# ASA 7.x/PIX 6.x e superior: Exemplo de configuração de abrir/bloquear portas

## Contents



## Introduction

Este documento fornece uma configuração de exemplo para abrir ou bloquear as portas para vários tipos de tráfego, como http ou ftp, no Security Appliance.

**Observação:** os termos "abrindo a porta" e "permitindo a porta" têm o mesmo significado. Da mesma forma, "bloquear a porta" e "restringir a porta" também oferecem o mesmo significado.

## Prerequisites

### Requirements

Este documento pressupõe que o PIX/ASA está configurado e funciona corretamente.

### Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que executa a versão 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM) versão 6.3(5)

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Produtos Relacionados

Essa configuração também pode ser usada com o Cisco 500 Series PIX Firewall Appliance com o software versão 6.x e superior.

## Conventions

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

# Configurar

Cada interface deve ter um nível de segurança de 0 (mais baixo) a 100 (mais alto). Por exemplo, você deve atribuir sua rede mais segura, como a rede do host interno, ao nível 100. Embora a rede externa conectada à Internet possa ser de nível 0, outras redes, como DMZs, podem ser posicionadas entre elas. Você pode atribuir várias interfaces ao mesmo nível de segurança.

Por padrão, todas as portas são bloqueadas na interface externa (nível de segurança 0) e todas as portas são abertas na interface interna (nível de segurança 100) do Security Appliance. Dessa forma, todo o tráfego de saída pode passar pelo Security Appliance sem nenhuma configuração, mas o tráfego de entrada pode ser permitido pela configuração da lista de acesso e dos comandos estáticos no Security Appliance.

**Observação:** em geral, todas as portas são bloqueadas da Zona de Segurança Inferior para a Zona de Segurança Superior e todas as portas são abertas da Zona de Segurança Superior para a Zona de Segurança Inferior, desde que a inspeção stateful seja habilitada para tráfego de entrada e de saída.

Esta seção é composta pelas subseções, conforme mostrado:

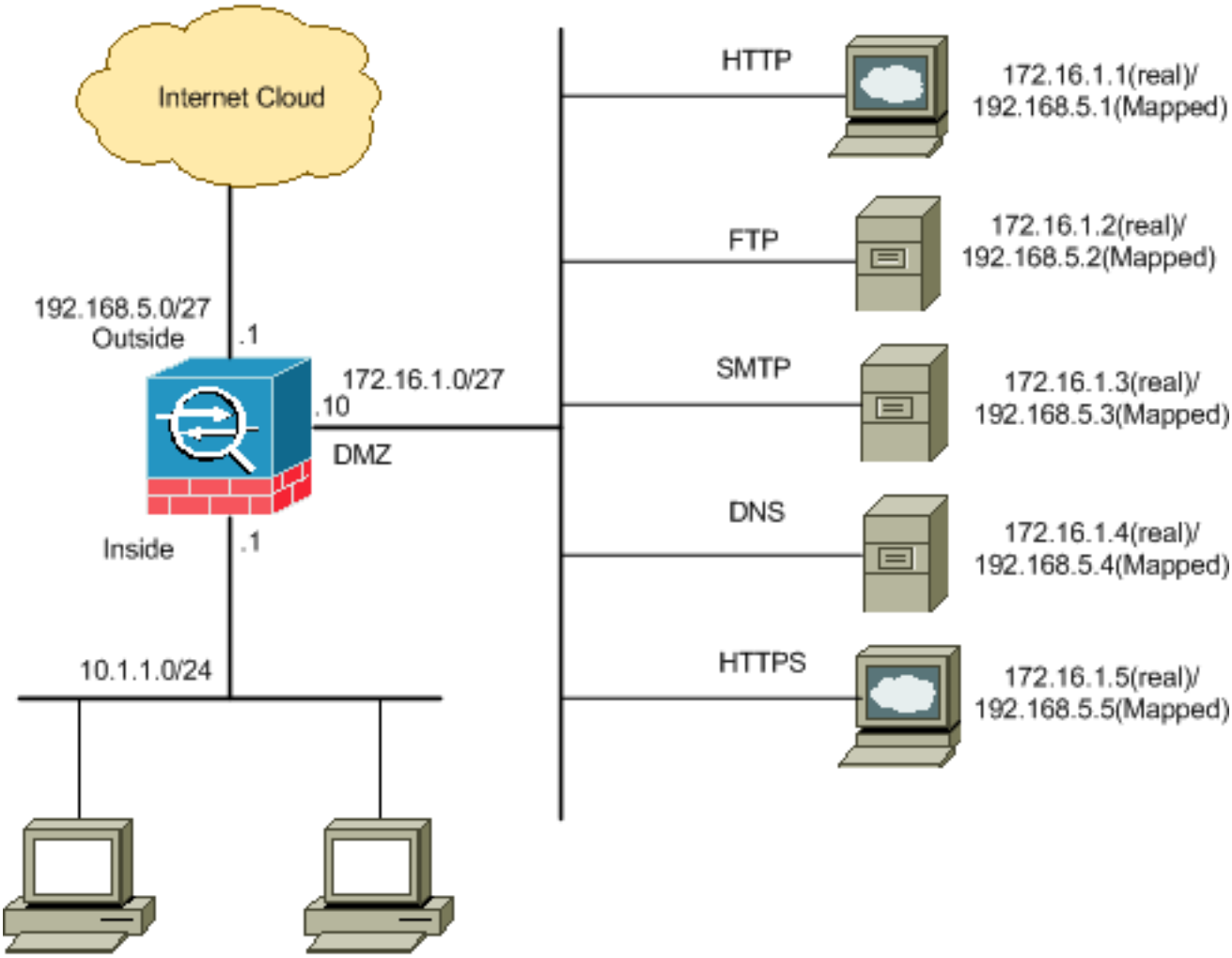
- Diagrama de Rede
- Bloqueando a configuração das portas
- Abrindo a configuração de portas

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.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Bloqueando a configuração das portas

O Security Appliance permite qualquer tráfego de saída, a menos que ele seja explicitamente bloqueado por uma lista de acesso estendida.

Uma lista de acesso é composta por uma ou mais entradas de controle de acesso. Dependendo do tipo de lista de acesso, você pode especificar os endereços origem e destino, o protocolo, as portas (para TCP ou UDP), o tipo ICMP (para ICMP) ou o EtherType.

**Observação:** para protocolos sem conexão, como o ICMP, o Security Appliance estabelece sessões unidirecionais, portanto, você precisa de listas de acesso para permitir o ICMP em ambas as direções (pela aplicação de listas de acesso às interfaces de origem e de destino) ou precisa habilitar o mecanismo de inspeção do ICMP. O mecanismo de inspeção ICMP trata as sessões ICMP como conexões bidirecionais.

Conclua estes passos para bloquear as portas, que geralmente se aplicam ao tráfego originado do interior (zona de segurança mais alta) para o DMZ (zona de segurança mais baixa) ou o DMZ para o exterior.

1. Crie uma lista de controle de acesso de forma que você bloqueie o tráfego de porta especificado.

   ```
   access-list
   ```

2. Em seguida, vincule a lista de acesso ao comando **access-group** para estar ativa.

```
access-group
```

**Examples:**

1. **Bloquear o tráfego da porta HTTP:** Para bloquear o acesso da rede interna 10.1.1.0 ao http (servidor web) com o IP 172.16.1.1 colocado na rede DMZ, crie uma ACL como mostrado:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

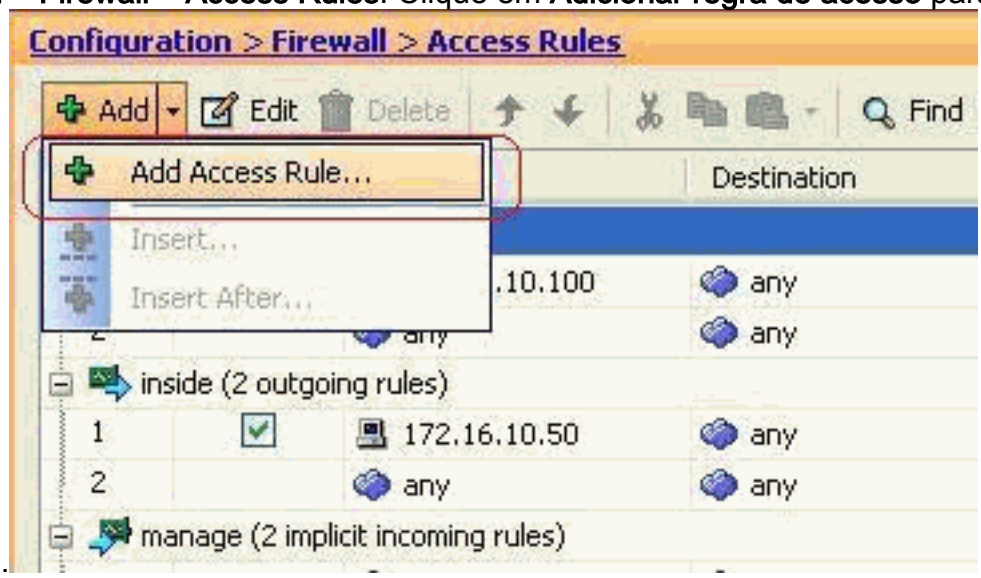
   **Observação:** use **no** seguido pelos comandos da lista de acesso para remover o bloqueio de porta.
2. **Bloquear o tráfego da porta FTP:** Para bloquear o acesso da rede interna 10.1.1.0 ao FTP (servidor de arquivos) com o IP 172.16.1.2 colocado na rede DMZ, crie uma ACL como mostrado:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

**Observação:** consulte portas IANA para saber mais sobre atribuições de porta.

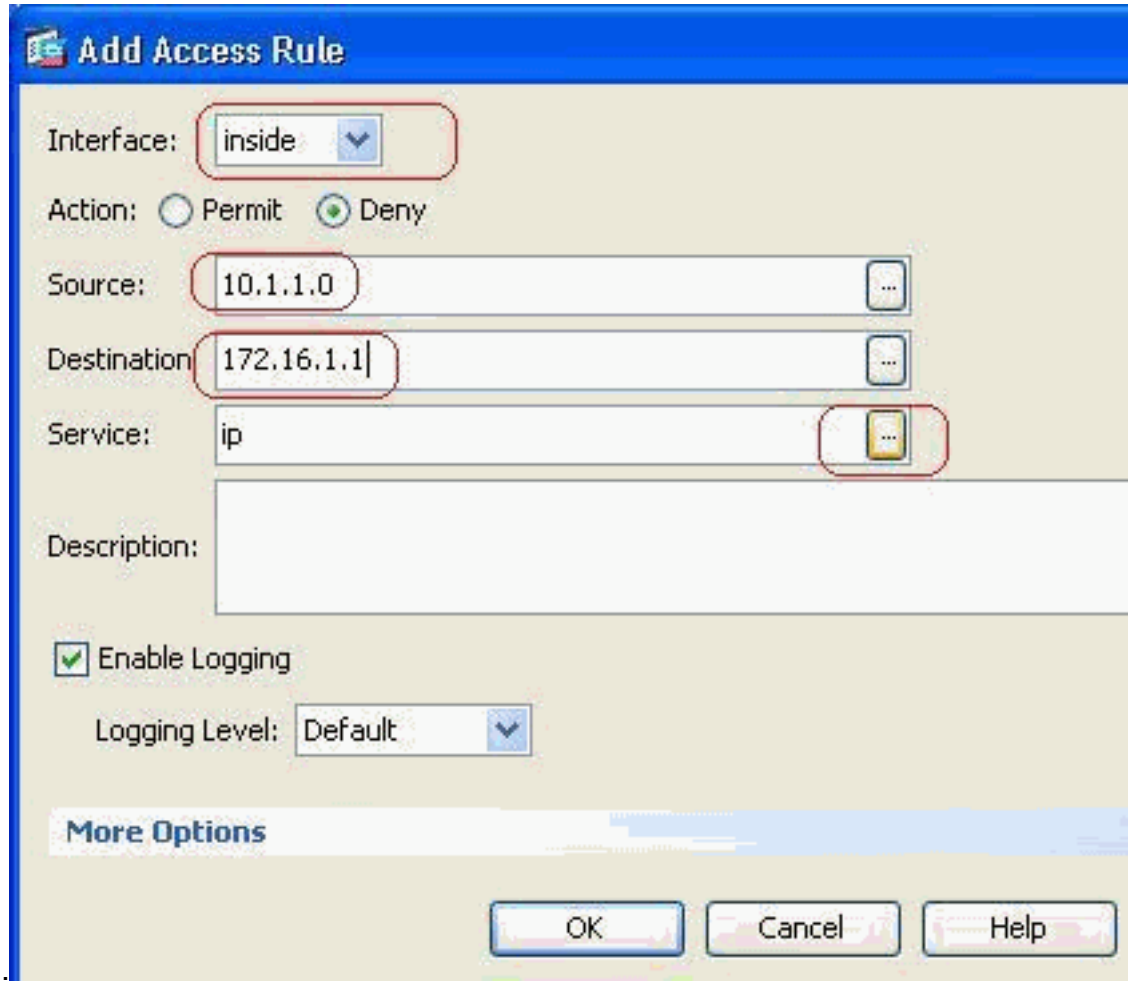
A configuração passo a passo para executar isso através do ASDM é mostrada nesta seção.

1. Vá para **Configuration > Firewall > Access Rules**. Clique em **Adicionar regra de acesso** para criar a lista de acesso.

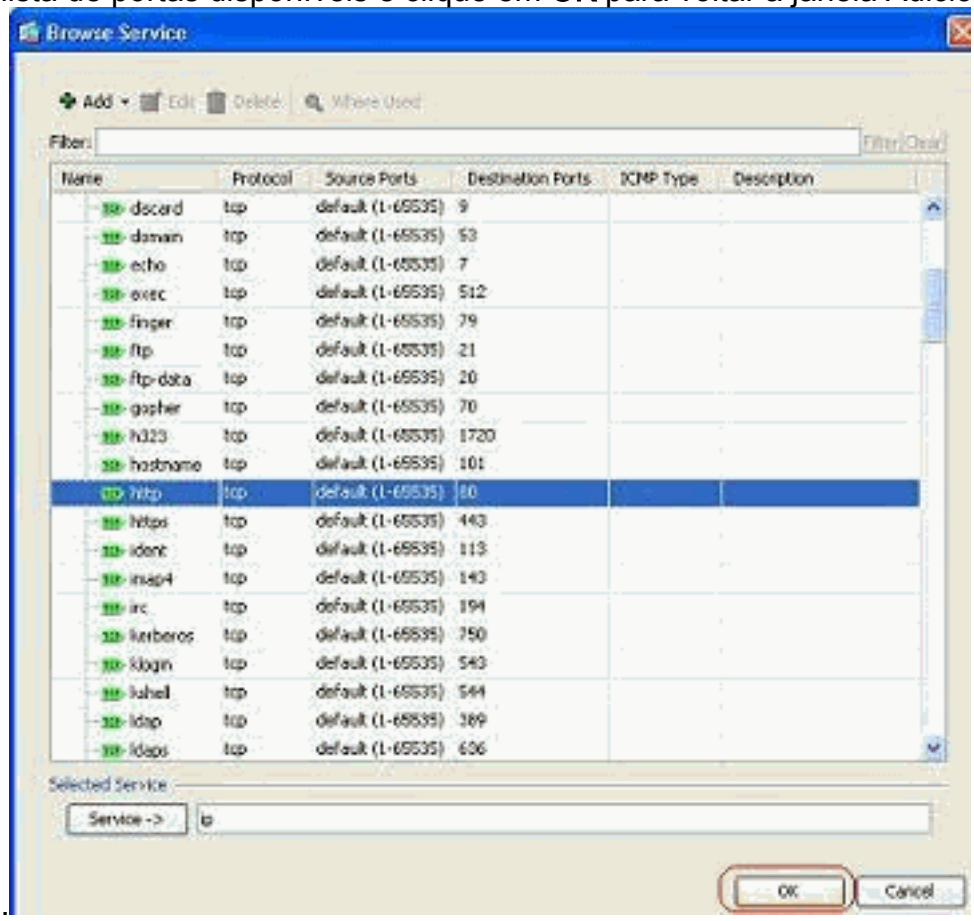



2. Defina a origem e o destino e a ação da regra de acesso junto com a interface à qual essa regra de acesso será associada. Selecione os detalhes para escolher a porta específica a ser

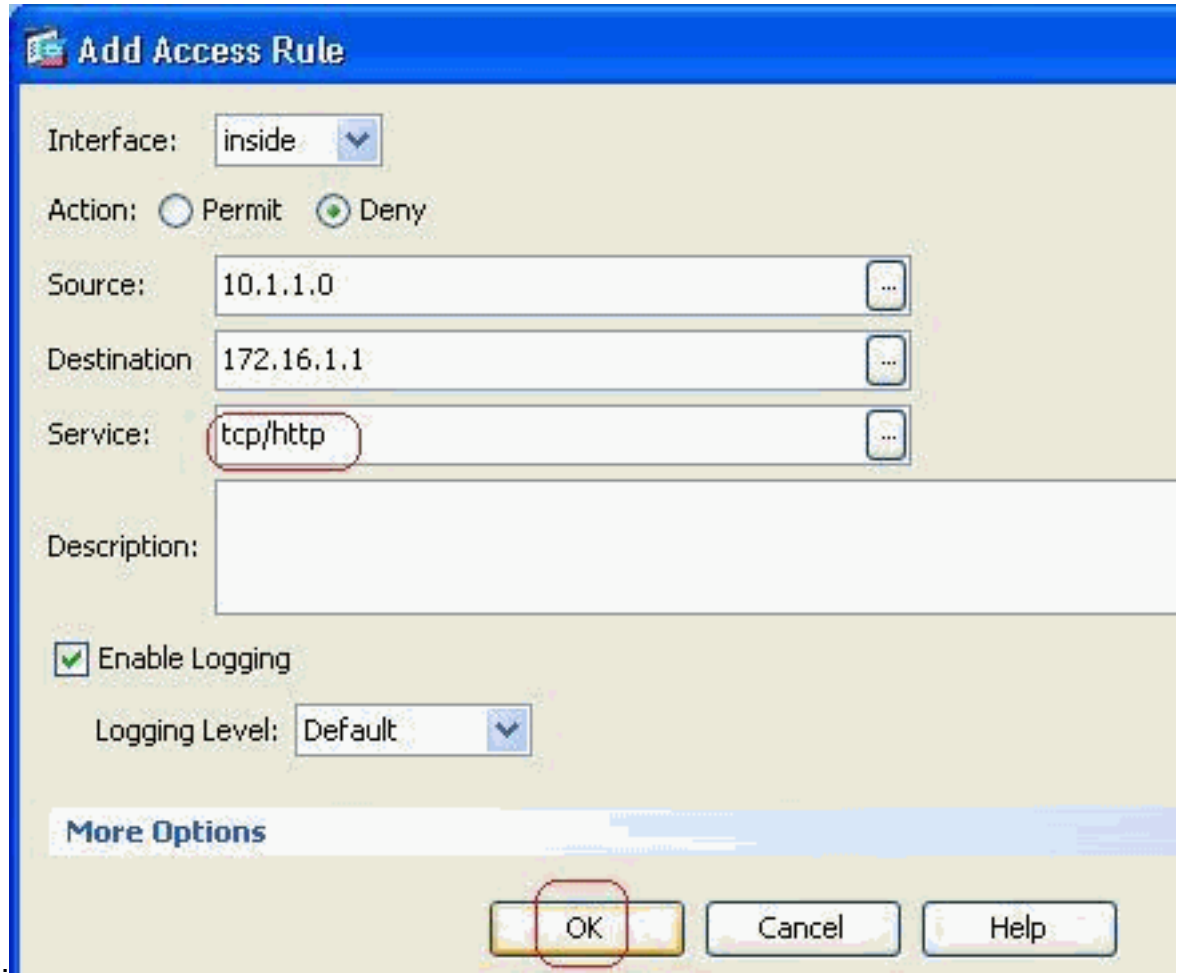
bloqueada.




3. Escolha **http** na lista de portas disponíveis e clique em **OK** para voltar à janela Adicionar regra de acesso.

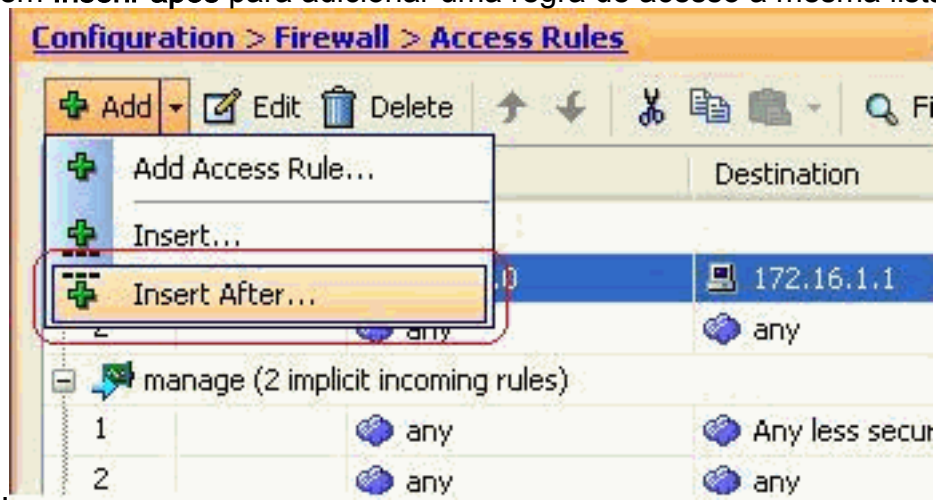



4. Clique em **OK** para concluir a configuração da regra de



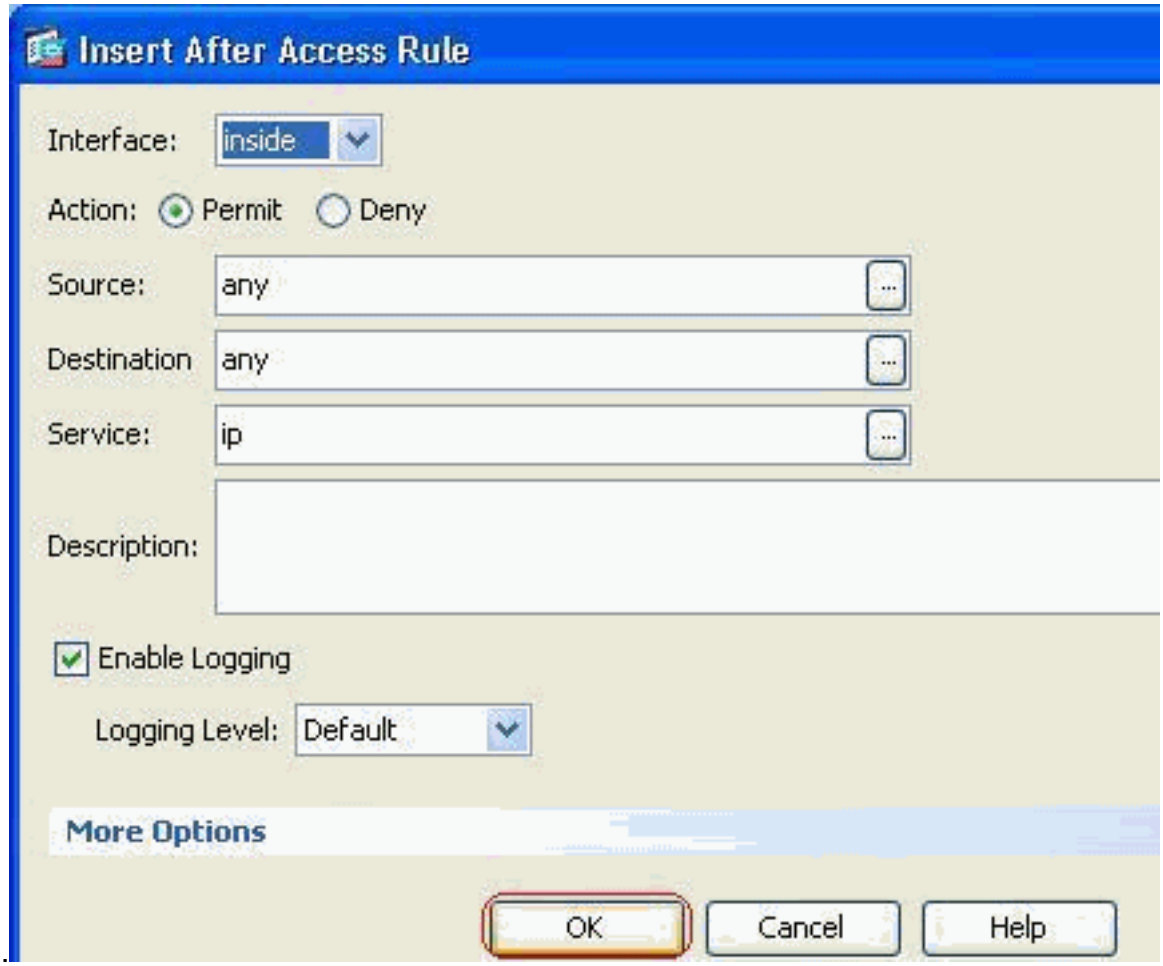

acesso.

5. Clique em **Inserir após** para adicionar uma regra de acesso à mesma lista de



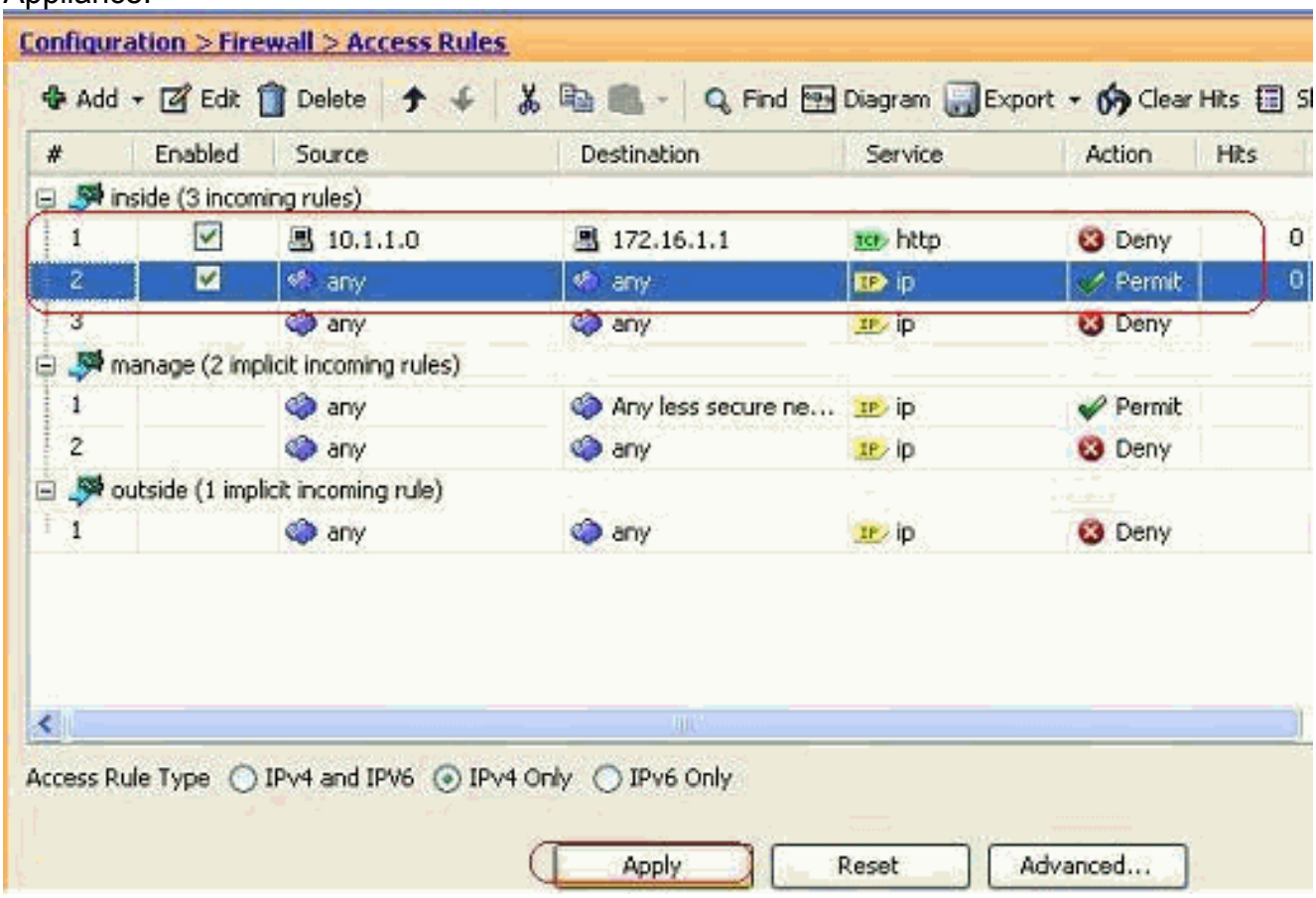

acesso.

6. Permita que o tráfego entre "any" e "any" para evitar a "negação implícita". Em seguida, clique em **OK** para concluir a adição desta regra de




acesso.

7. A lista de acesso configurada pode ser vista na guia Regras de acesso. Clique em **Apply** para enviar esta configuração para o Security Appliance.



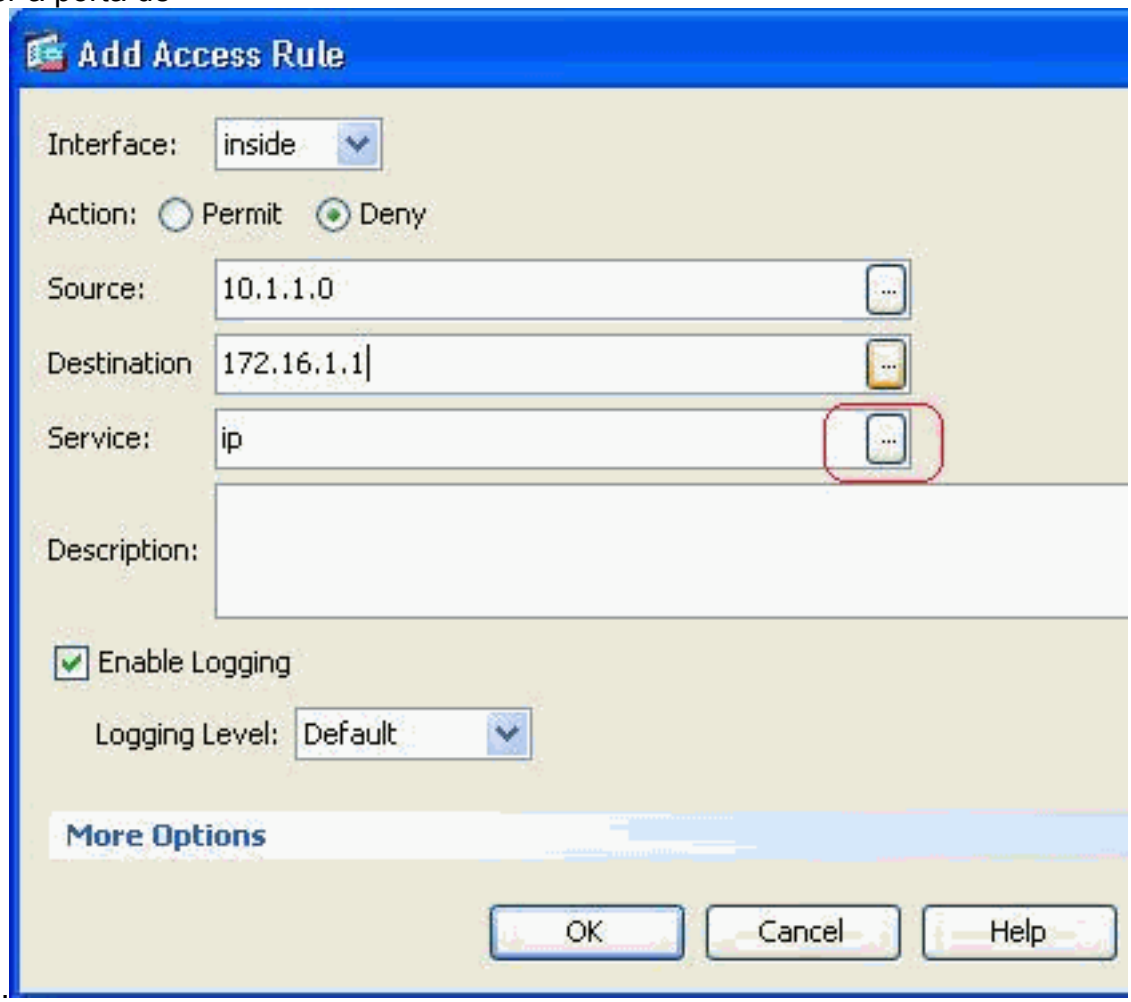

A configuração enviada do ASDM resulta nesse conjunto de comandos na CLI (Command

Line Interface, interface de linha de comando) do ASA.

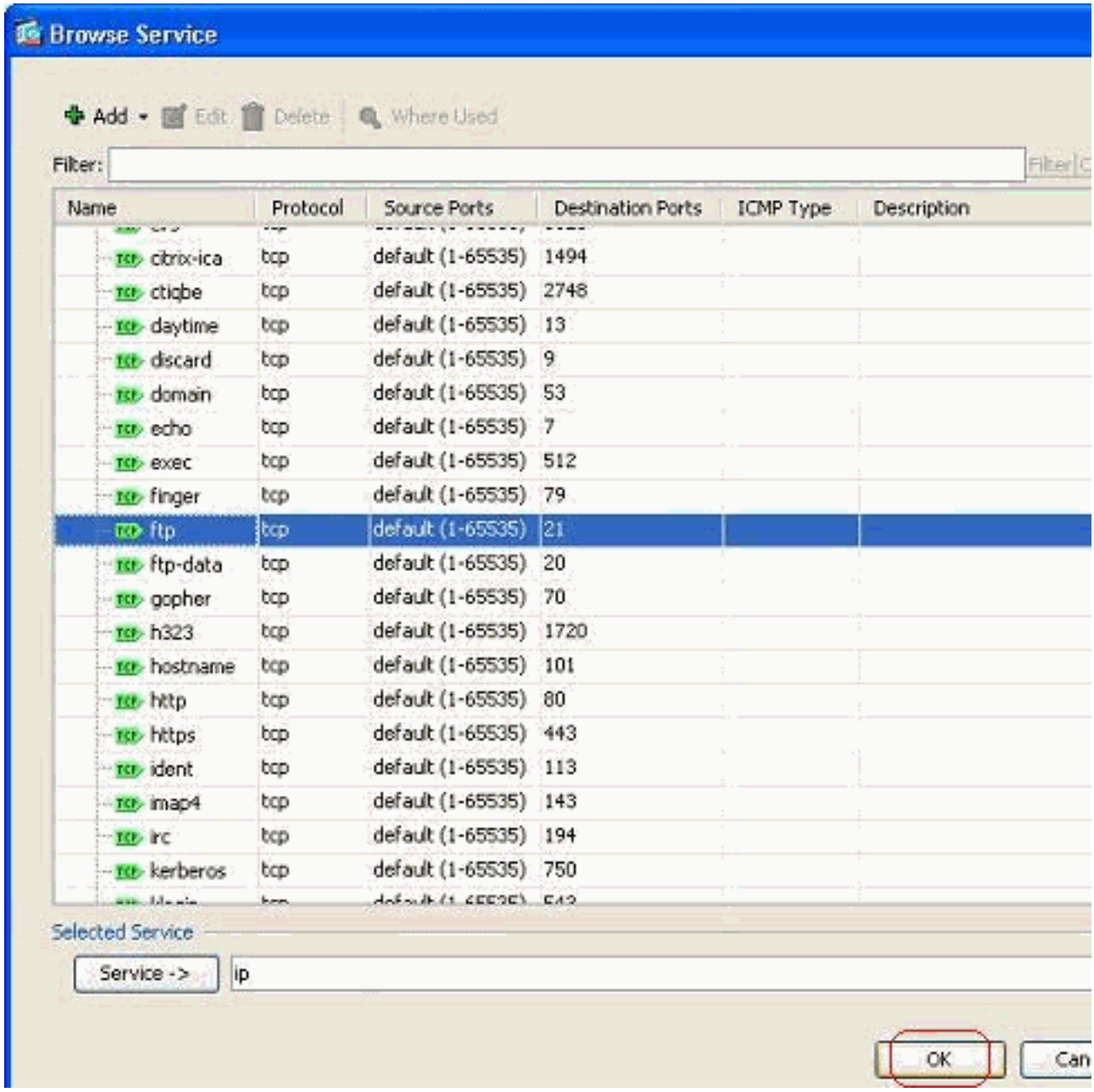
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Por meio dessas etapas, o exemplo 1 foi executado por meio do ASDM para impedir que a rede 10.1.1.0 acesse o servidor web, 172.16.1.1. O exemplo 2 também pode ser obtido da mesma forma para bloquear o acesso de toda a rede 10.1.1.0 ao servidor FTP, 172.16.1.2. A única diferença estará no ponto de escolher a porta.**Observação:** esta configuração de regra de acesso para o exemplo 2 é presumida como uma nova configuração.

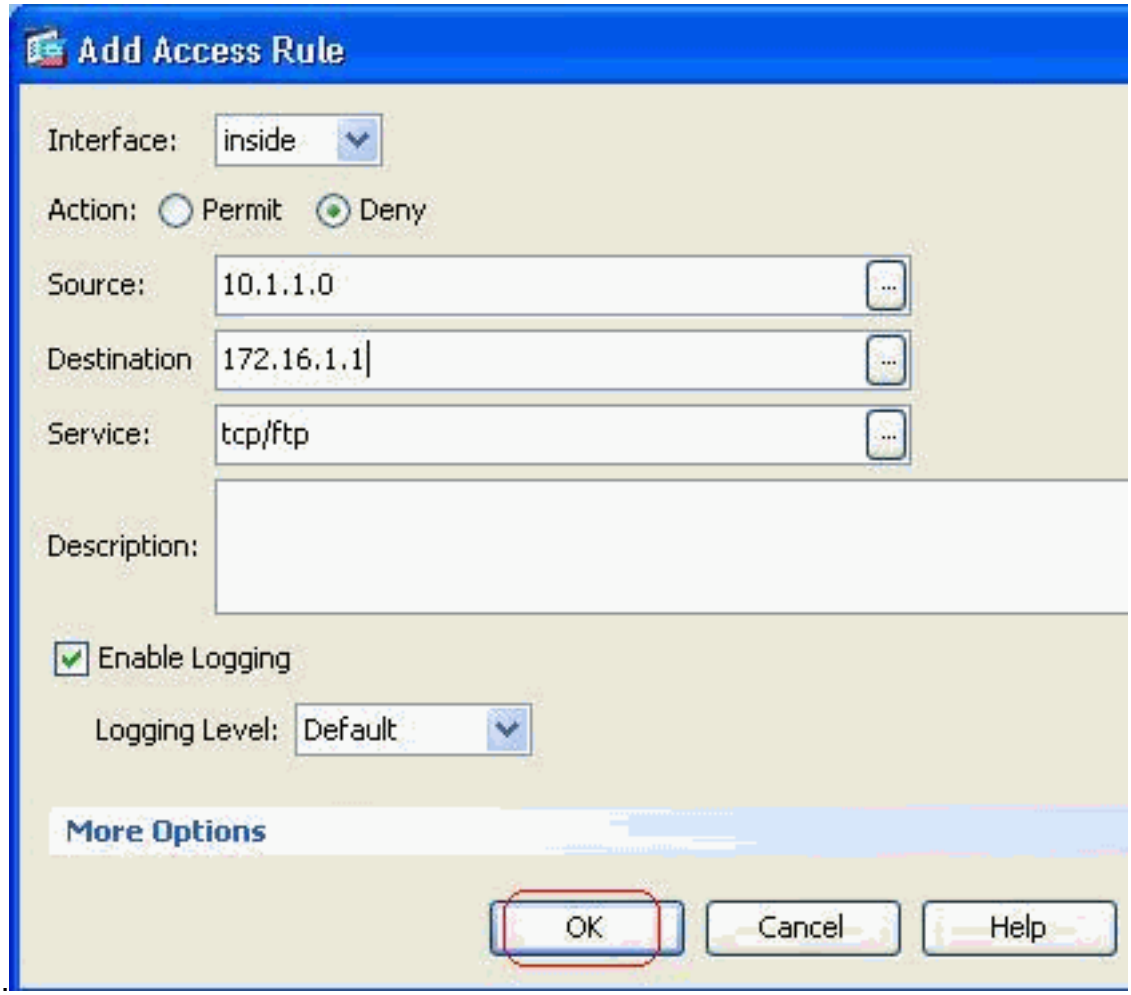
8. Defina a regra de acesso para bloquear o tráfego FTP e clique na guia **Detalhes** para escolher a porta de destino.




9. Escolha a porta **ftp** e clique em **OK** para voltar à janela Adicionar regra de acesso.

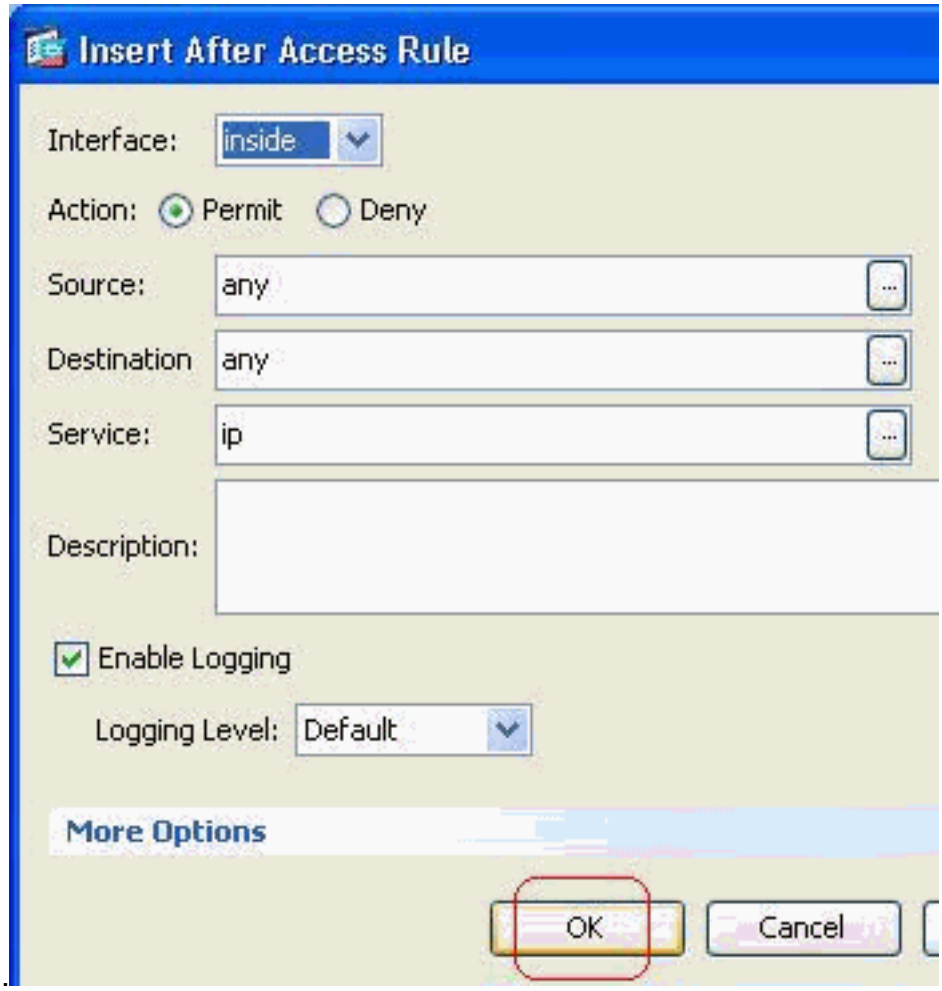



10. Clique em **OK** para concluir a configuração da regra de



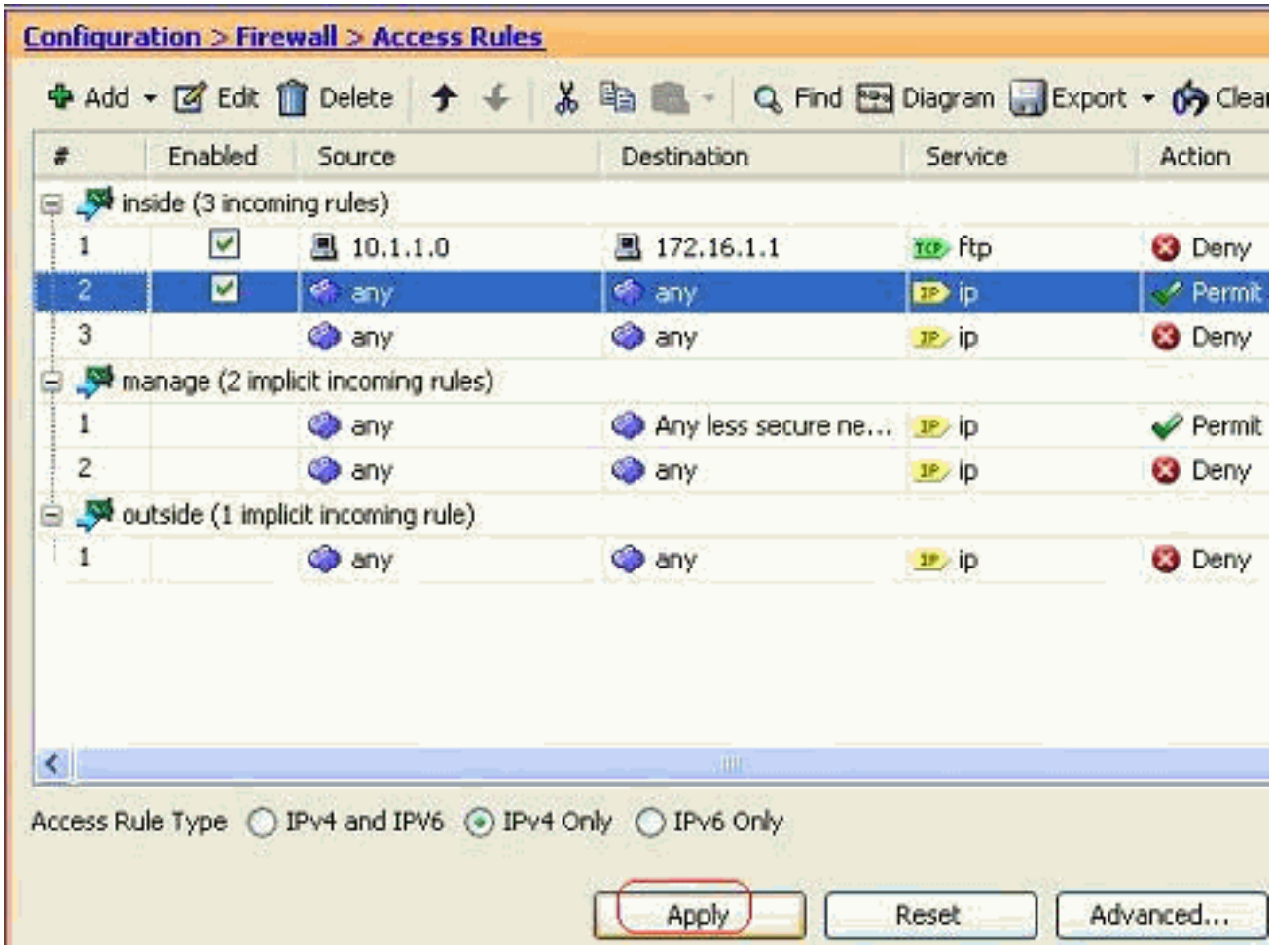

acesso.

11. Adicione outra regra de acesso para permitir qualquer outro tráfego. Caso contrário, a regra Negar implícito bloqueará todo o tráfego nessa




interface.

12. A configuração completa da lista de acesso é semelhante a esta na guia Regras de acesso.



13. Clique em **Apply** para enviar a configuração para o ASA. A configuração de CLI equivalente é semelhante a esta:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

## Abrindo a configuração de portas

O Security Appliance não permite nenhum tráfego de entrada, a menos que seja explicitamente permitido por uma lista de acesso estendida.

Se quiser permitir que um host externo acesse um host interno, você pode aplicar uma lista de acesso de entrada na interface externa. Você precisa especificar o endereço traduzido do host interno na lista de acesso porque o endereço traduzido é o endereço que pode ser usado na rede externa. Conclua estes passos para abrir as portas da zona de segurança inferior para a zona de segurança superior. Por exemplo, permita o tráfego de fora (zona de segurança inferior) para a interface interna (zona de segurança superior) ou DMZ para a interface interna.

1. O NAT estático cria uma tradução fixa de um endereço real para um endereço mapeado. Esse endereço mapeado é um endereço que hospeda na Internet e pode ser usado para acessar o servidor de aplicativos na DMZ sem a necessidade de saber o endereço real do servidor.

   ```
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
      access-list access_list_name | interface}
   ```

   Consulte a seção NAT estático da referência de comando para PIX/ASA para saber mais.
2. Crie uma ACL para permitir o tráfego de porta específico.

   ```
   access-list
   ```

3. Vincule a lista de acesso ao comando **access-group** para estar ativa.

   ```
   access-group
   ```

**Examples:**

1. **Abra o tráfego da porta SMTP:** Abra a porta **tcp 25** para permitir que os hosts de fora (Internet) acessem o servidor de e-mail colocado na rede DMZ.O comando **Static** mapeia o endereço externo 192.168.5.3 para o endereço DMZ real 172.16.1.3.

   ```
   ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
    netmask 255.255.255.255
   ciscoasa(config)#access-list 100 extended permit tcp
    any host 192.168.5.3 eq 25
   ciscoasa(config)#access-group 100 in interface outside
   ```

2. **Abra o tráfego da porta HTTPS:** Abra a porta **tcp 443** para permitir que os hosts externos (Internet) acessem o servidor web (seguro) colocado na rede DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **Permitir o tráfego DNS:** Abra a porta **udp 53** para permitir que os hosts externos (Internet) acessem o servidor DNS (seguro) colocado na rede DMZ.

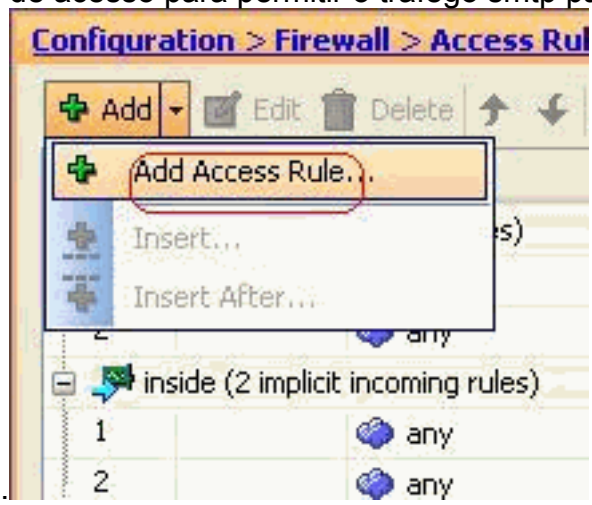
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

**Observação:** consulte portas IANA para saber mais sobre atribuições de porta.

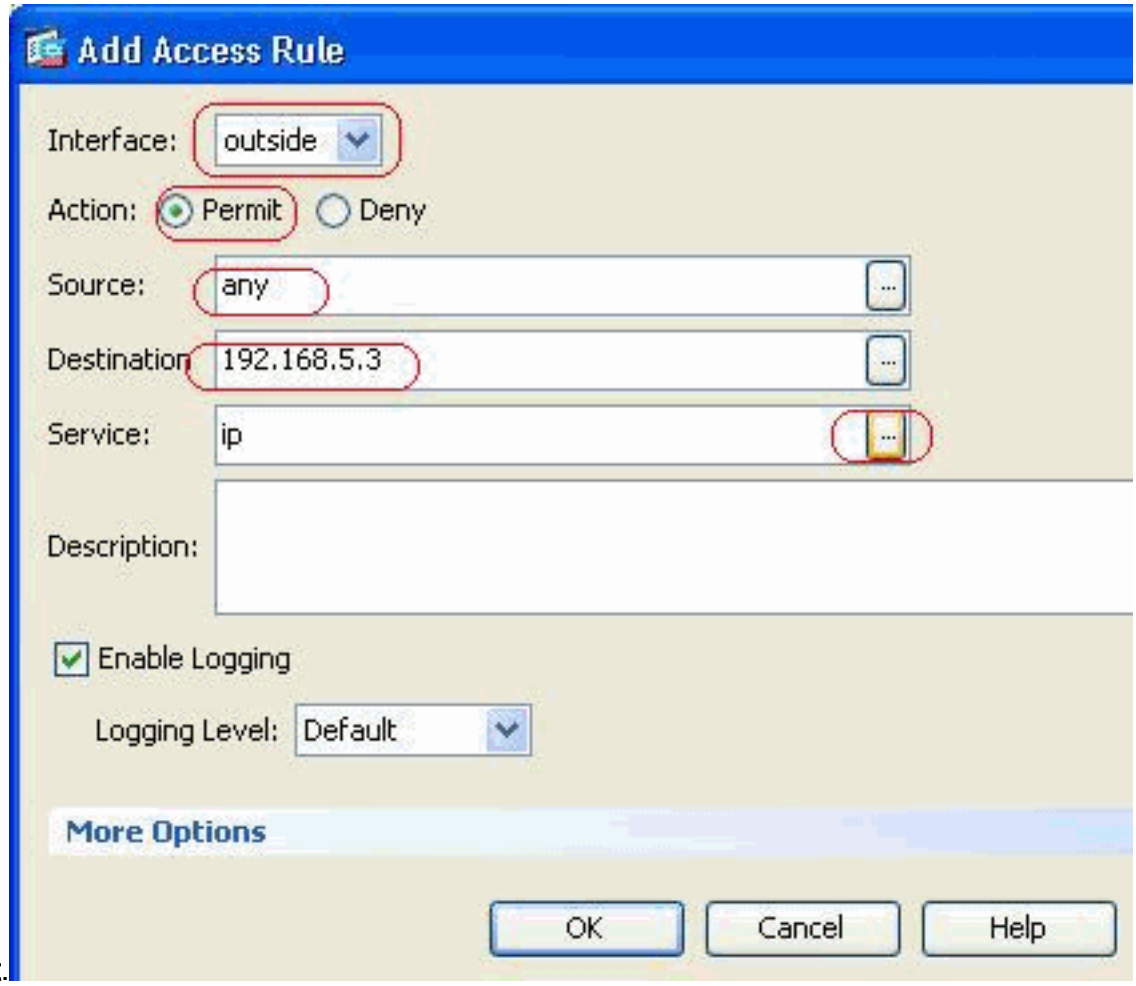
## Configuração por meio do ASDM

Nesta seção, uma abordagem passo a passo para executar as tarefas acima mencionadas através do ASDM é mostrada.

1. Crie a regra de acesso para permitir o tráfego smtp para o servidor 192.168.5.3.

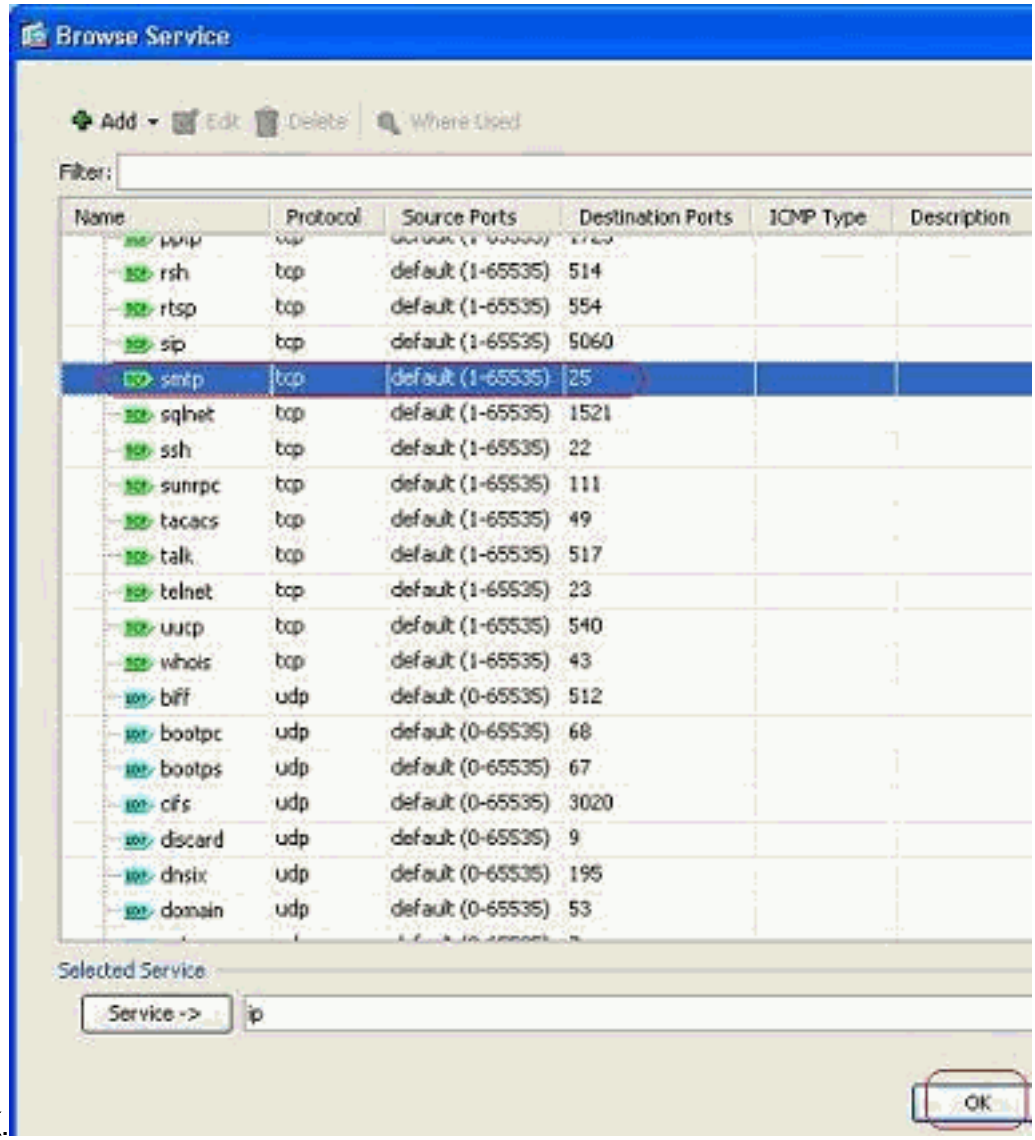



2. Defina a origem e o destino da regra de acesso e a interface com a qual essa regra se vincula. Além disso, defina a Ação como



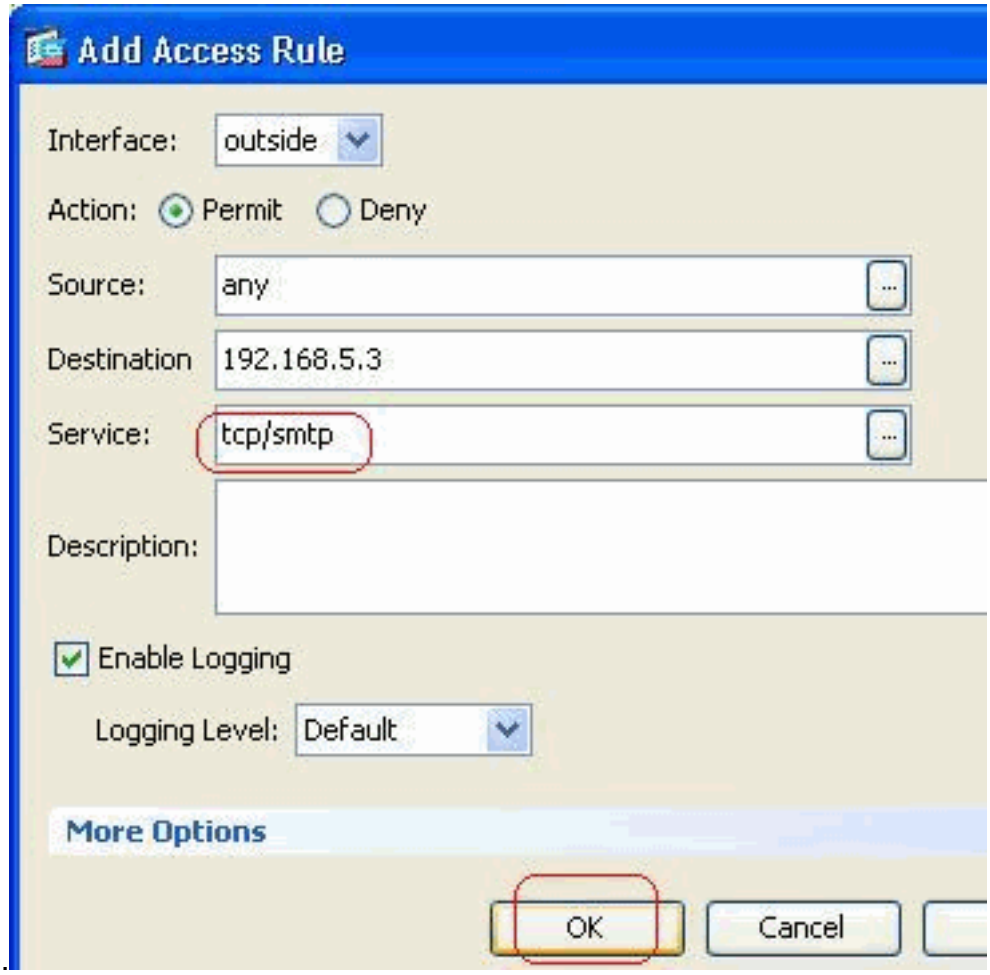

**Permit**.

3. Escolha **SMTP** como a porta e clique em



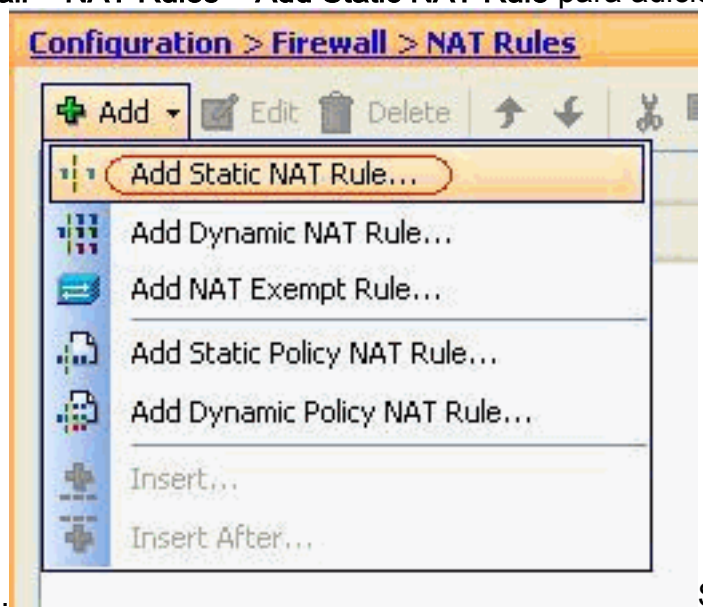

OK.

4. Clique em **OK** para concluir a configuração da regra de

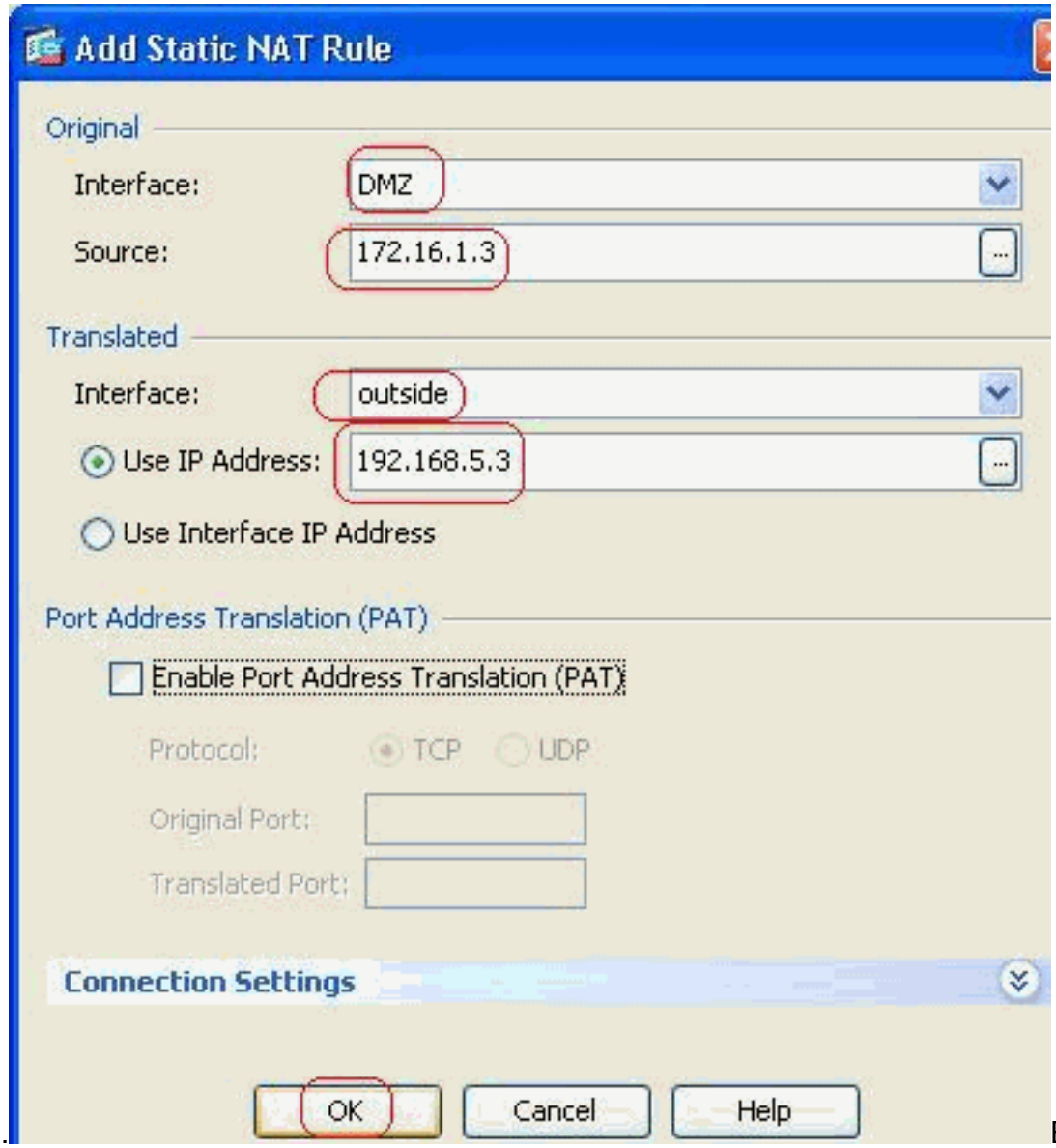



acesso.

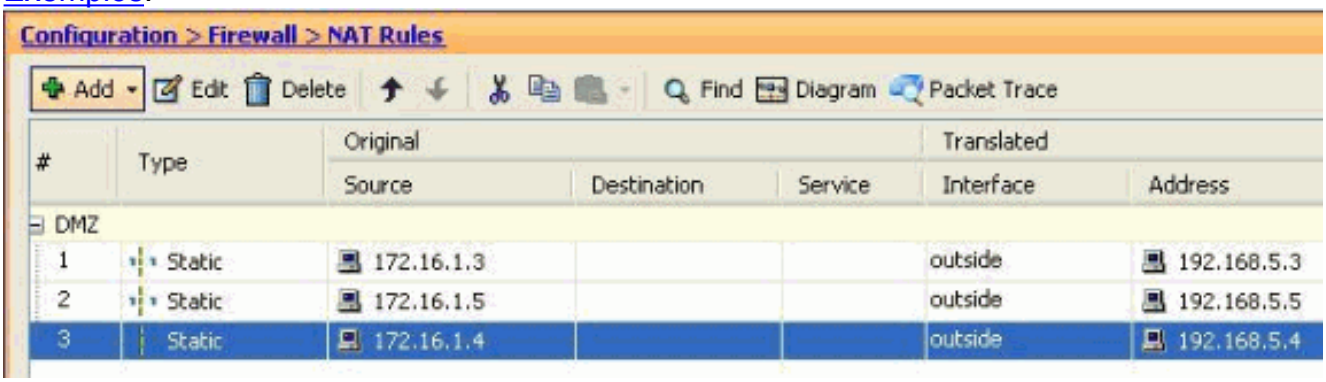
5. Configure o NAT estático para converter 172.16.1.3 para 192.168.5.3Vá para **Configuration > Firewall > NAT Rules > Add Static NAT Rule** para adicionar uma entrada de NAT



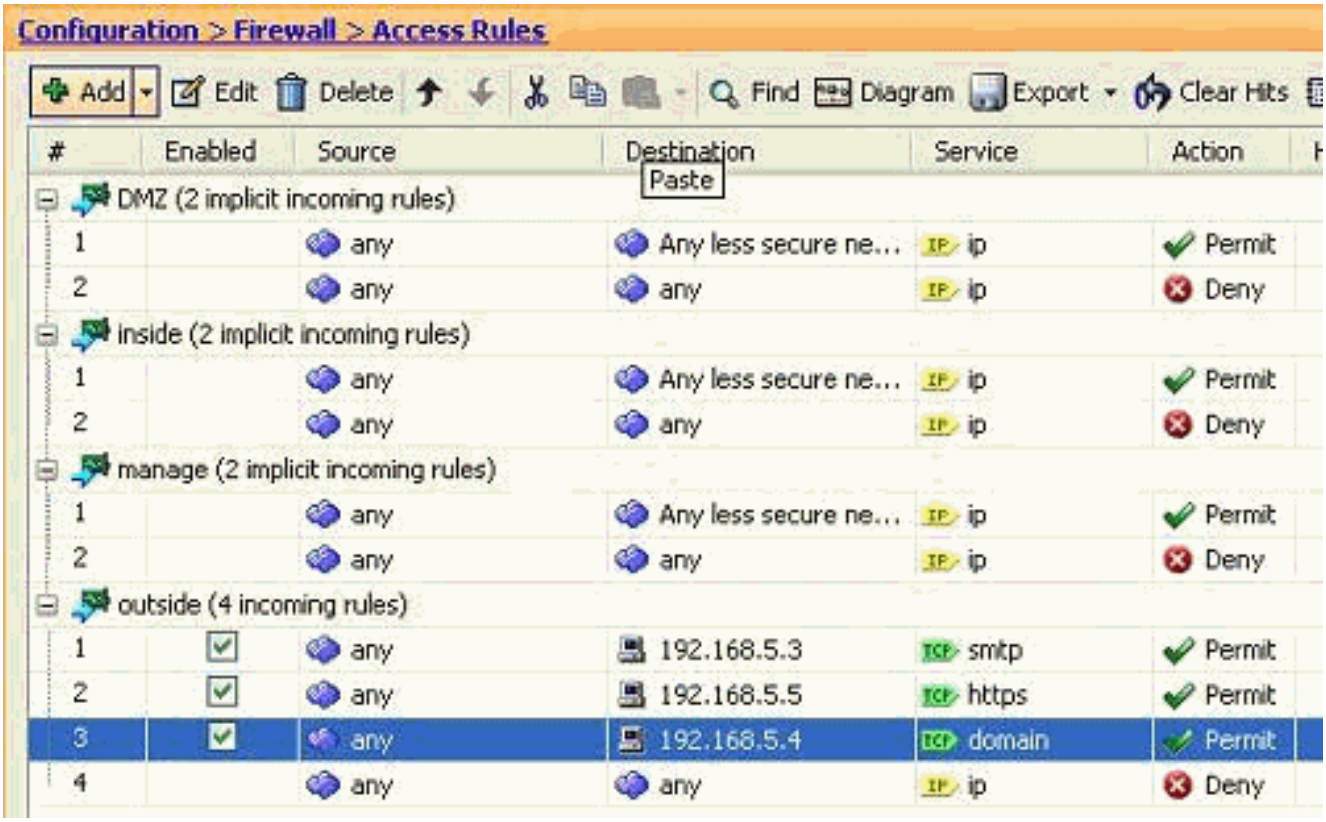

estático. Selecione a origem original e o endereço IP traduzido juntamente com suas interfaces associadas e clique em **OK** para concluir a configuração da regra de NAT




estático. Esta imagem descreve as três regras estáticas listadas na seção Exemplos:




Esta imagem descreve as três regras de acesso listadas na seção Exemplos:




## Verificar

Você pode verificar com determinados comandos **show**, como mostrado:

- **show xlate —** exibe informações de conversão atuais
- **show access-list** — exibir contadores de ocorrências para políticas de acesso
- **show logging** — exibe os logs no buffer.

A Output Interpreter Tool ( somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

## Troubleshoot

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

## Informações Relacionadas

- PIX/ASA 7.x: Ativar/Desativar Comunicação Entre Interfaces
- PIX 7.0 e Adaptive Security Appliance Port Redirection(Forwarding) com comandos nat, global, estático, conduit e access-list
- Usando comandos nat, global, estático, conduit e access-list e redirecionamento de porta (encaminhamento) no PIX
- PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP
- PIX/ASA 7.x: Exemplo de Configuração de Serviços de Habilitação de VoIP (SIP, MGCP, H323, SCCP)
- PIX/ASA 7.x: Exemplo de Configuração de Acesso ao Servidor de Correio no DMZ

- Suporte Técnico e Documentação - Cisco Systems