

PIX/ASA 7.x e mais tarde: Conectando redes internas múltiplas com o exemplo de configuração do Internet

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Configurar](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração de PIX usando o ASDM](#)

[Configuração de PIX usando o CLI](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Procedimento de Troubleshooting](#)

[Incapaz de alcançar por nome Web site](#)

[Informações Relacionadas](#)

Introdução

Este documento fornece uma configuração de exemplo do PIX/ASA Security Appliance, versão 7.x e posteriores, com redes internas múltiplas conectadas à Internet (ou a uma rede externa) que usam a interface de linha de comando CCLI) ou o Security Device Manager (ASDM) 5.x e versões posteriores.

Consulte [para estabelecer e pesquisar defeitos a Conectividade através do dispositivo do Cisco Security](#) para obter informações sobre de como estabelecer e pesquisar defeitos a Conectividade com o PIX/ASA.

Refira a [utilização nat, global, estática, a conduíte, e os comandos access-list e a porta Redirection\(Forwarding\) no PIX](#) para obter informações sobre dos comandos pix comuns.

Nota: Algumas opções em outras versões ASDM podem parecer diferentes das opções em ASDM 5.1. Consulte a [documentação do ASDM](#) para obter mais informações.

Pré-requisitos

Requisitos

Quando você adiciona mais de uma rede interna atrás de um PIX Firewall, mantenha estes pontos na mente:

- O PIX não apoia o endereçamento secundário.
- Um roteador tem que ser usado atrás do PIX a fim conseguir o roteamento entre a rede existente e a rede recentemente adicionada.
- O gateway padrão de todos os anfitriões precisa de apontar ao roteador interno.
- Adicionar uma rota padrão no roteador interno esses pontos ao PIX.
- Cancele o esconderijo do Address Resolution Protocol (ARP) no roteador interno.

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:

- Ferramenta de segurança 515E PIX com versão de software 7.1
- ASDM 5.1
- Roteadores Cisco com Software Release 12.3(7)T de Cisco IOS®

Nota: Este documento recertified com versão de software 8.x PIX/ASA e Cisco IOS Software Release 12.4.

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

Esta configuração pode igualmente ser usada com versão 7.x e mais recente da ferramenta de segurança de Cisco ASA.

Convenções

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

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

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.

Informações de Apoio

Nesta encenação, há três redes internas (10.1.1.0/24, 10.2.1.0/24 e 10.3.1.0/24) a ser conectadas ao Internet (ou a uma rede externa) com o PIX. As redes internas são conectadas à interface interna do PIX. A conectividade de Internet é através de um roteador que seja conectado à interface externa do PIX. O PIX tem o endereço IP de Um ou Mais Servidores Cisco ICM NT 172.16.1.1/24.

As rotas estáticas são usadas para distribuir e vice-versa os pacotes das redes internas ao Internet. Em vez de usar as rotas estáticas, você pode igualmente usar um protocolo de roteamento dinâmico tal como o Routing Information Protocol (RIP) ou o Open Shortest Path First (OSPF).

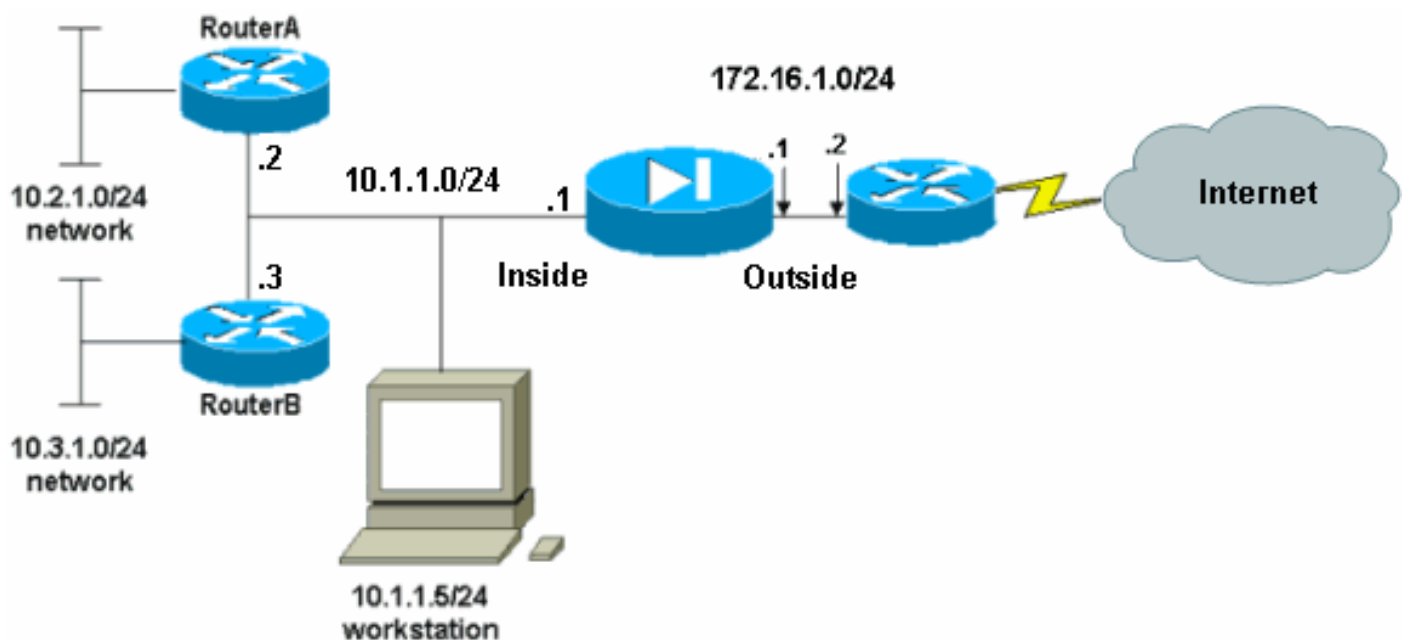
Os host internos comunicam-se com o Internet traduzindo as redes internas no PIX usando NAT dinâmico (pool dos endereços IP 172.16.1.5 a 172.16.1.10). Se o pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT é esgotado, o PIX PANCADINHA (que usa o endereço IP 172.16.1.4) os host internos alcançará o Internet.

Refira [indicações PIX/ASA 7.x NAT e de PANCADINHA](#) para obter mais informações sobre do NAT/PAT.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



O gateway padrão dos hosts na rede 10.1.1.0 aponta para o RoteadorA. Uma rota padrão no roteadorB é adicionada que aponte ao roteadorA. O roteador A tem uma rota padrão que aponta para a interface dentro do PIX.

Configurações

Este documento utiliza as seguintes configurações:

- [Configuração do Roteador A](#)
- [Configuração do roteador B](#)
- [Configuração da ferramenta de segurança 7.1 PIX](#)
[Configuração de PIX usando o ASDM](#)
[Configuração de CLI da ferramenta de segurança PIX](#)

Configuração do Roteador A

```
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service config service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterA ! interface Ethernet2/0 ip address
10.2.1.1 255.255.255.0 half-duplex ! interface
Ethernet2/1 ip address 10.1.1.2 255.255.255.0 half-
duplex ! ip classless ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3 ! ! line con 0
line aux 0 line vty 0 4 ! end RouterA#
```

Configuração do roteador B

```
RouterB#show running-config Building configuration...
Current configuration : 1132 bytes ! version 12.4
service config service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname RouterB ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed
auto ! interface Ethernet1/0 ip address 10.3.1.1
255.255.255.0 half-duplex ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! end RouterB#
```

Se você quer usar o ASDM para a configuração da ferramenta de segurança PIX, mas não amarrou o dispositivo, termine estas etapas:

1. Console no PIX.
2. De uma configuração esclarecida, use as alertas interativas a fim permitir o ASDM para o Gerenciamento do PIX da estação de trabalho 10.1.1.5.

Configuração da ferramenta de segurança 7.1 PIX

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
```

```
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 14:45:00 Mar 15 2005
Firewall Mode: Routed
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
INFO: Security level for "inside" set to 100 by
default.
Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
INFO: converting 'fixup protocol ftp 21' to MPF
commands
INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
INFO: converting 'fixup protocol rsh 514' to
MPF commands
INFO: converting 'fixup protocol rtsp 554' to
MPF commands
INFO: converting 'fixup protocol sip 5060' to
MPF commands
INFO: converting 'fixup protocol skinny 2000'
to MPF commands
INFO: converting 'fixup protocol smtp 25' to
MPF commands
INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
INFO: converting 'fixup protocol tftp 69' to
MPF commands
INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

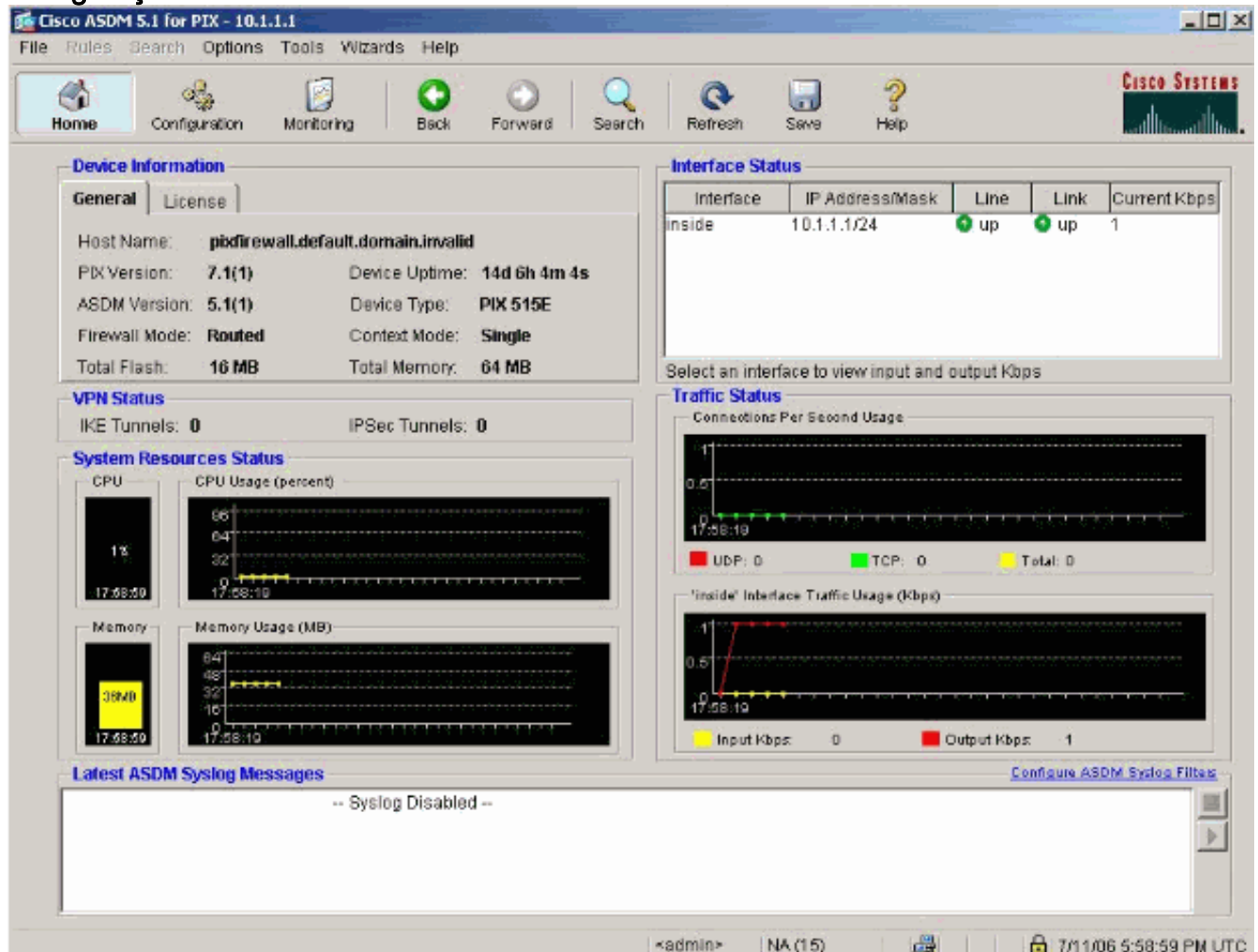
Type help or '?' for a list of available commands.
OZ-PIX>
```

Configuração de PIX usando o ASDM

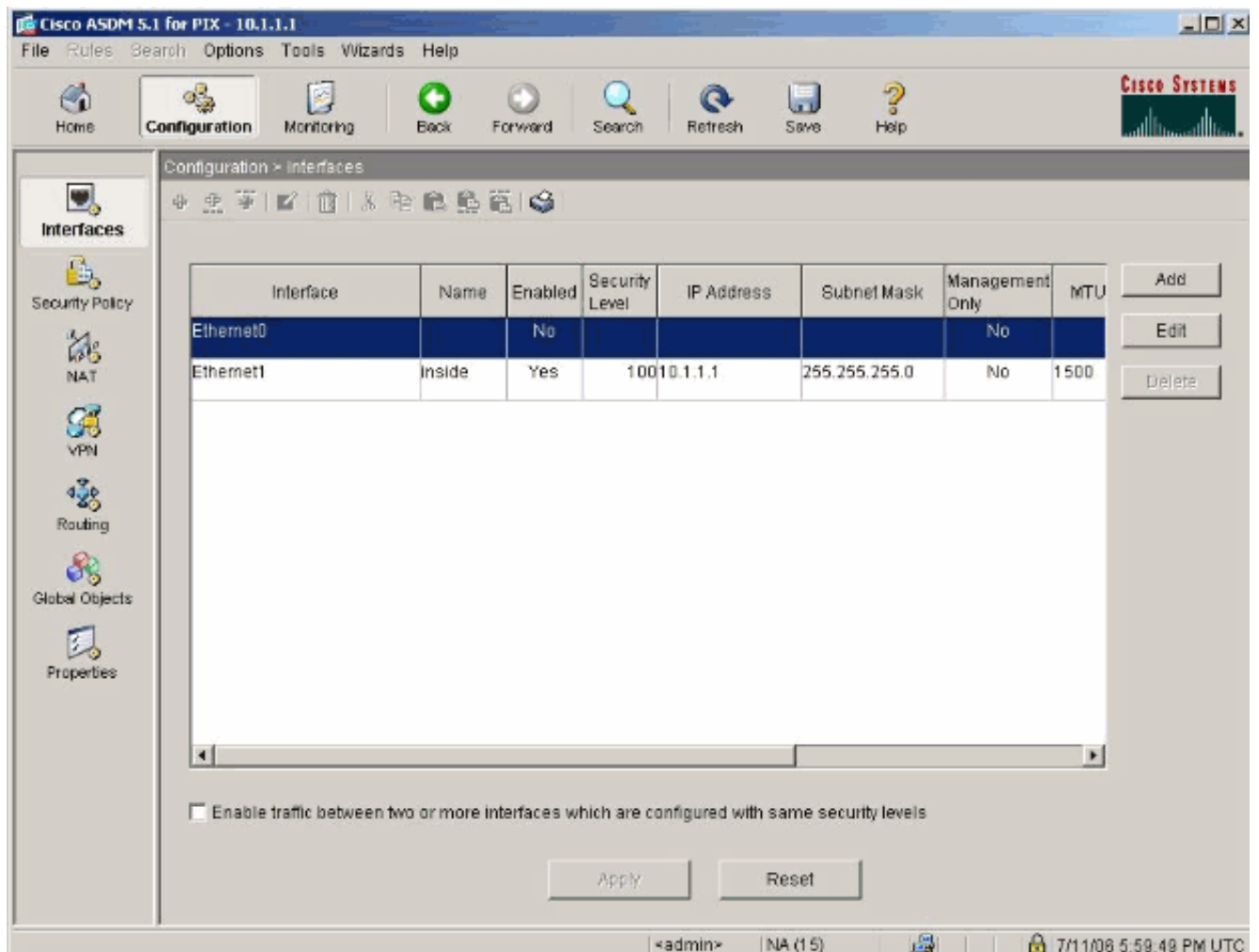
Termine estas etapas a fim configurar através do ASDM GUI:

1. Da estação de trabalho 10.1.1.5, abra um navegador da Web para usar o ADSM (neste exemplo, <https://10.1.1.1>).
2. Clique **sim** nas alertas do certificado.
3. Início de uma sessão com a senha da possibilidade, como configurada previamente.

- Se isto é a primeira vez o ASDM está executado no PC, você é alertado usar a launcher ASDM ou o ASDM como um App das Javas. Neste exemplo, a launcher ASDM é selecionada e instalada.
- Vá à janela ASDM Home e clique a **configuração**.



- Escolha a **relação** > **editam** a fim configurar a interface externa.



7. Incorpore os detalhes da relação e clique a **APROVAÇÃO** quando você é feito.

Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

Description:

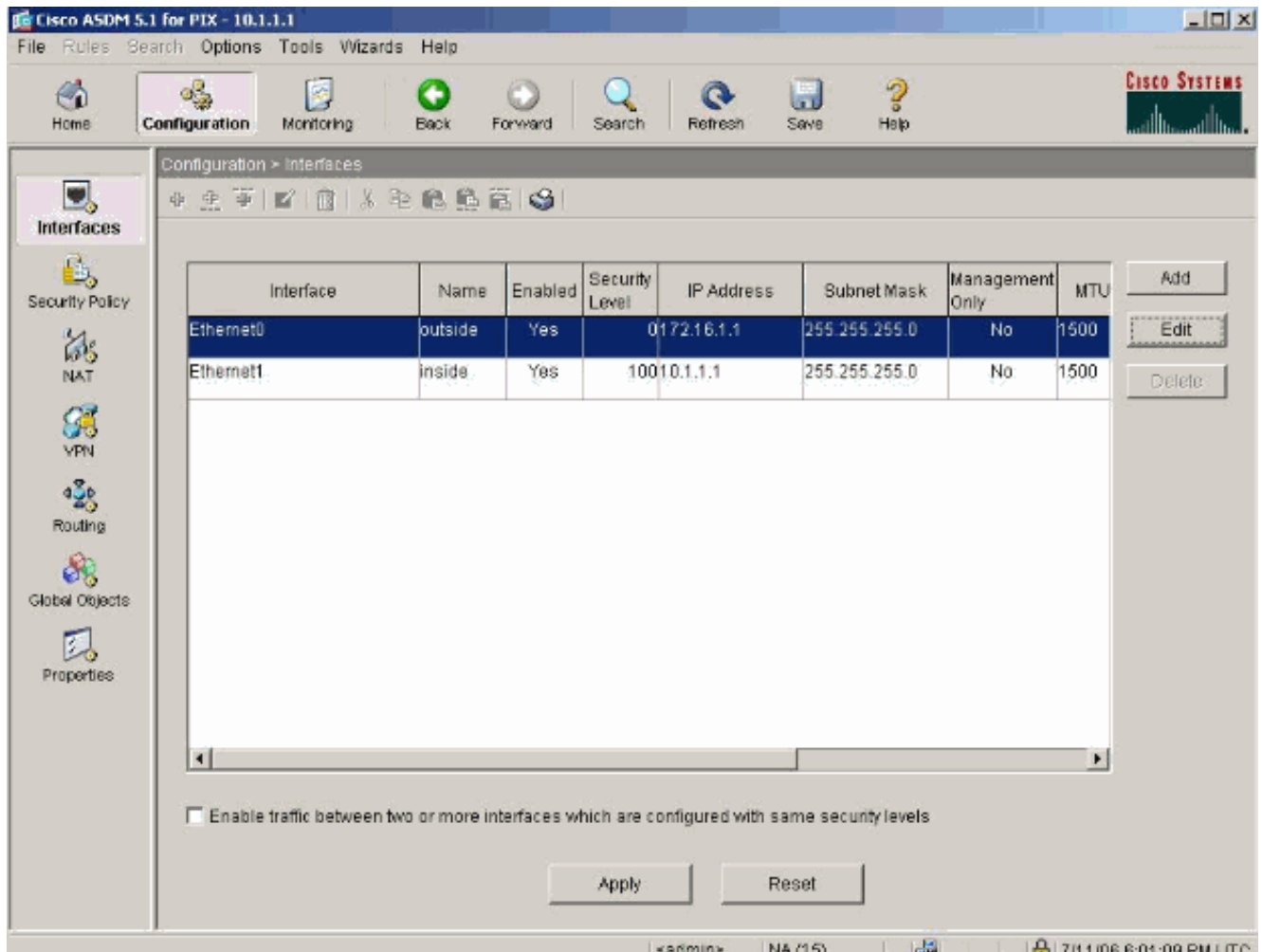
OK Cancel Help

8. Clique a **APROVAÇÃO** na caixa de diálogo da mudança do nível de segurança.

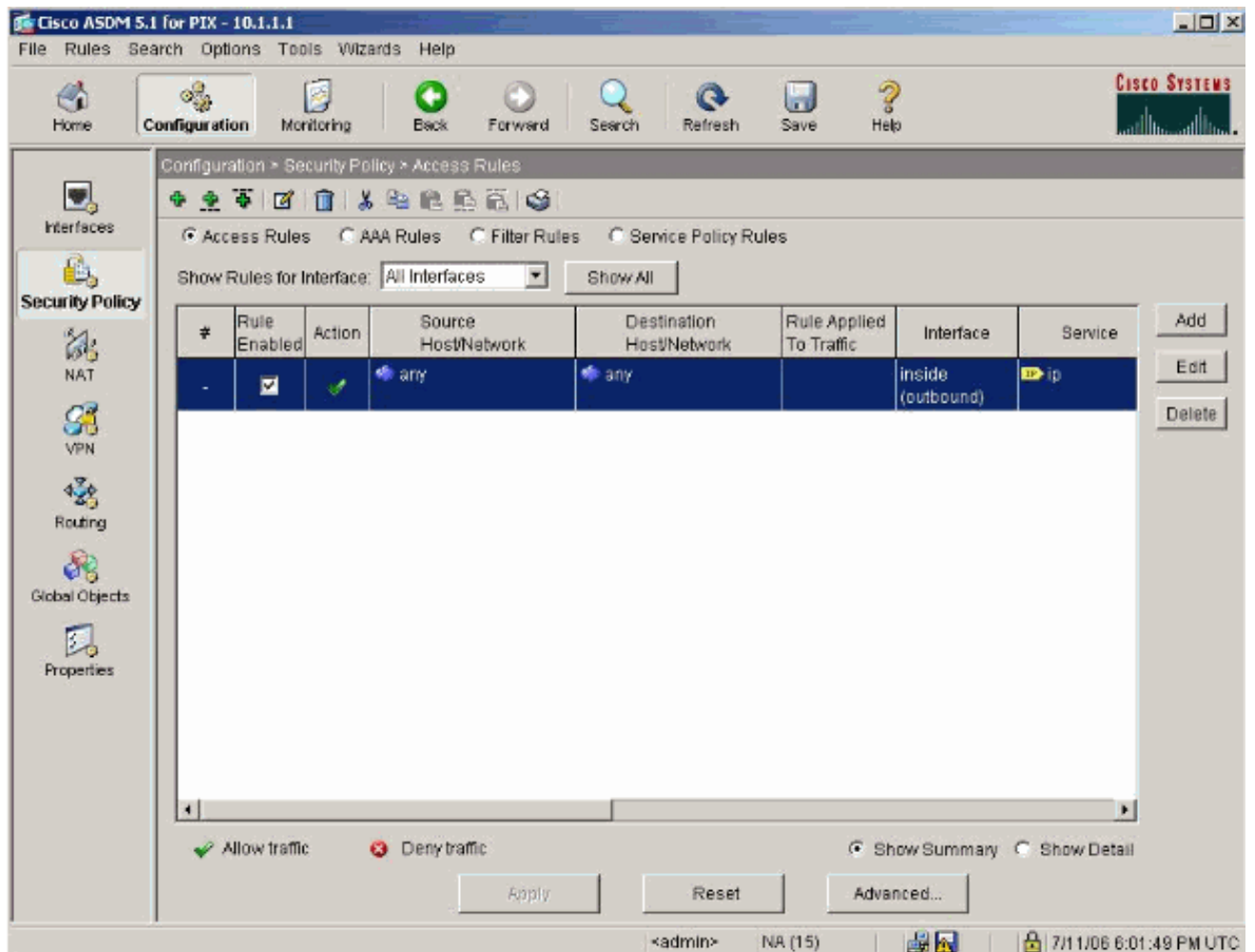
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

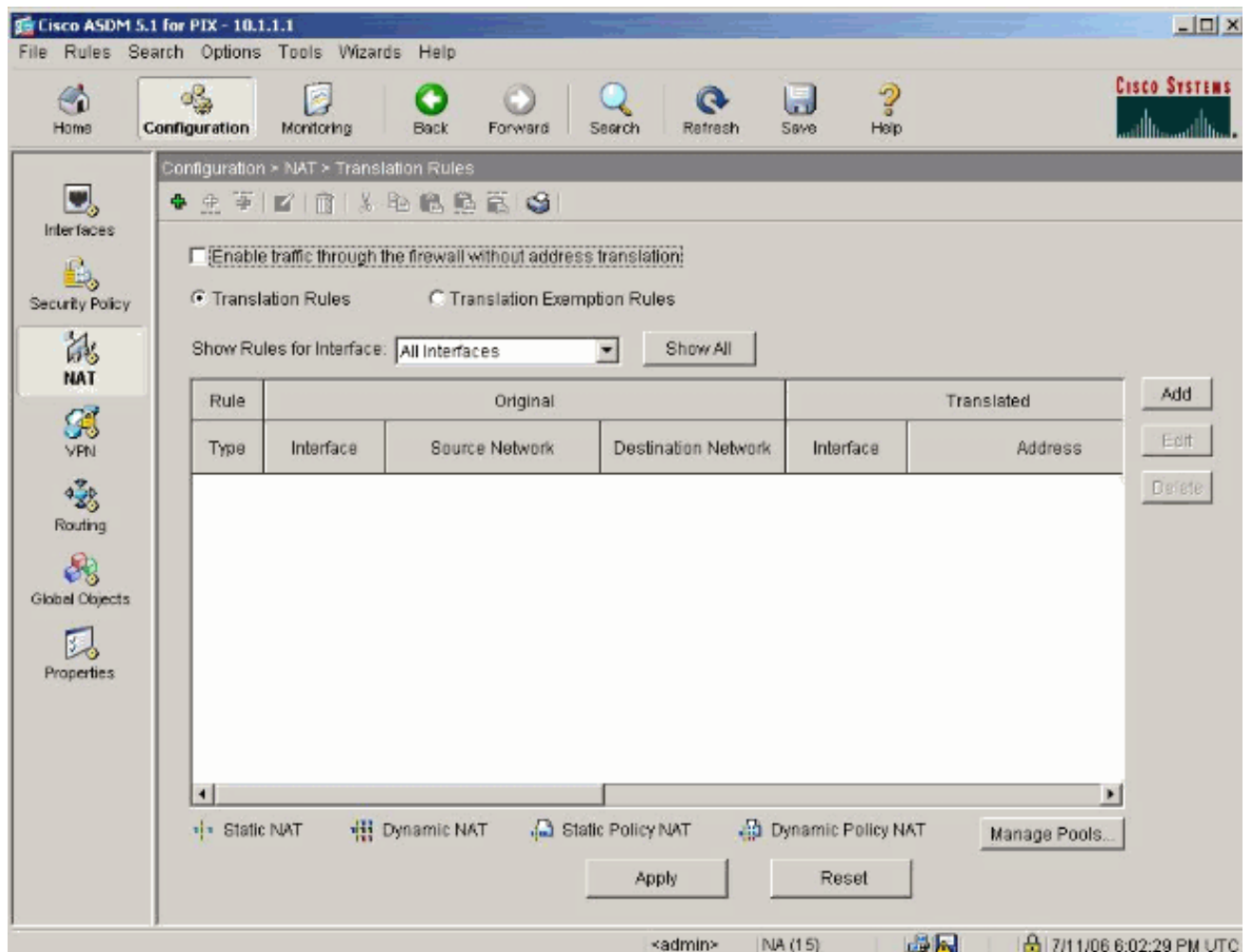
9. O clique **aplica-se** para aceitar a configuração da interface. A configuração igualmente obtém empurrada no PIX.



10. Escolha a política de segurança na aba das características a fim rever a regra da política de segurança usada. Neste exemplo, a regra interna do padrão é usada.



11. Neste exemplo, o NAT é usado. Desmarcar o **tráfego da possibilidade** com o Firewall sem caixa de verificação da **tradução de endereços** e o clique **adiciona** a fim configurar a regra NAT.



12. Configurar a rede da fonte. Neste exemplo, 10.0.0.0 é usado para o endereço IP de Um ou Mais Servidores Cisco ICM NT, e 255.0.0.0 é usado para a máscara. Clique em **Manage Pools** para definir os endereços do pool de NAT.

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

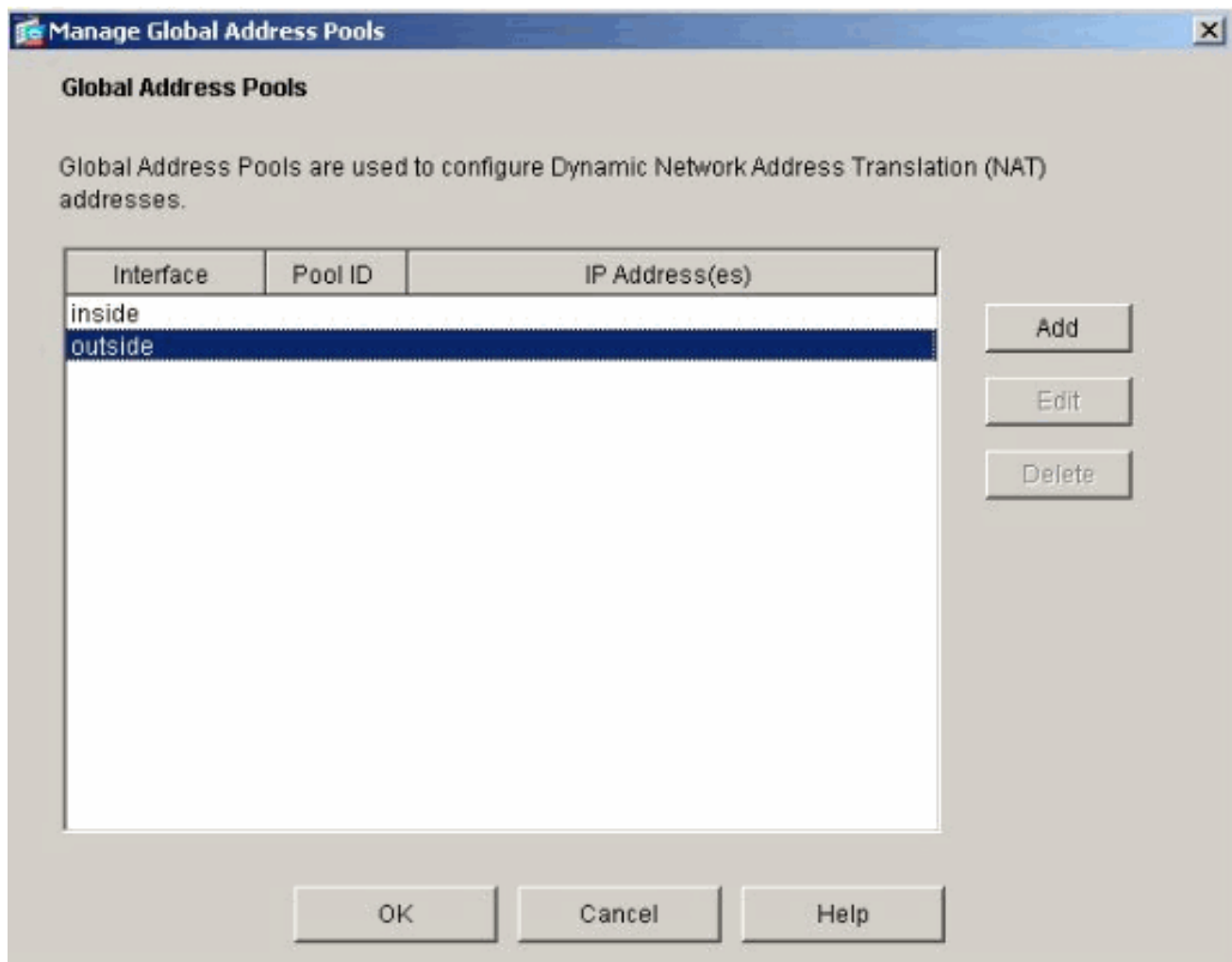
TCP Original port: Translated port:

 UDP

 Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

13. Seleccione a interface externa e o clique **adiciona**.



14. Neste exemplo, o pool de uma escala e do endereço PAT é configurado. Configurar o endereço do conjunto NAT da escala e clique a **APROVAÇÃO**.

Add Global Pool Item

Interface: Pool ID:

Range
 Port Address Translation (PAT)
 Port Address Translation (PAT) using the IP address of the interface

IP Address: —

Network Mask (optional):

15. Selecione a interface externa em etapa 13 a fim configurar o endereço PAT. Clique em OK.

Add Global Pool Item

Interface: Pool ID:

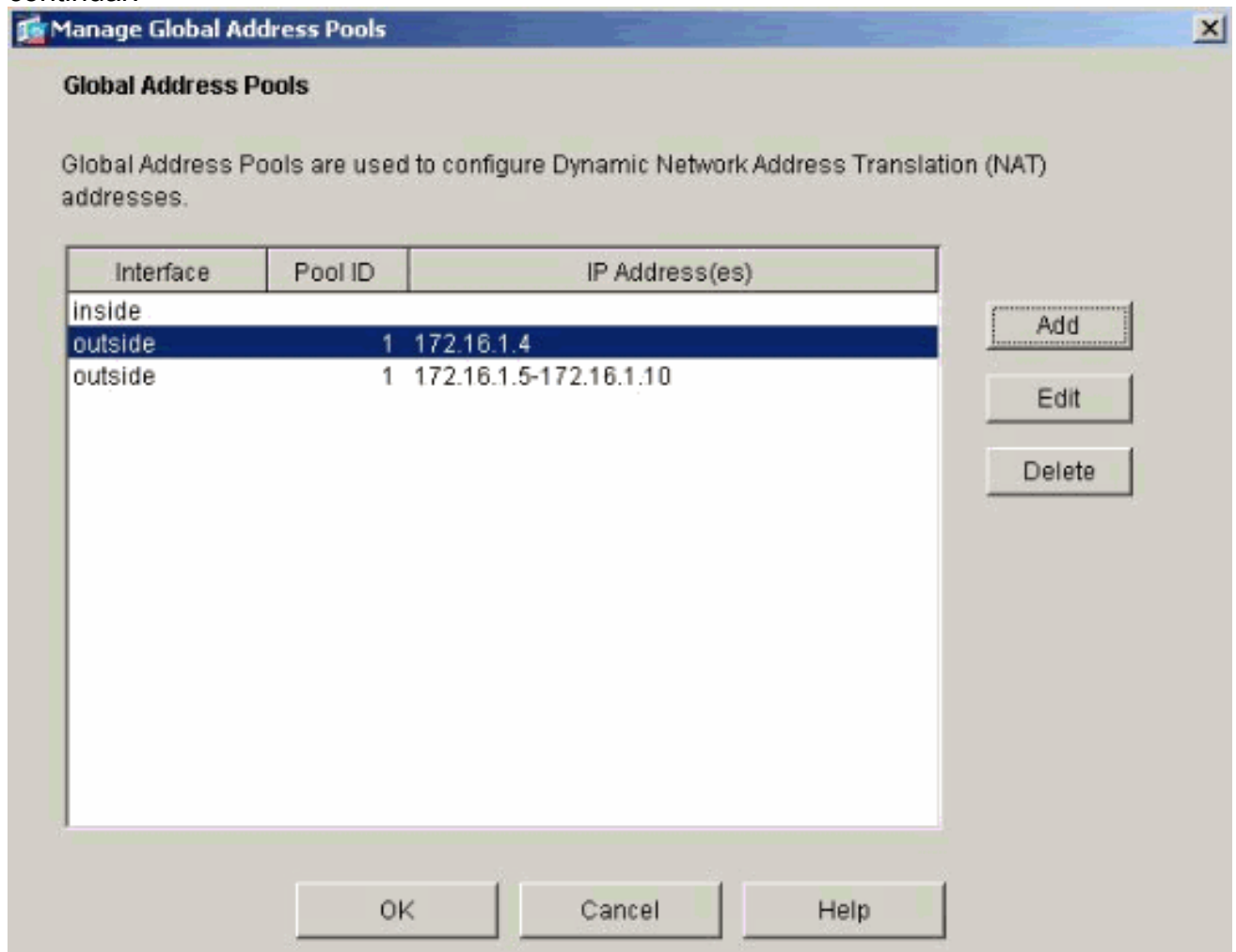
Range
 Port Address Translation (PAT)
 Port Address Translation (PAT) using the IP address of the interface

IP Address: —

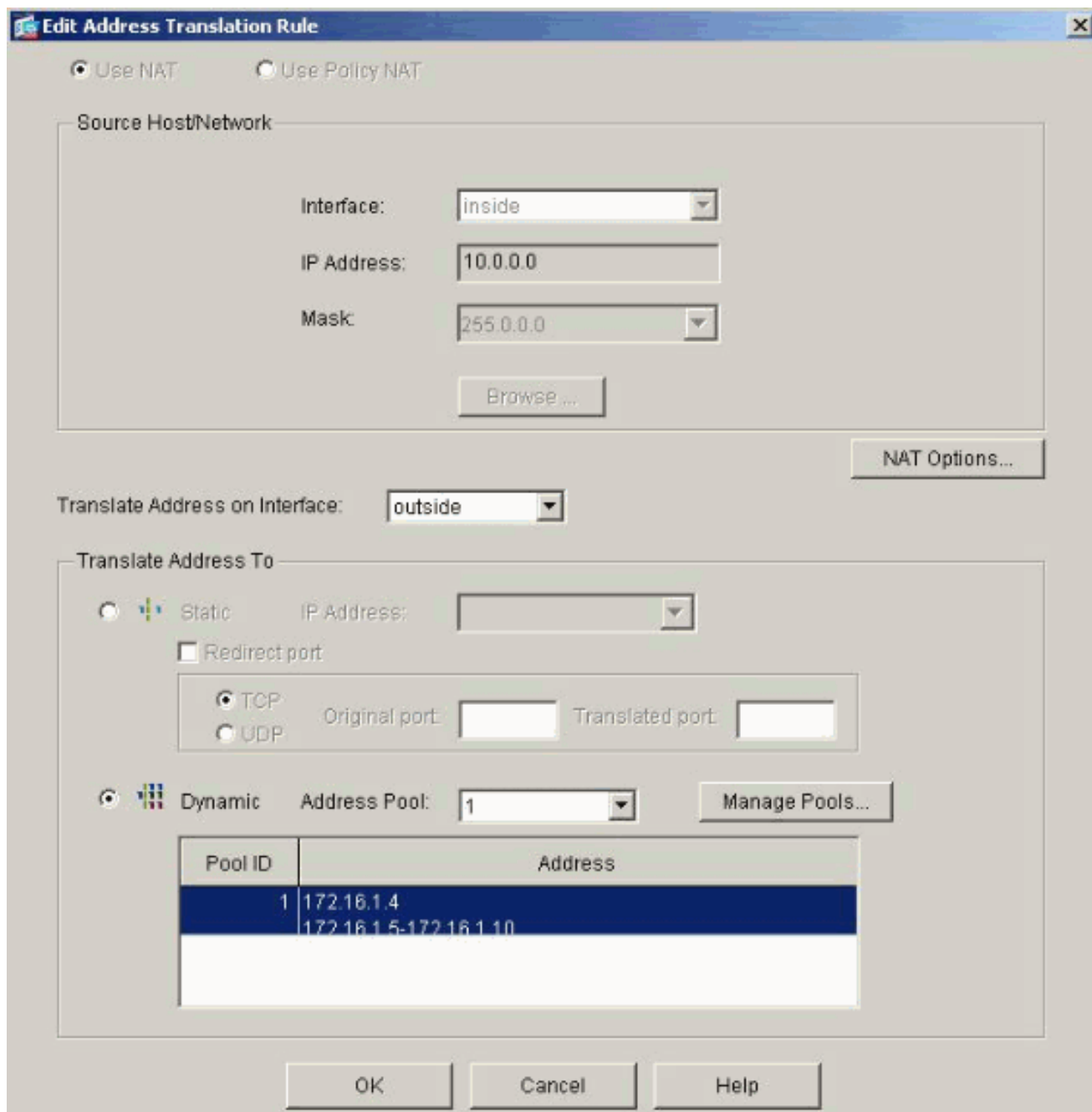
Network Mask (optional):

Clique a **APROVAÇÃO** a fim

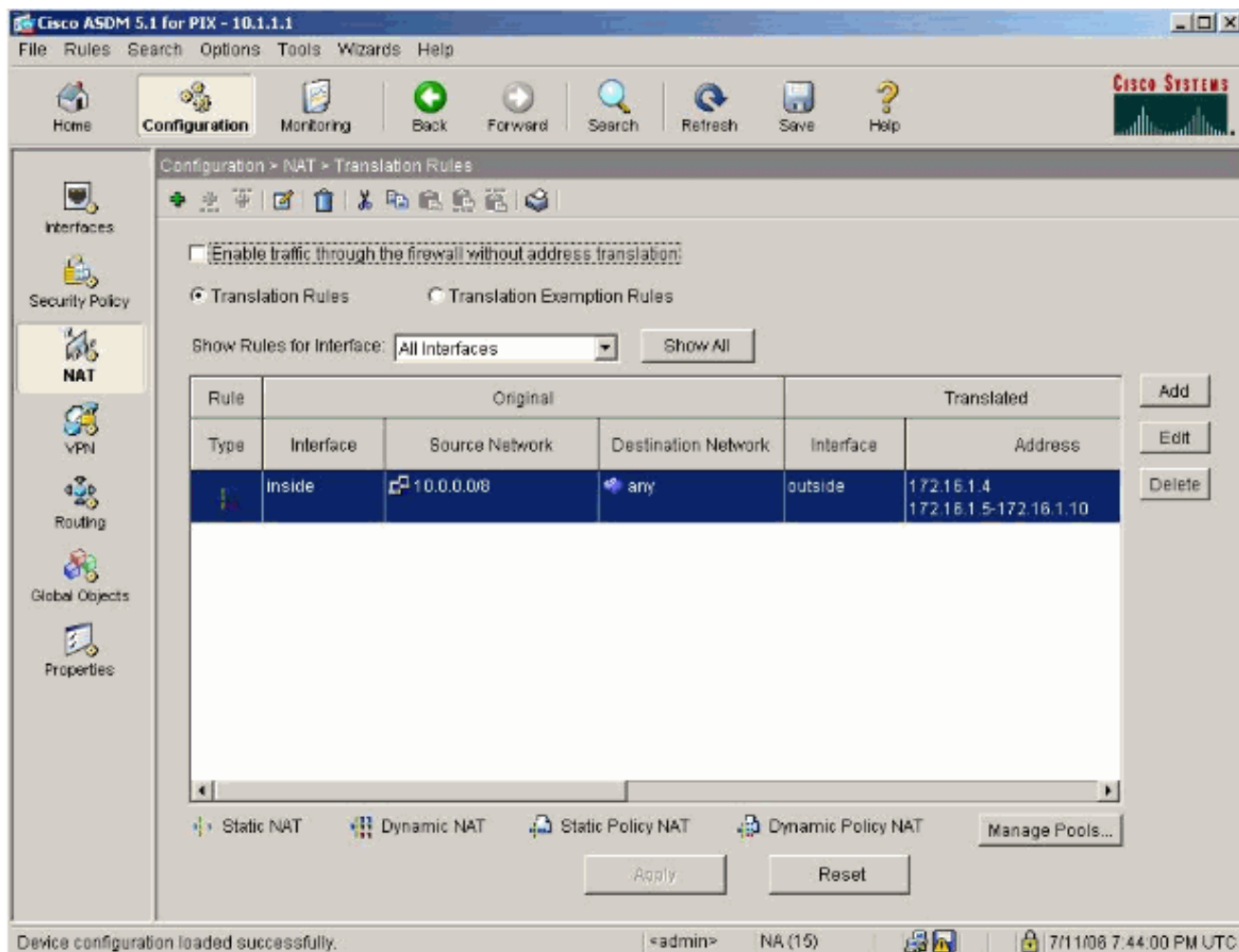
continuar.



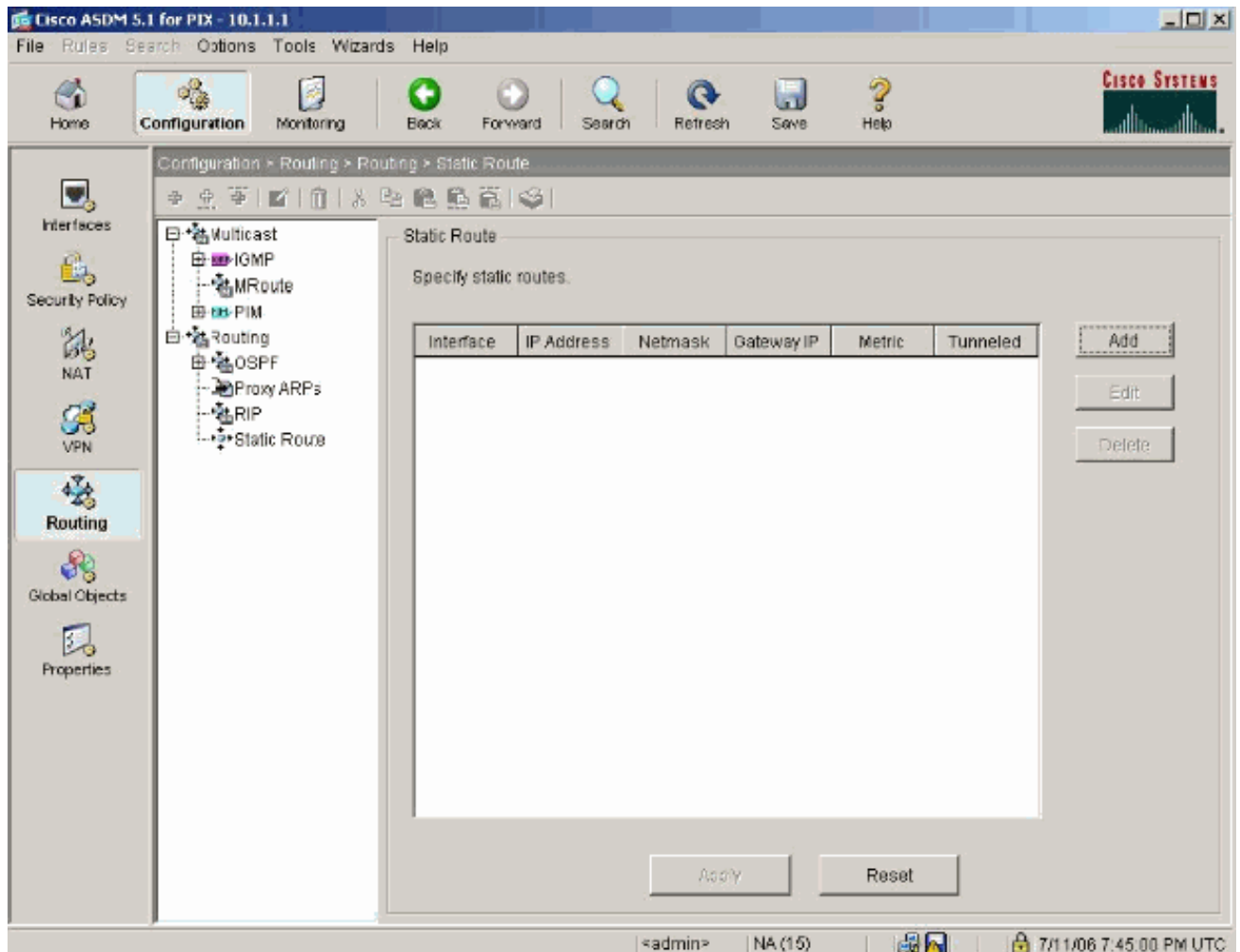
16. No indicador da regra de tradução de endereço da edição, selecione o pool ID para ser usado pela rede da fonte configurada. Clique em **OK**.



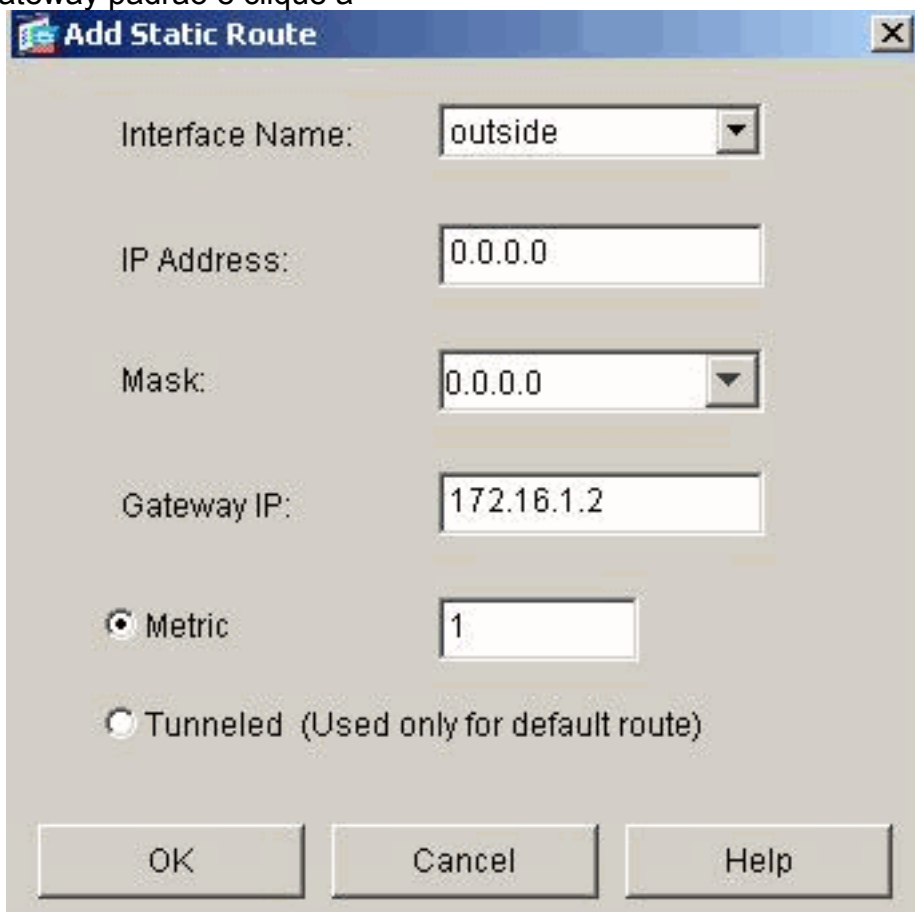
17. O clique **aplica-se** a fim empurrar a regra configurada NAT para o PIX.



18. Neste exemplo, as rotas estáticas são usadas. Clique o roteamento, escolha a rota estática e o clique adiciona.



19. Configurar o gateway padrão e clique a



APROVAÇÃO.

20. O clique **adiciona** e adiciona as rotas às redes

Add Static Route

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

internas.

Add Static Route

Interface Name:

IP Address:

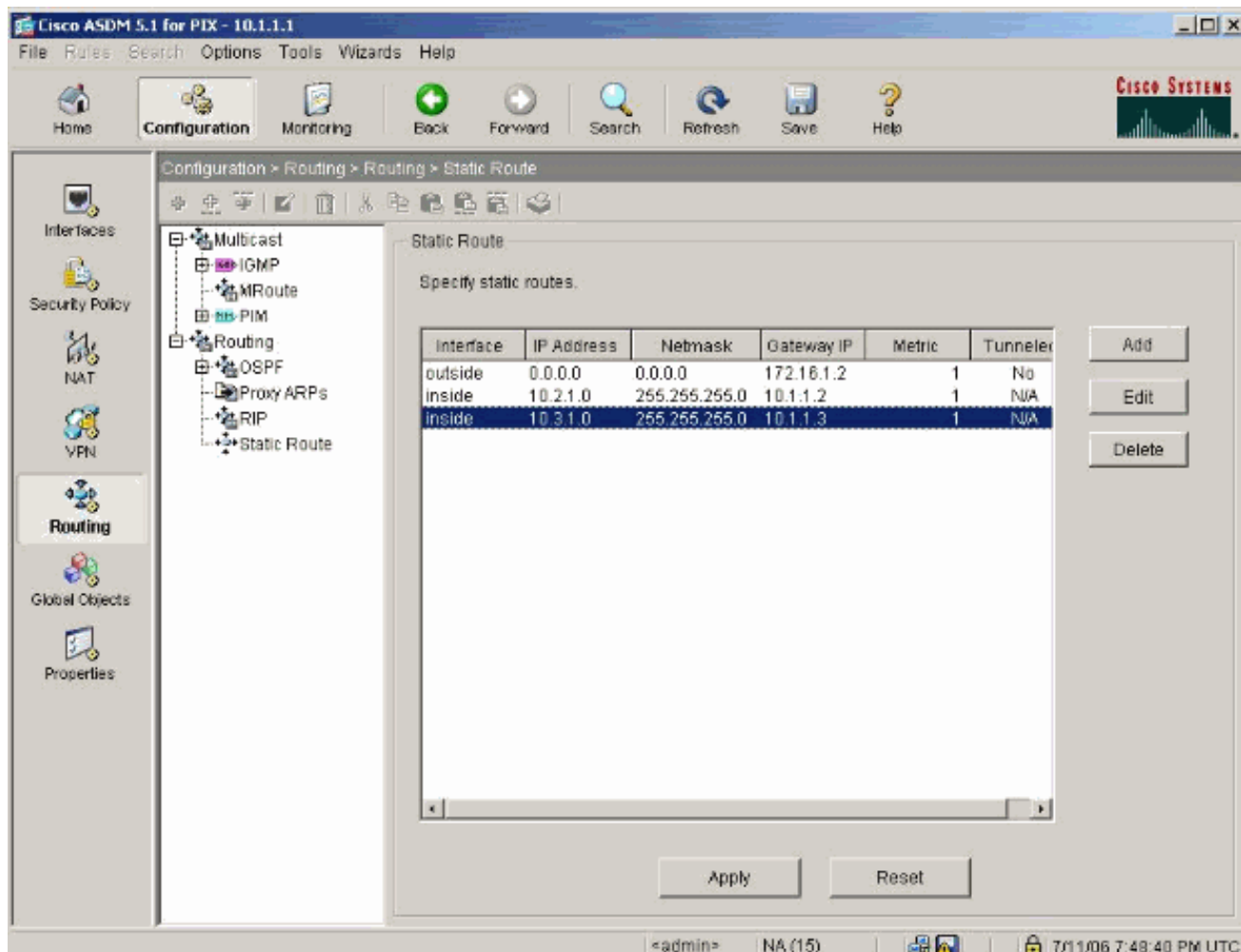
Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

21. Confirme que as rotas corretas estão configuradas e o clique se aplica.



Configuração de PIX usando o CLI

A configuração através do ASDM GUI está agora completa.

Você pode ver esta configuração através do CLI:

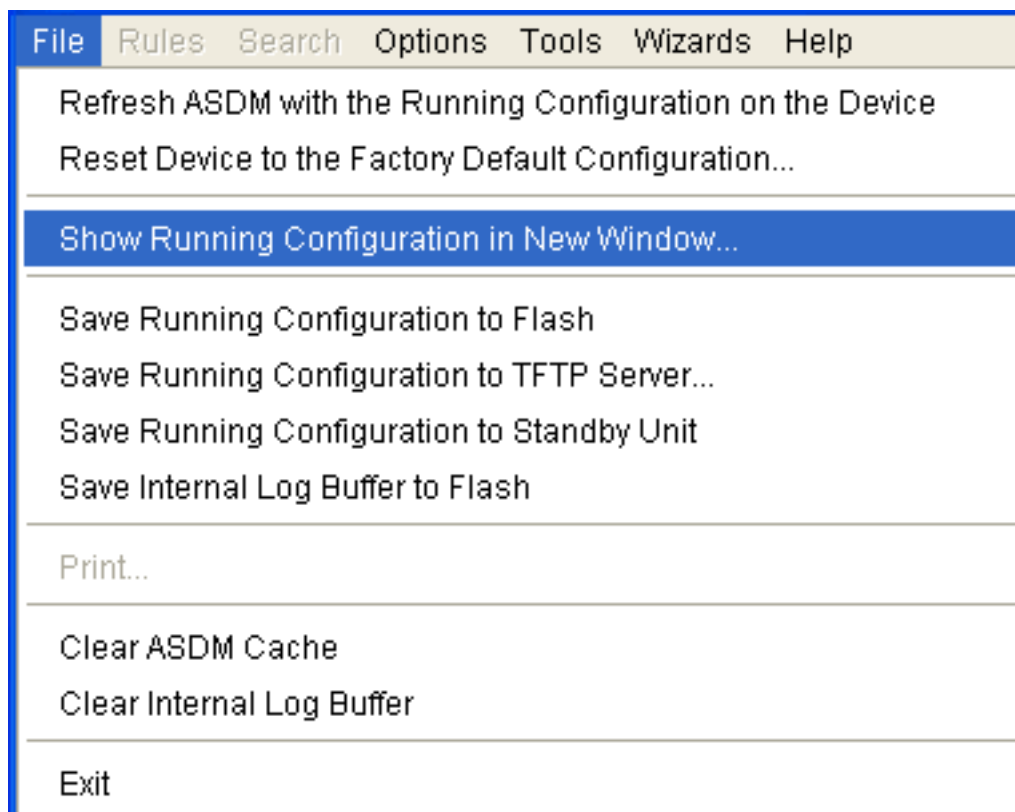
```

Ferramenta de segurança CLI PIX
pixfirewall(config)#write terminal PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 172.16.1.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- Assign name and IP address
to the interfaces enable password 2KFQnbNIdI.2KYOU
encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control !--- Enforce a strict NAT for all the
traffic through the Security appliance global (outside)
1 172.16.1.5-172.16.1.10 netmask 255.255.255.0 !---
Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0 !--- Define
a single IP address 172.16.1.4 with NAT ID 1 to be used
for PAT nat (inside) 1 10.0.0.0 255.0.0.0 !--- Define
the inside networks with same NAT ID 1 used in the
global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1 route inside 10.2.1.0
255.255.255.0 10.1.1.2 1 !--- Configure static routes
for routing the packets towards the internal network
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !---

```

```
Configure static route for routing the packets towards
the Internet (or External network) timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 timeout uauth 0:05:00 absolute http server
enable !--- Enable the HTTP server on PIX for ASDM
access http 10.1.1.5 255.255.255.255 inside !--- Enable
HTTP access from host 10.1.1.5 to configure PIX using
ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

Escolha **configuração running do arquivo > da mostra na nova janela** a fim ver a configuração de CLI no ASDM.



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Comandos para Troubleshooting

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debug icmp trace** - Exibe se as requisições de ICMP dos hosts alcançam o PIX. A fim

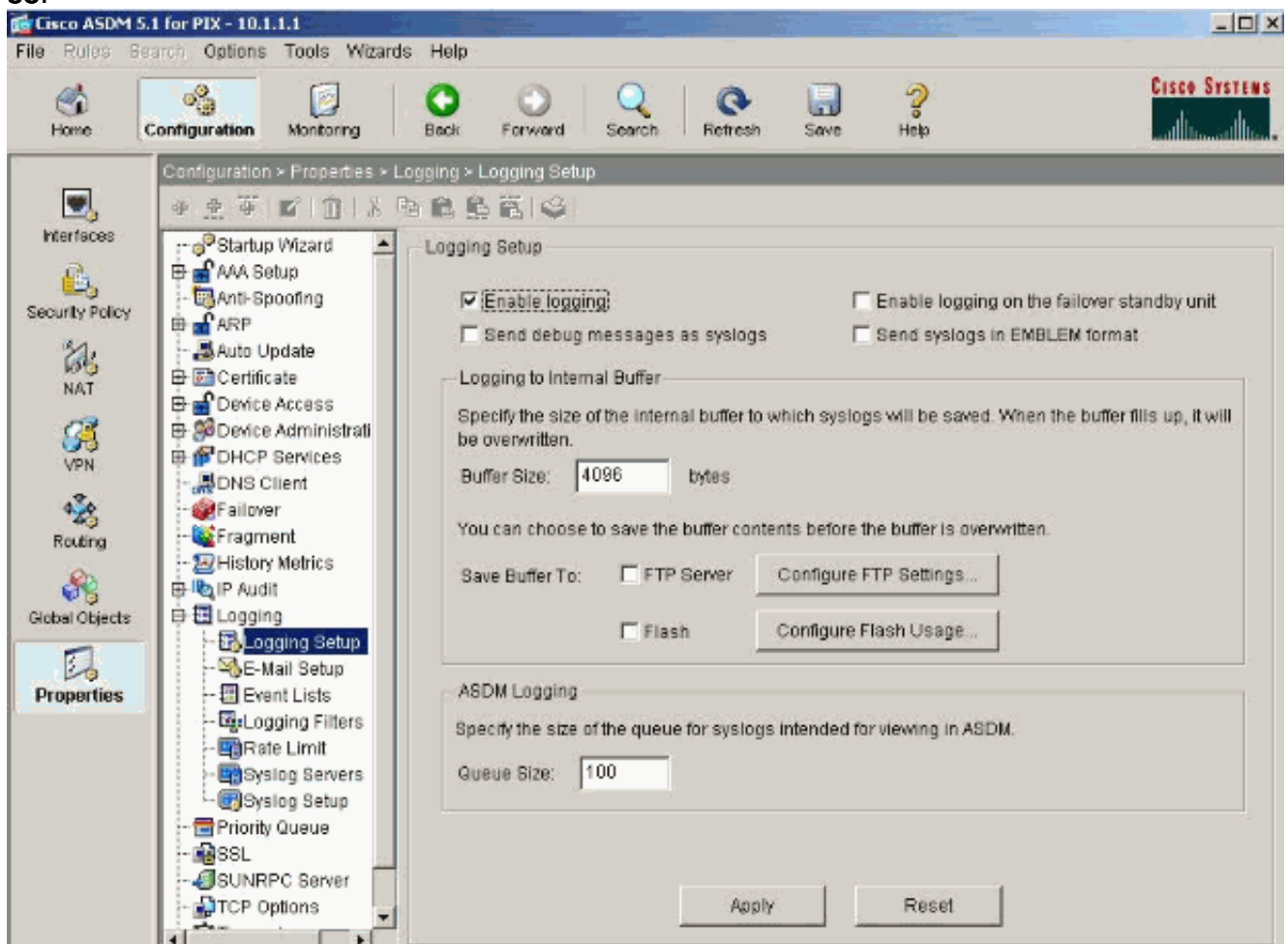
executar isto debugar, você precisam de adicionar o **comando access-list** permitir o ICMP em sua configuração.

- **eliminação de erros do logging buffer** — Mostra as conexões que são estabelecidas e negadas aos anfitriões que atravessam o PIX. A informação é armazenada no buffer de registro PIX e você pode ver a saída com o **comando show log**.

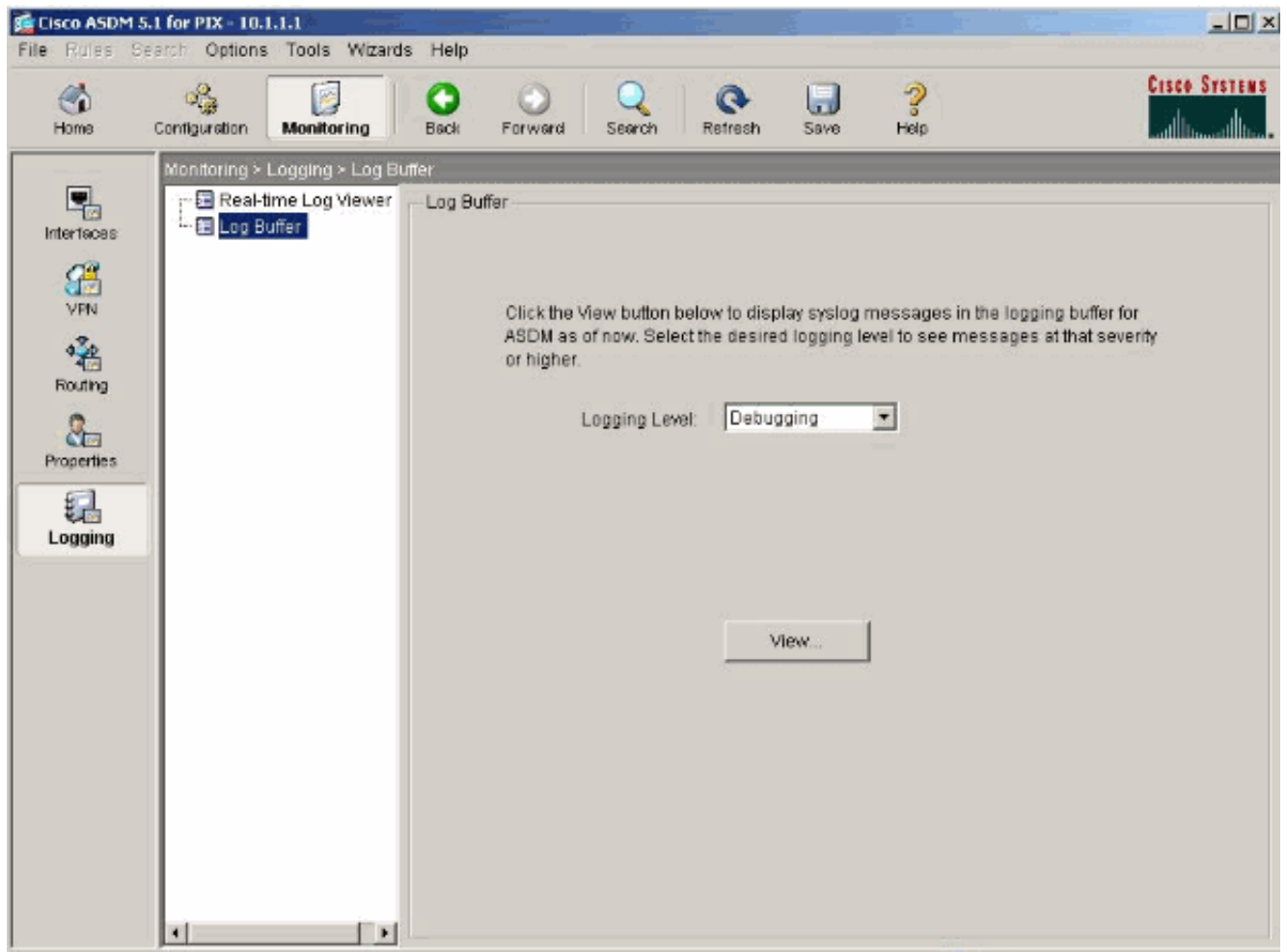
Procedimento de Troubleshooting

O ASDM pode ser usado para permitir o registro, e para ver igualmente os logs:

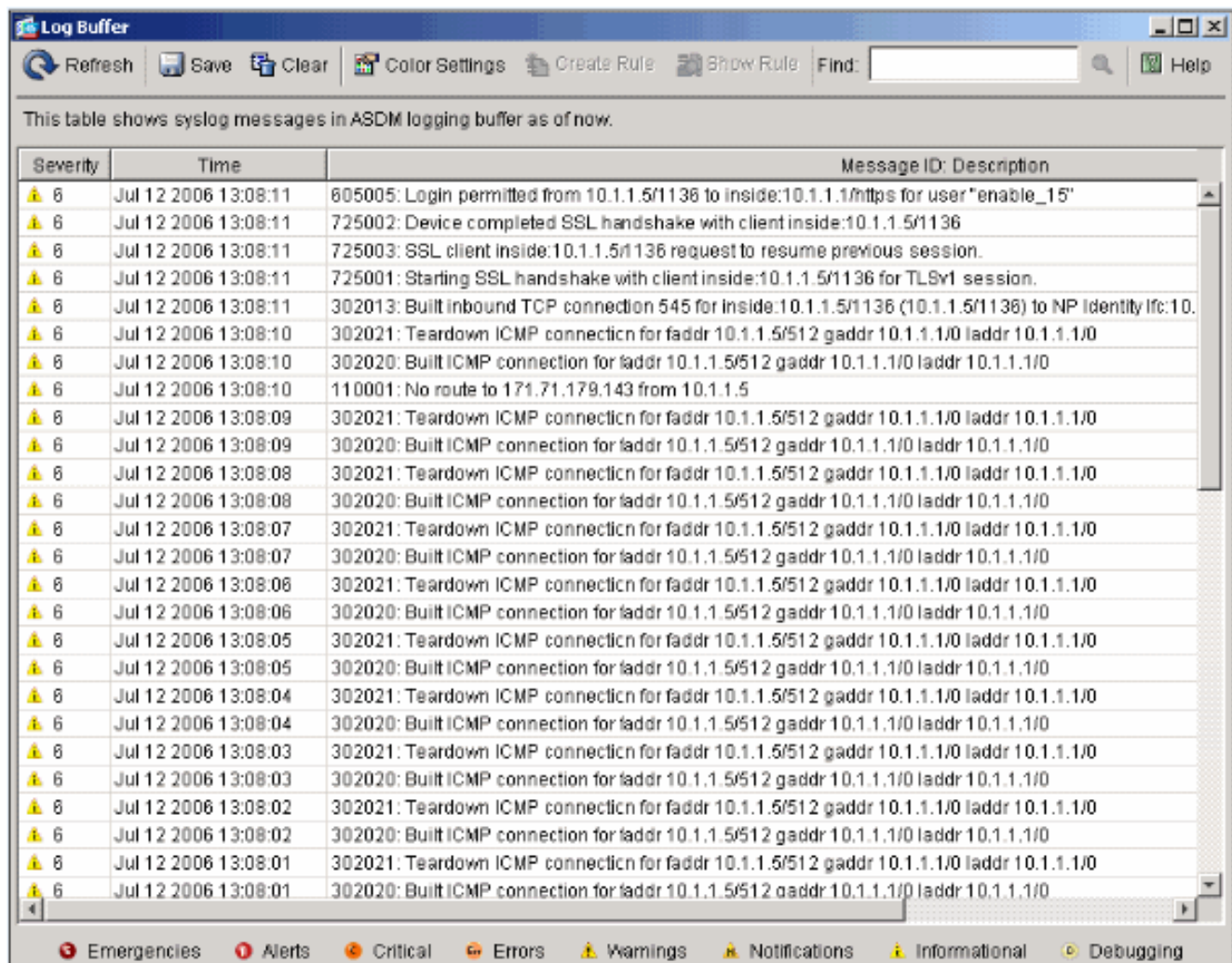
1. Escolha a **configuração > as propriedades > instalação de registro > de registro**, a verificação **permite o registro**, e o clique **aplica-se**.



2. Escolha a **monitoração > registrando > buffer de registro > nível de registro** e escolha o **logging buffer** da lista de drop-down. Clique a **vista**.



3. Está aqui um exemplo do buffer de registro:



Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	805005: Login permitted from 10.1.1.5/1136 to inside:10.1.1./https for user "enable_15"
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

[Incapaz de alcançar por nome Web site](#)

Em determinadas encenações, as redes internas não podem alcançar os Web site do Internet usando o nome (trabalhos com endereço IP de Um ou Mais Servidores Cisco ICM NT) no navegador da Web. Esta edição é comum e ocorre geralmente se o servidor DNS não é definido, especialmente nos casos onde o PIX/ASA é o servidor DHCP. Também, isto pode ocorrer nos casos se o PIX/ASA é incapaz de empurrar o servidor DNS ou se o servidor DNS não é alcançável.

[Informações Relacionadas](#)

- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Cisco Adaptive Security Device Manager](#)
- [Troubleshooting e Alertas do Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)