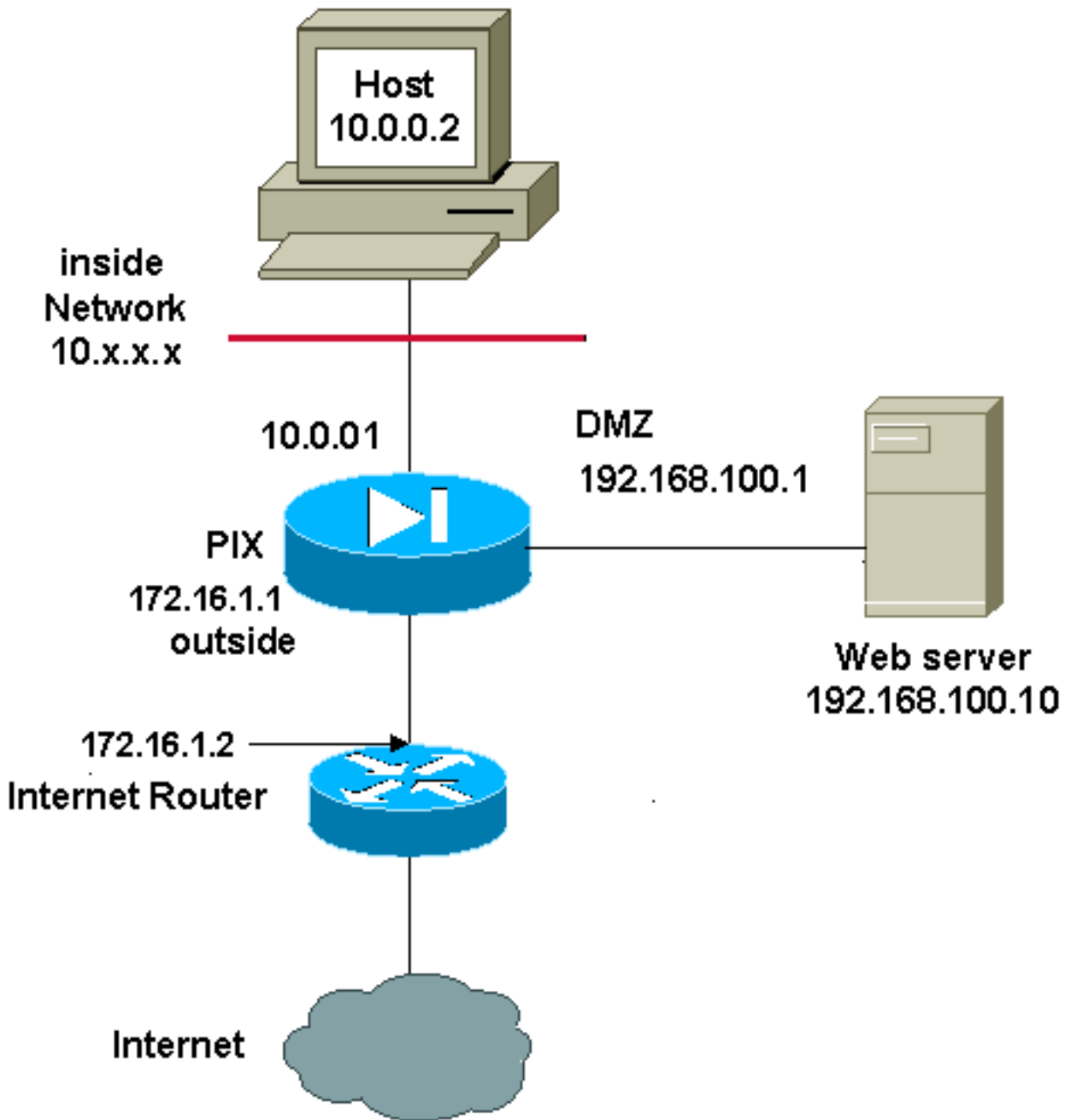
```
global (outside) 1 172.16.199.3 netmask 255.255.255.192
```

```
global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Você pode usar a [ferramenta do Output Interpreter \(clientes registrados somente\)](#) a fim indicar problemas potenciais e reparos.

[NAT estático](#)

[Diagrama de Rede](#)



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Uma configuração do NAT estático cria um mapeamento um a um e traduz um endereço específico a um outro endereço. O este tipo de configuração cria uma entrada permanente na tabela NAT enquanto a configuração esta presente e a permite tanto dentro como fora dos anfitriões de iniciar uma conexão. Isto é na maior parte útil para os anfitriões que proporcionam serviços de aplicativo como o correio, a Web, o FTP e o outro. Neste exemplo, as indicações do NAT estático são configuradas para permitir que os usuários no interior e os usuários na parte externa alcancem o servidor de Web no DMZ.

Esta saída mostra como uma instrução estática é construída. Note a ordem do traçado e dos endereços IP real.

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

Está aqui a tradução estática criada para dar usuários no acesso da interface interna ao server no DMZ. Cria um mapeamento entre um endereço no interior e o endereço do server no DMZ. Os usuários no interior podem então alcançar o server no DMZ através do endereço interno.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

Está aqui a tradução estática criada para dar usuários no acesso da interface externa ao server no DMZ. Cria um mapeamento entre um endereço na parte externa e o endereço do server no DMZ. Os usuários na parte externa podem então alcançar o server no DMZ através do endereço exterior.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Nota: Porque a interface externa tem um nível de segurança mais baixo do que o DMZ, uma lista de acessos deve igualmente ser criada a fim permitir usuários no acesso exterior ao server no DMZ. A lista de acessos deve conceder o acesso de usuários ao **endereço traçado na tradução estática**. Recomenda-se que esta lista de acessos esteja feita o mais específico possível. Neste caso, todo o host é acesso permitido somente às portas 80 (WWW/HTTP) e 443 (https) no servidor de Web.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

A lista de acessos deve então ser aplicada à interface externa.

```
access-group OUTSIDE in interface outside
```

Refira a [lista de acesso estendida](#) e o [acesso-grupo](#) para obter mais informações sobre dos comandos `access-list` e `access-group`.

[Como contornar o NAT](#)

Esta seção descreve como contornar o NAT. Você pôde querer contornar o NAT quando você permite o controle NAT. Você pode usar a identidade NAT, a identidade estática NAT, ou a isenção NAT a fim contornar o NAT.

[Configurar a identidade NAT](#)

A identidade NAT traduz o endereço IP real ao mesmo IP address. Somente os anfitriões “traduzidos” podem criar traduções NAT, e o tráfego de resposta é permitido para trás.

Nota: Se você muda a configuração de NAT, e você não quer esperar traduções existentes para cronometrar para fora antes que a informação nova NAT esteja usada, você usa o **comando clear xlate** a fim cancelar a tabela de tradução. Contudo, todas as conexões atual que usam traduções são desligadas quando você cancela a tabela de tradução.

A fim configurar a identidade NAT, incorpore este comando:

```
hostname(config)#nat (real_interface) 0 real_ip
[mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
udp_max_conns]
```

Por exemplo, a fim usar a identidade NAT para a rede do interior 10.1.1.0/24, incorpore este comando:

```
hostname(config)#nat (inside) 0 10.1.1.0  
255.255.255.0
```

Refira a [referência de comandos do dispositivo do Cisco Security, versão 7.2](#) para obter mais informações sobre o comando `nat`.

Configurar a identidade estática NAT

A identidade estática NAT traduz o endereço IP real ao mesmo IP address. A tradução é sempre ativa, e ambos “traduzidos” e os host remotos podem originar conexões. A identidade estática NAT deixa-o usar NAT regular ou política NAT. A política NAT deixa-o identificar o real e os endereços de destino ao determinar os endereços reais traduzir (veja a seção da [política NAT do uso](#) para obter mais informações sobre da política NAT). Por exemplo, você pode usar a identidade estática NAT da política para um endereço interno quando alcança a interface externa e o destino é o server A, mas usar uma tradução normal ao alcançar o server exterior B.

Nota: Se você remove um comando `static`, as conexões atual que usam a tradução não são afetadas. A fim remover estas conexões, incorpore o comando [claro do host local](#). Você não pode traduções estáticas claras da tabela de tradução com o **comando `clear xlate`**; você deve remover o comando `static` pelo contrário. Somente as traduções dinâmica criadas pelos comandos `nat` and `global` podem ser removidas com o [comando `clear xlate`](#).

Para configurar a identidade estática NAT da política, incorpore este comando:

```
hostname(config)#static  
(real_interface,mapped_interface) real_ip access-list acl_id [dns]  
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

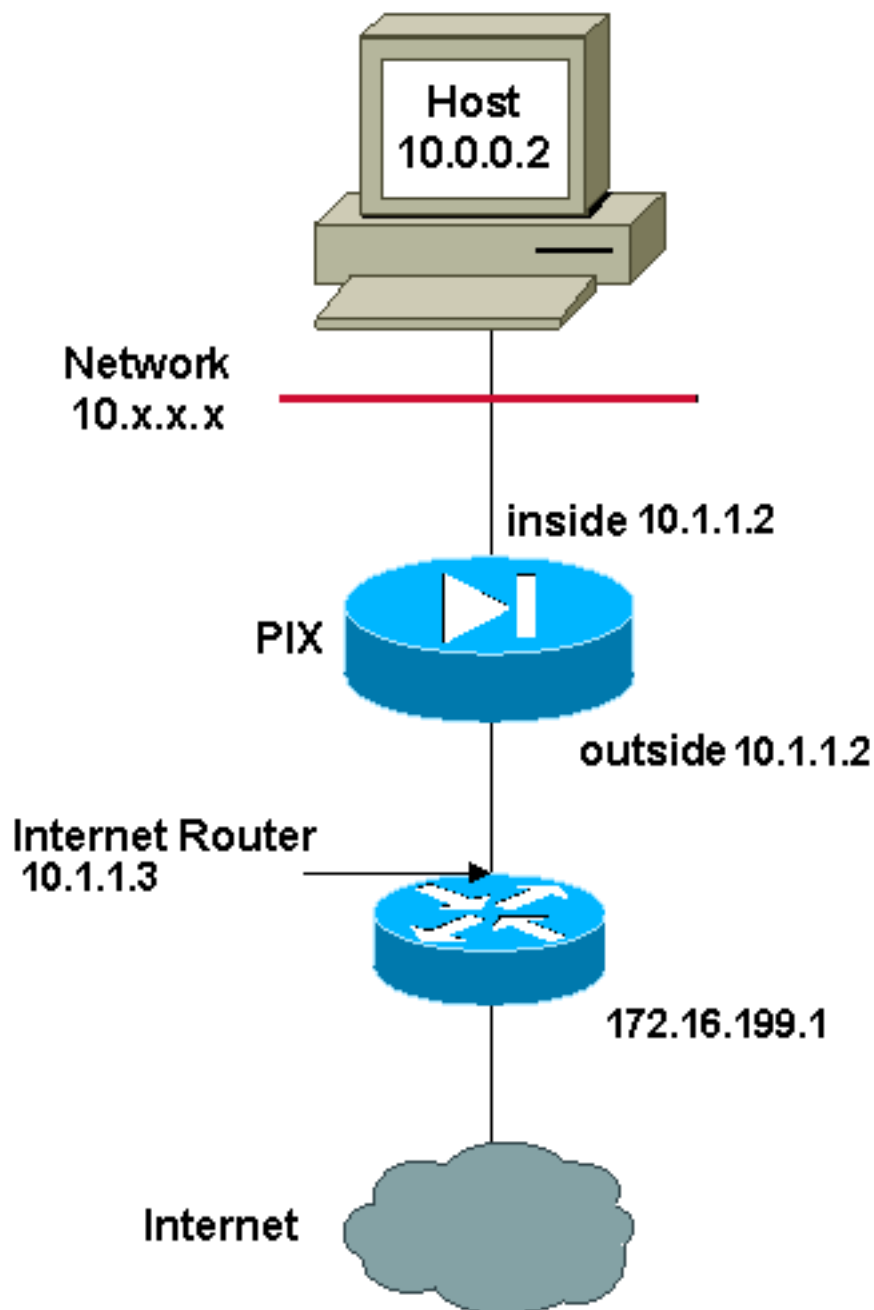
Use o comando **estendido lista de acesso** a fim criar a [lista de acesso estendida](#). Esta lista de acessos deve incluir somente a licença ACE. Certifique-se que o endereço de origem na lista de acessos combina o `real_ip` neste comando. A política NAT não considera as palavras-chaves inativas ou da tempo-escala; todos os ACE são considerados ser ativos para a configuração de NAT da política. Veja a seção da [política NAT do uso](#) para mais informação.

A fim configurar a identidade estática regular NAT, incorpore este comando:

```
hostname(config)#static  
(real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]  
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp  
udp_max_conns]
```

Especifique o mesmo IP address para ambos os argumentos do `real_ip`.

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#) que foram usados em um ambiente de laboratório.

Por exemplo, este comando usa a identidade estática NAT para um IP address interno (10.1.1.2) quando alcançado pela parte externa:

```
hostname(config)#static (inside,outside) 10.1.1.2
10.1.1.2 netmask 255.255.255.255
```

Refira a [referência de comandos do dispositivo do Cisco Security, versão 7.2](#) para obter mais informações sobre do **comando static**.

Este comando usa a identidade estática NAT para um endereço exterior (172.16.199.1) quando alcançado pelo interior:

```
hostname(config)#static (outside,inside) 172.16.199.1
172.16.199.1 netmask 255.255.255.255
```

Este comando traça estaticamente uma sub-rede inteira:

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
netmask 255.255.255.0
```

Este exemplo de NAT estático da política da identidade mostra um único endereço real que use a identidade NAT ao alcançar um endereço de destino e uma tradução ao alcançar outro:

```
hostname(config)#access-list NET1 permit ip host
10.1.1.3 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET2 permit ip host
10.1.1.3 172.16.199.224 255.255.255.224
```

```
hostname(config)#static (inside,outside) 10.1.1.3
access-list NET1
```

```
hostname(config)#static (inside,outside) 172.16.199.1
access-list NET2
```

Nota: Para obter mais informações sobre do comando **static**, consulte a [referência de comandos do Dispositivo de segurança adaptativo Cisco ASA 5580, versão 8.1](#).

Nota: Para obter mais informações sobre das listas de acesso, consulte o [guia do comando line configuration do Dispositivo de segurança adaptativo Cisco ASA 5580, versão 8.1](#).

[Configurando a isenção NAT](#)

A isenção NAT isenta endereços da tradução e reserva-os real e host remotos original conexões. A isenção NAT deixa-o especificar o real e os endereços de destino ao determinar o tráfego real isentar (similar à política NAT), assim que você tem o maior controle usando a isenção NAT do que a identidade NAT. Contudo ao contrário da política NAT, a isenção NAT não considera as portas na lista de acessos. Use a identidade estática NAT para considerar portas na lista de acessos.

Nota: Se você remove uma configuração da isenção NAT, as conexões existentes que usam a isenção NAT não são afetadas. Para remover estas conexões, incorpore o comando [claro do host local](#).

A fim configurar a isenção NAT, incorpore este comando:

```
hostname(config)#nat (real_interface) 0 access-list
acl_name [outside]
```

Crie a [lista de acesso estendida](#) usando o comando [estendido lista de acesso](#). Esta lista de

acessos pode incluir a licença ACE e negar ACE. Não especifique o real e as portas do destino na lista de acessos; A isenção NAT não considera as portas. A isenção NAT igualmente não considera as palavras-chaves inativas ou da tempo-escala; todos os ACE são considerados ser ativos para a configuração da isenção NAT.

À revelia, este comando isenta o tráfego do interior à parte externa. Se você quer o tráfego da parte externa ao interior contornar o NAT, a seguir adicionar um **comando nat** adicional e entre-o fora para identificar o exemplo NAT como o NAT exterior. Você pôde querer usar a isenção exterior NAT se você configura o NAT dinâmico para a interface externa e o quer isentar o outro tráfego.

Por exemplo, a fim isentar uma rede interna ao alcançar todo o endereço de destino, incorpore este comando:

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0  
255.255.255.0 any
```

```
hostname(config)# nat (inside) 0 access-list  
EXEMPT
```

A fim usar o NAT exterior dinâmico para uma rede do DMZ, e isentar uma outra rede do DMZ, incorporam este comando:

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0  
outside dns
```

```
hostname(config)#global (inside) 1  
10.1.1.2
```

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0  
255.255.255.0 any
```

```
hostname(config)#nat (dmz) 0 access-list  
EXEMPT
```

A fim isentar um endereço interno ao alcançar dois endereços de destino diferentes, entre nisto comanda:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0  
255.255.255.0 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET1 permit ip 10.1.1.0  
255.255.255.0 172.16.199.224 255.255.255.224
```

```
hostname(config)#nat (inside) 0 access-list NET1
```

Verificar

Trafiqne que corre através da ferramenta de segurança se submete muito provavelmente ao NAT. Refira o [PIX/ASA: Monitore e pesquise defeitos problemas de desempenho](#) a fim verificar as traduções que estão no uso na ferramenta de segurança.

O comando **show xlate count** indica a corrente e o número máximo de traduções com o PIX. Uma tradução é um mapeamento de um endereço interno a um endereço externo e pode ser um mapeamento um a um, tal como o NAT, ou um mapeamento many-to-one, tal como a PANCADINHA. Este comando é um subconjunto do [comando show xlate](#), que outputs cada tradução com o PIX. A saída do comando mostra traduções “no uso,” qual refere o número de traduções ativa no PIX quando o comando é emitido; “o mais usado” refere as traduções máximas que foram consideradas nunca no PIX desde que foi posto sobre.

Troubleshooting

Mensagem de Erro recebido ao adicionar um PAT estático para a porta 443

Problema

Você recebe este Mensagem de Erro quando você adiciona um PAT estático para a porta 443:

```
netmask estático 255.255.255.255 tcp 0 de 192.168.1.87 443 da relação 443 tcp do [ERROR] (PARA DENTRO, FORA) 0 UDP 0
```

```
incapaz de reservar a porta 443 para o PAT estático
```

```
ERRO: incapaz de transferir a política
```

Solução

Este Mensagem de Erro ocorre quando o ASDM ou o WebVPN estão sendo executado na porta 443. A fim resolver esta edição, início de uma sessão ao Firewall, e terminar uma destas etapas:

- A fim mudar a porta ASDM a qualquer coisa a não ser 443, execute estes comandos:

```
ASA(config)#no http server enable  
ASA(config)#http server enable 8080
```

- A fim mudar a porta WebVPN a qualquer coisa a não ser 443, execute estes comandos:

```
ASA(config)#webvpn  
ASA(config-webvpn)#enable outside  
ASA(config-webvpn)#port 65010
```

Depois que você executa estes comandos, você deve poder adicionar um NAT/PAT na porta 443 a um outro server. Quando você tenta usar o ASDM para controlar no futuro o ASA, especifique a porta nova como 8080.

ERRO: conflito do traçar-endereço com estática existente

Problema

Você recebe este erro quando você adiciona uma instrução estática no ASA:

```
ERRO: conflito do traçar-endereço com estática existente
```

Solução

Verifique que uma entrada já não existe para a fonte que estática você quer adicionar.

[Informações Relacionadas](#)

- [Página de suporte do PIX](#)
- [Referências de comando PIX](#)
- [Página de suporte ASA](#)
- [Referências de comandos ASA](#)
- [Request for comments \(RFC\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)