ASA 7.x/PIX 6.x e acima: Aberto/bloco o exemplo de configuração das portas

Índice

Introdução

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.

Nota: Os termos “que abrem a porta” e “que permitem a porta” entregam o mesmo significado. Similarmente, “obstruir a porta” e “restringir a porta” igualmente entregam o mesmo significado.

Pré-requisitos

Requisitos

Este documento supõe que o PIX/ASA está configurado e trabalha corretamente.

Componentes Utilizados

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

- A ferramenta de segurança adaptável do Cisco 5500 Series (ASA) essa executa a versão 8.2(1)
- Versão 6.3(5) do Cisco Adaptive Security Device Manager (ASDM)

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 o dispositivo do PIX Firewall do Cisco 500 Series com versão de software 6.x e acima.

Convenções

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

Configurar

Cada relação deve ter um nível de segurança de 0 (mais baixo) a 100 (o mais altamente). Por exemplo, você deve atribuir sua rede mais segura, tal como a rede do host interno, ao nível 100. Quando a rede externa que está conectada ao Internet puder ser o nível 0, outras redes, tais como DMZ, podem ser posicionadas in-between. Você pode atribuir interfaces múltiplas ao mesmo nível de segurança.

Àrevelia, todas as portas são obstruídas na interface externa (nível de segurança 0), e todas as portas estão abertas na interface interna (nível de segurança 100) da ferramenta de segurança. Desta maneira, todo o tráfego de saída pode passar através da ferramenta de segurança sem nenhuma configuração, mas o tráfego de entrada pode ser permitido pela configuração da lista de acessos e dos comandos static na ferramenta de segurança.

Nota: Geralmente, todas as portas são obstruídas da zona de Segurança mais baixa à zona de segurança mais elevada, e todas as portas estão abertas da zona de segurança mais elevada à zona de Segurança mais baixa que fornece que a inspeção stateful está permitida para ambos tráfego de entrada e de saída.

Esta seção consiste nas subseções como mostrado:

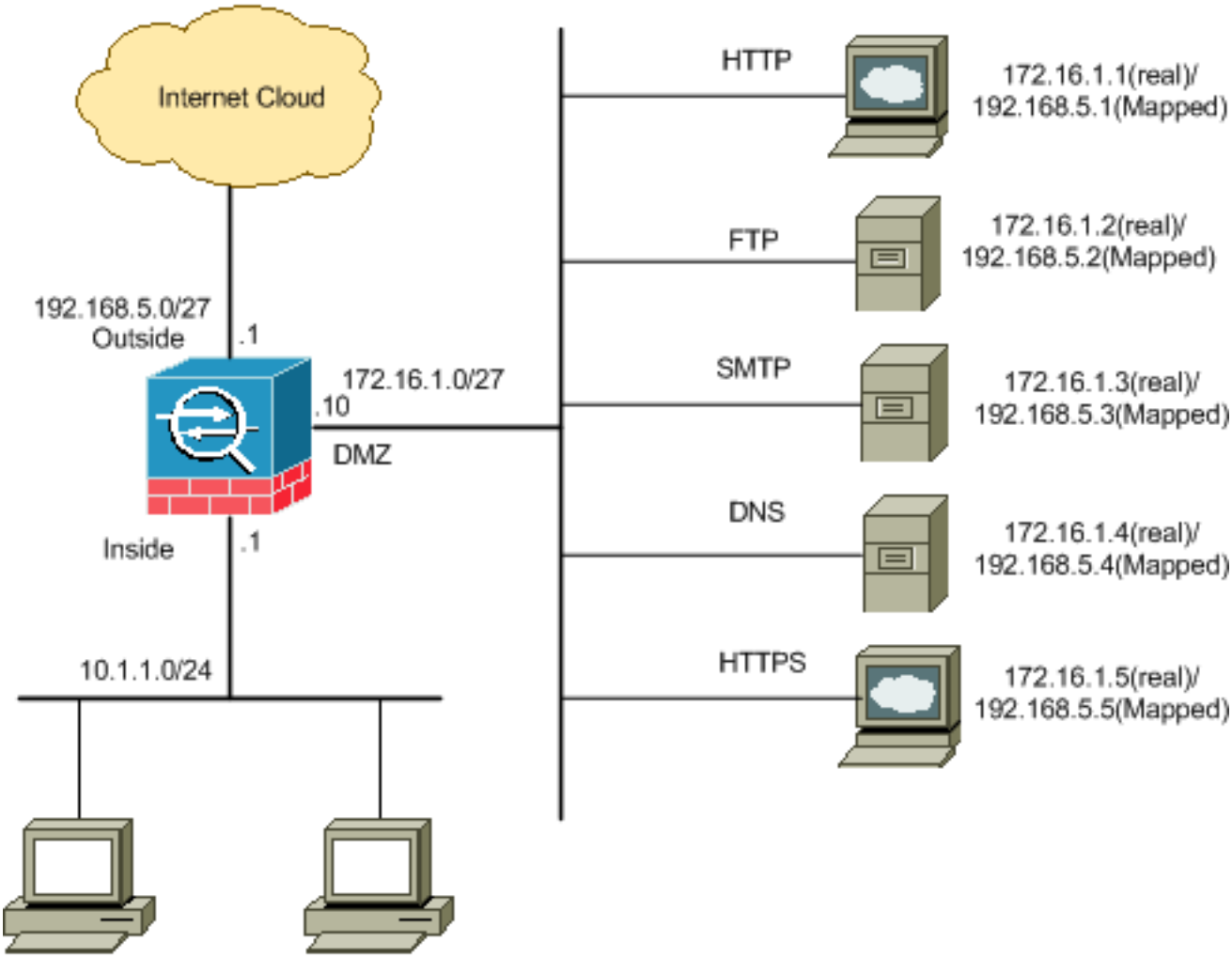
- Diagrama de Rede
- Obstruindo a configuração das portas
- Abrindo a configuração das portas

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:



Obstruindo a configuração das portas

A ferramenta de segurança permite todo o tráfego de saída a menos que for obstruída explicitamente por uma lista de acesso extendida.

Uma lista de acessos é composta de umas ou várias entradas de controle de acesso. Dependente em cima do tipo da lista de acessos, você pode especificar os endereços de rementente e destinatário, o protocolo, as portas (para o TCP ou o UDP), o tipo ICMP (para o ICMP), ou o Ethertype.

Nota: Para protocolos sem conexão, tais como o ICMP, a ferramenta de segurança estabelece sessões unidirecionais, assim que você ou precisa Listas de acesso de permitir o ICMP nos ambos sentidos (pelo aplicativo das Listas de acesso à fonte e às interfaces de destino), ou você precisa de permitir o motor da inspeção de ICMP. O motor da inspeção de ICMP trata sessões ICMP como conexões bidirecional.

Termine estas etapas a fim obstruir as portas, que se aplicam geralmente para traficar aquela originam do interior (zona de segurança mais elevada) ao DMZ (mais baixa zona de Segurança) ou ao DMZ à parte externa.

1. Crie um Access Control List de tal maneira que você obstrui o tráfego da porta especificada.
   `access-list <name> extended deny <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any`
2. Ligue então a lista de acesso com o **comando access-group** a fim ser ativo.
   `access-group <access list name> in interface <interface name>`

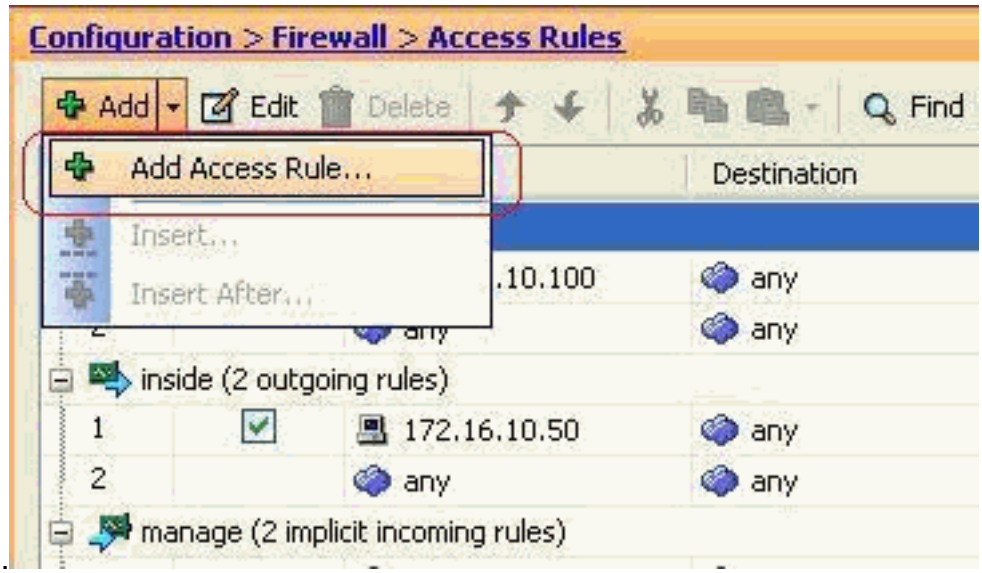
Exemplos:

1. **Obstrua o tráfego da porta de HTTP:** A fim obstruir a rede interna 10.1.1.0 do acesso ao HTTP (servidor de Web) com IP 172.16.1.1 colocado na rede do DMZ, crie um 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` **Nota:** Use o **nenhum** seguido pelos comandos de lista de acesso a fim remover a obstrução da porta.
2. **Obstrua o tráfego da porta FTP:** A fim obstruir a rede interna 10.1.1.0 do acesso ao FTP (servidor de arquivo) com IP 172.16.1.2 colocado na rede do DMZ, crie um 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`

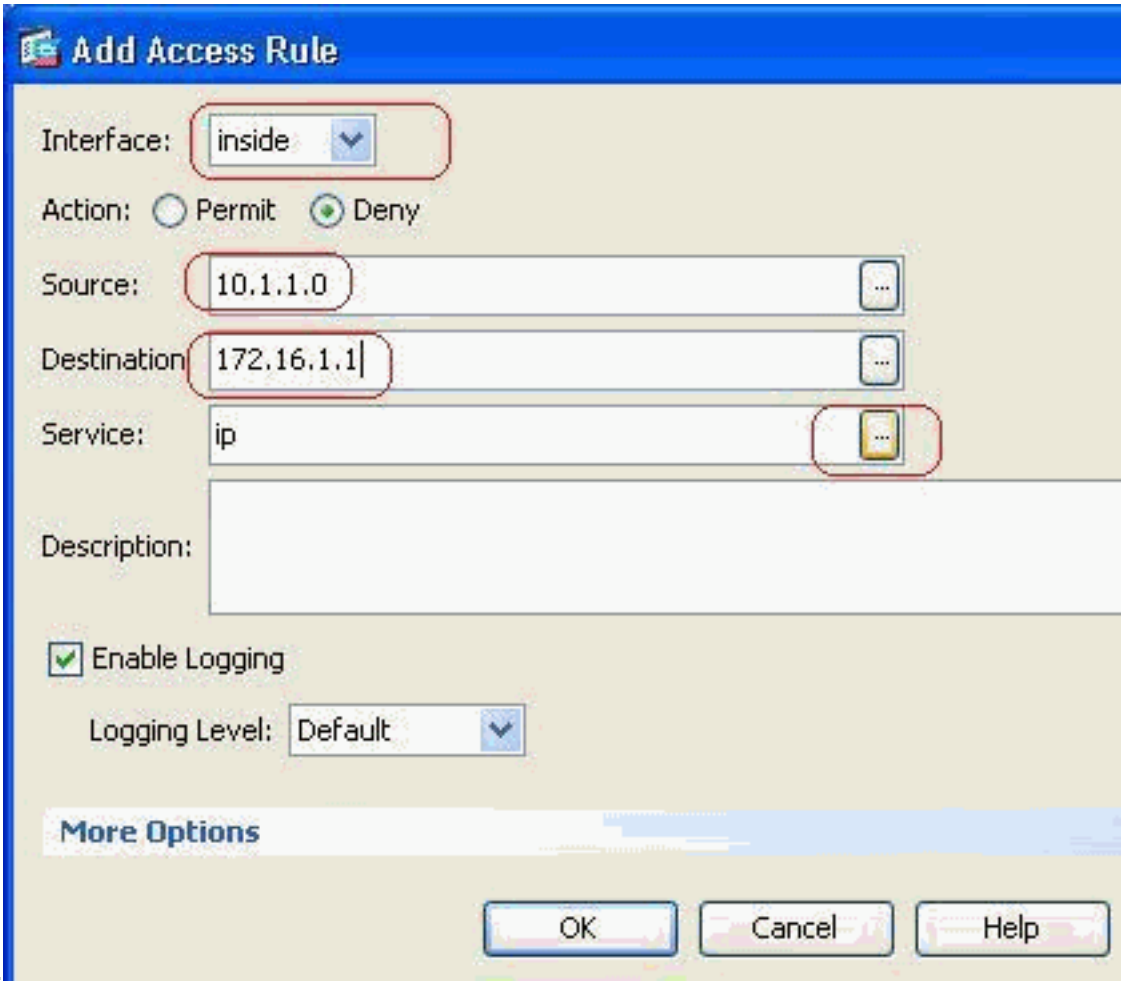
Nota: Refira portas IANA a fim aprender mais informação sobre atribuições de porta.

A configuração passo a passo para executar isto com o ASDM é mostrada nesta seção.

1. Vá às **regras da configuração > do Firewall > do acesso**. O clique **adiciona a regra do acesso** para criar a lista de acesso.

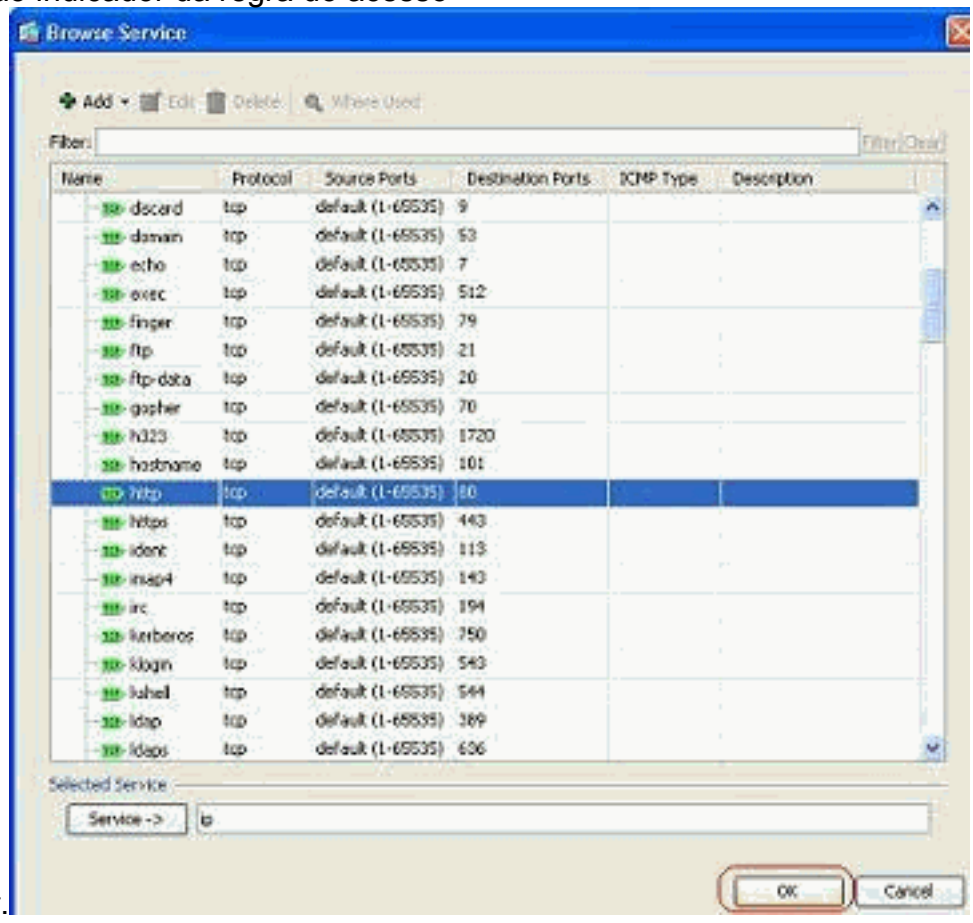


2. Defina a fonte e o destino e a ação da acesso-regra junto com a relação que esta regra do acesso será associada. Selecione os detalhes escolher a porta específica



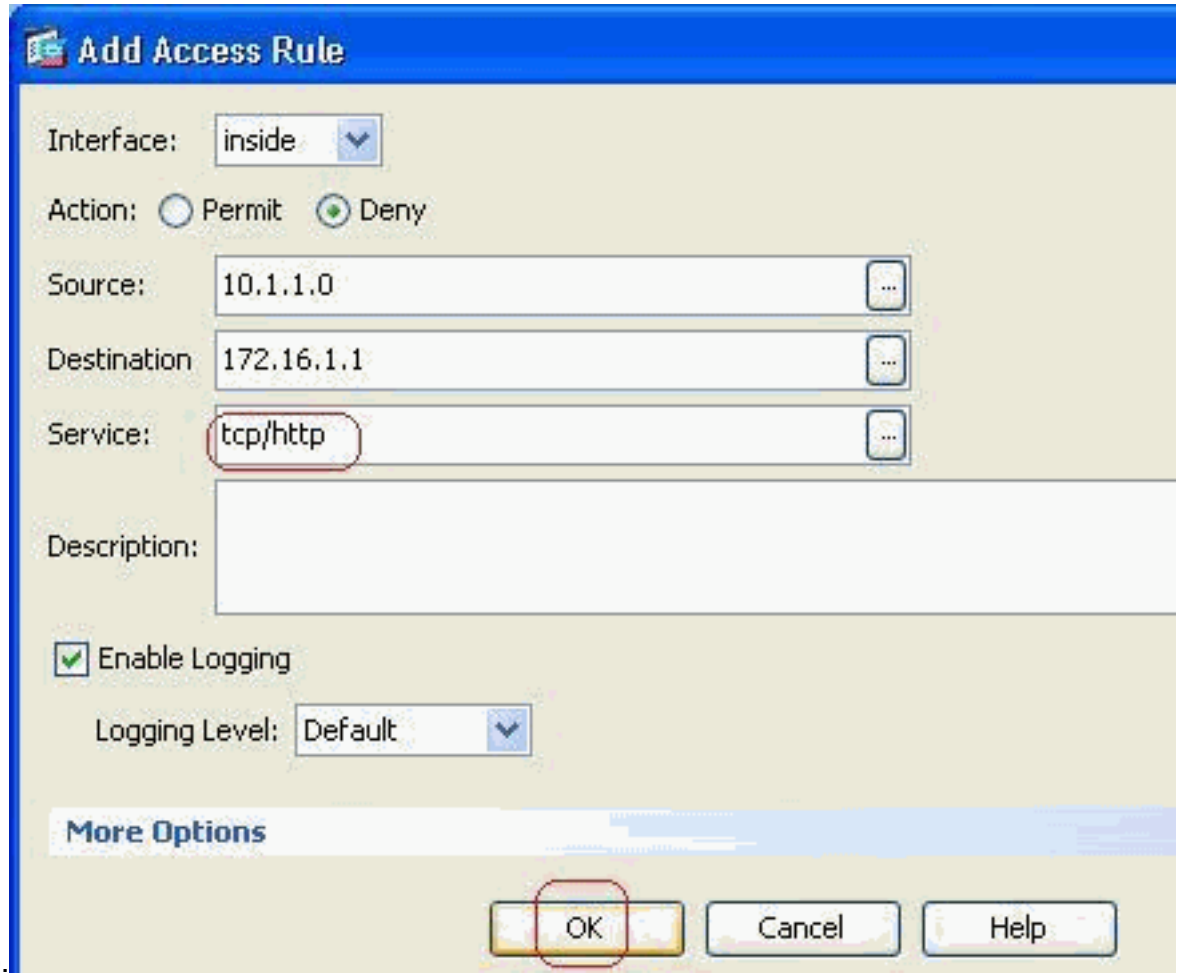
obstruir.

3. Escolha o **HTTP da** lista de portos disponíveis, a seguir clique a **APROVAÇÃO** para reverter de volta ao indicador da regra do acesso



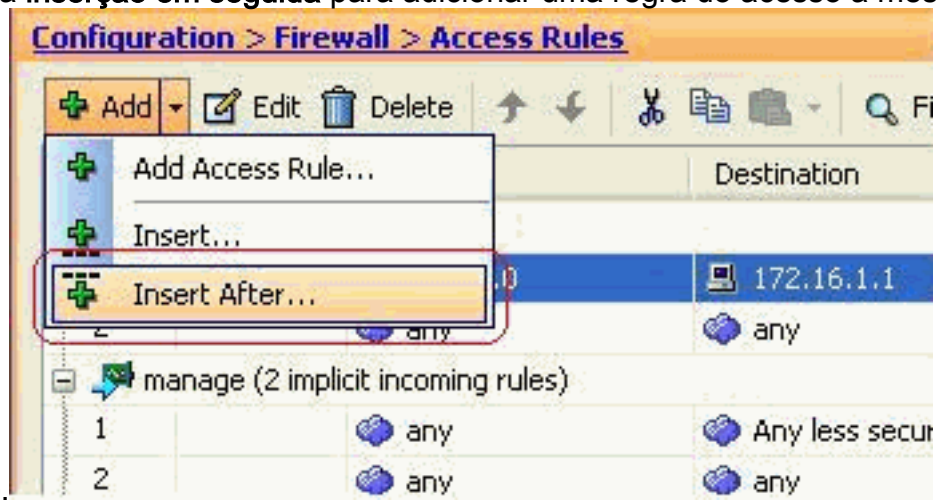
adicionar.

4. Clique a **APROVAÇÃO** para terminar a configuração da regra do



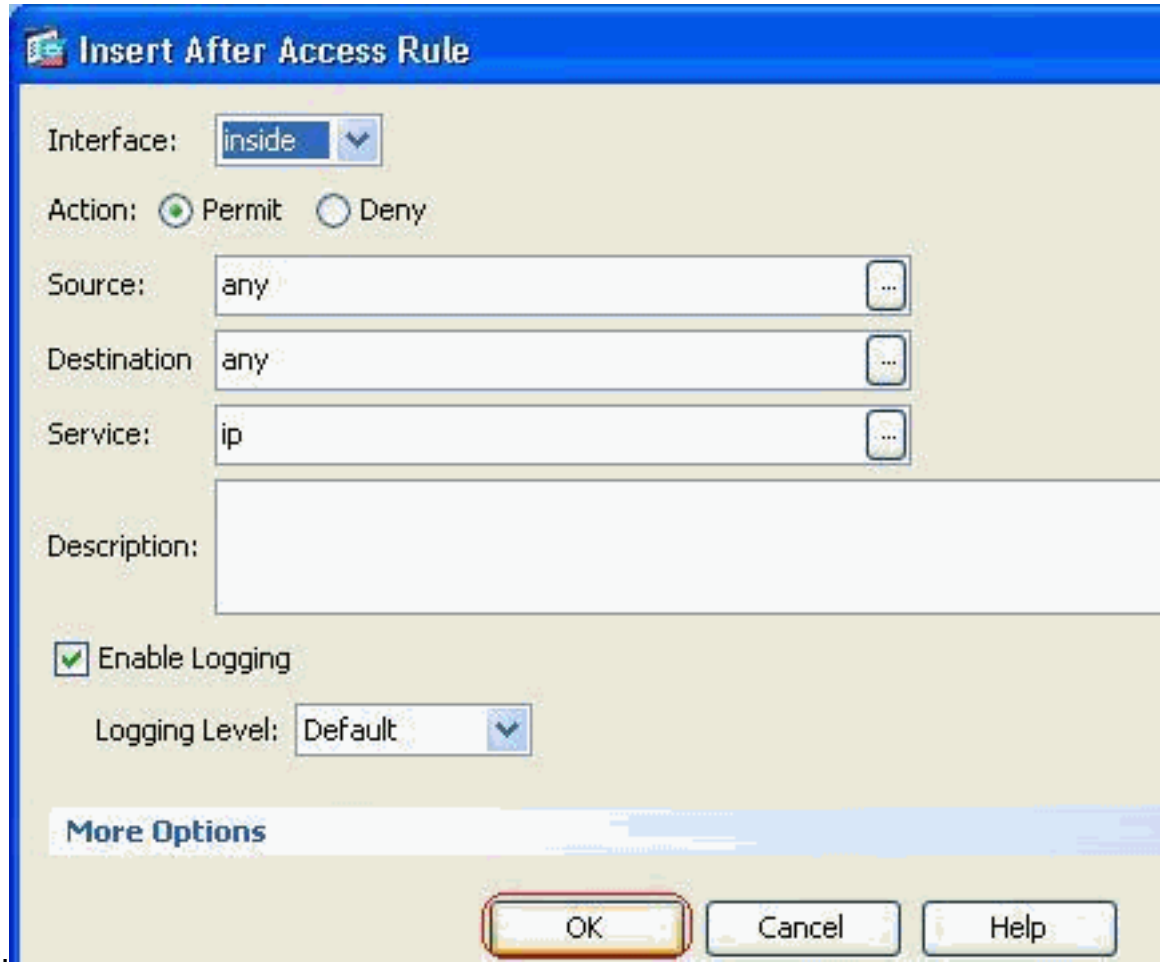
acesso.

5. Clique a **inserção em seguida** para adicionar uma regra do acesso à mesma lista de



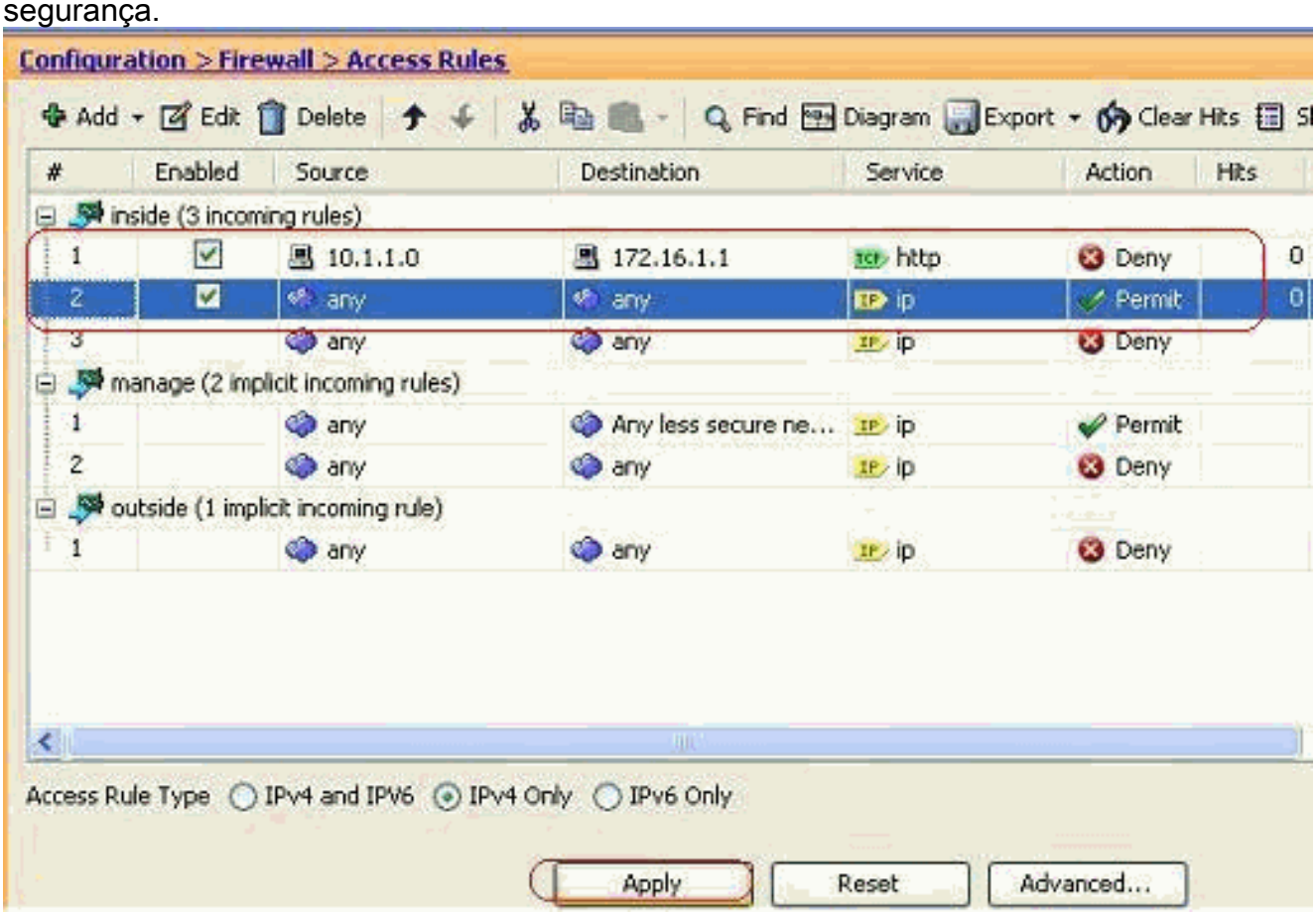
acesso.

6. Permita o tráfego de “” a “” impedir o “implícito negam”. Então, **APROVAÇÃO do** clique para terminar adicionar esta regra do



acesso.

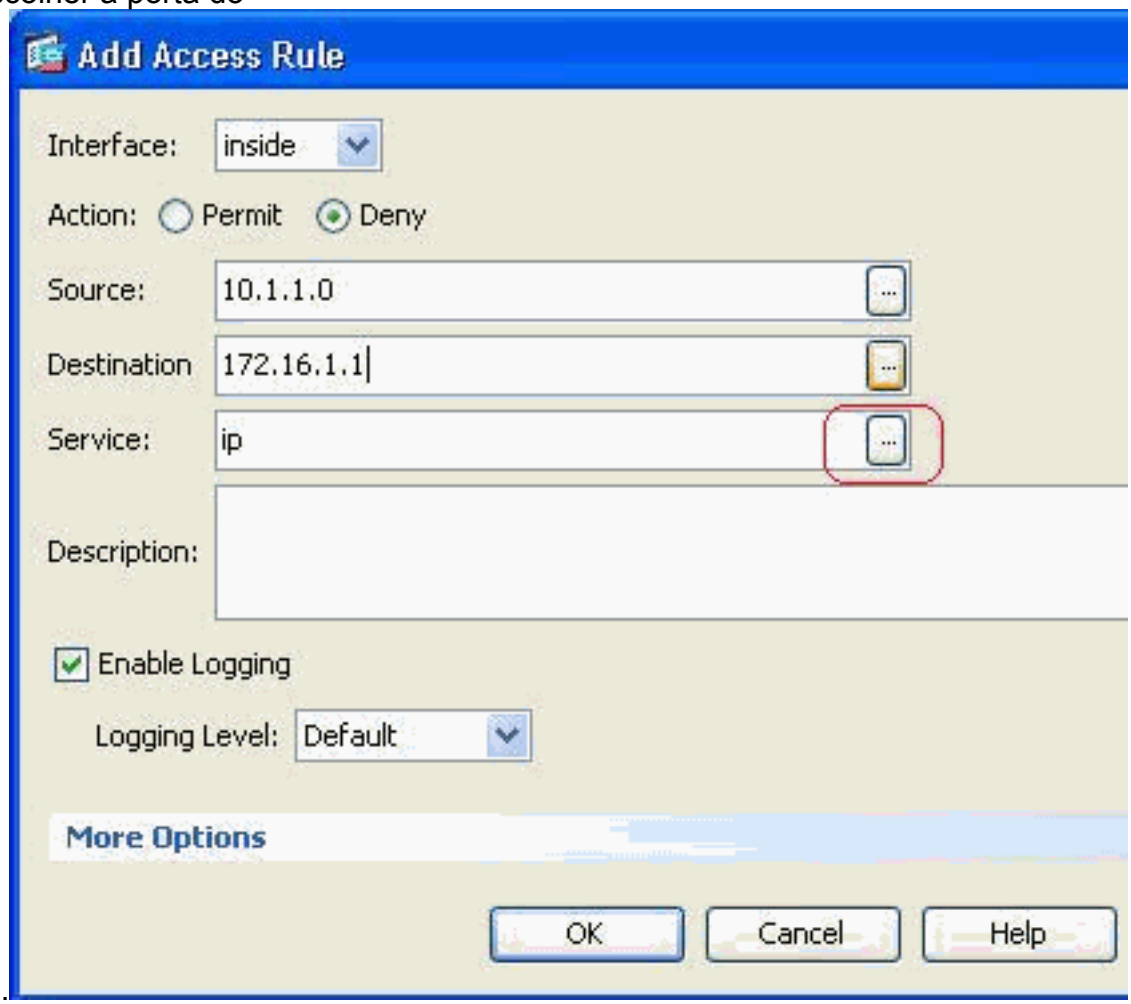
7. A lista de acesso configurada pode ser considerada na aba das regras do acesso. O clique **aplica-se** para enviar esta configuração à ferramenta de segurança.



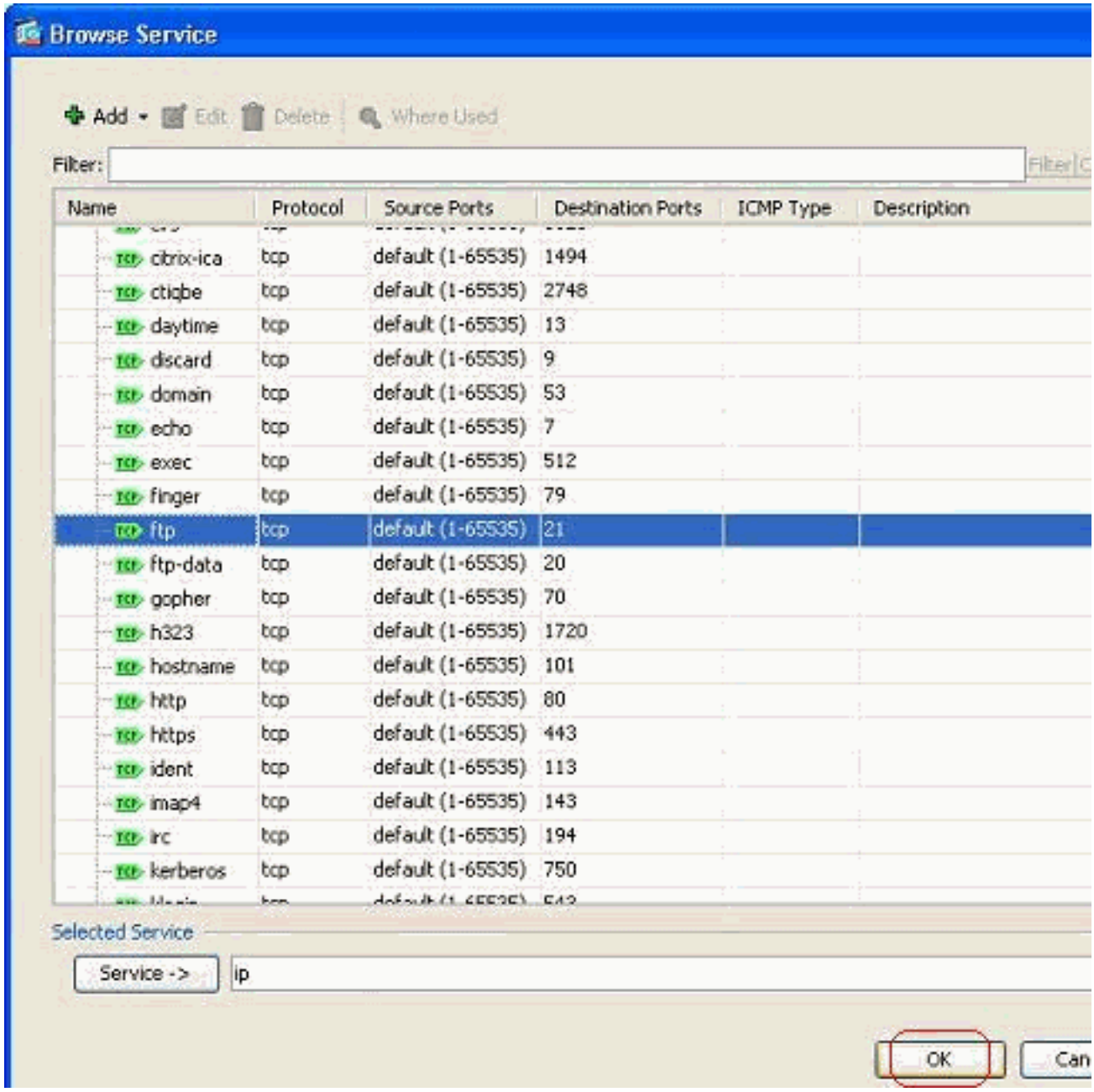
A configuração enviada do ASDM conduz a este conjunto de comandos no comando line

interface(cli) 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`Com estas etapas, o exemplo 1 foi executado com o ASDM para obstruir a rede de 10.1.1.0 de alcançar o servidor de Web, 172.16.1.1. O exemplo 2 pode igualmente ser conseguido da mesma forma para obstruir a rede inteira de 10.1.1.0 de alcançar o servidor FTP, 172.16.1.2. A única diferença estará no ponto de escolher a porta.**Nota:** Esta configuração por exemplo 2 da regra do acesso é suposta para ser uma configuração de atualização.

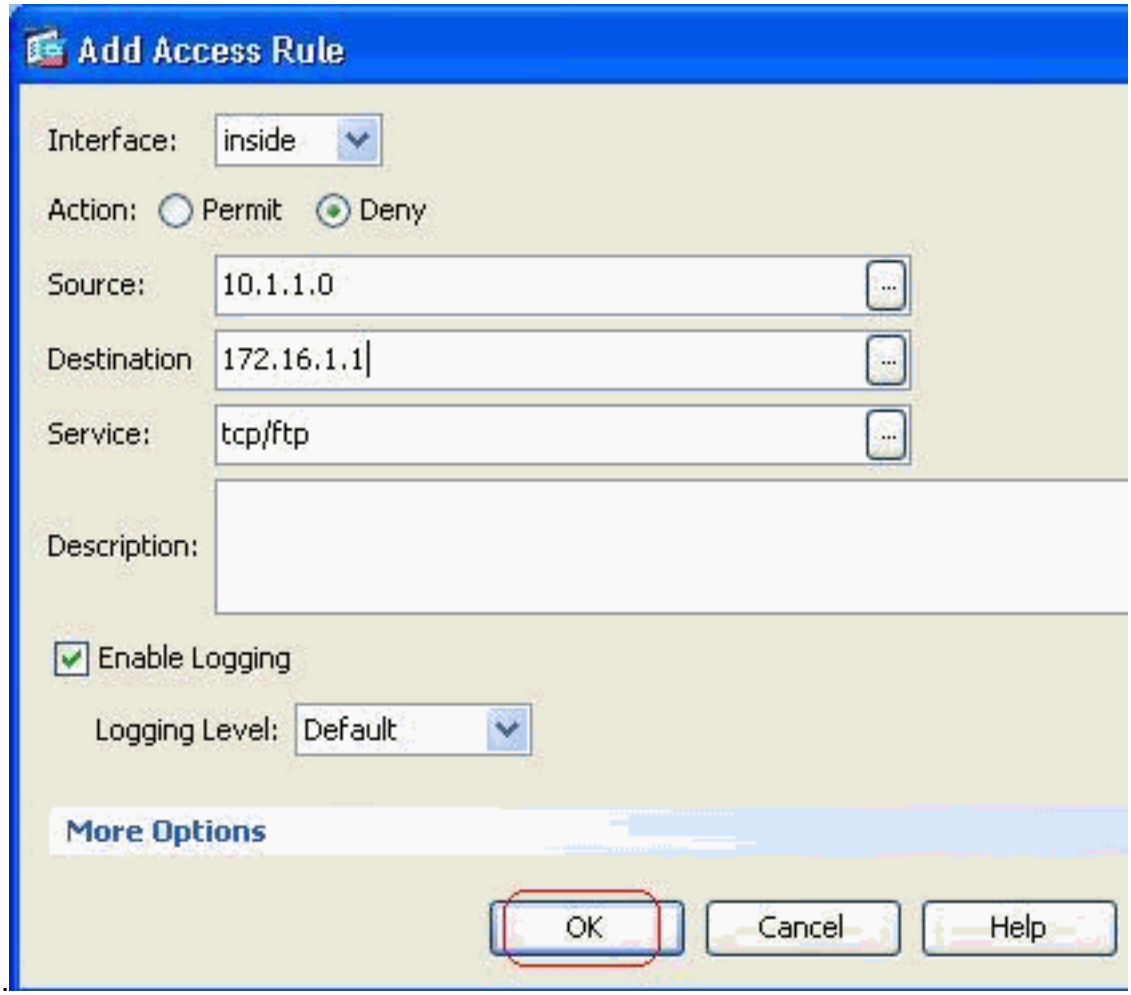
8. Defina a regra do acesso para obstruir o tráfego FTP, a seguir clique a aba dos **detalhes** para escolher a porta do destino.



9. Escolha a porta **ftp** e clique a **APROVAÇÃO** para reverter de volta ao indicador da regra do acesso
adicionar.

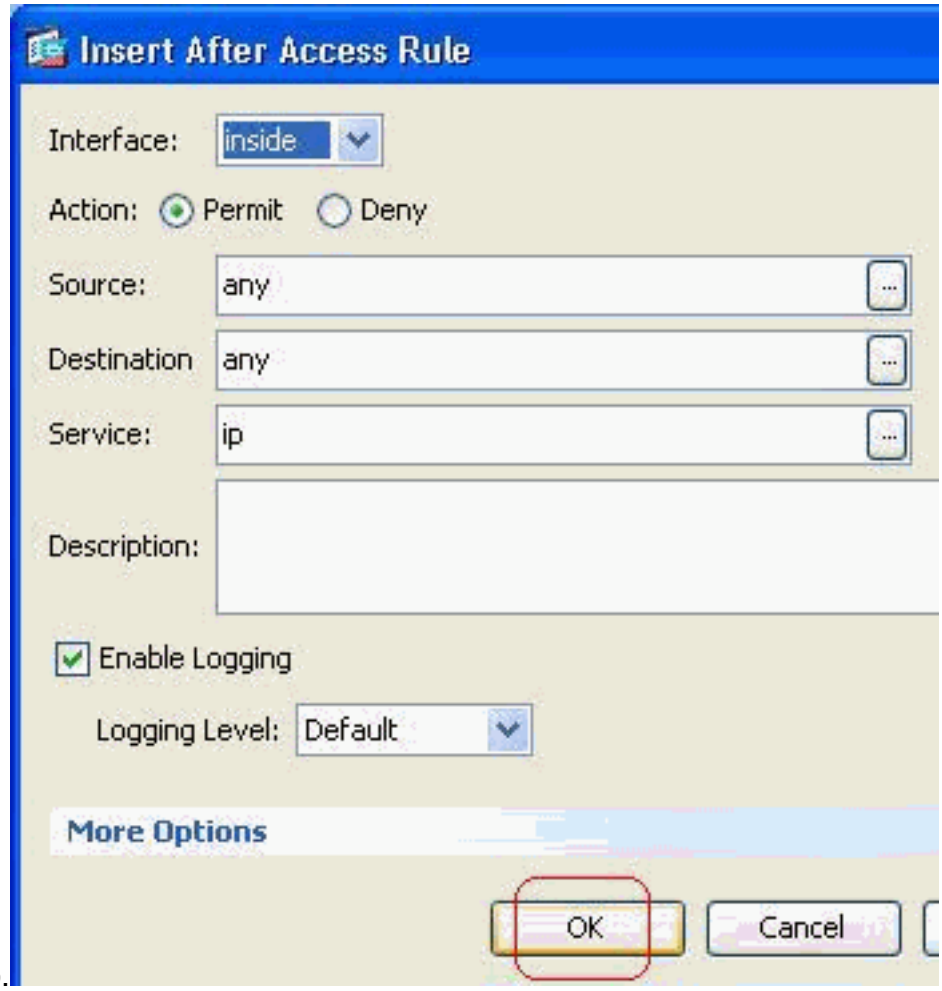


10. Clique a **APROVAÇÃO** para terminar a configuração da regra do



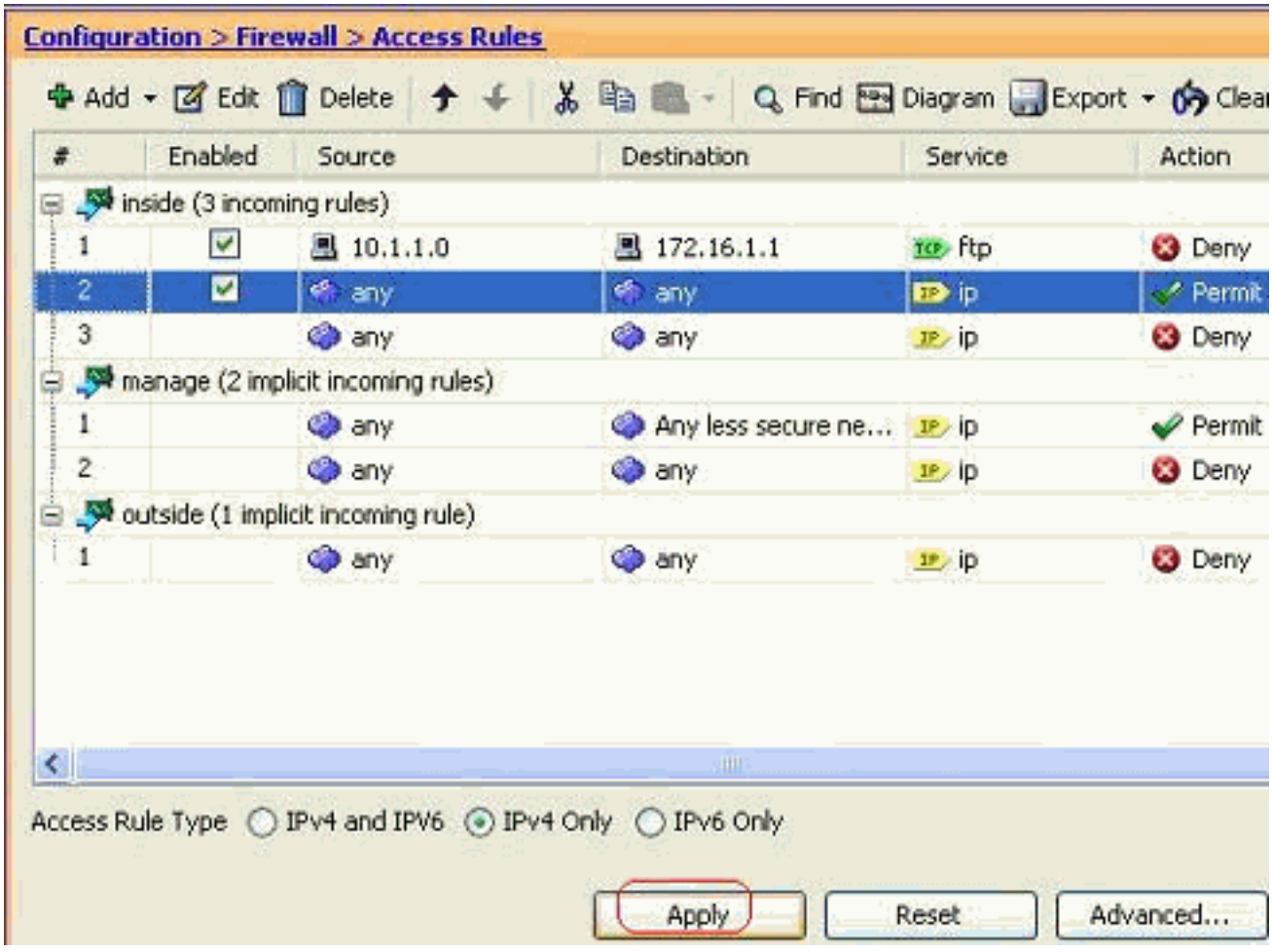
acesso.

11. Adicionar uma outra regra do acesso para permitir todo o outro tráfego. Se não, o implícitos negam a regra obstruirão todo o tráfego nesta



relação.

12. A configuração de lista de acesso completa olha como esta sob a aba das regras do acesso.



13. O clique **aplica-se** para enviar a configuração ao ASA. A configuração de CLI equivalente olha como 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 das portas

A ferramenta de segurança não permite nenhum tráfego de entrada a menos que for permitida explicitamente por uma lista de acesso extendida.

Se você quer permitir que um host exterior alcance um host interno, você pode aplicar uma lista de acessos de entrada na interface externa. Você precisa de especificar o endereço traduzido do host interno na lista de acessos porque o endereço traduzido é o endereço que pode ser usado na rede externa. Termine estas etapas a fim abrir as portas da zona de Segurança mais baixa à zona de segurança mais elevada. Por exemplo, permita o tráfego da parte externa (mais baixa zona de Segurança) à interface interna (zona de segurança mais elevada) ou do DMZ à interface interna.

1. O NAT estático cria uma tradução fixa de um endereço real a um endereço traçado. Este endereço traçado é um endereço que hospede no Internet e possa ser usado para alcançar o server de aplicativo no DMZ sem a necessidade de conhecer o endereço real do server. **static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] | access-list access_list_name | interface}** Refira a seção do NAT estático da referência de comandos para o PIX/ASA a fim aprender mais informação.
2. Crie um ACL a fim permitir o tráfego específico da porta.
access-list <name> extended permit <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number>
3. Ligue a lista de acesso com o **comando access-group** a fim ser ativo.
access-group <access-list name> in interface <interface name>

Exemplos:

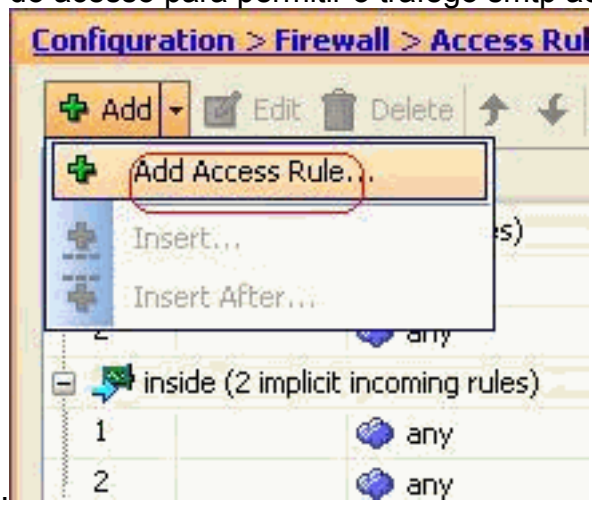
1. **Abra o tráfego da porta S TP:** Abra a porta **tcp 25** a fim permitir que os anfitriões da parte externa (Internet) alcancem o mail server colocado na rede do DMZ.**O comando static** traça o endereço exterior 192.168.5.3 ao endereço real 172.16.1.3 DMZ.`ciscoasa(config)#`**`static (DMZ,Outside) 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** a fim permitir que os anfitriões da parte externa (Internet) alcancem o servidor de Web (seguro) colocado na rede do 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. **Permita o tráfego DNS:** Abra o **UDP 53 da** porta a fim permitir que os anfitriões da parte externa (Internet) alcancem o servidor DNS (seguro) colocado na rede do 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`**

Nota: Refira portas IANA a fim aprender mais informação sobre atribuições de porta.

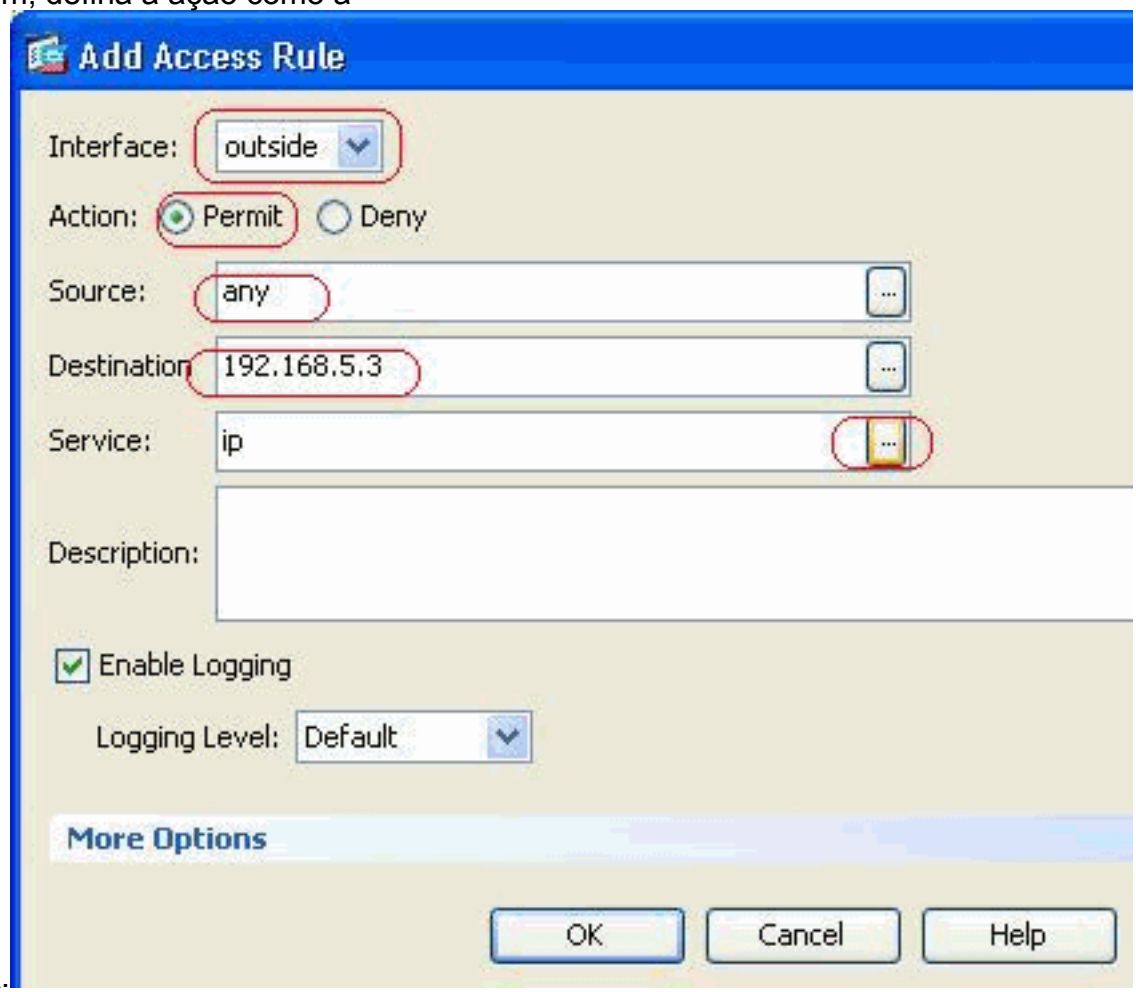
Configuração com o ASDM

Uma aproximação passo a passo para executar as tarefas acima mencionadas com o ASDM é mostrada nesta seção.

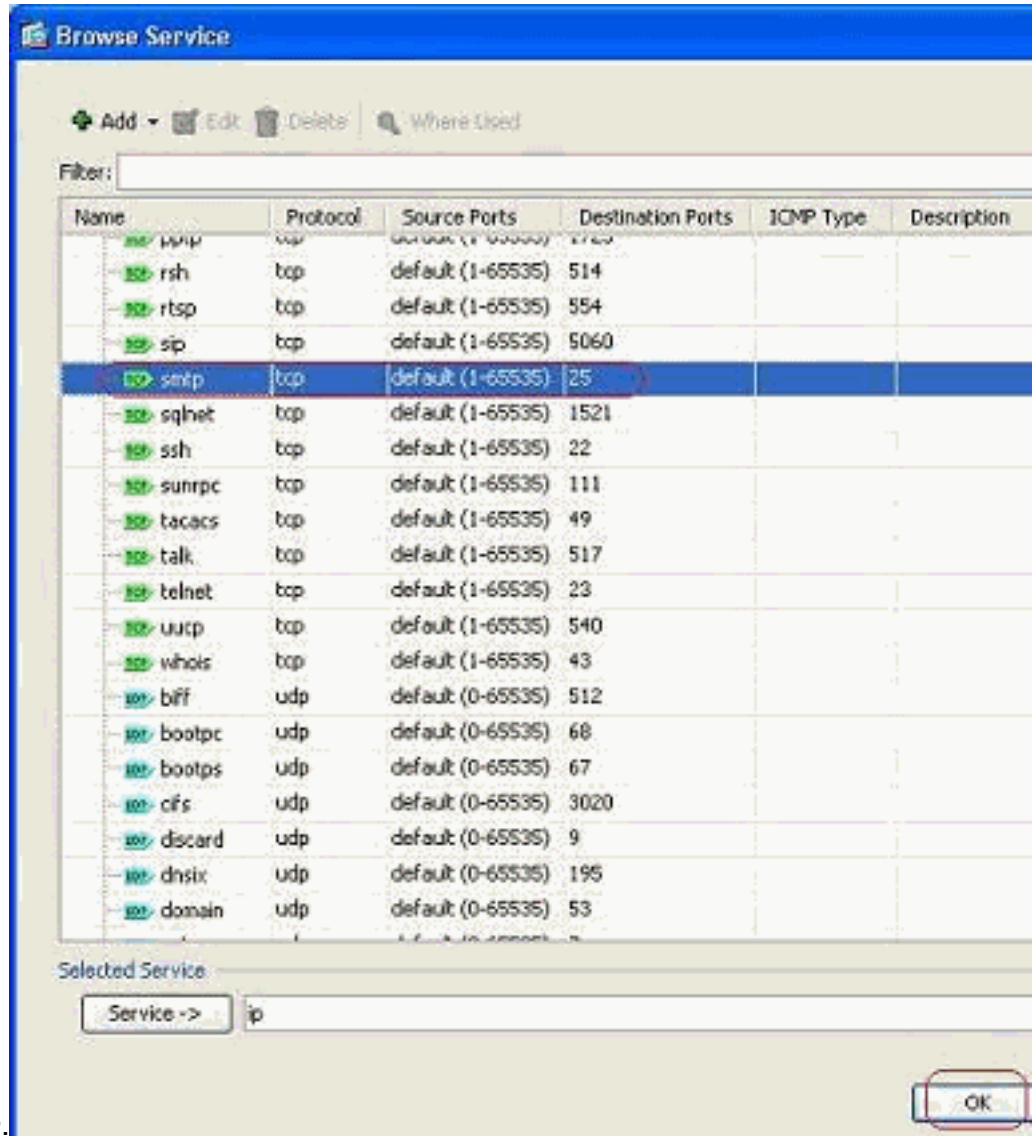
1. Crie a regra do acesso para permitir o tráfego smtp ao server de 192.168.5.3.



2. Defina a fonte e o destino da regra do acesso, e a relação ligamentos desta regra com. Também, defina a ação como a licença.

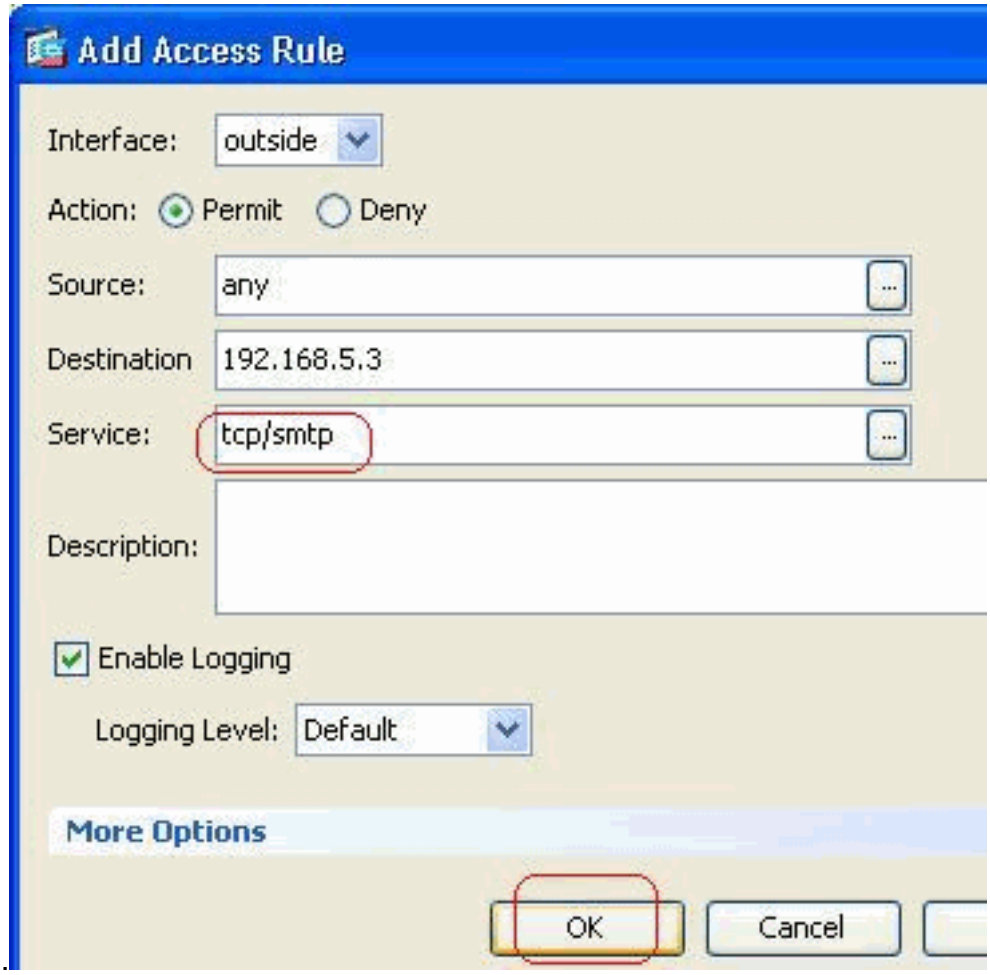


3. Escolha o **S TP** como a porta, a seguir clique a



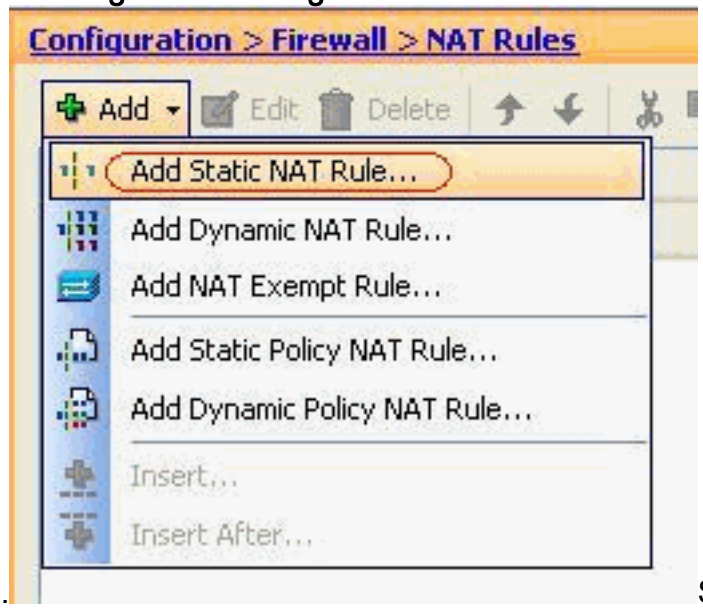
APROVAÇÃO.

4. Clique a **APROVAÇÃO** para terminar configurar a regra do

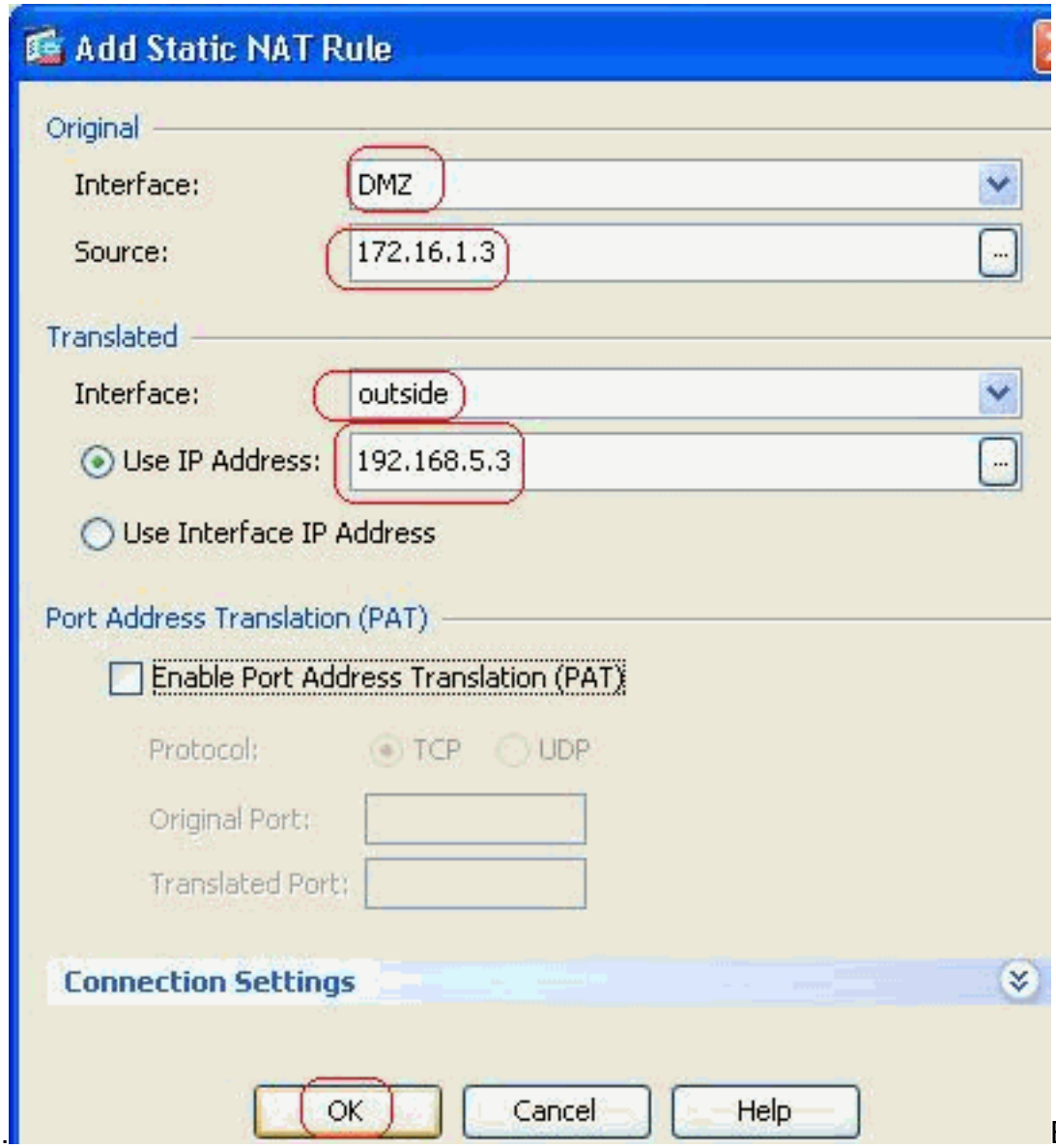


acesso.

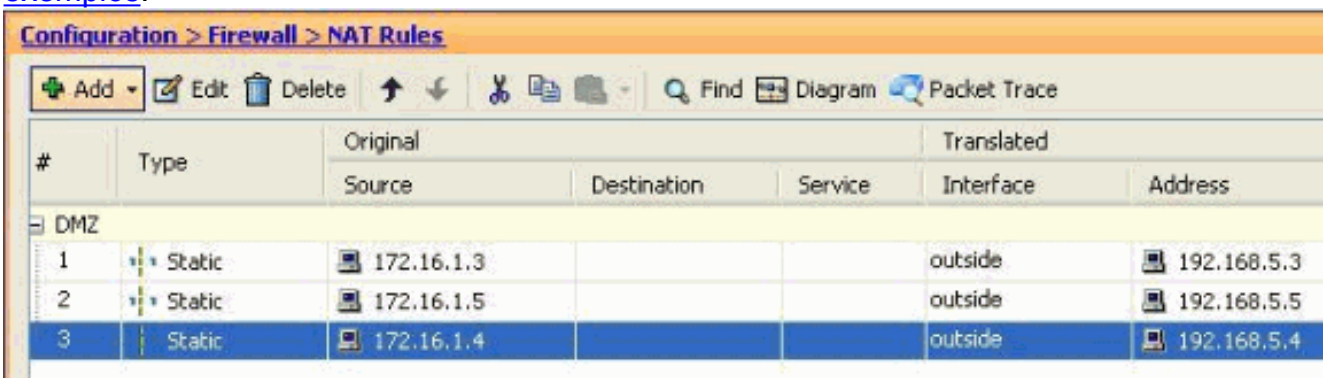
5. Configurar o NAT estático a fim traduzir 172.16.1.3 a 192.168.5.3Vai à **configuração > ao Firewall > às regras NAT a regra do NAT estático do > Add** a fim adicionar uma entrada NAT



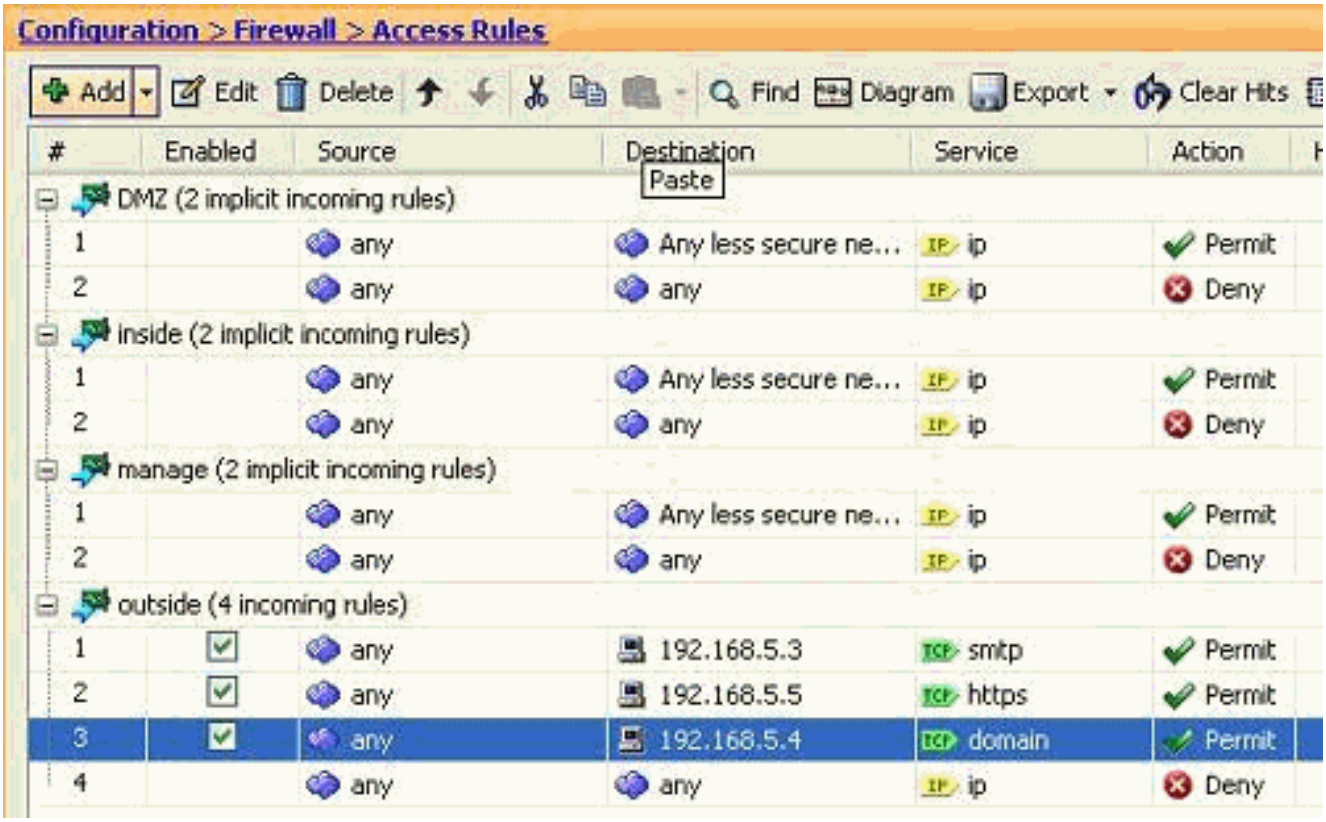
estática. Selecione a fonte original e o endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido junto com suas relações associadas, a seguir clique a **APROVAÇÃO** para terminar configurar a regra do NAT



estático. Esta imagem descreve todas as três regras estáticas que são alistadas na seção dos exemplos:



Esta imagem descreve todas as três regras do acesso que são alistadas na seção dos exemplos:



Verificar

Você pode verificar com determinados comandos de exibição, como mostrado:

- **xlate da mostra** — informação da tradução atual do indicador
- **lista de acesso da mostra** — contadores de acertos do indicador para políticas de acesso
- **registro da mostra** — indique entra o buffer.

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.

Troubleshooting

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

Informações Relacionadas

- PIX/ASA 7.x: Permita/comunicação do desabilitação entre relações
- PIX 7.0 e porta adaptável Redirection(Forwarding) da ferramenta de segurança com nat, o global, o estático, a conduíte, e os comandos access-list
- Utilização nat, global, estática, conduíte, e comandos access-list e redirecionamento de porta (transmissão) no PIX
- PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP
- PIX/ASA 7.x: Permita o exemplo de configuração dos serviços de VoIP (SIP,MGCP,H323,SCCP)
- PIX/ASA 7.x: Acesso do mail server no exemplo da configuração DMZ

- Suporte Técnico e Documentação - Cisco Systems